ISSN: 1646-9895

risti

Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

A b r i l 1 8 • A p r i l 1 8



©AISTI 2016 http://www.aisti.eu

Nº E15

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Edição / Edition
Nº. E15, 04/2018

ISSN: 1646-9895

Indexação / Indexing
Academic Journals Database, CiteFactor, Dialnet, DOAJ, DOI, EBSCO, EI-Compendex, GALE, IndexCopernicus, Index of Information Systems Journals, Latindex, ProQuest, QUALIS, SCImago, SCOPUS, SIS, Ulrich's.

Propriedade e Publicação / Ownership and Publication
AISTI – Associação Ibérica de Sistemas e Tecnologias de Informação
Rua Quinta do Roseiral 76, 4435-209 Rio Tinto, Portugal
E-mail: aistic@gmail.com
Web: http://www.aisti.eu

Director
Álvaro Rocha, Universidade de Coimbra, PT

Coordenadores da Edição / Issue Coordinators
Teresa Guarda, Universidad Estatal Península de Santa Elena, Ecuador
Avelino Victor, ISMAI - Insituto Universitáro da Maia, Portugal

Conselho Editorial / Editorial Board
Carlos Ferrás Sexto, Universidad de Santiago de Compostela, ES
Gonçalo Paiva Dias, Universidade de Aveiro, PT
Jose Antonio Calvo-Manzano Villalón, Universidad Politécnica de Madrid, ES
Luís Paulo Reis, Universidade do Minho, PT
Manuel Pérez Cota, Universidad de Vigo, ES
Ramiro Gonçalves, Universidade de Trás-os-Montes e Alto Douro, PT

Conselho Científico / Scientific Board
Adolfo Lozano-Tello, Universidad de Extremadura, ES
Adriano Pasqualotti, Universidade de Passo Fundo, BR
Alberto Fernández, Universidad Rey Juan Carlos, ES
Alberto Bugarín, Universidad de Santiago de Compostela, ES
Alejandro Medina, Universidad Politécnica de Chiapas, MX
Alejandro Rodríguez González, Universidad Politécnica de Madrid, ES
Alejandro Peña, Escuela de Ingeniería de Antioquia, CO
Alexandre L'Erario, Universidade Tecnológica Federal do Paraná, BR
Alma María Gómez-Rodríguez, Universidad de Vigo, ES
Álvaro E. Prieto, Universidad de Extremadura, ES
Ana Azevedo, Instituto Politécnico do Porto, PT
Ana Cristina Ramada Paiva, FEUP, Universidade do Porto, PT
Ana Isabel Veloso, Universidade de Aveiro, PT
Ana Maria Correia, ISEGI, Universidade Nova de Lisboa, PT
Anabela Mesquita, Instituto Politécnico do Porto, PT
Angelica Caro, Universidad del Bío-Bío, CL
Ania Cravero, Universidad de La Frontera, CL
Antoni Lluís Mesquida Calafat, Universitat de les Illes Balears, ES

Antonia Mas Pichaco, Universitat de les Illes Balears, ES
António Coelho, FEUP, Universidade do Porto, PT
António Godinho, ISLA-Gaia, PT
Antonio Jesus Garcia Loureiro, Universidad de Santiago de Compostela, ES
António Pereira, Instituto Politécnico de Leiria, PT
Armando Mendes, Universidade dos Açores, PT
Arnaldo Martins, Universidade de Aveiro, PT
Arturo J. Méndez, Universidad de Vigo, ES
Baltasar García Pérez-Schofield, Universidad de Vigo, ES
Benjamim Fonseca, Universidade de Trás-os-Montes e Alto Douro, PT
Bráulio Alturas, ISCTE - Instituto Universitário de Lisboa, PT
Brenda L. Flores-Rios, Universidad Autónoma de Baja California, MX
Brígida Mónica Faria, ESTSP, Instituto Politécnico do Porto, PT
Carlos Costa, Universidade de Aveiro, PT
Carlos Rabadão, Instituto Politécnico de Leiria, PT
Carlos Carreto, Instituto Politécnico da Guarda, PT
Carlos Morais, Instituto Politécnico de Bragança, PT
Carlos Vaz de Carvalho, Instituto Politécnico do Porto, PT
Carmen Galvez, Universidad de Granada, ES
César Gonçalves, Universidade do Algarve, PT
Ciro Martins, Universidade de Aveiro, PT
Cristina Alcaraz, Universidad de Málaga, ES
Daniel Castro Silva, Universidade de Coimbra, PT
Daniel Polónia, Universidade de Aveiro, PT
Daniel Riesco, Universidad Nacional de San Luis, AR
David Fonseca, Universitat Ramon Llull, ES
Dora Simões, Universidade de Aveiro, PT
Eduardo Sánchez Vila, Universidad de Santiago de Compostela, ES
Emiliano Reynares, CIDISI - UTN FRSF - CONICET, AR
Eusébio Ferreira da Costa, Escola Superior de Tecnologias de Fafe, PT
Feliz Gouveia, Universidade Fernando Pessoa, PT
Fernando Bandeira, Universidade Fernando Pessoa, PT
Fernando Diaz, Universidad de Valladolid, ES
Fernando Moreira, Universidade Portucalense, PT

Francisco Restivo, Universidade Católica Portuguesa, PT
Gerardo Gonzalez Filgueira, Universidad da Coruña, ES
Gerardo Rodriguez, Universidad de Salamanca, ES
Germano Montejano, Universidad Nacional de San Luis, AR
Guilhermina Lobato Miranda, Universidade de Lisboa, PT
Hélder Zagalo, Universidade de Aveiro, PT
Hélia Guerra, Universidade dos Açores, PT
Henrique Gil, Instituto Politécnico de Castelo Branco, PT
Henrique Santos, Universidade do Minho, PT
Higino Ramos, Universidad de Salamanca, ES
Hugo Paredes, Universidade de Trás-os-Montes e Alto Douro, PT
Isabel Pedrosa, Instituto Politécnico de Coimbra, PT
Isaura Ribeiro, Universidade dos Açores, PT
Isidro Calvo, Universidad del País Vasco (UPV/EHU), ES
Ismael Etxeberria-Agiriano, Universidad del País Vasco (UPV/EHU), ES
Ivan Garcia, Universidad Tecnologica de la Mixteca, MX
Javier Garcia Tobio, CESGA-Centro de Supercomputacion de Galicia, ES
Jezreel Mejia, Centro de Investigación en Matemática (CIMAT), MX
João Pascual Faria, FEUP, Universidade do Porto, PT
João Paulo Costa, Universidade de Coimbra, PT
João Tavares, FEUP, Universidade do Porto, PT
Joaquim José Gonçalves, Instituto Politécnico do Cávado e do Ave, PT
Joaquim Madeira, Universidade de Aveiro, PT
Joaquim Reis, ISCTE - Instituto Universitário de Lisboa, PT
Jörg Thomaschewski, University of Applied Sciences OOW - Emden, DE
José Augusto Fabri, Universidade Tecnológica Federal do Paraná, BR
José Braga de Vasconcelos, Universidade Atlântica, PT
José Felipe Cocón Juárez, Universidad Autónoma del Carmen, MX
Jose J. Pazos-Arias, Universidad de Vigo, ES
José Luís Silva, Universidade da Madeira, PT
José Paulo Lousado, Instituto Politécnico de Viseu, PT
José Luis Pestrana Brincones, Universidad de Málaga
José Luís Reis, ISMAI - Instituto Superior da Maia, PT
Jose M Molina, Universidad Carlos III de Madrid, ES

Jose Maria Zavala Perez, Eticas Research & Consulting, ES
José Martins, Universidade de Trás-os-Montes e Alto Douro, PT
Jose R. R. Viqueira, Universidade de Santiago de Compostela, ES
José Silvestre Silva, Academia Militar, PT
Josep M. Marco-Simó, Universitat Oberta de Catalunya, ES
Juan D'Amato, PLADEMA-UNCPBA-CONICET, AR
Juan M. Santos Gago, Universidad de Vigo, ES
Juan Manuel Fernández-Luna, Universidad de Granada, ES
Juan-Manuel Lopez-Zafra, Universidad Complutense de Madrid, ES
Leonardo Bermon, Universidad Nacional de Colombia, CO
Leila Weitzel, Universidade Federal Fluminense, BR
Lilia Muñoz, Universidad Tecnológica de Panamá, PA
Luis Alvarez Sabucedo, Universidad de Vigo, ES
Luís Correia, Universidade de Lisboa, PT
Luis de Campos, Universidad de Granada, ES
Luis Enrique, Sicaman Nuevas Tecnologías S.L., ES
Luis Fernandez-Sanz, Universidad de Alcalá, ES
Luis Vilán-Crespo, Universidad de Vigo, ES
Luisa María Romero-Moreno, Universidad de Sevilla, ES
Luisa Miranda, Instituto Politécnico de Bragança, PT
Lus Sussy Bayona Ore, Universidad Nacional Mayor de San Marcos, PE
Magdalena Arcilla Cobián, Universidade Nacional de Educación a Distancia, ES
Marcelo Mendonça Teixeira, Universidade Federal Rural de Pernambuco, BR
Marco Painho, ISEGI, Universidade Nova de Lisboa, PT
Maria Hallo, Escuela Politécnica Nacional, EC
María J. Lado, Universidad de Vigo, ES
Maria João Castro, Instituto Politécnico do Porto, PT
Maria João Ferreira, Universidade Portucalense, PT
Maria João Gomes, Universidade do Minho, PT
Maria José Angélico, Instituto Politécnico do Porto, PT
Maria José Marcelino, Universidade de Coimbra, PT
Maria José Sousa, Universidade Europeia, PT
Marisol B. Correia, Universidade do Algarve, PT
Maristela Holanda, Universidade de Brasília, BR

Martín Llamas Nistal, Universidad de Vigo, ES
Mercedes Ruiz, Universidad de Cádiz, ES
Miguel A. Brito, Universidade do Minho, PT
Miguel Bugalho, Universidade Europeia, PT
Miguel Casquilho, IST, Universidade de Lisboa, PT
Mirna Ariadna Muñoz Mata, Centro de Investigación en Matemáticas (CIMAT), MX
Nelson Rocha, Universidade de Aveiro, PT
Nuno Lau, Universidade de Aveiro, PT
Nuno Ribeiro, Universidade Fernando Pessoa, PT
Orlando Belo, Universidade do Minho, PT
Oscar Mealha, Universidade de Aveiro, PT
Paula Peres, Instituto Politécnico do Porto
Paula Prata, Universidade da Beira Interior, PT
Paulo Martins, Universidade de Trás-os-Montes e Alto Douro, PT
Paulo Pinto, FCT, Universidade Nova de Lisboa, PT
Pedro Abreu, Universidade de Coimbra, PT
Pedro Miguel Moreira, Instituto Politécnico de Viana do Castelo, PT
Pedro Nogueira Ramos, ISCTE - Instituto Universitário de Lisboa, PT
Pedro Sánchez Palma, Universidad Politécnica de Cartagena, ES
Pedro Sanz Angulo, Universidad de Valladolid, ES
Pilar Mareca Lopez, Universidad Politécnica de Madrid, ES
Raul Laureano, ISCTE - Instituto Universitário de Lisboa, PT
Renata Spolon Lobato, UNESP - Universidade Estadual Paulista, BR
Reinaldo Bianchi, Centro Universitário da FEI, BR
Rita Santos, Universidade de Aveiro, PT
Roberto Rodrígues Echeverría, Universidad de extremadura, ES
Rogério Eduardo Garcia, Universidade Estadual Paulista, BR
Rubén González Crespo, Universidad Internacional de La Rioja, ES
Rui Cruz, IST, Universidade de Lisboa, PT
Rui José, Universidade do Minho, PT
Rui Pedro Marques, Universidade de Aveiro, PT
Santiago Gonzales Sánchez, Universidad Inca Garcilaso de la Vega, PE
Sergio Gálvez Rojas, Universidad de Málaga, ES
Sérgio Guerreiro, Universidade Lusófona de Humanidades e Tecnologias, PT

Silvia Fernandes, Universidade do Algarve, PT
Solange N Alves de Souza, Universidade de São Paulo, BR
Tomás San Feliu Gilabert, Universidad Politécnica de Madrid, ES
Valéria Farinazzo Martins, Universidade Presbiteriana Mackenzie, BR
Vitor Carvalho, Instituto Politécnico do Cávado e do Ave, PT
Vitor Santos, ISEGI, Universidade Nova de Lisboa, PT
Wagner Tanaka Botelho, Universidade Federal do ABC, BR
Xose A. Vila, Universidad de Vigo, ES

Editorial

Innovación, Sistemas y Tecnologías

Innovation, Systems and Technologies

Teresa Guarda[1,2,3], José Avelino Victor[4], Álvaro Rocha[5]

tguarda@gmail.com, javemor@iiporto.com, amrocha@dei.uc.pt

[1] Universidad Estatal Península de Santa Elena – UPSE, La Libertad, Ecuador

[2] Universidad de las Fuerzas Armadas-ESPE, Sangolqui, Quito, Ecuador

[3] Algoritmi Centre, Minho University, Guimarães, Portugal

[4] Instituto Politécnico da Maia, Maia, Portugal

[5] Universidade de Coimbra, Departamento de Engenharia Informática, Pólo II - Pinhal de Marrocos, Coimbra, Portugal

Pages: –xi

Introducción

La innovación puede ser entendida como una variable estratégica para la competitividad de los estados y organizaciones. Los estados tienen que enfrentar los cambios provocados por la innovación teniendo en cuenta la situación socioeconómica del país y sus especificidades geopolíticas y geoestratégicas.

El proceso de globalización, las alteraciones geopolíticas, la economía estancada, mercados saturados, competencia feroz, junto con los avances científicos y tecnológicos, son algunos de los factores que llevan los estados, en particular a las organizaciones gubernamentales y privadas a repensar sus estrategias globalmente. La globalización es una transformación que conduce a un mundo más interdependiente, que para además de constituir un factor de progreso, tiende a producir realidades potencialmente peligrosas, llevando los estados a modificar los respectivos sistemas de seguridad y defensa.

En este contexto, es cada vez mayor el esfuerzo de los estados y organizaciones para ajustar sus estrategias en un entorno cada vez más competitivo con más riesgos y

desafíos, lo que hace imperativa la sinergia de disciplinas de la ciencia, tecnología, estrategia, política y humanidades.

Esta edición de RISTI incluye temas de investigación multidisciplinaria que cubren paradigmas, metodologías de transferencia de conocimiento y estrategias de innovación que emplean conocimiento e inteligencia en un sentido amplio, que pueden aplicarse a la solución de problemas mundiales a nivel de gobierno, organizacional, industria, medio ambiente y la comunidad.

Estructura

Los artículos presentados en este número fueron seleccionados de los artículos aceptados en la Conferencia Internacional en Tecnologías de la Información y Sistemas (ICITS'18), realizada en la Ciudad de La Libertad, Santa Elena, Ecuador del 10 al 12 de enero del 2018; y en la Conferencia Internacional Multidisciplinaria de Investigación Aplicada a la Defensa y Seguridad (MiCRADS'18), que se celebró en la Academia Naval Ecuatoriana "Cmdte Rafael Morán Valverde", en la Ciudad de Salinas, Santa Elena, Ecuador del 18 al 20 de Abril del 2018. x

La Conferencia Internacional e Tecnologías de la Información y Sistemas (ICITS'18) es un foro internacional para investigadores y profesionales para presentar y debatir sobre las innovaciones, tendencias, resultados, experiencias y preocupaciones más recientes en las diversas perspectivas de Tecnología y Sistemas de la Información. También incluyó varias sesiones de talleres paralelas a las de la conferencia el 1er Taller sobre Medios, Tecnología Aplicada y Comunicación (WMETACOM'18).

La Conferencia Internacional Multidisciplinaria de Investigación Aplicada a la Defensa y Seguridad (MiCRADS'18), es un foro internacional para investigadores y profesionales para presentar y discutir las recientes innovaciones, tendencias, resultados, experiencias y preocupaciones en las diversas perspectivas de la Defensa y Seguridad.

El conjunto de los 29 artículos publicados en este número RISTI fue el resultado de la selección de los trabajos presentados por los autores procedentes de seis países, dieciocho de Ecuador, cuatro de Colombia, dos de Portugal, dos de España, dos de Brazil y uno de Chile.

En este número de la Revista Ibérica de Sistemas y Tecnologías de la Información (RISTI), aborda temas multidisciplinares relacionados a: Big Data Analytics y Aplicaciones; Ciberseguridad y Ciberdefensa; Estrategia, geopolítica y Oceanopolítica; Ética, Computadoras y Seguridad; Medios, Tecnología Aplicada y Comunicación; Redes informáticas, Movilidad y Sistemas Penetrantes; Sistemas de Software, Arquitecturas, Aplicaciones y Herramientas; Tecnologías de la Información en Educación.

Agradecimientos

Se concluye esta introducción, expresando nuestro agradecimiento a todos los autores y revisores involucrados en esta edición, esperando que este número de la RISTI se revele una lectura provechosa para todos.

Un agradecimiento especial a AISTI, y a las entidades que han contribuido a hacer de RISTI una referencia: Academic Journals Database, CiteFactor, Compendex, Dialnet, DOAJ, DOI, EBSCO, GALE, IndexCopernicus, Index of Information Systems Journals, ISI Web of Knowledge, Latindex, ProQuest, CUALIS, SciELO, SCImago y Scopus.

Índice / Index

EDITORIAL

Innovación, Sistemas y Tecnologías ix
Teresa Guarda, José Avelino Victor, Álvaro Rocha

ARTIGOS / ARTICLES

Metodología para el almacenamiento y visualización de datos masivos en invernadero basado en el Internet de las Cosas..... 1
Stalin Marcelo Arciniegas Aguirre, Diego Raúl Mafla Rivadeneira, Laura Rosa Guerra Torrealba, Luis David Narváez Erazo, Francklin Iván Rivas-Echeverría, Dulce Milagro Rivero Albarran

Plataforma de Big Data para la Administración de Recursos Hídricos en Cuencas Chilenas 13
Orlando Saldaña, Ania Cravero, Roberto Espinosa

Aplicación de una metodología de seguridad avanzada en redes inalámbricas 24
Franklin Sánchez Espinosa, Jorge Vivero García, Diego Baroja Llanos

Estratégias nacionais de segurança cibernética na América Latina: oportunidades para convergência de interesses e construção de consenso..... 39
Eduardo Izycki

Firmwares: Vulnerabilidades e Ameaças aos Serviços de Inteligência de Estado e de Inteligência de Segurança Pública 53
Regilberto Girão

Hacia la unificación de radares civiles y militares: Sistema de integración de la señal de radares de la Dirección General de Aviación Civil como apoyo a la Defensa y Seguridad del espacio aéreo ecuatoriano. 66
Juan Romero Mediavilla, Alex Jiménez Vélez

Repensando los fundamentos de la gestión de riesgos. Una propuesta conceptual desde la incertidumbre y la complejidad 76
Jeimy J. Cano M.

Guerras del Futuro: Causas y Estrategias 88
Marco Salinas Haro

Insertion in the Asia-Pacific the Economic Cooperation Forum: Challenges for the Countries of the South-East Pacific from the Security Perspective..... 100
Marfiu Rodríguez Jara, Teresa Guarda

Adoção de Políticas de Segurança de Sistemas de Informação nas Universidades Moçambicanas..... 106
Isabel Maria Lopes, Joaquina Rafael Monteiro

Aplicabilidade do Regulamento Geral sobre Proteção de Dados em Clínicas de Saúde 118
Isabel Maria Lopes, Pedro Oliveira

Detección de anomalías con selección negativa y gráfos de perfiles de comportamiento del usuario 130
César Byron Guevara Maldonado, Janio Jadán-Guerrero

Seguridad Informática para Pequeñas y Medianas Empresas de la Provincia de Santa Elena 144
Julio Reyes, Carlos Muñoz, Teresa Guarda

Gobernanza y nuevos medios en la radiotelevisión pública europea. Panorámica sobre las pruebas de valor público 153
Marta Rodríguez-Castro, Francisco Campos-Freire

La promoción de la diversidad lingüística en las radiotelevisiones públicas europeas 163
Sara Pérez-Seijo, Francisco Campos-Freire

Telemedicina en la Salud para la Provincia de Santa Elena 174
Carlos Lindao, Evelyn Castillo, Teresa Guarda

Análisis de las Tecnologías de Redes Heterogéneas (HetNet) en los Sistemas Móviles 181
Dayana Tigrero, Jimmy González, Teresa Guarda

OWITest: Metodología de test de penetración en redes inalámbricas 187
Luis David Narváez, Stalin Marcelo Arciniegas, Laura Guerra, Francklin Rivas Echeverría

Gestión de correspondencia física a través de aplicación móvil y códigos QR 201
Yuri V. Nieto A, José F López Q, Carlos E Montenegro M

Metodología de selección de IDE para el desarrollo de aplicaciones Android 214
Moreira Robles Jenny Mariela, Pusdá Chulde Segundo Eliceo

Selección de configuraciones de despliegue usando Sistemas de Recomendación en Android 221
Jorge L. Rodas, José A. Galindo, David Benavides, Robert Soriano

Desarrollo de un framework metodológico para la innovación educativa en el contexto de la acción tutorial basado en metodologías ágiles y estándares de conocimiento de ingeniería de software 233
Fernanda Maricela Soto-Guerrero, Pablo Alejandro Quezada–Sarmiento, Lorena del Cisne Condolo–Herrera, Santiago Mengual –Andrés, Diego Israel Moreno–León, Israel Leonardo Rey- Mendoza

Diseño de un sistema de apoyo al proceso de Enseñanza-Aprendizaje 243
Rivero-Albarrán D, Rivas-Echeverría F, Yépez-Durán P, Quishpe-Morales S

Estudio de innovación tecnológica aplicada en procesos formativos con sistemas de gestión de aprendizaje (LMS) en la educación universitaria del Ecuador 256
Darwin Marcelo Pillo Guanoluisa, Leandro Alexander Bermúdez Herrera

Gestión emergente de espacios colaborativos de aprendizaje..... 271
Luis Barba-Guamán, Priscila Valdiviezo-Diaz, José Aguilar

Metodología contra Vulnerabilidades en Ambientes de Aprendizaje Virtuales 282
Diego Fernando Baroja Llanos, Luis David Narváez Erazo

Propuesta de innovación educativa utilizando TIC´s y el Diseño Universal para el Aprendizaje implementada a la asignatura de Psicología General de la Universidad de las Fuerzas Armadas "ESPE" 292
Daysi Karina Flores Chuquimarca, Ramiro Delgado Rodriguez, Aida Noemí Bedón Bedón

Sociedad de la tecnología la información y el conocimiento: tecnologías en la formación de ingenieros..... 304
Claudio C González, Yuri V Nieto A, Carlos E Montenegro M, José F López Q

TICs en Colombia: revisión a partir de la Curva de Gartner 318
Yuri V Nieto A, Carlos E. Montenegro M, José F López Q, Yesid Díaz G

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 05/09/2017
Aceitação/Acceptance: 28/03/2018

Metodología para el almacenamiento y visualización de datos masivos en invernadero basado en el Internet de las Cosas

Stalin Marcelo Arciniegas Aguirre[1], Diego Raúl Mafla Rivadeneira[1], Laura Rosa Guerra Torrealba[1], Luis David Narváez Erazo[1], Francklin Iván Rivas-Echeverría[1,2], Dulce Milagro Rivero Albarran[1,2]

smarciniegas@pucesi.edu.ec, drmafla@pucesi.edu.ec, lrguerra@pucesi.edu.ec, ldnarvaez@pucesi.edu.ec, firivas@pucesi.edu.ec, dmrivero@pucesi.edu.ec

[1] Pontificia Universidad Católica del Ecuador, Aurelio Espinosa Polit, 100112, Ibarra, Ecuador.

[2] Universidad de los Andes, Avenida 3, 5101, Mérida, Venezuela.

Pages: 1–12

Resumen: Los avances tecnológicos han permitido mejorar la eficiencia en los procesos de siembra en invernadero. En esta investigación se ha desarrollado una metodología que permite almacenar las variables ambientales en invernadero basado en el Internet de las Cosas, la cual contribuye a la mejora de producción de siembra. Para ello, primeramente, se adquirieron datos por medio de la modificación del código de una placa Arduino concernientes a temperatura y humedad del ambiente, así como la humedad del suelo. Seguido a esto, se almacena la información en una base de datos NoSQL MongoDB, utilizando NodeJS para conectarlos. Finalmente, se utilizó la herramienta Tableau para conectar la base de datos y visualizar la información en la nube, a través de un Dashboard

Palabras-clave: Internet de las Cosas; NoSQL; Visualización de datos; Transmisión de datos.

Internet of Things-based Methodology for the storage and visualization of massive data in greenhouses

Abstract: The current technological advances have allowed the improvement of the efficiency in the processes of sowing in a greenhouse. In this research, an Internet of Things-based methodology has been developed for storing the environmental variables in a greenhouse, which contributes to the improvement of sowing production. First, it was modified the code of an Arduino plaque in order to send the data concerning environmental temperature and humidity, as well as the humidity of the ground. Then, the information is stored in a Non SQL MongoDB database, using NodeJS to connect them. Finally, the Tableau tool was used in order to connect the database and display the information in the cloud, through a Dashboard.

Keywords*:* Internet of Things; NoSQL; Data visualization; Data transmission.

1. Introducción

La población mundial está en constante aumento y esto ha llevado a la demanda de una mayor cantidad de alimentos, esto ha incidido en que los productores deban optimizar su producción. La causa principal, por la cual no se produce alimentos con eficiencia, es decir incrementar su producción, es el desconocimiento de los factores que inciden en el proceso de producción. Un factor importante que puede mejorar la es incluir la tecnología en los procesos de producción.

Los avances tecnológicos en la última década han permitido la captura y almacenamiento de datos de manera masiva, así como la incorporación de dispositivos electrónico, tales como sensores y actuadores, que permiten un control inteligente de los ambientes, estos sistemas se integran de disciplinas o paradigmas como la inteligencia artificial, el internet de las cosas (IoT de sus siglas en inglés) y el big data, en especial las bases de datos no sólo SQL (NoSQL).

La internet de las cosas es un paradigma que permite la conexión de objetos que nos rodean a través de la internet (International Telecommunication Union, 2005). Estos objetos tienen incorporado sensores que permiten la captura de datos y el envío de los mismos a través las redes.

Las bases de datos no solo SQL permiten el almacenamiento de grandes volúmenes de datos, mantiene una estructura jerárquica, y son útiles para almacenan tipos de datos semiestructurado y estructurados. Estas características hacen que este tipo de base de datos sean idóneas para el desarrollo de aplicaciones en tiempo real.

Tanto la IoT como las bases de datos NoSQL son paradigmas fundamentales cuando se pretende construir una aplicación que apoye la optimización de los procesos de producción. Por otro lado, es necesario incorporar a cualquier sistema de monitores ambiental un dashboard, que permita la visualización de los indicadores del ambienta a monitorear y que el mismo se actualice automáticamente.

En este trabajo se propone un sistema de almacenamiento para variables ambientales en invernadero basado en IoT, que tiene como objetivo proveer información del comportamiento de la variable que influye en el proceso de siembra. Además, se pretende diseñar una metodología capaz de capturar, almacenar y visualizar la información de un invernadero, para que pueda visualizarse a través de una plataforma web.

2. Fundamentación técnica

2.1. Internet de las cosas

El paradigma internet de las cosas (IoT, de las siglas en ingles Internet of Things) nace en 1999 por la intervención de Kevin Ashton en Procter and Gamble, la cual hace referencia a la tecnología RFID, pero no fue hasta 2005 donde se publica una investigación realizada por International Telecommunications Union (ITU) donde se menciona lo siguiente: "Internet de las cosas es una revolución tecnológica que representa el futuro de la informática y las comunicaciones, y su desarrollo depende de la innovación técnica

dinámica en una serie de campos importantes, desde los sensores inalámbricos a la nanotecnología" (International Telecommunication Union, 2005).

2.2. Internet de las cosas en la agricultura

La competencia en la producción agrícola y los efectos del cambio climático han llevado a perfeccionar los métodos de cosecha de los alimentos y la utilización de la tecnología en este campo. Por tal motivo, la Organización de las Naciones Unidas para la Alimentación y Agricultura determina que: "La agricultura climáticamente inteligente (CSA) pretende mejorar la capacidad de los sistemas agrícolas para prestar apoyo a la seguridad alimentaria, e incorporar la necesidad de adaptación y las posibilidades de mitigación en las estrategias de desarrollo agrícola sostenible" (FAO, 2017).

En la actualidad existen varios trabajos de investigación relacionados que se han realizados con anterioridad, como es el caso de (Castro-Silva, 2016), en el cual se realiza un sistema de riego autónomo basado en la Internet de las Cosas para la Universidad Internacional de la Rioja. El proyecto mencionado se centra en el intercambio de información entre tres sistemas: el de predicción, riego y cliente, usando servicios web tipo RESTful. Para la predicción se usó Machine Learning empleando servicios en la nube, para el riego se buscó determinar los parámetros agroclimáticos por medio del cálculo de la evapotranspiración (Castro-Silva, 2016). La arquitectura se puede visualizar en la figura 1.

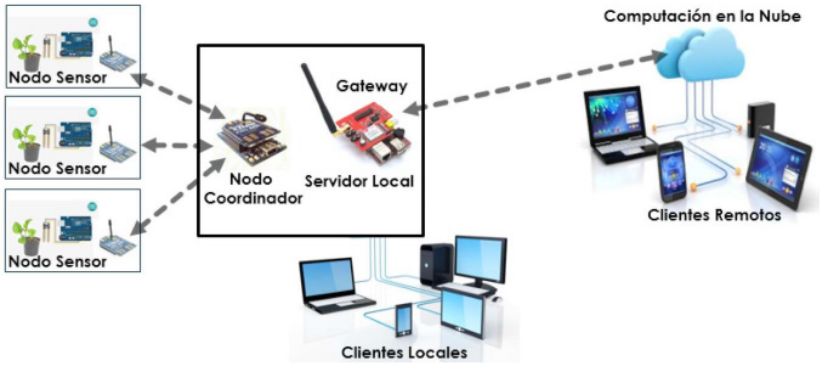


Figura 1 – Arquitectura del Sistema de Riego Autónomo basado en la Internet de las Cosas

El sistema de riego autónomo basado en la Internet de las Cosas se centra más en el cálculo de riego. Sin embargo, la arquitectura es similar a la propuesta en la captura y almacenamiento, pero difiere en la visualización y en las herramientas utilizadas. Además, para la interoperabilidad se usa los servicios Web tipo RESTful y en la propuesta se pretende el uso de la multiplataforma Node.js. En conclusión, la diferencia del proyecto con la propuesta es en el enfoque ya que el proyecto se centra en el cálculo y predicción del riego, y la propuesta en el almacenamiento masivo y visualización de los datos en tiempo real en la nube.

Otro trabajo relevante, sin duda, es el desarrollado por el Institute for Research & Technology Thessaly en Grecia, que trata sobre las redes de sensores inalámbricos para clima invernadero y evaluación de la condición de la planta. Dicho proyecto, se enfoca en "crear una representación precisa y detallada del clima en varias regiones dentro de un invernadero" (Ferentino, 2017). Así también, el prototipo se basa en una plataforma de código abierto la cual usa motas CM3000 de la empresa Advanticsys, la cual se comunica inalámbricamente a través de radiofrecuencia por medio del chip CC2420 de Texas Instruments. También, los datos capturados por las motas son almacenados en un ordenador personal para su interpretación. Finalmente, los factores importantes de este proyecto es el uso de cinco motas distribuidas en el invernadero, las cuales miden la temperatura y la humedad relativa en sus variantes baja, media y alta. La distribución de los sensores se puede observar en la figura 2.

El proyecto Redes de Sensores sin Cables para Agricultura de Precisión en Regiones Minifundistas se centra solo en la captura de datos, y no maneja metodologías para el almacenamiento y visualización de datos masivos. Así mismo, la gran diferencia es que este proyecto está enfocado a la captura de datos en ambientes abiertos, mientras que la propuesta es para invernadero.



Figura 2 – Arquitectura Redes de Sensores sin Cables para Agricultura de Precisión en Regiones Minifundistas

Por otro lado, el proyecto desarrollado por Neusoft Institute of Information en China trata sobre los sistemas inteligentes de monitoreo de ambiente de invernaderos basado en el IoT. En dicho proyecto, se utiliza una arquitectura de captura de datos, a través de una red de sensores inalámbrico con la tecnología ZigBee que se detalla en la Figura 3. Además, para el control y almacenamiento se usa la plataforma LabVIEW, la cual permite el monitoreo en tiempo real. También, a través de la plataforma pueden tener acceso los dispositivos finales con el uso del internet (Dan, 2015).

El proyecto redes de sensores inalámbricos para clima invernadero y evaluación de la condición de la planta tiene la finalidad de determinar los recursos necesarios,

para representar de forma precisa las variables ambientales dentro del invernadero. Sin embargo, al ser un estudio experimental no tiene el enfoque al almacenamiento y visualización masiva, pero sirve de gran ayuda como referencia para determinar las ubicaciones de los sensores en una implementación para producción.

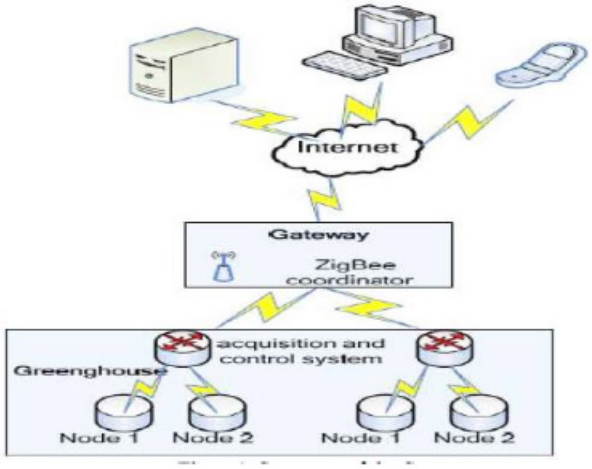


Figura 3 – Arquitectura del sistema inteligente de monitoreo de ambiente de invernaderos basado en el IoT.

Finalmente, el proyecto desarrollado por la University of Peradeniya en Sri Lanka trata sobre Monitorización del entorno en tiempo real asequible para sistema en invernadero. Dicho proyecto, habla sobre la captura de datos a través de red de sensores, las cuales envían información por medio de una plataforma en Java a una base de datos NoSQL. Además, para la interface Web se desarrolla por medio de AngularJS que es un framework de JavaSript (Athukorala, 2016). La arquitectura se detalla en la figura 4.

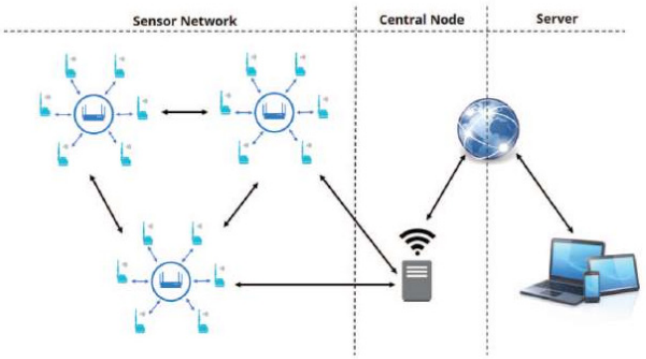


Figura 4 – Arquitectura Affordable Real-time Environment Monitoring System for Greenhouses

El proyecto Monitorización del entorno en tiempo real, asequible para sistema en invernadero, es el más parecido a la propuesta ya que maneja un método de captura; utiliza una base de datos NoSQL MongoDB para el almacenamiento masivo y la visualización, lo realiza por medio de JavaScript. La diferencia es que la propuesta para la captura de datos se utiliza la multiplataforma Node.js, y en el proyecto mencionado se desarrolla una interface en JavaScript. También, para la visualización de la propuesta se propone manejarlo desde la nube y en el proyecto analizado lo realiza localmente.

2.3. Proceso de visualización

Para el proceso de visualización existen ciertos conceptos y reglas que permiten transmitir la información de forma clara sin distracciones, optimizando recursos visuales. Entre ellas, se encuentran el concepto de Data- Ink Ratio y las leyes de la Gestalt. Primeramente, el concepto Data-Ink Ratio inicia en 1983 por medio de Edward Tuft en la publicación de un libro titulado The Visual Display of Quantitative, el cual trata sobre el diseño de presentaciones efectivas de datos. Además, un aspecto importante es la utilización de tinta en la visualización ya que se menciona que la tinta que no genere información debe ser borrada (Saric, 2013). Al mismo tiempo, uno de los aportes significativos es la fórmula del Data-Ink Ratio la cual trata de medir la cantidad de tinta utilizada solo en datos, sobre el total de tinta utilizado en todo el gráfico. Otro aspecto, es que el objetivo de la medición del Data-Ink Ratio se aproxime a uno.

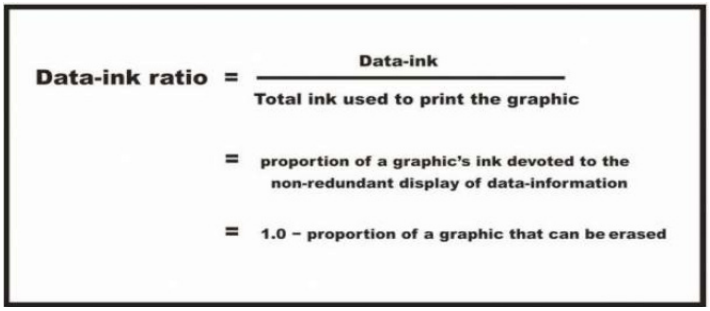


Figura 5 – Formula Data-Ink Ratio

3. Diseño metodológico

3.1. Arquitectura

La arquitectura está compuesta por tres partes fundamentales: la captura, el almacenamiento y la visualización. Primeramente, en la captura se encuentra todo lo referente a la parte electrónica y forma como se adquiere las señales físicas del entorno. Seguido a esto, tenemos el almacenamiento, en el cual se acumulan todos los datos adquiridos en la captura. Finalmente, es en la visualización donde mostramos toda la información de forma gráfica para que se puede interpretar. A continuación, se muestra en la figura 6 toda la arquitectura (Arciniegas, 2017):

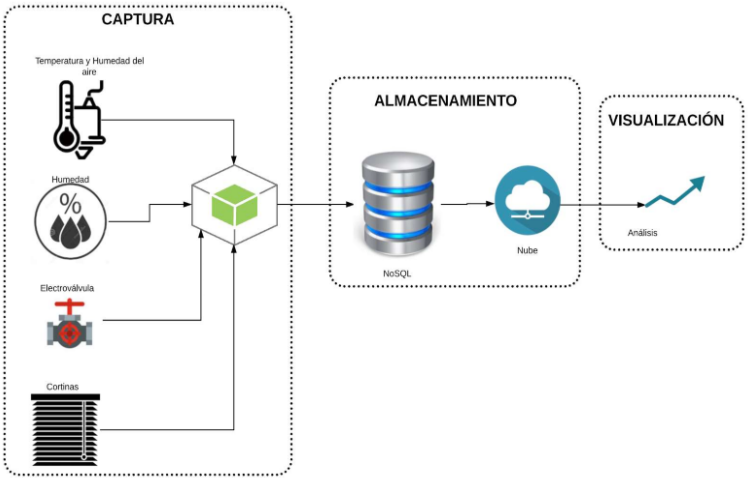


Figura 6 – Arquitectura Propuesta

3.2. Captura

Para la captura de datos se utiliza la plataforma de JavaScript Robotics & IoT denominada Johnny-Five. A su vez, dicha plataforma permite la programación de la placa Arduino desde en el entorno Node.js. De esta manera, se permite integrar varias plataformas en un mismo entorno. En la figura 7 se detalla el diagrama de flujo de la captura.

Este proceso inicia con la adquisición de los datos por medio de la plataforma Johnny Five. A continuación, los datos provenientes del entorno son almacenados en variables. Luego, se realiza un tratamiento de señales con la intención de obtener datos entendibles para los usuarios.

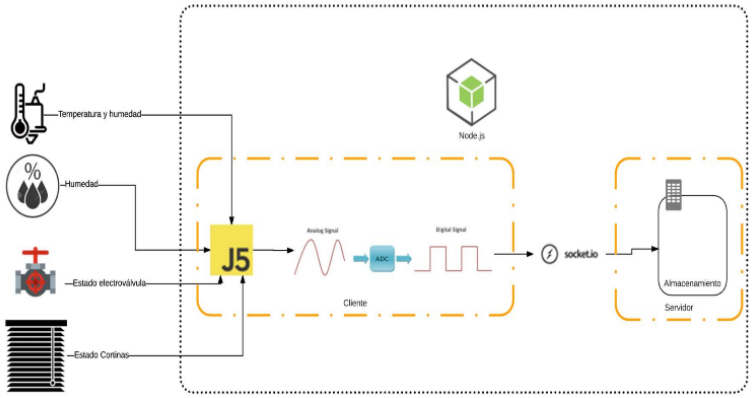


Figura 7 – Captura de Datos

Además, todo el proceso antes mencionado se realiza del lado del cliente. Seguido a esto, la librería socket.io se encarga de pasar las variables de la plataforma Johnny Five al lado del servidor, mejorando por lo tanto el flujo de datos (Arciniegas, 2017).

Para poder utilizar la plataforma Johnny-Five en la placa Arduino hay que grabar previamente el código de la librería Firmata, llamado StandardFirmata. La librería Firmata permite comunicar las placas electrónicas con cualquier software, a través de la comunicación serial que es emulada por la comunicación USB. Seguido a esto, para la captura de datos se realiza un programa en el entorno multiplataforma de Node.js, en el cual se integrarán los subsistemas propuestos.

En primer lugar, la librería Johnny-Five permite conectar la placa Arduino con la multiplataforma Node.js a través del programa Firmata, previamente cargado con el IDE de Arduino de la propuesta. En segundo lugar, se realiza el llamado a la librería Socket.io para el manejo de los datos en tiempo real. Algo importante es que para el uso de las librerías Johnny Five y Socket.io se debe tenerlas previamente instaladas, esto se lo realiza a través de la consola de Windows, puesto que, todos los complementos que trabajan con la multiplataforma Node.js se los adquiere con los paquetes npm (Node Package Manager).

Luego, se declara las variables análogas de la temperatura, humedad del suelo y humedad del aire. A continuación, se declaran las variables digitales que detectan el estado de las cortinas y la electroválvula. De este modo, dichas variables se utilizan para que se almacenen los datos provenientes de la placa Arduino a través de la librería Johnny-Five. Seguido a esto, se inicializa la conexión con socket.io, el cual trabaja una parte del lado del cliente, que en este caso es la placa Arduino. De igual importancia, la otra parte permite almacenar los datos en el servidor y de esta manera mantener el flujo en tiempo real. Después, se inicia la librería Johnny-Five para la lectura tanto de los pines análogos como los digitales. Así mismo, para la configuración de la lectura de los pines análogos existe una configuración previa en la cual se detalla el pin a leer, la frecuencia con la cual se realiza la lectura y umbral desde el cual empieza a capturar los datos.

3.3. Almacenamiento

Para el almacenamiento se utiliza el controlador MongoDB-Node.js, el cual permite interactuar entre las aplicaciones de Node.js y MongoDB. Además, el controlar permite utilizar los comandos más comunes de MongoDB desde el entorno de Node.js. Por otra parte, para sacar el mejor provecho a la base de datos NoSQL MongoDB se debe configurar la Replicación y el Sharding. En la figura 8 se presenta el método del almacenamiento.

El proceso de almacenamiento de datos empieza con la configuración previa del servidor, donde se especifica direcciones y variables. Luego, se almacena en la base de datos MongoDB donde se verifica los posibles errores tanto de la sintaxis como de estructura de los datos (Arciniegas, 2017).

Primeramente, para poder almacenar la información previamente capturada se tiene que llamar a la librería de MongoDB a través de MongoClient. Igualmente, la librería requiere información como es la ubicación de la base de datos, que para este caso se utiliza el localhost y la base de datos llamada test. También, se crea el ObjetID que es un identificador único por cada documento insertado, de esta manera se evita duplicidad en

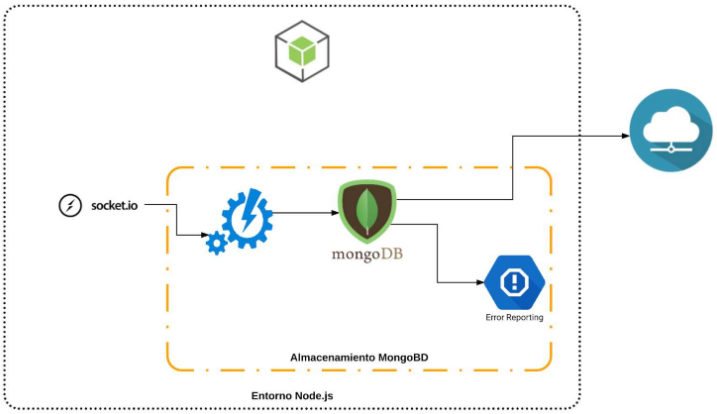


Figura 8 – Almacenamiento

la información. Para la inserción de un documento el proceso consta de tres partes: la primera es la estructura y los nombres de las variables que se van a guardar, la siguiente verifica errores en la estructura, y finalmente se apertura la conexión con la base de datos y se inserta el documento. A continuación, se detallan cada uno de ello.

- Función.- La función MongoClient es parte de la librería desarrollada por la empresa MongoBD para Node.js, por lo tanto, se garantiza la conexión sin tener inconvenientes. También, la función realiza un llamado para la apertura de la base de datos.
- Estructura.- La estructura que maneja se basa en el patrón de diseño uno a uno, es decir, una clave para cada valor. También, todas variables globales de la captura se condensan para ser insertadas.
- Conexión con la base de datos.- Siempre que se vaya a insertar un documento se realiza la conexión con la base de datos, luego una vez que finaliza el proceso de inserción se vuelve a cerrar la conexión con la base de datos.

A continuación, se presenta la estructura para almacenar un documento el cual consta de la apertura de la conexión a la base de datos, la verificación de errores en la conexión, la inserción del documento y el cierre de la conexión. Cada uno de los elementos se detalla de la siguiente manera.

- Apertura de la base de datos.- Es el primer paso en el que Node.js establece una conexión con MongoDB, especificando ciertos parámetros como es la ruta y el nombre de la base de datos. Además, se realiza un llamado a una función que comprueba errores en la conexión.
- Comprueba errores.- En la comprobación de errores determina si no existe problema en la conexión, para lo cual utiliza una comprobación del error peguntando si es igual a null.
- Insertar documento.- Luego de la apertura de la base de datos y de comprobar que no existe errores, se puede insertar el documento llamando a la función insertDocument.

- Cierre de conexión.- Una vez finalizado la inserción del documento se procede a cerrar la conexión con la base de datos, y se retorna al método de captura.

3.4. Visualización

La visualización es el proceso mediante el cual se pasa los datos a información de una forma gráfica, para ello se tiene que tomar en cuenta todas las leyes y principios de la visualización. Entre ellos, se encuentran las leyes de las Gestalt y el principio Data-Ink Ratio. Además, un paso importante es la conexión entre la base de datos y el software de visualización. Para ello, se utiliza un conector que permite la correcta integración. En la figura 9 se muestra la metodología propuesta para la visualización de la información (Arciniegas, 2017).

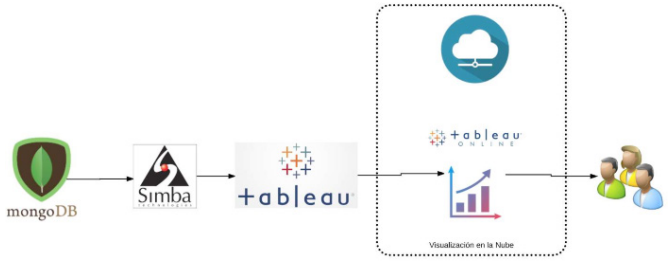


Figura 9 – Visualización de la información

Para iniciar el proceso de visualización, primeramente, se debe configurar el conector el cual permite la conexión de la base de datos MongoDB y el software Tableau. Seguido a esto, se debe configurar la sincronización de datos con la nube y poder visualizar la información on line. A continuación, el conector es el elemento que permite extraer el esquema de datos almacenados en MongoDB y transformarlos a un esquema relacional con la intención de poder conectarse a la herramienta de visualización. Para ello, se utiliza el conector SIMBA ODBC; que posee un editor de esquemas que permite crear un esquema, modificar un esquema o modificar un esquema NoSQL.

Una vez ingresado a la modificación de esquema de un base de datos definidas, que para la propuesta es una NoSQL, nos permite escoger el método de conexión que para este caso es Sample Simba MongoDB ODBC DSN. Al usar este tipo de conexión, a través de ODBC, nos da la posibilidad de acceder a cualquier base de datos sin importar el sistema de gestión. Finalmente, Para la conexión a la nube, Tableau permite sincronizar el trabajo realizado a través de Tableau On-Line, y de este modo se puede crear un sitio donde están almacenadas las principales vistas del dashboard.

4. Resultados

Se realizó una prueba por tres días y los resultados se muestran en dos tipos de gráficas diferentes. La primera se compone de una gráfica lineal de las tres variables temperatura,

humedad y humedad del suelo. Además, se escoge este tipo de gráfica porque en primer lugar se desea comparar los datos unos con otros. Otro factor que permite escoger este tipo de gráfica es porque son muchos datos y estos varían en el tiempo. Otro aspecto importante, es que se usa la ley de la continuidad de Gestalt para clarificar la tendencia (Olcese, 2006).

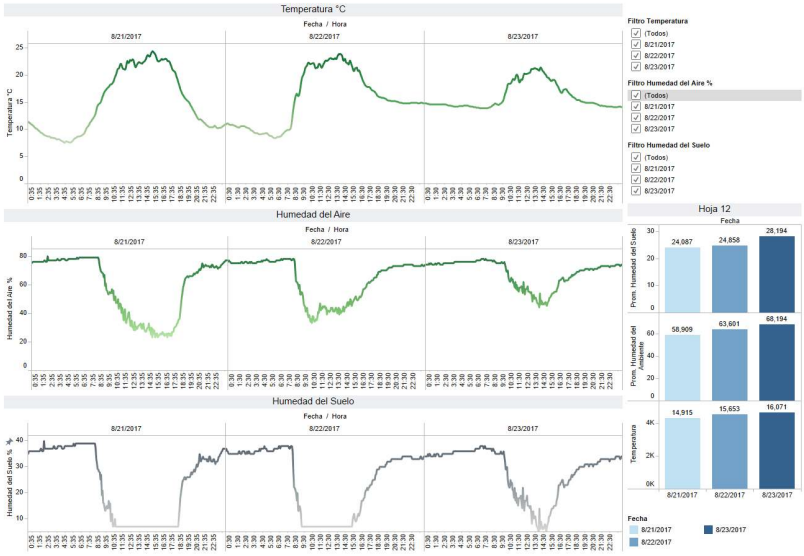


Figura 10 – Dashboard

5. Conclusiones

Luego de analizar los diferentes estudios realizados sobre el Internet de las Cosas en la agricultura, se puede determinar que se hace mucho énfasis en los métodos de captura y almacenamiento. Sin embargo, no se le da mucha importancia a la visualización de la información.

Con la aplicación correcta de la metodología planteada, se pudo determinar las siguientes herramientas. Primeramente, para la captura se estableció Arduino para la lectura de los datos, y se programó mediante la plataforma Johnny Five perteneciente al entorno Node. js. En segundo lugar, para el almacenamiento en la base de datos se determinó la librería MongoDB. Finalmente, para la visualización se utilizó Tableau, la cual se enlaza a la nube con Tableau On-line, y se conecta con la base de datos por medio del conector Simba.

Mediante el uso adecuado de las leyes de la Gestalt y el Data-ink Ratio, se puede diseñar un Dashboard capaz de representar gráficamente los datos almacenados de las variables de invernadero.

Referencias

Arciniegas, S. (2017). Sistema de almacenamiento para variables. Ibarra: UNIR.

Athukorala. (2016). Affordable Real-time Environment Monitoring System for Greenhouses. Sri Lanka : Proceedings of the 1st Manufacturing & Industrial Engineering Symposium.

Castro-Silva, J. A. (2016). Sistema de riego automatizado basado en la internetr de las cosas. Rioja: UNIR.

Dan, L. (2015). Intelligent Agriculture Greenhouse Environment Monitoring System Based on IoT Technology. China: Internacional of Intelligent Transportation, Big Data and Smart City.

FAO. (2017). Organización de las naciones unidades para la alimentación y la agricultura. Obtenido de http://www.fao.org/climatechange/epic/que-hacemos/que-es-la-agricultura-climaticamente-inteligente/es/

Ferentino. (2017). Wireless sensor networks for greenhouse climate and plant condition. GRECIA: ELSEVIER.

Fidalgo. (2010). Redes de Sensores sin Cables para Agricultura de Precisión en. Galicia: CONAMA 10.

International Telecommunication Union. (2005). The internet of Things. Geneva.

Olcese, C. V. (19 de Septiembre de 2006). Monografias . Obtenido de http://www.monografias.com/trabajos13/enfogest/enfogest.shtml#biblio

Saric. (13 de 8 de 2013). InfoVis. Recuperado el 20 de 7 de 2017, de http://www.infovis-wiki.net/index.php/DataInk_Ratio

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 22/09/2017
Aceitação/Acceptance: 02/03/2018

Plataforma de Big Data para la Administración de Recursos Hídricos en Cuencas Chilenas

Orlando Saldaña, Ania Cravero, Roberto Espinosa

o.saldana01@ufromail.cl, ania.cravero@ufrontera.cl, roberto.espinosa@ufrontera.cl

Departamento de Cs de la Computación e Informática, Universidad de La Frontera, Temuco, Chile.

Pages: 13–23

Resumen: A lo largo del tiempo, los recursos hídricos del mundo se han visto afectados por diversos factores como el cambio climático, el cambio de vegetación, el aumento de la población, el aumento de la agricultura, entre otros. La combinación del crecimiento de la demanda de agua, el clima y la brecha hidrológica impulsaron a los responsables de la toma de decisiones y a los administradores del agua a buscar estrategias para una gestión eficaz de los recursos hídricos. En los últimos años se han propuesto soluciones de Big Data para problemas de gestión de los recursos hídricos en general. Este trabajo propone una plataforma de Big Data para mejorar la toma de decisiones analizando las variables que influyen en el estado del recurso hídrico en Chile.

Palabras claves: big data, plataforma, cuenca, recursos hídricos.

Big Data Platform for the Administration of Water Resources in Chilean Basins

Summary: Over time, the world's water resources have been affected by various factors such as climate change, vegetation change, population growth, increased agriculture, among others. The combination of growing water demand, climate and the hydrological gap prompted decision makers and water managers to seek strategies for effective water resources management. In recent years, Big Data solutions have been proposed for problems of water resources management in general. This paper proposes a Big Data platform to improve decision making by analyzing the variables that influence the state of the water resource in Chile.

Keywords: big data, platform, basin, water resources.

1. Introducción

Los recursos hídricos son el punto de partida para la vida en todas las especies que viven en nuestro planeta. La mayoría de los seres vivos necesitan agua dulce, pero sólo el 0,3% del agua que está en el planeta está catalogado como agua potable (Gleick, 1993). La demanda de agua ha aumentado (García, 2015) debido al crecimiento de la población

como consecuencia del desarrollo económico, mientras que en varias regiones sufren de inundaciones y de sequía, lo que lleva a la mala gestión de los recursos hídricos. Por otra parte, el cambio climático ejerce un gran impacto en los sistemas de agua causando grandes cambios en los recursos hídricos debido a sus efectos directos sobre los procesos hidrológicos como la precipitación, evaporación y humedad. La combinación de un crecimiento en la demanda de agua, el clima y la brecha hidrológica empujó a los tomadores de decisiones y los gestores de los recursos hídricos para buscar estrategias para la gestión eficaz de los recursos hídricos (Ciolofan, 2013a).

Aunque Chile es considerado uno de los países privilegiados respecto a la disponibilidad de recursos hídricos, su disponibilidad es desigual a lo largo del territorio nacional. La relación extracción/disponibilidad de agua es favorable en las regiones del sur, mientras que en las del norte, las extracciones superan el caudal disponible.

Existe gran cantidad de datos, estudios e informes los cuales se entrelazan con más de 40 actores institucionales responsables de la ejecución de más de 100 funciones. Esta situación, develada en el informe del banco mundial (2016) (Banco-Mundial, 2016), plantea el desafío de enfrentar las deficiencias en cuanto a la cobertura, dispersión, calidad y accesibilidad de la información sobre los recursos hídricos en nuestro país. En este contexto, las barreras (o limitaciones) presentes en los procesos de generación, gestión y difusión de la información relacionada con el recurso hídrico es, actualmente en Chile, una de las mayores preocupaciones de los tomadores de decisión al momento de diseñar políticas públicas efectivas para una gestión sustentable de los recursos hídricos.

Un factor no menos importante es la multiplicidad de formatos en que se presenta la información disponible: hojas de cálculo, archivos de texto, formatos de información geo-referenciada, etc. Para quien no se encuentre familiarizado/a con estos términos, o no posea habilidades computacionales intermedias, analizar estos archivos le demandará meses de aprendizaje, búsqueda de software adecuados, o finalmente no podrá obtener la información que necesita.

Los principales desafíos al momento de enfrentar el manejo de la información del agua son: gran volumen de información medida insitu como también remotamente mediante satélites y radares; visualización efectiva de datos espacio temporales; tamaño y heterogeneidad de los datos; diversidad de fuentes de datos y datos nuevos generados por modelos de cuencas.

Según Mocanu et al. (2013), hay varios desafíos relacionados con el desarrollo de TIC para la gestión del agua de hoy en día (Mocanu, 2013):

- La cantidad de datos crece progresivamente, por lo que se necesitan métodos para gestionar grandes volúmenes de datos;
- Los datos provienen de muchos sistemas heredados que recogen y procesan la información (por ejemplo, con respecto a los ríos afluentes, o su afluente) por lo que a menudo tienen que componer las aplicaciones existentes.
- La zona geográfica para el análisis es amplia.
- Los datos son de distinto tipo, lo que hace el análisis de los mismos, más complejo.

En este sentido, pensado en una nueva tecnología que permita el procesamiento de datos a gran escala, con una estructura compleja y un conjunto de datos de distintos tipos, estructurados y semi-estructurados, es que sale a la luz lo que se conoce hoy como Big Data (Al-Najran & Dahanayake, 2015). Gartner (2013) define Big Data como "un volumen de datos muy grande y de alta velocidad, y/o son los activos de información de alta variabilidad que requieren nuevas formas de procesamiento para mejorar la toma de decisiones, los descubrimientos, y la optimización de los procesos" (Regina, 2013). Posteriormente Demchenko et al. (2013) propusieron una nueva definición que incluye las siguientes propiedades conocidas como las 5V: Volumen, Velocidad, Variedad, que constituyen las propiedades originales de Big Data; y agregan el Valor y Veracidad como resultado de la clasificación inicial y procesamiento de datos en el contexto de un proceso o modelo específico (Demchenko, 2013).

Como resultado del análisis de las prácticas existentes en las diferentes comunidades científicas y dominios tecnológicos de la industria, se ha propuesto una arquitectura para Big Data, que considera los siguientes componentes o bloques: (1) identificación de las fuentes de datos, (2) almacenamiento; (3) clasificación y filtrado, (4) análisis, (5) visualización, (6) análisis por los tomadores de decisiones (Demchenko, 2013).

Hasta el momento, no existe una estrategia común para el diseño de la arquitectura de Big Data. Pero en los últimos años, se han propuesto soluciones de Big Data para problemas de administración de los recursos hídricos en general. En Ciolofan et al. (2013), presentan una solución particular de Big Data para apoyar la toma de decisiones en casos de contaminación de los recursos hídricos, logrando que los tomadores de decisiones puedan evitar, mitigar o simplemente ser conscientes de los riesgos que se pueden alcanzar en casos de contaminación(Ciolofan et al., 2013b). Por otro lado, Dmitriyev et al. (2015) demostraron la utilidad de una arquitectura de Big Data para ampliar el potencial en la gestión del agua, consolidando los datos de sensores y del acontecimiento, y ofreciendo un análisis interactivos mediante informes normalizados (Dmitriyev, 2015). Ai et al. (2015) propone un modelo de análisis de escenas para organizar y aplicar la información objetiva bajo la condición de Big Data. Este nuevo modelo tiene la capacidad de combinar el análisis causal y la deducción asociativa. La ventaja del método propuesto radica en su capacidad para el procesamiento rápido y análisis dinámico de los recursos hídricos cuando el volumen de datos es grande, para resolver problemas de evaluación de los recursos hídricos y la mejora en la toma de decisiones (Ai, 2015).

A partir de la situación descrita, se puede definir como problema de investigación, la ausencia de un mecanismo que permita la integración de la enorme cantidad de datos existentes en instituciones públicas para poder ser analizados, en aras de obtener una gestión eficiente de los recursos hídricos a partir de una toma de decisiones correctamente respaldada. El uso de Big Data en este contexto, se convierte en una gran oportunidad para que todos puedan aprovechar su análisis.

Para dar solución a la problemática planteada, en este trabajo se propone una plataforma de Big Data que permita mejorar la toma de decisiones al analizar las variables que influyen en el estado del recurso hídrico en Chile. La particularidad de esta propuesta está dada por la inexistencia de una solución que integre datos provenientes de múltiples

fuentes de la región de la Araucanía, como información de estaciones meteorológicas, de la DGA (Dirección Regional Agua), y de imágenes satelitales, entre otros.

A modo de prototipo, en este estudio, se utilizaron datos, de los últimos 30 años, sobre los recursos hídricos de la micro cuenca denominada Malleco-Vergara, ubicada en una de las zonas más afectadas por la escasez de precipitaciones en el último tiempo en la región.

El documento se estructura de la siguiente manera. La sección 2 describe la plataforma de Big Data diseñado para el análisis en recursos hídricos. La sección 3 describe el análisis y resultados. Finalmente, la sección 4 contiene las conclusiones.

2. Plataforma de Big Data para la gestión de datos en cuencas chilenas

En esta sección se describen la realización de un conjunto de tareas debidamente diseñadas con el objetivo de identificar todos los posibles requerimientos a tener en cuenta. Para ello se consideró las experiencias positivas encontradas en el estado del arte de propuestas similares, se identificaron un conjunto de requisitos a través de reuniones con las principales instituciones relacionadas con el proyecto (DGA, Comisión Regional de Riego y Mesa del Agua Regional) y el conocimiento del dominio de varios expertos vinculados a la propuesta.

Los requisitos más importantes para la plataforma de Big Data son los siguientes:

- Manipular la diversidad heterogénea de bases de datos existentes, incluyendo herramientas para manipular el pre o post procesamiento.

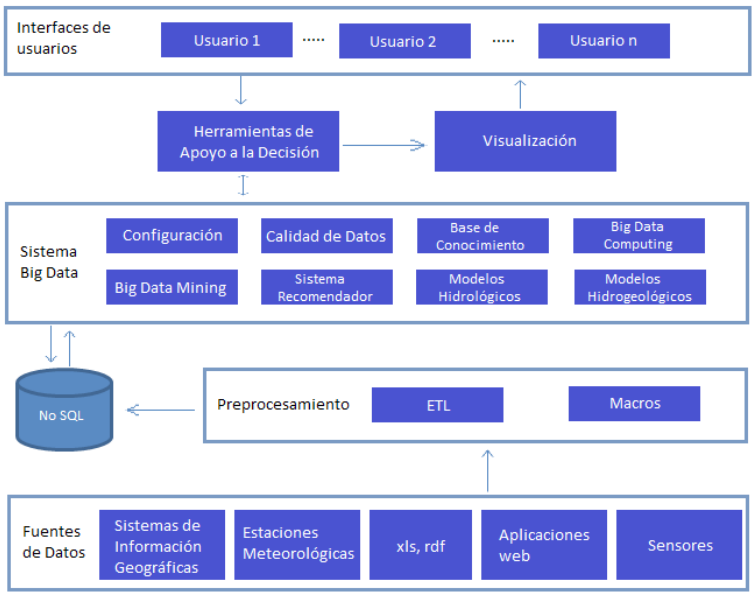


Figura 1 – Arquitectura de Big Data para la plataforma.

- Crear una arquitectura distribuida que permita utilizar varias plataformas informáticas.
- Proporcionar la interacción con modelos hidráulicos e hidrológicos.
- Interactuar con el sistema de análisis Big Data para recolectar, analizar y visualizar datos.
- Manejar eficientemente información georeferenciada empleando Sistemas de Información Geográfica (SIG).

En nuestro diseño se consideró los siguientes componentes o bloques: (1) fuentes de datos, (2) preprocesamiento, (3) Sistema de Big Data, e (4) Interfaces de usuario. La Figura 1 presenta un esquema de la arquitectura diseñada.

A continuación se detallará las funcionalidades de cada bloques.

1. Fuentes de Datos: La arquitectura consta con un primer bloque donde se define el acceso a las distintas fuentes de datos. Estas provienen de orígenes diversos: portales de datos públicos como es el caso de la DGA y el sistema meteorológico de Chile, archivos en diferentes formatos como es el caso de planillas electrónicas obtenidas desde la DGA, sistemas de información geográfica donde se obtienen imágenes satelitales e información actualizada, etc. Todos los datos fueron almacenados en una base de datos Hbase utilizando la plataforma Hadoop[1], debido a la variedad y volumen de la información requerida.
2. Preprocesamiento: En este bloque se analizan los datos provenientes de los distintos repositorios, y se implementan distintas tareas de preprocesamiento para transformarlos. Se busca vincular los conjuntos de datos no estructurados y estructurados para que puedan ser almacenados y formen parte del sistema. El propósito final es poder dejar los datos listos para ser insertados en el repositorio general de la plataforma de Big Data. Las fuentes de información fueron tomadas de bases de datos de entidades públicas tales como Dirección General de Aguas, Dirección de Obras Públicas, Gobierno Regional, Comisión Nacional de Riego del Ministerio de Agricultura, así como de servidores de información atmosférica disponible en satélites tales como Advanced Very High Resolution Radiometers (AVHRR) y Moderate Resolution Imaging Spectrometers (MODIS, USA).

   Más que resultados para usuarios finales, resulta importante describir el procedimiento llevado a cabo durante el proceso de implementación de la arquitectura en cada uno de sus niveles. Se hará énfasis en algunas experiencias vividas en dos de los componentes fundamentales en el desarrollo de la arquitectura, el preprocesado de los datos y su posterior almacenamiento.

   En el caso específico del preproceso de los datos, el objetivo fue lograr almacenar los datos con la mejor calidad posible. Para cada tipo de archivo el preprocesado fue diferente, los datos se transformaron teniendo en cuenta las reglas del negocio. Una parte considerable de las fuentes de datos provenían en formato xls, para ello se requirió un arduo trabajo semiautomático a través de la implementación de macros en Excel y el uso de Kettle para lograr prepararlos y limpiarlos. Esta tarea fue necesaria a partir de la necesidad de contar con los datos con una estructura homogénea. Se decidió almacenar las fuentes de

[1] Hadoop http://hadoop.apache.org/

datos en formato No SQL para obtener mayor rendimiento y posibilidad de utilización de la información.

La gran parte de las fuentes de datos analizadas eran estructuradas o semiestructuradas, aunque en su mayoría no contaban con información georeferencial. Sólo pudimos obtener este tipo de información a partir de imágenes satelitales obtenidas de Sistemas de Información Geográfica (Satélites MODIS y LANDSAT) disponibles de la región.

Se debe resaltar la importancia que tiene la geolocalización de cada dato, como factor incidente en la interpretación del resultado por los usuarios finales. La Fig. 2 es un ejemplo de imagen del satélite MODIS que se ha procesado para obtener el índice de vegetación y obtener la cantidad de agua del sector. Esto debido a que la zona está rodeada de empresas forestales y las plantaciones han cambiado en estos últimos 10 años considerablemente.

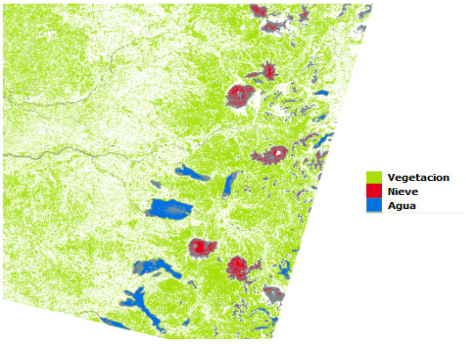


Figura 2 – Ejemplo de imagen procesada a través de un SIG

3. Sistema Big Data: Este módulo fue definido por un conjunto de componentes necesarios para la implementación y gestión del sistema Big Data. La interacción entre todos ellos garantiza las posibles respuestas a las solicitudes realizadas por los usuarios y el propio sistema. Cada subsistema tiene su función específica dentro de la arquitectura:

- Configuración: Permite configurar las distintas opciones generales del sistema permitiendo el óptimo funcionamiento de todos sus componentes.
- Big Data Computing: Se establecen las acciones a realizar sobre los grandes volúmenes de datos almacenados, para que puedan ser procesados eficientemente y de esta forma mejorar el rendimiento de la aplicación. En este caso, se procesaron una serie de indicadores, como temperaturas medias máximas y mínimas, medias de humedad y porcentaje de plantación nativa, versus la exótica.
- Big Data Mining: Permite implementar el uso de librerías de algoritmos de minería de datos para ejecutar análisis inteligente. Permite la exploración de los datos para comprender el comportamiento de las variables, predecir valores, así como ofrecer servicios personalizados de obtención de conocimiento a partir de

la información almacenada. Se utilizó Weka[2] como herramienta de análisis de datos con todos los datos procesados en formato csv.
- Base de Conocimiento: Permite almacenar de forma homogénea, las características de las fuentes de datos analizadas (incluyendo meta-características), resultados de minería de datos obtenidos al aplicar ciertos algoritmos sobre fuentes de datos concretas y criterios de calidad de datos.
- Modelos Hidrológicos e Hidrogeológicos: Estos componentes permitirán que especialistas hidrólogos e hidrogeológicos creen sus modelos de pronósticos, permitiendo analizar la gran cantidad de fuentes de datos disponibles y hacerlos disponibles para su utilización por la ciudadanía. Se pretende a su vez demostrar la disponibilidad de las ciencias medioambientales para facilitar el avance en la predicción de los recursos hídricos. También facilitar problemas a gran escala relacionados con el agua [26].

4. Interfaces de Usuarios: Este es el nivel externo de la arquitectura, donde se implementa la interacción con los usuarios finales para identificar sus intereses y extraer la información para construir las consultas a los datos. Se ha utilizado el sistema IBM Watson Analytics[3] para mostrar diversos análisis y gráficos de los datos.

3. Resultados y Discusión

En términos generales, se logró la integración de cada uno de los componentes de la plataforma propuesta, siendo los módulos más importantes el Sistema de Análisis Big Data y el SIG para el intercambio y obtención de información. La extracción de datos se presenta en diferentes formatos, es decir, estructurados, semiestructurados y/o datos no estructurados que pueden ser utilizados por los sistema de almacenamiento, visualización y análisis posterior.

Los resultados se devuelven a la plataforma para ser utilizadas por herramientas de apoyo a la decisión relacionadas con problemas de recursos hídricos. Se ha prestado especial atención a la normalización de las entradas/salidas de datos de manera modular e independiente. Para lograr el desarrollo del sistema, la aplicación fue configurada en la herramienta IBM Watson Analytics. Ver ejemplos en figuras 3, 4 y 5.

El sitio experimental para este estudio de caso es la subcuenca Malleco-Vergara que se encuentra en el sur de Chile, perteneciente a la provincia de Malleco en la Región de La Araucanía. El área de la cuenca es alrededor de 1158 km cuadrados.

Esta cuenca fue seleccionada debido a que presenta características relevantes para un análisis de sus recursos hídricos. En primer lugar es una cuenca utilizada para la agricultura, debido al micro-clima existente. Además existen varias empresas forestales que realizan plantaciones de pino y eucaliptus, cambiando las plantaciones en torno a la cuenca. Por último, en esta cuenca se están llevando a cabo plantaciones de viñedos lo que la hace atractiva para los grandes empresarios. Por ello, interesan diversos análisis

[2] Weka http://www.cs.waikato.ac.nz/ml/weka/
[3] IBM Watson Analytics https://www.ibm.com/watson-analytics

para la toma de decisiones, como creación de represas, pasarelas de riego para el riego agrícola, y el riego en forestales.

Uno de los análisis que se decidió utilizar es el caudal del rio Vergara debido al cambio climático, al cambio en plantaciones, aumento de la agricultura y el aumento en habitantes. Todos estos datos, además de los explicados anteriormente, fueron procesados para ser guardados en la plataforma de Big Data a través de Hadoop, para evaluar algunos otros indicadores, por ejemplo, recursos hídricos actuales, capacidad de almacenamiento de cuencas hidrográficas, el uso de suelos de las forestales y de la vegetación en general.

Se realizaron análisis representativos de los indicadores ambientales seleccionados dentro de la cuenca, tales como la evaluación de la vegetación, evaluación de la agricultura, variación de recursos, potencialidades de almacenamiento de cuencas hidrográficas, y la variación del caudal del rio Vergara.

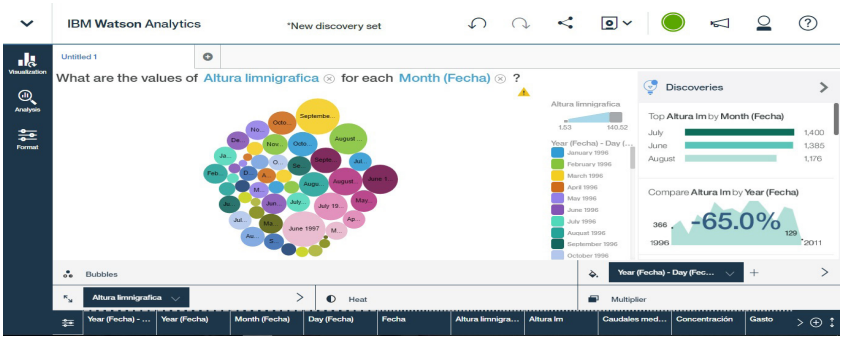


Figura 3 – Ejemplo de gráficos obtenidos en Watson Analytics (Valores de la altura limnigráfica para cada mes).

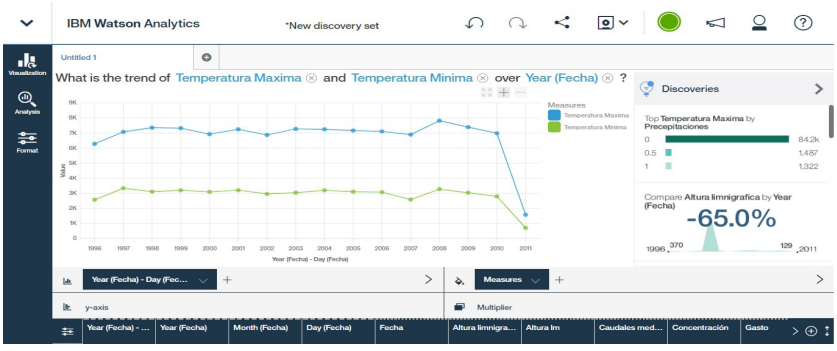


Figura 4 – Ejemplo de gráficos obtenidos en Watson Analytics (Tendencia de la temperatura máxima y mínima durante un año).

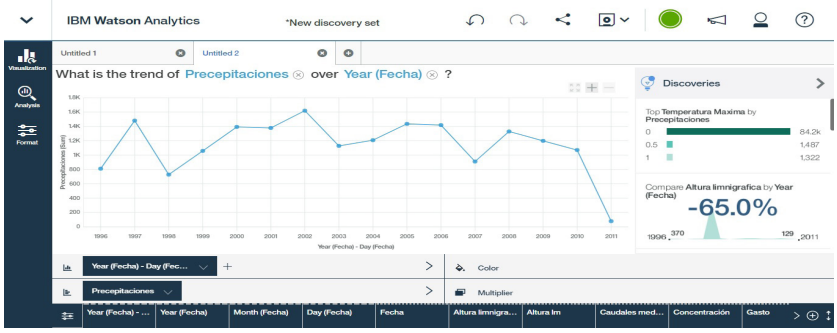


Figura 5 – Ejemplo de gráficos obtenidos en Watson Analytics (Precipitaciones por año).

A partir de los resultados expuestos, los expertos concluyeron que un aumento en la temperatura disminuye el valor del caudal, debido fundamentalmente al aumento en la evaporación del agua a mayor temperatura. Además, se comprobó que de manera contraria a lo que se pensaba de antemano, las precipitaciones no son el factor principal en el aumento del caudal de la cuenca, aunque se debe tener en cuenta el problema de la medición antes mencionado.

A pesar de que la aplicación de la arquitectura es bastante reciente y aún en desarrollo, es evidente el aporte de nuestra investigación en la búsqueda de soluciones para un problema de envergadura nacional como es la organización y acceso a la información vinculada a los recursos hídricos y medioambientales para la posterior toma de decisiones.

El impacto alcanzado es de gran magnitud puesto que los/as tomadores de decisión, no contaban con información disponible en forma integrada y procesada acerca de las variables que afectan el recurso hídrico en la cuenca como unidad de análisis, lo cual dificultaba el abordar políticas de mediano y largo plazo.

4. Conclusiones

En este artículo se ha presentado una arquitectura de Big Data “ad hoc” a partir de los requisitos específicos particulares identificados durante la interacción con los tomadores de decisiones de la región. La plataforma obtenida está orientada a integrar, normalizar y visualizar la información obtenida de las múltiples variables que determinan el estado de los recursos hídricos en la región de La Araucanía.

Esta propuesta ofrece una plataforma de comunicación efectiva para los tomadores de decisiones del sector público regional acerca de las variables que afectan la disponibilidad y calidad de los recursos hídricos. Para la implementación de la plataforma fue necesaria la participación de diversos actores relevantes, como ingenieros de software, ingenieros de datos, hidrólogos e ingenieros forestales, además de tomadores de decisiones de la DGA, la mesa del agua regional y de la Dirección de Riego.

En la medida que se desarrollen nuevos modelos de pronósticos y se consuman con mayor profundidad los resultados de algoritmos de minería de datos por la ciudadanía, esta plataforma aumentará el impacto obtenido. El consumo de conocimiento no puede solo estar restringido a las personas vinculadas al sector público, sino que debe estar disponible a la ciudadanía. Esta propuesta tiene como trabajo futuro extender la participación ciudadana como ente fundamental en el proceso, contribuyendo de esta forma a la democratización del conocimiento que todos deseamos.

Agradecimientos

Este trabajo ha sido financiado por la Universidad de La Frontera a través del proyecto DIUFRO DI17-0043.

Referencias

Ai, P., Yue, Z., Yuan, D., Liao, H., & Xiong, C. (2015). A scene analysis model for water resources big data. 2015 14th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES)(200–283).

Al-Najran, N., & Dahanayake, A. (2015). A requirements specification framework for big data collection and capture. New trends in databases and information systems. 12–19.

Banco-Mundial. (2016). Informe anual. https://openknowledge.worldbank.org/bitstream/handle/10986/24985/210852SP.pdf.

Ciolofan, S., Mocanu, M., & Ionita, A. (2013a). Distributed cyberinfrastructure for decision support in risk related environments. 2013 IEEE 12th International Symposium on Parallel and Distributed Computing, 109–115.

Ciolofan, S., Mocanu, M., & Ionita, A. (2013b). Distributed cyberinfrastructure for decision support in risk related environments.

Demchenko, Y., Membrey, P., Grosso, P., & de-Laat, C. (2013). Addressing big data issues in scientific data infrastructure. First International Symposium on Big Data and Data Analytics in Collaboration (BDDAC 2013). Part of The 2013 Int. Conf. on Collaboration Technologies and Systems (CTS 2013). San Diego, California, USA.

Dmitriyev, V., Gómez, J., & Osmers, M. (2015). Big data inspired water management platform for sensor data. INFORMATIK'15. Lecture Notes in Informatics (LNI), Gesellschaft fuÈr Informatik.

García, D., Quevedo, J., Puig, V., & Saludes, J. (2015). Water demand estimation and outlier detection from smart meter data using classification and big data methods. 2nd New Developments in IT \& Water Conference, 8-10 February 2015, Rotterdam (Holland), 1–8.

Gleick, P. (1993). Water in crisis: A guide to the world's fresh water resources. Oxford University Press, Inc.

Mocanu, M., Muste, M., Lungu, V., & Drobot, R. (2013). Composite application for water resource management. Advances in Intelligent Control Systems and Computer Science, 295–306.

Regina, C., Beyer, M., Adrian, M., Friedman, T., Logan, D., Buytendijk, F., et al. (2013). Top 10 technology trends impacting information infra- structure. Gartner publication.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 10/09/2017
Aceitação/Acceptance: 19/03/2018

Aplicación de una metodología de seguridad avanzada en redes inalámbricas

Franklin Sánchez Espinosa[1], Jorge Vivero García[2], Diego Baroja Llanos[3].

fsanchez@pucesi.edu.ec, jjvivero@pucesi.edu.ec, dfbaroja1@pucesi.edu.ec

[1] Departamento de Sistemas, Pontificia Universidad Católica del Ecuador Sede Ibarra, Av. Jorge Guzmán y Av. Aurelio Espinosa Polit, 100111, Ibarra, Ecuador.

[2] Escuela de Ingeniería, Pontificia Universidad Católica del Ecuador Sede Ibarra, Av. Jorge Guzmán y Av. Aurelio Espinosa Polit, 100111, Ibarra, Ecuador.

[3] Escuela de Ingeniería, Pontificia Universidad Católica del Ecuador Sede Ibarra, Av. Jorge Guzmán y Av. Aurelio Espinosa Polit, 100111, Ibarra, Ecuador.

Pages: 24–38

Resumen: Las redes inalámbricas WLAN (802.11) en la actualidad se han convertido en una infraestructura de muy común uso por hogares y sobre todo por organizaciones con el propósito de extender sus recursos y servicios corporativos de red a más usuarios, fuera del alcance de una red con cables. Lo que ha provocado nuevas oportunidades a personas no autorizadas tratar de conseguir acceso no autorizado, obtener información sensible o provocar en forma parcial o definitiva la indisponibilidad del servicio, ayudado por las peculiaridades del medio de transporte de los datos y del tráfico que por el circula. Para ello se propone el desarrollo de una metodología que permita mejorar el proceso de seguridad de una red WLAN basado en el proceso de mejora continua y buenas prácticas de la industria, con el objetivo de vislumbrar una cadena de recomendaciones de seguridad para el diseño de redes WLAN y posibles implantaciones.

Palabras-clave: WLAN; metodología; seguridad; diseño; IEEE 802.11; WI-FI.

Application of an advanced security methodology in wireless networks

Abstract: WLAN wireless networks (802.11) have now become an infrastructure very common for households and especially for organizations with the purpose of extending their corporate network resources and services to more users, beyond the reach of a network with cables. What has caused new opportunities for unauthorized persons to try to obtain unauthorized access, obtain sensitive information or partially or definitively cause the unavailability of the service, aided by the peculiarities of the means of transport of data and traffic that circulates through it. To this end, it is proposed to develop a methodology to improve the security process of a WLAN network based on the process of continuous improvement and good practices of the industry, with the aim of glimpsing a chain of security recommendations for the design of networks WLAN and possible implementations.

Keywords*:* WLAN, methodology, security, design, IEEE 802.11, WI-FI.

1. Introducción

En la actualidad las redes inalámbricas (Wireless Local Área Network - WLAN) dentro del estándar 802.11 publicado en el año 1997 por el Institute of Electrical and Electronics Engineers (Instituto de Ingenieros Eléctricos y Electrónicos – IEEE) (1999) siguen siendo una de las tecnologías ampliamente usadas en cualquier escenario donde exista la necesidad de transferir información como: el hogar, el trabajo, en lugares públicos, comunitarios, organizaciones públicas / privadas y por supuesto en los centros educativos y aprovechar los beneficios proporcionados de movilidad, escalabilidad, flexibilidad, ahorro de costes, reducción de tiempos en la instalación, entre otros. De igual manera reconocer que existe problemas de diseño, implementación y administración respecto a la seguridad que acarrea esta tecnología al ser una conexión sin cables expuesto en el aire mediante ondas perceptibles en el ambiente por su dispersión espacial que resulta difícil de controlar.

El reto es aún mayor en la Universidad debido a que ofrecen servicios a diferentes tipos de usuarios en su entorno a diferencia de las oficinas de negocios o empresas de negocio, debido a la transferencia de información académica tanto de estudiantes, docentes, facultades e investigaciones.

Por otro lado en el Ecuador existe el ente de aseguramiento de la calidad de la universidad ecuatoriana CEAACES (Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior) encargado de categorizar a la universidad de acuerdo a estándares de calidad que entre los cuales se figura el de conectividad que básicamente tiene que ver con el acceso a internet por parte de sus integrantes (estudiantes, docentes, administrativos e invitados) con el uso de redes inalámbricas, siendo un medio muy susceptible y vulnerable donde puedan generarse y aprovecharse de puertas traseras, botnets y malware; asimismo intentar acceder sin autorización a la red pudiendo comprometer la confidencialidad e integridad de la información, debido a que este tipo de conectividad suele tener implementado restricciones mínimas de acceso; y a la indisponibilidad de los servicios ofrecidos por esta tecnología.

Debido a la no consideración de la seguridad como buena práctica a la hora de implementar e implantar la tecnología inalámbrica WLAN, como extensión a la red de área local, ha conllevado a problemas o riesgos de seguridad que no únicamente afecta a la tecnología WLAN sino que también se vería afectada la LAN cableada (IEEE 802.3) por la baja o nula seguridad en protocolos y mecanismos de cifrado; que aumenta considerablemente a la hora de proteger la información afectando a la disponibilidad del servicio, privacidad, no repudio, confidencialidad e integridad de la información provocando un impacto negativo en la organización.

Como lo expresa la OSSTMM “The information to be found within the wireless spectrum is not limited to product specifications.” (OSSTMM, 2010) La solución no está solamente en adecuar la red en base a las especificaciones y/o características de los productos, sino que va más allá de estos límites, como:

- Falta o deficiente política de seguridad en entornos inalámbricos.
- Falta de seguridad perimetral física de dispositivos inalámbricos (AP, controladoras)
- Interferencia en las señales EMT por dispositivos comunes (impresoras, microondas,)

- No consideración de casos de abuso en el diseño e implementación de redes inalámbricas locales.
- La mala práctica de mantener la configuración por defecto de los productos o servicios.
- La desactualización de sistemas, software, firmware y servicios de aplicaciones requeridas para la operación
- Desconocimiento interno del personal técnico y no técnico de redes inalámbricas.
- EL uso de protocolos de autenticación y autorización insuficientes y deficientes
- Uso de protocolos de confidencialidad y cifrado débil, de fácil configuración, por comodidad de los técnicos.
- El Mal funcionamiento de los equipos.

Partiendo del criterio del estándar para la seguridad de la información "The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed." (ISO/IEC 27001:2013, 2013) Es relevante señalar que es importante precautelar con uno de los activos más importantes de la organización, como la información organizacional y personal, generada en el entorno del instituto de educación superior (IES), como responsabilidad técnica y social de resguardar la información ante cualquier acto por personal no autorizado, frente a:

- Obtención de información personal, debido a que en la red inalámbrica se encuentra información de aplicaciones, datos bancarios y financieros, información de investigaciones, datos académicos, etc.
- Hacer uso de la red inalámbrica para cometimiento de delitos informáticos o hechos ilícitos, dejando rastro falso.
- Aprovechar de la Internet de las cosas (IoT), y realizar ataques enmascarados.
- Controlar los equipos remotamente mediante el uso de aplicaciones malware, amenazas persistentes avanzadas (APT) mediante la ingeniería social.
- Husmeo de la red en busca de información que comprometa a la organización como patentes, investigaciones, accesos privilegiados, documentos secretos, etc.

2. Fundamentación técnica

"Una red inalámbrica de área local (WLAN) es aquella en la que una serie de dispositivos (PC, estaciones de trabajo, impresoras, servidores, laptop, PDA, etc.) se comunican entre sí mediante emisiones radioeléctricas que se propagan a través del aire, sin necesidad de ningún tendido de cable." (Pellejero, Andreu, & Lesta, 2006) En la actualidad a esto hay que sumarle la interacción dispositivos contemplados en la Internet de las Cosas (IoT) que no se trata de dispositivos meramente técnicos de capas inferiores dentro del modelo OSI (electrodomésticos inteligentes) y que están al alcance de cualquier usuario, que gracias a las configuraciones predeterminadas y su fácil implementación hacen que cualquier persona hagan uso de ellos y logrando conexión directa a Internet, para citar: televisores, aires acondicionados, neveras, lavadoras, interruptores, cafeteras, etc. Incrementando en forma preocupante los riesgos de seguridad que conlleva el tener conectado un dispositivo en la red.

Estadísticas recopiladas y presentada por Afshar (2014) se logra identificar aquellas que de alguna u otra manera inciden en temas de seguridad de la información:

- La mayoría de las empresas están planeando aumentar la capacidad Wi-Fi en al menos 20% en 2014.
- 2/3 de las empresas permiten a sus empleados traer sus propios dispositivos a la empresa hoy en día.
- Un ataque Wi-Fi en una red abierta puede tardar menos de 2 segundos.
- En los próximos 3 años habrá más de 7 mil millones de dispositivos Wi-Fi.
- 11ac / Wave2 está configurado para ofrecer velocidades inalámbricas de varias gigas en menos de 2 años.
- El 90% de todos los teléfonos inteligentes están equipados con Wi-Fi.
- El 71% de todos los flujos de comunicaciones móviles es a través de Wi-Fi.
- 79% de los usuarios de teléfonos inteligentes tienen su teléfono con ellos durante 22 horas al día.
- 90% de las actividades de BYOD se componen de; correo electrónico, calendario, compras, actividades bancarias y sociales.
- Para 2017, el 50% de las empresas no suministrarán dispositivos informáticos para empleados.
- 80% de las empresas no proporcionan educación / formación en BYOD. 60% de las empresas están sin una política escrita BYOD.
- Más de la mitad de todas las redes Wi-Fi abiertas son susceptibles de abuso.
- El 80% del sistema operativo global del mercado de teléfonos inteligentes es Android, el 79% de todo el malware de Smartphone está en Android Apps.
- Más de 2,7 millones de personas utilizaron Internet en 2013. Eso representa más de la mitad de la población mundial.
- Para 2020, se prevé que 24 billones de dispositivos estarán conectados a Internet. La gran mayoría usará alguna forma de acceso inalámbrico.

2.1. Topologías más usadas

Las LAN inalámbricas bajo el estándar 802.11 pueden tener dos tipos de topología de red:

Topología AD HOC

En la Figura 1 indica un conjunto de servicios básicos independientes, la comunicación es punto a punto entre dos dispositivos inalámbricos sin necesidad de un equipo de red intermedio, ejemplo de esta topología es WI-FI Direct. Una variante de redes ad hoc es la ofrecida por los Smartphone, que tienen la capacidad de ofrecer una zona de cobertura inalámbrica temporal para compartir el acceso a internet (CISCO CCNA, 2016).



Figura 1 – Topología AD HOC (Sánchez E. Franklin, 2017)

Topología Infraestructura

En la Figura 2 se observa la topología en modo infraestructura, existen dos elementos principales, el conjunto de servicios básicos (BSS) y un conjunto de servicios extendidos (ESS). El primero refiere a la cobertura de los puntos de acceso, indicados en el círculo, identificado por la dirección MAC del punto de acceso y representada con un nombre de red conocido como BSSID o SSID; si un cliente sale de su BSS ya no puede comunicarse con los otros dispositivos inalámbricos dentro de BSA o BSS.

Cuando la cobertura de radio frecuencia de un BSA es insuficiente es necesario la extensión del servicio mediante ESS por medio de un sistema de distribución cableado o inalámbrico. El área rectangular representa un ESS, a esta área se le conoce como Área de servicio extendida (ESA) que permite a los clientes inalámbricos poder trasladarse de un BSS a otro sin perder conectividad o en el peor escenario volverá a conectarse sin dificultad (CISCO CCNA, 2016).

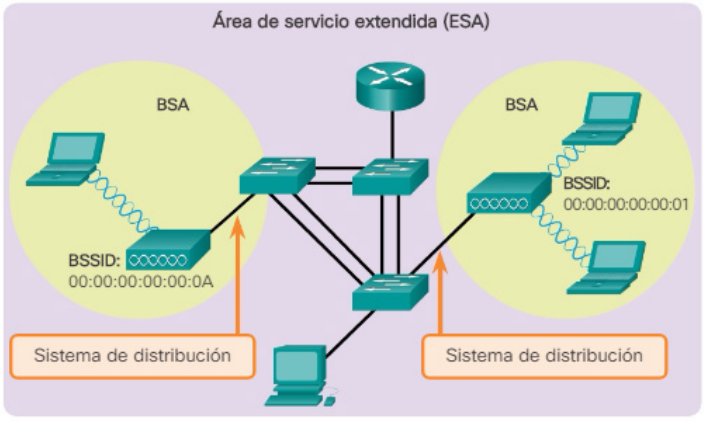


Figura 2 – Topología infraestructura (CISCO CCNA, 2016)

2.2. Riesgos de seguridad

En la actualidad cada vez más se implementan redes inalámbricas 802.11 (WLAN) por las necesidades propias de cada organización, es cuando, se ve necesario e importante el entendimiento de los diferentes tipos de amenazas y vulnerabilidades que conlleva esta tecnología, con el propósito de implementar controles o medidas de seguridad apropiadas de acuerdo a las buenas prácticas y estándares de la industria. La mayoría de estos problemas de seguridad son innatos al estándar 802.11 que afectan a la confidencialidad, integridad y disponibilidad

Falta de confidencialidad

Debido a la utilización de ondas de radio para la transmisión de datos por un medio público, como es el espacio, hace que sea difícil garantizar la confidencialidad haciendo que el acceso a la red sea más fácil, a diferencia que una red cableada, siendo una puerta de acceso hacia la LAN organizacional.

Otro de los ataques que compromete la confidencialidad es el denominado Eavesdropping, que es la interceptación, en tiempo real, no autorizada de una comunicación privada, como una llamada telefónica, un mensaje instantáneo, videoconferencia, navegación internet o uso de aplicaciones web. Esta vulnerabilidad se presenta cuando se omite la configuración de confidencialidad de los dispositivos de puntos de acceso; para ello el estándar 802.11 definió el protocolo WEP para proteger la información, pero hoy en día existen herramientas (Aircrack, Wifi Auditor, Acrylic) que rompen su seguridad. Este ataque es el más peligroso porque permite aperturar más opciones de ataque.

Actualmente con herramientas de escaneo un intruso puede capturar toda la información que están atravesando por el medio inalámbrico; pudiendo obtener información de usuarios, contraseñas, datos de configuración, identificadores de red o lo que resulta peor información confidencial y sensible; pensar que el atacante con una antena de alta ganancia podría capturar mensajes de datos a largas distancias, evitando estar en las cercanías de la infraestructura objetivo.

Puntos de accesos falsos (Rogue AP) o ilegales, que se implementan en una red privada sin autorización del departamento encargado, con la intención de que los usuarios se conecten a él y así lograr capturar datos sensibles como sus credenciales, haciendo creer que se trata de un Punto de Acceso legítimo logrando engañar a los clientes inalámbricos y vulnerando todos los algoritmos de seguridad; por otro lado, también sirven como punto de intrusión a la red corporativa desde otras ubicaciones, logrando saltar los controles de seguridad perimetral de la organización; y lo más penoso de todo es que los instalan personal, no necesariamente con fines de intrusión sin previa autorización y sin contemplar ninguna medida de seguridad en su configuración (Leston & Begoña, 2012).

Falta de integridad

Un ataque que vulnere la integridad es el cambio de contenido en un mensaje de datos haciendo diferente al mensaje de datos enviado originalmente, por ejemplo, un atacante podría cambiar el (Frame Check Sequence - FCS) volviendo a recalcular el valor de un mensaje capturado y alterado para volver a retransmitirlo. El FCS ayuda a la comprobación de errores durante la transmisión del mensaje de datos, este calcula un hash de todo el mensaje de datos con algoritmos conocidos y envía como texto legible sin cifrar. Anteriormente la 802.11 implementó protocolos WEP, específicamente CRC-32 (Cyclic Redundancy Check) para la gestión de la integridad que actualmente está en desuso, aparecen los estándares MIC (Michael Message Authentication Code) de forma transitoria al protocolo WEP y finalmente en vigencia el protocolo AES (Advanced Encryption Standar) (Stallings & Stallings, 2005).

Falta de disponibilidad

Esto implica a menudo el ataque de denegación de servicio DoS. Los conocidos métodos de ataque: jamming y flooding hacen que la red inalámbrica quede inutilizada por clientes legítimos que requieren los servicios o recursos ofrecidos. El jamming provoca la interferencia del espectro mediante la emisión externa de señales de alta potencia, en cambio, el flooding satura a los puntos de acceso o algún cliente inalámbrico con mensajes de datos grandes provocando la degradación o inutilización total de la comunicación en la red (Leston & Begoña, 2012).

Según Pellejero (2006), Existen otros tipos de denegación de servicio como:

- Wireless DoS. Qué consiste en la disociación de los clientes legítimos mediante el envío de tramas.
- SYN Flooding. Este ataque consiste en la inundación de segmentos de datos, en la capa de transporte del modelo TCP/IP, cuando hacia un servidor existen peticiones de establecimiento de sesión.
- Smurf. Corresponde a un ataque de denegación de servicio distribuido a nivel capa de red, mediante la utilización de una IP falsa puede provocar que los clientes atiendan las solicitudes de respuesta a dicha IP provocando la saturación de la red con tráfico innecesario.
- DNS Spoofing. Consiste en la suplantación de un servidor DNS legítimo, cuyo propósito es entregar direcciones falsas a las peticiones de los usuarios o clientes inalámbricos.
- DHCP DoS. Este ataque radica en la suplantación de un servidor DHCP en la red WLAN para asignación de direccionamiento IP falsos a los clientes de la red inalámbrica que intentan conectarse (Pellejero et al., 2006).

OWISAM 2013 - DRAFT (Open Wireless Security Assessment Methodology) se encuentra en versión borrador basado en la estructura del Proyecto OWASP (Open Web Application Security Project) y CVSS (Common Vulnerability Scoring System) es una metodología abierta que nace con el propósito de estandarizar los procesos de análisis de redes inalámbricas, medir los riesgos en forma objetiva y proteger las redes corporativas. Este proyecto contiene una licencia abierta CC-BY-SA con el ánimo de recibir aportes de experiencias para el crecimiento y mejora de la metodología.

Según la empresa TARLOGIC define el TOP 10 de riesgos de seguridad más comunes en las organizaciones que atentan contra la comunicación y cuyo medio de transporte son las redes inalámbricas WLAN y que deben priorizarse y en la medida de lo posible mitigarse (Tarlogic, 2013). A continuación, se enlistan los 10 riesgos de seguridad principales:

Control	**Descripción**
OWISAM-TR-001	Red de comunicaciones Wi-Fi abierta.
OWISAM-TR-002	Presencia de cifrado WEP en redes de comunicaciones.
OWISAM-TR-003	Algoritmo de generación de claves del dispositivo inseguro (contraseñas y WPS).
OWISAM-TR-004	Clave WEP/WPA/WPA2 basada en diccionario.
OWISAM-TR-005	Mecanismos de autenticación inseguros (LEAP,PEAP-MD5,..)
OWISAM-TR-006	Dispositivo con soporte de Wi-Fi protected setup PIN activo (WPS).
OWISAM-TR-007	Red Wi-Fi no autorizada por la organización.
OWISAM-TR-008	Portal hotspot inseguro.
OWISAM-TR-009	Cliente intentando conectar a red insegura.
OWISAM-TR-010	Rango de cobertura de la red demasiado extenso.

Tabla 1 – Top 10 de Riesgos de seguridad en WLAN (Tarlogic, 2013)

3. Identificación requisitos

Para la identificación de las tecnologías, arquitecturas, roles y los contenidos necesarios de configuraciones de redes inalámbricas WLAN en un campus de un Instituto de Educación Superior (IES) que de acuerdo a su modelo de organización tiene implementada cuatros tipos diferentes de redes inalámbricas con acceso solamente para Internet.

Red eduroam (education roaming)

Como indica la Figura 3 esta red federada fue creada para la comunidad académica y de investigación, que permite a los usuarios de las instituciones participantes mantener conectividad de internet desde su propio campus u otras instituciones con sus credenciales de usuario institucionales. La autenticación y autorización hace uso del protocolo RADIUS que tiene implementado cada institución. La autenticación se logra mediante el uso de dominios, por ejemplo usuario@pucesi.edu.ec, usuario2@institucionB.edu.ec, usuario3@ institucionC.edu.ec que gracias a un servidor Proxy RADIUS de nivel alto redirecciona las peticiones a las diferentes instituciones dependiendo del dominio. La seguridad está dada bajo el protocolo 802.11i con WPA2 modo infraestructura tipo EAP-TLS.

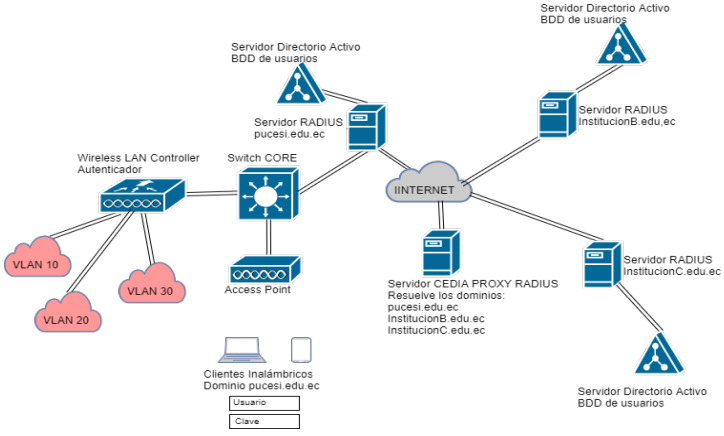


Figura 3 – Red EDUROAM en campus universitario (Sánchez E. Franklin, 2017)

Red Wifiaulas

Esta red es utilizada por los docentes en los computadores de las salas aula-clase de todas las carreras, utiliza filtrado de direcciones MAC con clave precompartida TKIP y con protocolo de seguridad WPA2-Personal.

Red Temporales abiertas

Estas redes son creadas de forma temporal, cuando se realizan eventos académicos, conferencias, seminarios, cursos, etc. Este tipo de red se encuentra aislada de la red interna debido a que se segmenta en una VLAN diferente con las respectivas restricciones.

Red con portal cautivo

Esta red se utiliza como método de autenticación un cliente con portal cautivo seguro, mediante la utilización de certificado de seguridad de servidor (SSL) donde el usuario accederá de forma normal a la red inalámbrica, una vez establecida la conexión será redireccionada a una página de autenticación. Luego de ingresadas las credenciales de usuario, la controladora inalámbrica (WLC) por medio del protocolo RADIUS solicitará la validación de las credenciales al servidor de Directorio Activo (AD), donde se encuentran todos los perfiles de usuario. El Directorio activo, superada la comprobación la autenticidad del usuario enviará un token de autorización al servidor RADIUS, en caso contrario indicará que las credenciales no son válidas. La seguridad está dada bajo el protocolo 802.11i con WPA2 modo infraestructura con portal cautivo, ver Figura 4.

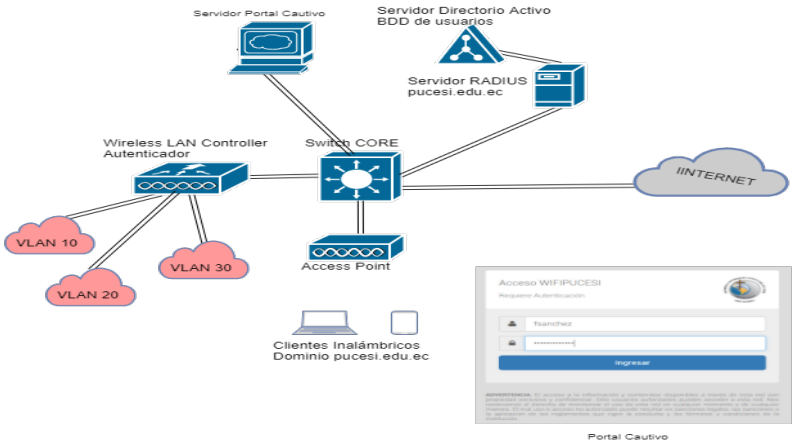


Figura 4 – Red Portal Cautivo (Sánchez E. Franklin, 2017)

4. Propuesta Metodología Aplicada

Luego de haber realizado el análisis de los requerimientos se pretende ofrecer una orientación metodológica general en la creación de un entorno de red inalámbrica segura 802.11 que permita reforzar las medidas de seguridad en los diseños de red debido a que al tratarse de una comunicación por radiofrecuencia (RF) existe mayores probabilidades de acceso a la red interna puesto a que no solo se limita al interior de los edificios, siendo posible nuevas vías de acceso a la red, sorteando los cortafuegos perimetrales cuidadosamente ubicados y las defensas perimetrales. Es oportuno ahora que la arquitectura de red incorpore el principio de defensa en profundidad.

Al diseñar redes inalámbricas es necesario construir sus medidas de seguridad en conjunción con las capas de seguridad de la red cableada 802.3. En caso de que una medida de seguridad se demuestre débil o carente, varias otras capas de la estrategia defensiva deben ofrecer protección a la red.

La siguiente propuesta no puede describir en forma detallada todas las posibles consideraciones de diseño e implementación seguras para el despliegue de una red

inalámbrica. Sin embargo, esta metodología intentará proporcionar una referencia a las consideraciones esenciales para el diseño e implementación de una WLAN empresarial segura.

"Debemos trabajar en los procesos no en el resultado de nuestros procesos" (Deming W. Edwards, 1986). Esta metodología se basa en el modelo de mejora continua de Deming denominado Plan – Do – Check – Act, el ciclo PDCA, que ayuda a generar una línea base con la característica de calidad incremental.

En la Figura 5 se adaptan criterios de seguridad de la información partiendo desde la creación de una política de seguridad basada en los escenarios comunes de implementación de redes inalámbricas que involucran servicios, infraestructura física-lógica y usuarios; que apoyarán a proteger los elementos de la seguridad principales como confidencialidad, integridad y disponibilidad. Con el análisis de riesgos determinar el uso de controles y mitigar incidencias que vayan a comprometer los elementos claves de seguridad. Ahora bien, es necesario la evaluación y revisión de los controles implementados con el objetivo de proponer acciones de mejora a la metodología.

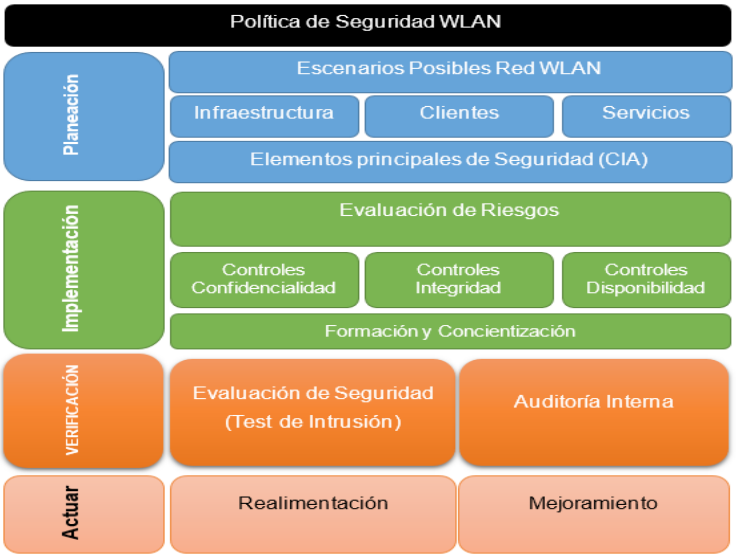


Figura 5 - Metodología de Securización WLAN (Sánchez E. Franklin, 2017)

Política de Seguridad WLAN

Antes de comenzar a diseñar la red o evaluar los mecanismos de autenticación, es indispensable crear una política corporativa sobre la implementación y el uso de la red inalámbrica. Se querrá afrontar muchos temas en la política, pero cantidad excesiva de normativas de seguridad puede resultar en reducir la utilidad y rapidez de la red, a continuación, se debe considerar los siguientes aspectos:

- Uso aceptable de la tecnología inalámbrica
- Instalaciones WLAN autorizadas
- Hardware permitido
- IDS inalámbrico
- BYOD (Bring Your Own Device)
- Administración del software de gestión de dispositivos
- Disponibilidad del Servicio
- Ingeniería social
- Uso de contraseñas adecuadas
- De monitoreo físico y lógico de la red
- Respecto a los protocolos de seguridad
- Respecto a los clientes

Planeación

Dentro de la organización es importante realizar una razonable gestión de los activos de la información (hardware, software, firmware, servicios, aplicaciones, comunicaciones, personal, etc.) que correspondan a la tecnología de redes WLAN, teniendo presente que un activo genera valor a la organización, es preciso que la misma tenga conocimiento de éstos activos que serán elementos principales para la administración de riesgos.

La organización deberá definir una metodología que permita la evaluación de los riesgos, para identificarlos, analizarlos y tratarlos; y dedicar esfuerzo aquellos que se consideren como críticos para la organización.

La institución debe realizar la identificación de las potenciales amenazas a los activos del inventario con respecto los elementos de seguridad: confidencialidad, integridad, disponibilidad y autenticidad que pueden ocasionar daños o pérdida en la información cuando se produzca su ocurrencia. A criterio de la NIST (Frankel, Eydt, Owens, & Scarfone, 2007) , señala que los tipos de fuentes de amenaza incluyen lo siguiente:

- Hostigamiento cibernético o ataques físicos.
- Errores humanos de omisión o comisión.
- Fallos estructurales de recursos controlados por la organización (por ejemplo, hardware, software y controles ambientales).
- Desastres naturales, causados por el hombre, accidentes y fracasos que escapan al control de la organización

Implementación - Evaluación

Para la implementación de seguridad en la WLAN se requiere una buena evaluación de riesgos a partir de la planeación con el propósito de determinar y tomar decisiones de prioridad para implementar su tratamiento, ver resumen en la Tabla 2.

Aspecto	Para qué	Cómo
Identificación	Determinar de manera minuciosa una lista de riesgos relacionados con la infraestructura WLAN de todos los posible sucesos que puedan causar el no alcance de los objetivos de la red, si en esta etapa no se identifican no será posible su análisis.	Con herramientas y técnicas para identificar el riesgo, con intervención de personas expertas o conocimientos apropiados.
Análisis	Evaluar la probabilidad de que ocurra un evento y definir la gravedad de las consecuencias del evento. También puede ser útil llevar a cabo una evaluación de la vulnerabilidad, que puede ayudar a identificar situaciones en las que la organización puede estar exponiéndose	Realice el análisis de esos riesgos, generalmente toman una de dos formas: cuantitativa, que busca identificar los riesgos y cuantificarlos basados en una escala numérica (p.e. de 1 a 10); y cualitativo, que se basa en obtener una impresión general sobre los riesgos para calificarlos. El proceso utiliza términos subjetivos como bajo a medio, alto a pobre, y bueno a excelente, en lugar de valores numéricos.
Evaluación	Tratar los riesgos por su magnitud, de acuerdo a su costo beneficio en la implementación de controles, considerando si son aceptables o tolerables al que la organización estaría dispuesta a asumir.	Mediante la priorización de los riesgos de acuerdo a las políticas organizacionales, su capacidad operativa y financiera

Tabla 2 – Resumen evaluación de Riesgos

Implementación – controles

En la Tabla 3 se enlista un resumen de controles para los posibles escenarios de red inalámbricos mencionados en el apartado de identificación de requisitos en conjugación con los elementos de seguridad de confidencialidad, integridad y disponibilidad.

Verificación

En esta etapa es importante considerar la contratación de personal profesional en seguridad (pentester) para realizar un test de intrusión contra la configuración de la infraestructura de red inalámbrica con el propósito de determinar y mitigar potenciales vulnerabilidades y el riesgo que contempla el no hacerlo. Esta prueba ayuda a la organización a disponer de documentación con información de seguridad debido a que el profesional actuará como un atacante con una mirada diferente a la del propio equipo de tecnología de información de la organización con el propósito de explotar las vulnerabilidades halladas e identificar qué información o acceso logró alcanzar.

Vulnerabilidad	Control	Elemento Seguridad
Existencia de dispositivos (clientes y AP Falsos) no autorizados	Es necesario establecer nombres de redes WIFI que no identifiquen a la organización. Establecimiento de políticas formales. Disponer de un inventario de todos los equipos de acceso inalámbrico. Implementar en la red un sistema de detector de intrusos.	Confidencialidad, Control de Acceso
Inseguridad por SSID Oculto	Al definir una red con SSID oculto, hacerlo con controles adicionales de seguridad como uso de protocolos de seguridad WPA-2 AES y filtrado por MAC.	Confidencialidad Autenticación
Enumeración de redes en el espectro	Inventario de todos los equipos de acceso inalámbrico. En el mejor de los casos ubicar en la red un sistema de detector de intrusos (WIDS/WIPS)	Confidencialidad Autenticación
Publicación de preferencias de red de clientes	Eliminar de la lista PNL (Prefered Network List) las redes públicas abiertas y las que no se volverán a usar. Deshabilitar la funcionalidad de conexión automática de las redes.	Confidencialidad Autenticación
Identificación activa de dispositivos	Deshabilitación de la redes, o en lo posible eliminar aquellas redes configuradas que se encuentran en la PNL y como buen práctica eliminar las redes de la organización.	Confidencialidad Autenticación
Adquisición de información del firmware, hardware y software	Mantener actualizado el firmware o el sistema operativo de todos los dispositivos inalámbricos	Disponibilidad, Confidencialidad, Integridad
Métodos de autenticación inseguros en 802.1x	Eliminación de los métodos de autenticación inseguros y deshabilitar aquellos que no se van a utilizar en un servidor RADIUS. Mantener actualizado el servicio RADIUS con los parches de seguridad respectivos.	Autenticación
Aislamiento de clientes	Habilitación de funcionalidad Client Isolation en los dispositivos AP o controladoras Wireless LAN (WLAN)	Confidencialidad, Control de acceso
Autenticación en redes Wi-Fi basado en MAC	Agregar controles de seguridad que garanticen un control de acceso a la red, no siendo suficiente el filtrado por MAC Address del dispositivo	Control de acceso
Acceso no autorizado a redes por WPS (Wifi Protected Setup)	Deshabilitar la característica WPS o establecer el número de intentos de conexión al PIN, para prevenir ataques de fuerza bruta	Control de acceso Confidencialidad
Debilidad en la creación de credenciales	Utilizar protocolo de autenticación WPA2-CMPP. No utilizar claves genéricas o de fácil predicción. Utilizar la renovación de claves	Control de acceso Confidencialidad
Deficiencia en servidores de credenciales de usuario	El almacenamiento de las credenciales de usuario debe ser cifrada, utilizando algoritmos fuertes como SHA-2. Mantener actualizado el sistema operativo y la base de datos con los parches de seguridad.	Confidencialidad Integridad
Denegación de servicio por solapamiento	Configuración de las redes WIFI en diferentes canales para evitar el solapamiento. Utilizar redes en la frecuencia 5MGHz.	Disponibilidad

Tabla 3 – Resumen controles de seguridad

Este test de intrusión se deberá ser aplicada con la técnica de prueba de caja gris, que permite al profesional en seguridad partir de información técnica de la infraestructura WLAN y simular un ataque real, siendo esta prueba considerada como la más efectiva a la hora de determinar una mayor cantidad de amenazas. Como práctica de seguimiento o evaluación es trascendental realizar una auditoría interna o externa de preferencia, a la arquitectura e infraestructura inalámbrica WLAN. Para ello es importante que se modele bajo el Manual de Metodologías de Prueba de Seguridad de Código Abierto OSSTMM 3 (Open Source Security Testing Methodology Manual) en su apartado "Prueba de seguridad inalámbrica" o la Metodología de evaluación abierta de seguridad inalámbrica OWISAM (Open Wireless Security Assessment Methodology)

Actuar

En esta etapa es donde se deben trabajar todos los hallazgos o no-conformidades reales y potenciales encontradas que pueden perjudicar su funcionamiento, tanto en la prueba de intrusión como en la auditoría o por reportes de incidencias por áreas de la organización, usuarios, colaboradores, etc., es primordial que se puede evidenciar el requisito (controles, procesos, clientes, legales, etc.) con la suficiente certeza de incumplimiento, la misma que deberá estar enunciada de forma explícita en cantidad, tiempo, relación de muestra y evidencia, eliminando toda ambigüedad.

5. Conclusiones

En la actualidad la redes WLAN enfrentan diferentes tipos de amenazas de gran nivel, que incluyen ataques de análisis de tráfico, enmascaramientos, hombre en el medio, degradación o denegación de servicio, escuchas, modificación de mensajes de datos, mayormente se presenta estas incidencias entre dos estaciones de trabajo (clientes) o entre una estación de trabajo y un punto de acceso. La implementación de esta metodología servirá como guía para el despliegue de una nueva WLAN o mejorar una existente, brindando elementos claves de seguridad y lograr mantener una seguridad razonable a la organización que le permita enfrentarse contra la mayoría de amenazas existentes.

Al momento de integrar las redes inalámbricas a las redes alámbricas se debe considerar seriamente la seguridad de la red interna debido a que podrían facilitan le evasión de cortafuegos perimetrales u otros niveles de seguridad, de ahí que las redes WLAN deben estar implementadas en zonas desmilitarizadas o en segmentos lógicos de red diferentes.

El usuario al ser considerado como el eslabón más débil de la cadena de seguridad, se debe implantar campañas de empoderamiento acerca de la seguridad de la información que permita al usuario comprender, desarrollar aptitudes, mantener valores y conductas para cumplimiento de los requisitos de seguridad implementados en la organización.

Como cultura de seguridad organizacional en forma periódica realizar la evaluación de riesgos para determinar nuevas vulnerabilidades y amenazas para crear o actualizar los controles de seguridad de la WLAN, debido al surgimiento de nuevas tecnologías, protocolos de seguridad, vulnerabilidades, herramientas de hacking, fallos en software, fallas en implementaciones de protocolos, etc.

Referencias bibliográficas.

Afshar, V. (2014). 50 Incredible WiFi Tech Statistics That Businesses Must Know [SLIDE DECK]. Recuperado el 24 de julio de 2017, a partir de http://www.huffingtonpost.com/vala-afshar/50-incredible-wifi-tech-s_b_4775837.html

C - IEEE Computer Society. (1999). ANSI/IEEE 802.11-1999.

CISCO CCNA. (2016). Escalamiento de redes. Recuperado el 30 de julio de 2017, a partir de https://static-course-assets.s3.amazonaws.com/ScaN503/es/index.html#4.1.3.2

Deming W. Edwards. (1986). *Out of the crisis*. Cambridge, Mass.: Massachusetts Institute of Technology, Center for Advanced Engineering Study, ©1986.

Frankel, S., Eydt, B., Owens, L., & Scarfone, K. (2007). Establishing wireless robust security networks: a guide to IEEE 802.11 i. *National Institute of Standards and Technology*.

ISO/IEC 27001:2013. (2013). ISO/IEC 27001:2013. Recuperado el 23 de julio de 2017, a partir de https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

Leston, O., & Begoña, M. (2012). Seguridad en comunicaciones sin hilos: Riesgos y amenazas Wi-Fi. Recuperado a partir de http://openaccess.uoc.edu/webapps/02/handle/10609/14995

OSSTMM. (2010). OSSTMM.3.pdf. Recuperado el 17 de marzo de 2017, a partir de http://www.isecom.org/mirror/OSSTMM.3.pdf

Pellejero, I., Andreu, F., & Lesta, A. (2006). *Fundamentos y aplicaciones de seguridad en redes WLAN: de la teoría a la práctica*. Marcombo.

Sánchez E. Franklin. (2017, septiembre 28). *Aplicación de una metodología de seguridad avanzada en redes inalámbricas*. UNIR, Ecuador.

Stallings, W., & Stallings, W. (2005). *Wireless communications and networks* (2nd ed). Upper Saddle River, NJ: Pearson Prentice Hall.

Tarlogic. (2013). OWISAM [WIKI]. Recuperado el 17 de agosto de 2017, a partir de https://www.owisam.org/es/P%C3%A1gina_principal

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 20/09/2017
Aceitação/Acceptance: 25/03/2018

Estratégias nacionais de segurança cibernética na América Latina: oportunidades para convergência de interesses e construção de consenso

Eduardo Izycki[1]

eduizycki@yahoo.com.br

[1] Presidência da República do Brasil, SPO – Área 5, Qd. 1, Bl. J, 70610-905, Brasília/DF, Brasil.

Pages: 39–52

Resumo: Um grupo de dez nações latino americanas publicou Estratégias Nacionais de Segurança Cibernética (ENSC). Este artigo analisa e compara as ENSC de Brasil, Chile, Colômbia, Costa Rica, Guatemala, Jamaica, México, Panamá, Paraguai, Trinidad e Tobago. As ENSC apresentam semelhanças em conceitos basais, na identificação de ameaças cibernéticas e na delimitação de objetivos estratégicos. A análise, a partir das abordagens comuns encontradas, propõe temas para a construção de consenso e de uma agenda positiva regional. A conclusão indica dois temas para cooperação regional: proteção de infraestruturas críticas e combate a criminalidade cibernética.

Palavras-chave: estratégia nacional segurança cibernética; segurança cibernética; infraestruturas críticas; criminalidade cibernética.

National Cyber Security Strategies in Latin America: opportunities for convergence of interests and consensus building

Abstract: A group of ten Latin American nations published national cybersecurity strategies (NCSS). This article analyzes and compares the NCSS of Brazil, Chile, Colombia, Costa Rica, Guatemala, Jamaica, Mexico, Panama, Paraguay, Trinidad and Tobago. NCSS present similarities in baseline concepts, the identification of cyber threats and strategic objectives. The analysis proposes themes for consensus building and a positive agenda for Latin America. The conclusion draws two subjects for regional cooperation: protection of critical infrastructures and fight against cyber crime.

Keywords*:* national cyber security strategy; cyber security; critical infrastructure; cybercrime.

1. Introdução

As estratégias nacionais são um plano de ação baseado em uma visão nacional para alcançar um conjunto de objetivos que contribuem para a segurança do ciberespaço (Luiijf, Besseling, & De Graaf, 2013).

Podem ser consideradas manifestações políticas do país subscritor na medida em que seu conteúdo tende a dividir responsabilidades entre as partes interessadas nacionais, estipular os objetivos estratégicos perseguidos, definir as metas concretas a serem atingidas em prazos definidos, e identificar as potenciais ameaças percebidas pelo país (Luiijf, Besseling, & De Graaf, 2013). Esse conteúdo permite apreender alguns dos reais interesses do país subscritor sobre a dimensão cibernética.

O presente artigo é o primeiro resultado de uma pesquisa abrangente sobre estratégias nacionais de segurança cibernética (ENSC). Nele se pretende identificar pontos de convergência entre dez países latino-americanos (Brasil (Brasil, 2015), Chile (Chile, 2017), Colômbia (Colômbia, 2016), Costa Rica (Costa Rica, 2016), Guatemala (Guatemala, 2017), Jamaica (Jamaica, 2015), México (México, 2017), Panamá (Panamá, 2013), Paraguai (Paraguai, 2017), Trinidad e Tobago (Trinidad e Tobago, 2012) e identificar oportunidades para construção de consenso em nível regional.

2. Formato de Página

Para realizar uma análise entre as ENSC são necessários parâmetros objetivos de comparação. Não há um consenso internacional sobre o conteúdo mínimo que ENSC devam possuir.

A seleção de uma das estratégias nacionais como paradigma de comparação frente às demais seria uma solução insatisfatória e arbitrária, pois imporia aos países características peculiares do país-autor do documento utilizado como paradigma.

A solução alternativa foi elaborar parâmetros de comparação a partir de cinco documentos produzidos por organizações internacionais independentes. São eles:

- *National Cybersecurity Strategy Guide*, da International Telecommunications Union (ITU)
- *Analyzing a new generation of national cybersecurity strategies for the Internet Economy*, da Organização para a Cooperação e Desenvolvimento Econômico (OCDE)
- *Guidebook on National Cyber Security Strategies*, da European Network and Information Security Agency (ENISA)
- *National Cyber Security Framework Manual*, Cooperative Cyber Defence Centre of Excellence (CCDCOE)
- *Commonwealth Approach for National Cybersecurity Strategies*, da Commonwealth Telecommunications Organization (CTO).

Os documentos da ITU (Wamala, 2011), da ENISA (ENISA, 2012) e da Commonwealth Telecommunications Organization (CTO, 2015) possuem características programáticas, pois seu objetivo é auxiliar a elaboração ou atualização de estratégias nacionais de segurança cibernética. As três instituições possuem programas de consultoria dedicados aos países membros nesse sentido.

O documento CCDCOE (Klimburg, 2012) problematiza a elaboração de uma ENSC, apresentando ferramentas e recomendações sobre o processo de confecção ou atualização de documentos nacionais na área cibernética.

O relatório da OCDE (OCDE, 2012) compara estratégias nacionais cibernéticas – dez países diferentes –, em uma proposta similar ao presente artigo, com destaque para semelhanças, diferenças e tendências identificadas a partir dos documentos apreciados.

Ao abordarem elementos constitutivos das estratégias nacionais os documentos variam quanto ao vocabulário empregado. A CTO (CTO, 2015) menciona "elementos chave", a ENISA (ENISA, 2012) denomina "objetivos específicos", a ITU (Wamala, 2011) chama de "elementos de um programa nacional de cibersegurança", a OCDE (OCDE, 2012) aponta para "conceitos compartilhados" e a CCDCOE (Klimburg, 2012) apresenta capítulos de "objetivos estratégicos" e "estruturas organizacionais".

A primeira etapa da análise comparativa foi avaliar o conteúdo dos elementos constitutivos apresentados pelos documentos de referência para identificar a existência de padrões entre eles. Os pontos de convergência identificados foram adotados como parâmetros de comparação entre as estratégias nacionais no escopo deste artigo.

Foram delimitados os seguintes parâmetros de comparação entre as ENSC: Proteção de infraestruturas críticas, Certificações e Padrões, Conscientização e treinamento, Privacidade, Legislação e Marcos Regulatórios, Coordenação e Protocolos, Combate ao Crime Cibernético, Cooperação Internacional, Combate a Ameaças Cibernéticas, Pesquisa e Desenvolvimento, Economia Digital e Parceria Público-Privada.

A segunda etapa da análise comparativa consistiu na busca desses conceitos apresentados nas estratégias nacionais como um dos seus objetivos estratégicos.

Durante essa etapa foram identificados outros conceitos comuns, quais sejam: espaço cibernético, defesa cibernética, guerra cibernética, segurança cibernética e ameaças cibernéticas.

3. Análise temporal

A análise temporal baseada no ano de publicação das ENSC revela a escalada da segurança cibernética como um dos temas de interesse para a defesa.

Entre os anos de 2003 e 2017, foram publicadas 112 estratégias por 86 países diferentes, conforme se observa na Figura 1. A partir de 2008 ocorre de forma ininterrupta a publicação anual de novos documentos.

Os países latino-americanos elaboraram tardiamente as suas ENSC quando comparados com o restante do mundo: Colômbia (2011), Trinidad e Tobago (2012), Panamá (2013), Brasil e Jamaica (2015), Costa Rica e Colômbia (segunda edição) (2016), Chile, Guatemala, México e Paraguai (2017).

O ano de 2008 parece ser o marco inicial da publicação anual de novas ENSC porque em abril de 2007 ocorreram os notórios ataques cibernéticos contra a Estônia – os quais se atribuem frequentemente à Rússia, ainda que careçam de evidências categóricas – e em 2008 ataques cibernéticos contra a Geórgia acompanharam a campanha militar convencional realizada pela Rússia na Ossétia do Sul.



Figura 1 – Total de ENSC publicadas anualmente

Em dez das oitenta e seis estratégias já publicadas foram observadas menções explícitas aos referidos casos. Apenas na estratégia nacional do Chile há referência explícita aos ataques ocorridos contra a Estônia (2007).

A quantidade de documentos publicados se ampliou significativamente entre 2010 e 2011, de cinco para onze estratégias.

Esse incremento nas publicações de novas estratégias pode ser atribuído ao caso Stuxnet, que ganhou notoriedade naquele ano, como exemplo icônico de ataque cibernético que produziu efeitos cinéticos no programa nuclear iraniano, o qual seria atribuído a ação conjunta entre Estados Unidos e Israel.

Em seis das oitenta seis estratégias já publicadas foram observadas menções explícitas ao referido caso. Nos países latino-americanos as estratégias nacionais de Trinidad e Tobago e do Chile fazem referência ao uso do Stuxnet como arma de ataque a sistemas de controle e automação (SCADA).

4. Estágio de maturidade

Para comparação entre os países latino-americanos foram buscadas as avaliações sobre a dimensão cibernética realizadas pela Organização das Nações Unidas (ONU) (ONU, 2016) e pela International Telecommunication Union (ITU) (ITU, 2017).

A classificação realizada pela ONU, o E–Government Development Index (EGDI) de 2016, indicou que os países latino-americanos estão classificados como alto e médio (Tabela 1). O índice é dividido em quatro níveis – Muito Alto, Alto, Médio e Baixo – e avalia a maturidade dos países em relação a sua presença e atuação na dimensão cibernética.

O Global Cybersecurity Index (GCI) 2017, da ITU, é um índice composto dedicado a avaliar o comprometimento dos países com a segurança cibernética, nele os países latino-americanos foram classificados como maturing state e initiating stage (Tabela 1). O índice é dividido em três níveis – *Leading Stage* (pontuação no percentil 90), *Maturing State* (entre o percentil 50 e 89) e *Initiating Stage* (abaixo de 50) – e seu objetivo é avaliar o comprometimento dos países com a segurança cibernética.

País	**EGDI**	**CGI**
Brasil	Alto	*Maturing State*
Chile	Alto	*Maturing State*
Colômbia	Alto	*Maturing State*
Costa Rica	Alto	*Maturing State*
Guatemala	Médio	*Initiating State*
Jamaica	Médio	*Maturing State*
México	Alto	*Maturing State*
Panamá	Médio	*Maturing State*
Paraguai	Médio	*Maturing State*
Trinidad e Tobago	Alto	*Maturing State*

Tabela 1 – Classificação dos países

Os países latino-americanos foram avaliados em ambos os índices em níveis similares e intermediários: alto/médio (EGDI) e *maturing state/initiating stage* (GCI).

As classificações pelos índices sugerem que os países latino-americanos estão em estágio similar de maturidade cibernética, o que facilita sua interação e a formação de consenso entre eles.

5. Conceitos basais

Uma ENSC deveria estabelecer conceitos basais a partir dos quais serão estipulados objetivos estratégicos e metas a serem perseguidas (Luiijf, Besseling, & De Graaf, 2013). Dois conceitos basais foram observados na maioria dos documentos latino americanos (Tabela 2): espaço cibernético e segurança cibernética.

Conceito	**Países**
Espaço cibernético	Chile, Colômbia Costa Rica, México, Panamá e Trinidad e Tobago
Segurança cibernética	Brasil, Chile, Colômbia, Costa Rica, Jamaica, México, Paraguai e Trinidad e Tobago

Tabela 2 – Conceitos basais comuns

Os conceitos "defesa cibernética" e "guerra cibernética" não foram identificados na maioria das ENSC. O primeiro constou apenas na ENSC de Chile e México e o segundo no documento brasileiro.

A harmonia entre os conceitos de espaço cibernético e segurança cibernética é um facilitador para convergência de interesses regionais.

5.1. Espaço Cibernético

Espaço cibernético foi definido explicitamente por seis países: Chile, Colômbia Costa Rica, México, Panamá e Trinidad e Tobago. Nos demais há referências ao espaço cibernético na delimitação do escopo da ENSC, sem que uma definição explícita seja apresentada.

Nas cinco definições apresentadas foram identificados referências a seres humanos, elementos físicos e lógicos como parte do conceito. O México e a Colômbia incluem na definição as redes de telecomunicação em seu conceito, sendo que a definição colombiana é orientada economicamente. A Costa Rica e o Panamá indicam apenas os sistemas de informação como parte do espaço cibernético. O Chile indica elementos físicos e lógicos, sem menção ao tipo de sistema. A definição de Trinidad e Tobago é a mais extensa e inclui até mesmo exemplos dos equipamentos que são considerados parte do espaço cibernético.

Os países apresentam alguma variação de conteúdo, mas possuem uma perspectiva holística para o espaço cibernético.

5.2. Segurança cibernética

O conceito de segurança cibernética foi observado em documentos de oito países: Brasil, Chile, Colômbia, Costa Rica, Jamaica, México, Paraguai e Trinidad e Tobago.

Seis países (Colômbia, Costa Rica, Jamaica, México, Paraguai e Trinidad e Tobago) indicam um conceito instrumental, no qual a segurança cibernética seria um conjunto de ferramentas a serem aplicadas por diferentes partes interessadas. Nos demais, os conceitos indicam a segurança como uma condição do espaço cibernético, no Chile a condição de menor risco para o espaço cibernético e no Brasil a existência e a continuidade da sociedade da informação.

Há relativo consenso sobre a definição de segurança cibernética entre os países latino-americanos.

6. Objetivos estratégicos

Os objetivos estratégicos são considerados um elemento recomendado para o conteúdo de uma ENSC (Luiijf, Besseling, & De Graaf, 2013) (Wamala, 2012) (ENISA, 2012) (CTO, 2015).

Por se tratarem de grandes metas perseguidas pelos países, a assinalação dos objetivos estratégicos é uma referência qualificada na comparação das ENSC, pois sugere genuíno compromisso da nação autora do documento. Presume-se que isso induza empenho de recursos humanos e materiais na consecução desse objetivo declarado, logo, essa seria uma genuína manifestação de vontade política nacional.

Assim, a análise dos objetivos estratégicos ao indicar pontos de convergência de interesses entre os países latino-americanos, reflete em um indicador para uma agenda positiva regional sobre a temática cibernética.

Todas as ENSC apresentaram objetivos estratégicos explicitamente definidos (Figura 2).

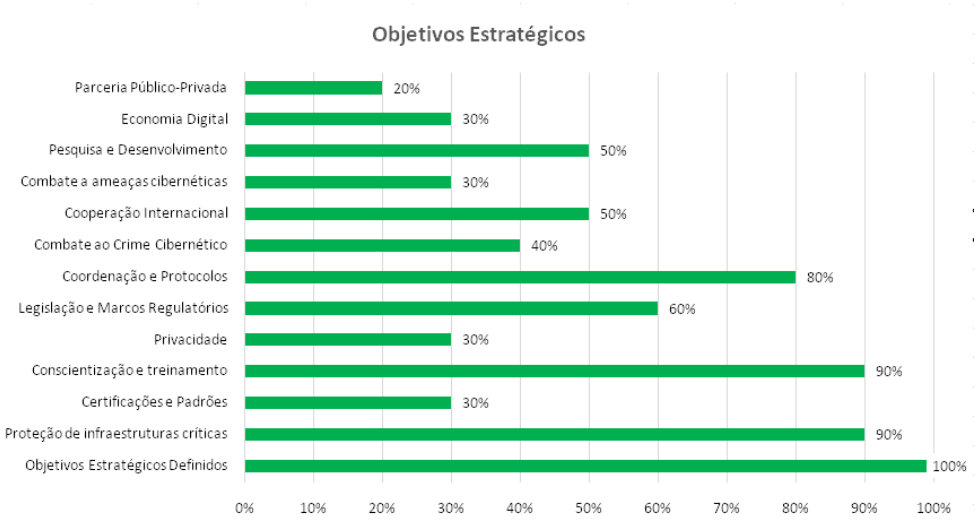


Figura 2 – Objetivos estratégicos observados nas ENSC

Dentre os doze critérios objetivos de comparação foram identificados seis deles com maior frequência (Tabela 3): conscientização e treinamento (9), proteção de infraestruturas críticas (9), coordenação e procedimentos (8), legislação cibernética (6), cooperação internacional (5) e pesquisa e desenvolvimento (5).

Conceito	**Países**
Conscientização e Treinamento	Brasil, Chile, Costa Rica, Guatemala, Jamaica, México, Panamá, Paraguai e Trinidad e Tobago
Proteção de Infraestruturas Críticas	Brasil, Chile, Colômbia, Costa Rica, Jamaica, México, Panamá, Paraguai e Trinidad e Tobago
Coordenação e Procedimentos	Brasil, Chile, Colômbia, Costa Rica, Guatemala, Panamá, Paraguai e Trinidad e Tobago
Legislação e marcos regulatórios	Colômbia, Costa Rica, Guatemala, Jamaica, México e Trinidad e Tobago
Pesquisa e Desenvolvimento	Brasil, Chile, México, Panamá e Paraguai
Cooperação Internacional	Brasil, Chile, Colômbia, Costa Rica, Jamaica e Paraguai

Tabela 3 – Objetivos estratégicos mais frequentes

6.1. Conscientização e treinamento

O objetivo "conscientização e treinamento" foi o mais frequente, indicado por nove países (Brasil, Chile, Costa Rica, Guatemala, Jamaica, México, Panamá, Paraguai e Trinidad e Tobago), decorrente da percepção que a maioria dos incidentes de segurança conta com a participação dos usuários – marcada pela expressão "o elo mais fraco" – seja pela imperícia ou a indução ao erro pelo atacante (p.ex. engenharia social).

Todos os nove países mencionaram a necessidade da criação de uma cultura de segurança que deveria ser incorporada pelos usuários de tecnologia em toda a sociedade. No Brasil há indicação de que servidores públicos deveriam ser estimulados a buscar treinamentos especializados, reflexo da ENSC brasileira que tem enfoque no setor público. No caso de Chile, Costa Rica e Guatemala há previsão de estímulo para educação formal – especialização – em áreas de segurança, presumidamente numa aproximação com o setor acadêmico daqueles países.

6.2. Proteção de Infraestruturas Críticas

O objetivo "proteção de infraestruturas críticas" também foi indicado por nove países (Brasil, Chile, Colômbia, Costa Rica, Jamaica, México, Panamá, Paraguai e Trinidad e Tobago). Uma das razões indicadas nas ENSC foi o potencial impacto de um ataque desferido contra as infraestruturas críticas (IC), que seria maximizado pela relação de interdependência que as IC possuem entre si (p.ex. ataque contra fornecimento de energia elétrica quase certamente interromperia telecomunicações).

Aspecto comum a todos os países latino-americanos foi o reconhecimento da necessidade de cooperação entre entidades públicas e privadas. Isso se deve ao fato de que os operadores das IC são, em sua ampla maioria, entidades privadas reguladas por normas exaradas pelo poder público. No caso de Chile e Colômbia a regulação será orientada por processos de gestão de riscos das IC, conduzidos por entidades públicas com estreita participação dos operadores privados.

Outro ponto de consenso – sinalizado por Chile, Jamaica, México, Paraguai e Panamá – se refere à necessidade de resiliência e da continuidade de operação das IC. Trata-se de corolário da definição de IC que considera como críticas aquelas infraestruturas que produzem impacto sistêmico se afetadas por um incidente.

6.3. Coordenação e Procedimentos

O objetivo "coordenação e procedimentos" foi o segundo mais frequente, observado em oito países (Brasil, Chile, Colômbia, Costa Rica, Guatemala, Panamá, Paraguai e Trinidad e Tobago). Seria decorrência natural de uma estratégia nacional ao distribuir atribuições e competências entre diferentes partes interessadas (públicas e privadas), delimitar de protocolos de ação e procedimentos, entre outras previsões de organização interna do país.

No caso de Chile, Costa Rica, México, Panamá e Paraguai esse objetivo estratégico foi associado a protocolos de detecção e resposta a incidentes cibernéticos, ainda que os cinco países já possuam centros de tratamento de incidentes nacionais. O que denota iniciativa desses países no sentido de aprimorar processos de compartilhamento de informações nacionais.

A ENSC da Colômbia apresenta a necessidade de construção de confiança entre as partes interessadas nacionais – públicas e privadas – por meio da atuação do *Ministerio de Tecnologías de la Información y Comunicaciones*. Por se tratar do país na segunda edição da ENSC, a Colômbia indica a necessidade de mecanismos concretos que viabilizem efetivamente a cooperação e a coordenação em nível nacional.

6.4. Legislação e marcos regulatórios

Na mesma linha de um item natural em uma estratégia nacional, o objetivo "legislação e marcos regulatórios", foi observado em seis países (Colômbia, Costa Rica, Guatemala, Jamaica, México e Trinidad e Tobago), pugnou pela identificação e atualização do arcabouço normativo que verse sobre a dimensão cibernética.

Todas as ENSC mencionaram a necessidade de revisão do arcabouço normativo, seguido pela edição de novas normas para a dimensão cibernética.

No caso de Costa Rica, Jamaica e Trinidad e Tobago há explícita menção a normas substantivas e processuais penais, numa sinalização de que o combate a criminalidade cibernética eficiente requererá esforço legislativo. Para Colômbia e México há enfoque orientado para o aproveitamento econômico da dimensão cibernética, ressaltada a necessidade de manutenção da segurança jurídica das partes interessadas.

6.5. Pesquisa e Desenvolvimento

O objetivo "pesquisa e desenvolvimento", identificado em cinco países (Brasil, Chile, México, Panamá e Paraguai), revela a autopercepção latino-americana sobre a necessidade de acompanhar o rápido desenvolvimento de soluções de tecnologia da informação (voltadas ou não para segurança), seja por instituições de ensino ou pelo fomento a empresas para que invistam em pesquisa e desenvolvimento.

Há consenso entre os países sobre a oportunidade que a segurança cibernética apresenta em termos de novo segmento de prestação de serviços, o esforço seria dirigido a fomentar um ecossistema empresarial no segmento.

6.6. Cooperação Internacional

Por fim, o objetivo "cooperação internacional", também observado em cinco países (Brasil, Chile, Colômbia, Costa Rica, Jamaica e Paraguai), constitui indicador de que os países latino-americanos estão dispostos a buscar soluções para dimensão cibernética no âmbito das relações internacionais. As formas pelas quais a cooperação ocorrerá – intermediada por organização multilateral, tratados internacionais ou cooperação técnica bilateral – permanecem em aberto.

O Brasil, Chile e a Colômbia indicam a disposição em engajar em cooperação internacional de caráter multilateral. Ao passo que a Jamaica e a Colômbia indicam a intenção de pactuar cooperação de forma bilateral.

Destaque para Colômbia, Guatemala e Paraguai pela intenção manifestada de adesão à Convenção do Conselho Europeu sobre Crimes Cibernéticos (Convenção de Budapeste), principal instrumento multilateral em vigor, dedicado ao combate dos crimes cibernéticos transnacionais.

7. Temáticas similares

Além da semelhança entre os objetivos estratégicos, quatro temáticas (Tabela 4) foram observadas de forma reiterada nas ENSC latino-americanas: combate a criminalidade cibernética, a preservação da privacidade e intimidade na internet, a necessidade de resiliência e a análise de risco cibernético.

Conceito	Países
Criminalidade cibernética	Chile, Colômbia, Costa Rica, Jamaica, México, Panamá e Trinidad e Tobago
Privacidade e Intimidade	Chile, Colômbia, Costa Rica, Guatemala, Jamaica, México, Paraguai e Trinidad e Tobago
Resiliência	Brasil, Chile, Costa Rica, Guatemala, Jamaica, México, Paraguai e Trinidad e Tobago
Análise de risco cibernético	Chile, Colômbia, Jamaica, México e Trinidad e Tobago

Tabela 4 – Temáticas similares em ENSC

7.1. Ameaças cibernéticas: criminalidade cibernética

A existência, periculosidade e a multiplicidade de ameaças cibernéticas foram indicadas como uma das grandes desafios da segurança cibernética por sete das dez ENSC. Para Guatemala, Jamaica e Trinidad e Tobago o "combate as ameaças cibernéticas" e para Chile, Colômbia, Panamá e Paraguai "combate ao crime cibernético" foram assinalados como objetivos estratégicos.

A expressão "ameaça cibernética" é ampla, por isso para considerar uma referência a ela na ENSC buscou-se por um dos seguintes itens: uma lista de categorias/tipos de ameaça ou definições/conceitos de ameaças cibernéticas. Seguindo esse padrão de busca, foram observadas menções a ameaças cibernéticas em sete documentos.

A partir da maior frequência e unidade conceitual das ameaças foi formulada a seguinte taxonomia:

- Divisão entre Atores Estatais e não-Estatais (Chile e Panamá),
- Hacktivismo ou Ativismo Cibernético (Costa Rica e Panamá),
- Crime Cibernético ou Deliquência Cibernética (Chile, Colômbia, Costa Rica, Jamaica, México, Panamá e Trinidad e Tobago),
- Terrorismo Cibernético (Colômbia, Panamá e Trinidad e Tobago),
- Espionagem/Sabotagem (Brasil, Chile e Panamá).

Conforme se observa da lista acima, o Crime Cibernético (7) é a categoria de ameaça cibernética mais comumente referenciada.

Essa ponderação quantitativa não indica que ele seja considerado a ameaça mais capaz tecnicamente ou a que produza maior impacto, porém indica que o seu combate é um ponto de convergência de interesses entre os países latino-americanos.

7.2. Privacidade e Intimidade

A segunda temática comum aos países latino-americanos se refere à preservação da privacidade e intimidade na internet. Ela foi assinalada como medida indispensável por oito países: Chile, Colômbia, Costa Rica, Guatemala, Jamaica, México, Paraguai e Trinidad e Tobago.

As ENSC consideram a privacidade e intimidade como direito fundamental e/ou parte de um plexo de direitos humanos a ser preservado, mesmo que tais garantias limitem o poder estatal ou tornem mais trabalhosa as ações cibernéticas (por exemplo, interceptação de comunicações).

Essa temática tem especial relevância para Costa Rica, Jamaica e Trinidad e Tobago que indicaram como objetivo estratégico inovação legislativa com menção a normas substantivas e processuais penais.

A ampliação de poderes para persecução criminal e a manutenção da privacidade dos usuários podem ser valores de difícil equilíbrio para os países latino-americanos. Esse debate parece inevitável, dada a disposição dos países em combater a criminalidade cibernética e proteger a privacidade e intimidade dos usuários.

7.3. Resiliência

Outra temática comum foi a necessidade de resiliência associada à dimensão cibernética. Assinalada como característica necessária por oito países: Brasil, Chile, Costa Rica, Guatemala, Jamaica, México, Paraguai e Trinidad e Tobago.

Não houve, contudo, clareza quanto a que aspecto da dimensão cibernética requer resiliência ou qual seria exatamente seu conceito. As ENSC convergem para um conceito de resiliência que contemple a "capacidade de operar e/ou recuperar-se após um ataque".

Há divergência sobre o que deve ser resiliente: para o Brasil, Jamaica e Paraguai (as IC), México (resiliência aos riscos cibernéticos), Chile (todo o espaço cibernético), Guatemala (redes públicas e privadas) e Costa Rica (suportar ou recuperar-se de ataques – sem indicar o objeto).

7.4. Análise de risco cibernético

Por fim, a análise de riscos cibernéticos é indicada por cinco países – Chile, Colômbia, Jamaica, México e Trinidad e Tobago – como uma ferramenta de trabalho para segurança cibernética.

Não foi possível observar, contudo, detalhes sobre como se daria o processo de avaliação de risco (metodologia) ou as formas pelas quais os riscos cibernéticos detectados serão mitigados.

8. Conclusão

A elaboração de ENSC é uma tendência global consolidada ao longo dos últimos quinze anos. Os países latino-americanos produziram suas estratégias nacionais tardiamente quando comparados ao restante do mundo.

Os países latino-americanos possuem avaliação similar nos índices GCI 2017 e EGDI 2016, o que sugere um nível equivalente de maturidade cibernética.

A semelhança entre as definições de espaço cibernético e segurança cibernética indicam que há uma base conceitual comum entre eles, o que facilita a formação de consenso.

A análise também revelou que existem objetivos estratégicos comuns aos países: conscientização e treinamento (9), proteção de infraestruturas críticas (9), coordenação e procedimentos (8), legislação cibernética (6), cooperação internacional (5) e pesquisa e desenvolvimento (5).

Outros pontos de convergência identificados entre as ENSC foram o combate a criminalidade cibernética (7), a preservação da privacidade e intimidade na internet (8), a necessidade de resiliência (8) e a análise de risco cibernético (5).

O histórico da América Latina revela baixa propensão a confrontos e a presença de elementos comuns extraídos na análise comparativa das ENSC permitem alinhavar dois grandes temas para convergência: a proteção de IC e o combate a criminalidade cibernética.

Um ponto inicial para a construção de uma agenda positiva regional parece ser a cooperação técnica na proteção de IC, objetivo estratégico em nove ENSC. A cooperação internacional nesse tema pode contemplar compartilhamento de planos para a resiliência das IC ou o compartilhamento dos resultados das análises de risco cibernético das IC.

Uma vertente adicional dessa cooperação poderia incluir o compartilhamento de experiências e realização de treinamentos conjuntos para a defesa das IC, numa combinação de dois objetivos estratégicos observados com frequência nas ENSC. Convém ponderar que, ainda que situadas em países diferentes, as IC podem estar sujeitas às mesmas ameaças.

O segundo ponto propenso a desencadear um processo de cooperação regional é o combate a criminalidade cibernética. Considerado objetivo estratégico por quatro países – Chile, Colômbia, Panamá e Paraguai –, a criminalidade cibernética foi a ameaça mais prevalente entre as ENSC, indicada por sete países (Chile, Colômbia, Costa Rica, Jamaica, México, Panamá e Trinidad e Tobago).

Uma forma de cooperação poderia ocorrer por meio de intercâmbio de informações entre entidades técnicas (centros de tratamento de incidentes nacionais) e/ou autoridades de aplicação da lei dos diferentes países.

Além disso, novas adesões à Convenção de Budapeste – Chile, Costa Rica e Panamá já acederam ao tratado e por parte de Colômbia, Guatemala e Paraguai houve explícita manifestação de vontade nesse sentido –, parecem uma forma de ampliar a cooperação internacional. Não se descarta a possibilidade de uma cooperação multilateral de caráter regional, haja vista o relativo consenso no combate ao crime cibernético e na disposição em preservar a privacidade de usuários.

Os países da América Latina que já publicaram ENSC possuem maturidade similar, apresentaram conceitos, objetivos estratégicos e temas em comum em suas estratégias

nacionais. A presença desses elementos facilitadores indica convergência de interesses e o alicerce para a construção de consenso por meio de uma agenda positiva regional.

Referências

Alexander Klimburg (Ed.) (2012), *National Cyber Security Framework Manual*, NATO CCD COE Publication, Tallinn 2012. Retrieved from https://www.oecd.org/sti/ieconomy/cybersecurity policy making.pdf.

Brasil (2015). *Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal*. Retrieved from http://dsic.planalto.gov.br/legislacao/4_Estrategia_de_SIC.pdf/view.

Chile (2017). *National Cybersecurity Policy*. Retrieved from https://ccdcoe.org/sites/default/files/documents/NCSP (ENG).pdf.

Colômbia (2016). *CONPES 3854 - Política Nacional de Seguridad Digital*. Retrieved from https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf.

Commonwealth Telecommunications Organization (2015), *Commonwealth Approach for developing National Cybersecurity Strategies*. Retrieved from http://www.cto.int/media/fo-th/cyb-sec/Commonwealth Approach for National Cybersecurity Strategies.

Costa Rica (2011). *Estrategia Nacional de Ciberseguridad de Costa Rica*. Retrieved from https://micit.go.cr/images/imagenes_noticias/10-11-2017__Ciberseguridad/Estrategia-Nacional-de-Ciberseguridad-de-Costa-Rica-11-10-17.pdf

European Network and Information Security Agency (2015), *National Cyber Security Strategies - Practical Guide on Development and Execution*, European Network and Information Security Agency (ENISA). Retrieved from http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide/at_download/fullReport.

Guatemala (2017). *Estrategia Nacional de Seguridad Cibernética*. Retrieved from http://seguridadcibernetica.mingob.gob.gt/wp-content/uploads/2016/09/ENSC2017.pdf.

International Telecommunications Union (ITU) (2017). *Global Cybersecurity Index 2017*. Genebra: ITU. Retrieved from http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspx

Jamaica (2015). *Jamaican National Cyber Security Strategy*. Retrieved from http://mstem.gov.jm/sites/default/files/Jamaica National%20Cyber%20Security%20Strategy.pdf.

Luiijf, E., Besseling, K. e De Graaf, P. (2013) *Nineteen national cyber security strategies*, Int. J. Critical Infrastructures, Vol. 9, Nos. 1/2, pp.3–31.

México (2017). *Estrategia Nacional de Ciberseguridad*. Retrieved from https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf.

Organisation for Economic Co-Operation and Development (2012). *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*, OECD Digital Economy Papers, No. 211, OECD Publishing, 2012. Retrieved from http://www.oecd.org/sti/ieconomy/cybersecurity policy making.pdf.

Panamá (2013). *Estrategia Nacional de Seguridad Cibernética y Proteción de Infraestruturas Críticas*. Retrieved from https://www.gacetaoficial.gob.pa/pdfTemp/27289_A/GacetaNo_27289a_20130517.pdf.

Paraguai (2017). *Plan Nacional de Ciberseguridad*. Retrieved from http://gestordocumental.senatics.gov.py/share/s/zkKW1CkKScSvapqlB7UhNg.

Trinidad e Tobago (2012). *Estrategia Nacional de Seguridad Cibernética*. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/TrinidadTobago_2012_National_Cyber_Security Strategy_Final.pdf.

United Nations (2016). *UN e-Government Survey 2016. E-Government in Support of Sustainable Development*. New York: UNPAN. Retrieved from https://publicadministration.un.org/egovkb/en-us/reports/un-e-government-survey-2016

Wamala, Frederick (2011). *The ITU National Cybersecurity Strategy Guide*, International Telecommunications Union (ITU), 2011. Disponível em: <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 17/09/2017
Aceitação/Acceptance: 06/03/2018

Firmwares: Vulnerabilidades e Ameaças aos Serviços de Inteligência de Estado e de Inteligência de Segurança Pública

Regilberto Girão[1]

rgirao@mpf.mp.br, rgirao@gmail.com

[1] Ministério Público Federal, Avenida Brasil, 1877, 30140-007, Belo Horizonte, Minas Gerais, Brasil.

Pages: 53–65

Resumo: Considerando as vulnerabilidades ocasionadas por sistemas operacionais embarcados em dispositivos digitais – *firmwares*, o quão ameaçados estão os serviços de Inteligência de Estado e Inteligência de Segurança Pública e o quanto podem ser reduzidas as probabilidades de exposição de seus sistemas, informações e/ou dados? A omissão do mercado, do meio acadêmico e dos profissionais de Tecnologia da Informação e Comunicações (TIC), além da falta de interação entre estes atores, nos proporciona trazer à baila um singular elemento que necessita da mesma – senão especial – atenção: os *Firmwares*. Negligenciados pela indústria de computadores e de outros ativos de rede e por Governos, despercebidos por boa parte dos profissionais de TIC, desprezados pela indústria de *softwares* de proteção contra códigos maliciosos, ignorados por usuários leigos e cobiçados pelos Serviços de Inteligência mundiais, podem ser vistos como a gênese das caixas-pretas digitais e como promotores da reatividade, ação histórica e recorrente que relega a premissa básica da Segurança das Informações e Comunicações – SIC à condição de gestão às cegas.

Palavras-clave: ameaça; firmware; inteligencia; segurança de estado; obsolescência; vazamento de dados; vulnerabilidade.

Firmwares: Vulnerability and Threats to State Intelligence and Public Security Intelligence S

Abstract: Considering the vulnerabilities caused by operating systems embedded in digital devices - firmwares, what are the possible threats and how threatened are the State Intelligence and Public Safety Intelligence services and how can be reduced the probability of exposure of their systems, information, and / or data? The omission of the market, universities and Information and Communications Technology (ICT) professionals, as well lack of interaction among these actors, brings us a basic element that needs the same attention: Firmwares. They are underrated by the computer industry and other network assets and governments, unnoticed by most ICT professionals, despised by the protection software industry against malicious code, ignored by lay users and coveted by world's Intelligence Services, and can be seen such as the genesis of digital black boxes and as promoters

of reactivity, a historical and recurring action that relegates the basic premise of Information and Communication Security (SIC) to the condition of blind management.

***Keywords**:* data leaking; firmware; intelligence; obsolescence; state security; threat; vulnerability.

1. Relevância

Este artigo advém de estudo realizado durante os anos de 2015 e 2016 que teve como finalidade o cumprimento de pré-requisito à obtenção de título acadêmico de especialista em Inteligência de Estado e Inteligência de Segurança Pública. Defendido em 2016, carrega o que foi apurado naquilo que de mais atual havia à época. Teve como foco eventos contemporâneos e de relevância e nos resultados que poderiam ser percebidos ao longo do tempo, quando da consciência coletiva de que ciências trabalham com ciências nos sentidos plural e multidisciplinar.

É uma obra multifacetada e de utilidade pública, pois abarca e transversaliza, implícita e explicitamente, inteligência e contrainteligência, tecnologias da informação e comunicações, seguranças física e lógica de infraestruturas, direito e justiça e educação e cidadania.

Poderá estimular o desenvolvimento seguro de dispositivos e aplicações com novos e elevados padrões de exigência e que destoem dos atuais modelos, bem como motivar investimentos em Ciência e Tecnologia (C&T) e em Pesquisa e Desenvolvimento (P&D), não raramente, destinados a países que utilizam mão de obra barata, que detêm domínio da engenharia das tecnologias e com capacidade de produção em larga escala.

Por se tratar de material que não tem fim em si e que se ressente das limitações e dificuldades de diálogo e de melhor interação entre governos, academia, indústria, investidores, empreendedores e usuários, deve ser melhor explorado e ampliado, com vistas a forjar a primazia e excelência, no que se refere ao desenvolvimento e integração de *hardwares* e *softwares*.

Inteligência e tecnologias agregadas em um só documento tem certa conotação de novo, visto que nos é desconhecido se há o que se assemelha. Há literaturas e referências ímpares em publicações, quando se considera estas Ciências isoladamente. No entanto, não houve oportunidade de encontrar algo diferente daquilo especificamente produzido pelas – e para – as áreas de Inteligência/Segurança de Estado e Tecnologias da Informação.

2. Objeto e Objetivo

2.1. Peopleware

Pessoas abastecem e retroalimentam o meio digital com massa imensurável de dados. Não ocorre diferentemente com a Inteligência e a Contrainteligência, pois manobram contextos sensíveis em ambientes digitais.

Sendo ponto pacífico que o ser humano não tem capacidade de assimilar tamanha evolução, fica prejudicada a necessária consciência das vulnerabilidades e ameaças embarcadas nos ambientes reais e virtuais, provocando com que cada indivíduo determine, subjetivamente, o quão vulnerável e ameaçado se percebe.

Considerando que não há o que seja feito pelo homem que não tenha o homem como destino final, seja direta ou indiretamente, um ato digital é uma ação humana objetiva, voluntária ou não, individual ou coletiva, realizada no mundo real, por meios digitais, mediada por ambiente simulado, com resultados e desdobramentos concretos e reais. Portanto, tem que ser provocado por pessoas, seja na produção de *hardwares*, seja no desenvolvimento *softwares*, seja na integração de ambos ou por meio de uma simples ação de um usuário leigo. (Girão, 2008)

A dinâmica entre os mundos real e virtual inspira tamanha abstração ao ser humano tal que este tente, invariavelmente, espelhar no mundo virtual a versão sintética de sua existência no mundo real.

2.2. Sensação de Segurança

Tradicionalmente, segurança é peculiar àqueles que à matéria se dedicam ou quando estes despertam interesse pela percepção de ameaças e de vulnerabilidades. Tal interesse se dá em relação diretamente proporcional entre proximidade e magnitude do evento indesejado que o atingiu de alguma forma, direta ou indiretamente. (Girão, 2016)

Segurança transpõe parâmetros e perímetros pessoais, setoriais, departamentais e organizacionais. Em sua essência, entremeia as corporações e as nossas vidas, visto se tratar um sentimento como outro qualquer - uma sensação, um "estado de espírito" que traduz momentos de conforto cerebral/mental em função da não percepção ou não identificação de ameaças e/ou por desconhecimento das vulnerabilidades e/ou por desconsideração às ameaças e/ou aos riscos, sejam materiais ou digitais – tangíveis ou intangíveis.

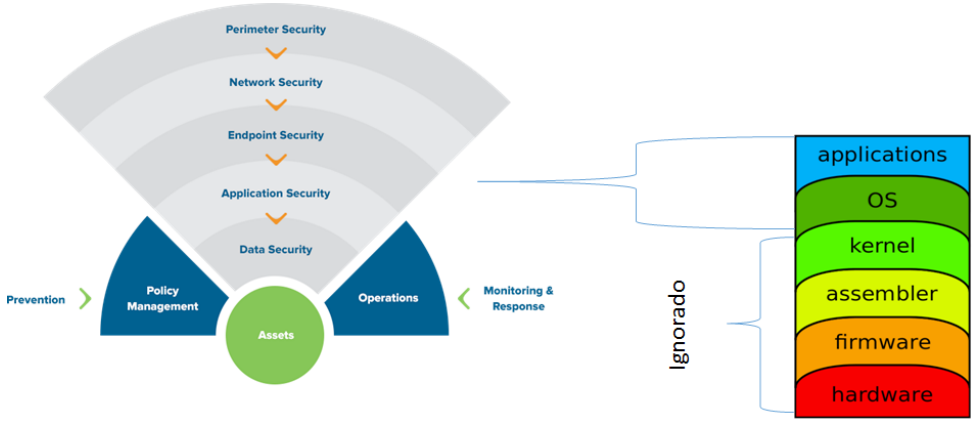


Figura 1 – Representação de camadas sob foco de proteção - *multi-layered security*
Fonte:Bridge2Solutions

É certo que não existem sistemas 100% seguros. Qualquer profissional de TIC e usuários melhor informados terão consciência sobre este fato. No entanto, há elemento que foi ignorado pelos tantos atores já mencionados: o *Firmware*.

Passou a usual que usuários de Tecnologias da Informação e Comunicações (TIC) sejam estimulados a manter sistemas operacionais e *antimalwares* instalados e atualizados, além de ativar aplicações de proteção, desde infraestruturas tecnológicas críticas a redes domésticas, bem como cada um dos dispositivos inseridos em seus contextos, o que não cabe considerar quando temos níveis mais baixos desprovidos de segurança e de boas práticas no desenvolvimento de *softwares*, visto que qualquer *framework* que exprima algo relacionado a segurança em camadas ignora os *kernel*, *assembler* e *firmware*, como ilustrado por meio da Figura 1.

2.3. Infraestrutura Mundial

Em plena era do conhecimento, a caminho da sabedoria, computadores passaram a ferramentas comuns, ao alcance de grande parte da população mundial, que vêm proporcionando ao mundo incontestáveis melhorias e suporte ao desenvolvimento dos mais diversos campos de atuação do ser humano e das suas ciências. Evoluímos a proporções inimagináveis aos olhos das comunidades mundiais dos períodos das revoluções agrícola, industrial e, até mesmo, do prelúdio da revolução tecnológica.

A conexão entre computadores estimulou o espírito colaborativo, o compartilhamento de dados e informações e impulsionou a popularização de máquinas eletrônicas digitais para processamento de dados, quando percebida a fluidez nos fluxos de processos, até então morosos e onerosos.

A *Internet* é constituída por um conjunto de redes de computadores interconectadas que, depois de atender interesses militares americanos, durante o período da guerra fria, foi popularizada nos anos 90 tornando o fluxo de dados mais dinâmico e com o propósito presumido de atender as demandas da sociedade naquilo que de útil e melhor pudesse usufruir.

Neste meio-tempo, a reboque, o desenvolvimento de *softwares* e *hardwares* chegaram a níveis tão significativos de sofisticação que alguns dispositivos eletrônicos digitais passaram a executar funções específicas e autônomas, tais quais os dispositivos da Internet das Coisas (*Internet of Things* – IoT). Que dirá quando da popularização da inteligência artificias e da computação quântica.

Aplicações, desenvolvidas com alto grau de complexidade, "substituiem" tradicionais ferramentas de cálculos, armazenamento, coleta e recuperação de dados, processamento e raciocínio e esforços humanos.

2.4. Firmwares e Coisas

Conjunto finito e definido de instruções que tem como finalidade executar tarefas elementares que foram previstas para um único e exclusivo conjunto de componentes eletrônicos e que produz resultado(s) esperado(s), *firmwares* são componentes lógicos vitais ao funcionamento de quaisquer equipamentos

eletrônicos digitais. Armazenados em mídias de tamanho diminuto, têm que estar presentes em todas estas estruturas. São vulneráveis e podem carregar as mais diversas ameaças e com potencial de ataque dos mais variados.

Dispositivos eletrônicos digitais não foram concebidos e providos de senso de autopreservação. Nada mais são que sistemas computacionais que sofrem de "imunodeficiência generalizada congênita", apesar de a obra da inteligência se dar, invariavelmente, nos meios acadêmicos e militares, aos quais podemos atribuir a condição de obsoleto desde o momento de sua aquisição, novo e em embalagem original e lacrada. (Girão, 2017)

2.4.1. Obsolescência

Apesar de poder ser classificada como programada ou planejada, perceptiva ou percebida, consideremos a obsolescência técnica ou funcional, pois, neste caso, "*a obsolescência de um produto é definida quando uma de suas partes, de hardware ou software, não é mais capaz de cumprir as funções requeridas adequadamente [...]*" Tradução livre. (Herold T., Verma, D., Lubert C., & Cloutier, R. ,2009)

Dito isto, podemos tomar estes *appliances* como elementos de alto grau de vulnerabilidade, por não serem foco de análise e leitura prévia de inconsistências, por meio de controle de qualidade no desenvolvimento de sua estrutura lógica, conformidade e auditoria, fazendo destes potenciais ameaças.

Os serviços de Inteligência de Estado e Inteligência de Segurança Pública, além de toda a comunidade digital mundial, estão sujeitos às ameaças ocasionadas pelos motivos apresentados. Como vítimas, podem se tornar fontes inesgotáveis de informações, bem como servir de ameaça ao próprio Estado – friendly fire, a outras nações, organizações públicas e privadas e aos cidadãos.

3. Marco Teórico

Houve momentos que a hipótese de buscar respostas junto a pessoas seria a forma ideal. No entanto, este elemento, como o mais vulnerável na cadeia de análise, foi método descartado. O que melhor se adequou ao desenvolvimento deste estudo foram os atos digitais e seus desdobramentos, fatos e consequências. Para tanto, toda a coleta de dados teve como origem as tecnologias e suas fontes abertas.

Este trabalho carrega em todo seu contexto a multidisciplinaridade. Para tanto, foram coletados dados e informações dos mais diversos canais de mídia especializados em comunicação digital, principalmente, aqueles canalizados sobre os temas Inteligência e Tecnologia, sobre as ameaças, pois delas pudemos tirar conclusões sobre as vulnerabilidades (eventos, relações temporais, comportamentos humanos e socioprofissionais, códigos exploradores e vazamento de dados), bem como os desdobramentos e resultados de atos digitais empreendidos em contraponto às lógicas filosóficas e matemáticas do certo ou errado e do sim ou não, respectivamente.

4. Evidências

Os fatos aqui apresentados correspondem à diversidade de ações que visaram à obtenção de prerrogativas administrativas, destruição de instalações, espionagem, vazamento de documentação classificada, obtenção de controle remoto sobre dispositivos, invasão de sistemas essenciais e críticos e interferência em sistemas estratégicos.

Foram selecionados apenas três fatos, de modo a expor o contexto de algumas das vulnerabilidades e das ameaças que podem ser, analogamente, adaptadas aos Serviços de Inteligência e Contrainteligência, bem como ao cidadão comum, que servirão como base para o entendimento e confirmação do quão importante são os *firmwares*.

4.1. BadUSB

A particularidade deste malware tem como foco quaisquer periféricos que usem conexões *Universal Serial Bus* (USB) e sustentem *firmware* em *Electrically-Erasable Programmable Read-Only Memory* (EEPROM) (e.g. *hubs*, placas-mãe, adaptadores de cartões SD, adaptadores SATA, teclados e *mouses*, *webcams*, *pendrives*), de forma, praticamente, indetectável e intratável. (Nohl, K. & Jakob, L., 2014)

Um *pendrive* comprometido pode usar interfaces de rede do hospedeiro fazendo com que se conecte a sites maliciosos disfarçados como sites legítimos, agir como *keylogger*, com vistas à captura de senhas de acesso privilegiado a sistemas operacionais em infraestruturas tecnológicas críticas.

A tentativa de retirada do código pode requerer abertura do equipamento e uso de engenharia reversa, pois a simples formatação não é solução. A área reservada ao *firmware* é protegida por ele mesmo, informando ao sistema operacional que aquela mídia só é acessível para escrita e leitura na área de armazenamento de dados, não tendo como contar com a proteção de sistemas antivírus, visto que *antimalwares* não trabalham nesta camada.

4.2. Stuxnet

O *worm* Stuxnet foi eleito como um dos mais sofisticados tipos de ataques, à época de seu alastramento pela Internet.

Construído com a finalidade específica de ataque a equipamentos de automação de usinas nucleares padrão Siemens, foi e ainda é exemplo de legítima arma de guerra cibernética.

Usinas nucleares e plantas industriais estratégicas seguem ou deveriam seguir rígidas normas de segurança. A principal delas é a de manter todos os processos de produção automatizados fora do campo de ação da Internet. O *National Institute of Standards and Technology* (NIST) recomenda a segregação de redes por meio do SP800-82 – *Guide to Industrial Control Systems* (ICS) *Security*.

Toda infraestrutura crítica deve ser segregada, justamente para evitar o acesso remoto indevido às instalações lógicas. No entanto, no ano de 2010, a usina nuclear do Irã, denominada Natanz, sofreu ataque que inutilizou algumas de suas centrífugas de enriquecimento de urânio.

O que se presume é que a ação se deu por meio de conexão de um *pendrive* comprometido por código malicioso inserido em seu *firmware* em um dos computadores da rede da usina.

O *worm* não foi detectado por *antimalwares* e nem pelo portador, inofensivo aos computadores e aos sistemas operacionais, se espalhou pela rede em busca do computador que continha o supervisório do sistema de automação, por meio do qual são definidos parâmetros de funcionamento dos equipamentos automatizados, bem como o monitoramento do comportamento destes.

Ao detectar a presença de aplicação de controle SCADA denominada STEP7, o *malware* apropriou-se de prerrogativas administrativas e promoveu mudanças de valores em variáveis que afetaram diretamente o funcionamento da planta.

Antes que estas mudanças fossem efetuadas, outros parâmetros teriam que ser alterados, tais quais, desligamento de alarmes, memorização e exposição de valores legítimos e inibição de interface entre o supervisório e os *firmwares* dos equipamentos.

Com o Sistema Supervisório STEP7 da Siemens blindado, executou mais uma de suas funcionalidades, gravando nos *firmwares* das *Programmable Logic Controllers* (PLC) dos equipamentos automatizados, blindando-os também, de forma que não respondessem a qualquer intervenção direta no hardware, assegurando as ações previstas.

Em modo de ataque, aumentou a velocidade de rotação das centrífugas em 40% e por somente 15 minutos, bem como interrompendo o sistema de arrefecimento. Velocidade, tempo e temperatura suficientes para causar danos físicos e tornar a planta inoperante, sem provocar acidente nuclear de maior proporção.

Mesmo que tentassem intervir por meio do sistema supervisório, os valores mostrados correspondiam à normalidade e sem efeito qualquer tentativa de interromper o processo de destruição.

Os procedimentos foram analisados e descritos em detalhes por pesquisadores da empresa Symantec e da Universidade do Arisona (Mueller, P. & Yadegari, B., 2012) (Falliere N., Murchu L. & Chien E., 2011).

4.3. Juniper Networks

Uma das maiores fabricantes de ativos de rede do mundo, a empresa Juniper Networks passou a alvo de investigação pelo Congresso Nacional Americano pelo fato de terem sido descobertas duas falhas embutidas no sistema operacional ScreenOS, *firmware* dos *firewall* por ela fabricados.

As falhas foram divulgadas por meio da mídia internacional digital, a partir do dia 17/12/2015, que revelou que eram graves e que davam prerrogativas administrativas máximas ao invasor, além de acesso ao tráfego de dados protegidos por *Virtual Private Network* (VPN). (NVD - CVE-2015-7754/7755/7756, 2015)

O código malicioso fazia parte do código escrito pela área de software da empresa Juniper e foi tratado pelo FBI e pelo DHS como um *backdoor* secreto e "não autorizado".

Tratando-se, portanto, de procedimento que levou a empresa a ser suspeita de ter inserido, propositalmente, linhas de código malicioso em seu *firmware*. Além disto, estes órgãos de investigação afirmaram não ser possível detectar a intrusão, pelo fato de os históricos de registros poderem ser apagados ou alterados pelo invasor.

Com permissões de administração, o invasor domina o *appliance*, eliminando rastros de registros de acesso e a capturar todo o fluxo de dados em texto plano por meio de VPN, guardando-o para posterior análise.

Peculiarmente, as suspeitas recaíram sobre os próprios americanos que dizem não crer que ataque tão sofisticado tenha partido da *National Security Agency* (NSA) em parceria com Reino Unido ou Israel. Seria caso de se pensar que a NSA, além de espionar todas as comunicações digitais do mundo, ainda o faria "dentro de casa". Mas, como exercício de contrapropaganda, elegeram as espionagens chinesa e russa como prováveis promotoras do *backdoor*, mesmo que a empresa tenha sido fundada e estabelecida em território americano.

Os equipamentos da Juniper eram, utilizados, presumidamente, pelo FBI, DHS, Departamento de Defesa (DoD), Departamento de Justiça (DoJ), Departamento do Tesouro Americano (DoT), dentre outros órgãos de governo em território americano e espalhados pelo mundo. Esta presunção está pautada por inúmeras matérias jornalísticas, publicadas à época, por agências de notícias acreditadas, tais como Reuters e CNN.

Além de intrigante, há a declaração expressa do SANS *Institute*, por meio do *Internet Storm Center* (ISC), que o código foi mantido no *firmware* (ScreenOS) do equipamento ao longo de, ao menos, três anos. Permaneceu nos equipamentos do ano de 2012 até dezembro de 2015, quando o código foi retirado pela Juniper e publicado patch de correção em 22/12/2015. (SANS Institute, 2015)

O caso Juniper pode ser considerado um dos mais graves, pelo tempo de exposição e na proporção que se deu por meio de supostos acessos a infraestruturas governamentais e de segurança nacional, tanto dos EUA quanto de outros tantos presumidos, em função da capilaridade mundial da empresa.

5. Discussão e Proposta

Lidamos com dados críticos, sensíveis e íntimos armazenados em infraestruturas tecnológicas críticas de Estado e de Segurança Pública, bem como em lares.

Os assuntos debatidos até então, por mais que chancelados por especialistas e personagens políticos com melhor adesão ao tema, acabaram por gerar mais papel. No caso do Brasil, sem efeitos práticos, citamos a Lei Nº 12.965/14 (Marco Civil da Internet) (BRASIL, 2013), que regula o uso da Internet no Brasil por meio da previsão de princípios, garantias, direitos e deveres para quem usa a rede, bem como da determinação de diretrizes para a atuação do Estado e o Decreto Nº 3.505 de 13 de junho de 2000 (BRASIL, 2000), que instituiu a política de segurança da informação nos órgãos e entidades da administração pública federal brasileira.

Temos potencial humano e ferramentas para levar a cabo as propostas de trabalho dispostas neste documento. Falta, para tanto, vontade política e resistência ao *lobby*

das indústrias estrangeiras, bem como atrelar fabricação e aquisição de equipamentos sensíveis a regras muito bem estabelecidas e claras.

Inteligência de Estado e a Inteligência de Segurança Pública são áreas de atuação que têm em comum produzir conhecimento para suas esferas de atuação em auxílio à tomada de decisão. Às contrainteligências, atribui-se a proteção do conhecimento produzido, bem como até a eliminação da inteligência adversa.

Personagens em plena atividade nos mundos real e virtual tendem a se render ao meio digital como ferramenta para, principalmente, armazenamento, tratamento e pesquisas em base de dados. Portanto, sujeitos às triviais ameaças digitais.

Os problemas apresentados nos obrigam a ponderar sobre a prejudicialidade ocasionada pelas exigências legais para as operações de inteligência e contrainteligência, quando se veem delimitadas pela conformidade, bem como sobre o contingente mundial que investe em ilicitudes digitais transnacionais e no grau de sofisticação de suas ações, rasos em legislação e penalidades, ao menos intimidantes, que são iminentemente cabíveis diante do alto nível de risco à humanidade e à coletividade, além do desprovimento de entendimento adequado, de recursos financeiros e de vontade política.

Caso garantíssemos conformidade e auditabilidade de *firmwares*, estaríamos melhor providos de *hardware* e *software*, bem como manteríamos o controle sobre as tecnologias desenvolvidas para uso em território nacional.

Firmwares seriam assinados digitalmente e protegidos por criptografias nacionais, passando por crivo de agência reguladora em modo *blindreview*, de tal forma que as indústrias seriam impelidas a se adequar a parâmetros ditados pelo Estado e aos preceitos cidadãos.

Os próprios *firmwares* seriam instruídos, em observância às exigência da agência reguladora, a acionar gestores de infraestruturas tecnológicas sobre a disponibilidade, integridade, confidencialidade e autenticidade do código do sistema operacional desenvolvido para *appliances* nacionais, remetendo-nos à ideia de haveria "quem vigia quem vigia quem vigia".

A Figura 2 ilustra proposta de ação com vistas ao controle racional dos *appliances* comercializados dentro do país, além de preencher lacuna promovida pela não observação sistemática de códigos de controle de *hardwares*.

Além disto, mitigaria as presumidas pressões exercidas sobre a industria para adulterar suas linhas de código, em função dos interesses de um Estado.

Aliado a isto, a promoção da educação do cidadão digital viria como coadjuvante à formal, de modo que o uso de ferramentas para proteção, de tal modo que o uso de VPN e criptografia se tornariam usuais. O Estado, por sua vez, se veria obrigado a realizar suas operações de inteligência de modo menos ostensivo, mais ético, em conformidade e melhor controlado.

As evidências apresentadas servem como base para o entendimento e confirmação de quão importante são os *firmwares* e o quanto devem ser usados como referência para ações de Estado no sentido de estabelecer parâmetros para aquisição de ativos de rede e incitar a comunidade mundial ao consenso sobre a necessidade de leis transnacionais

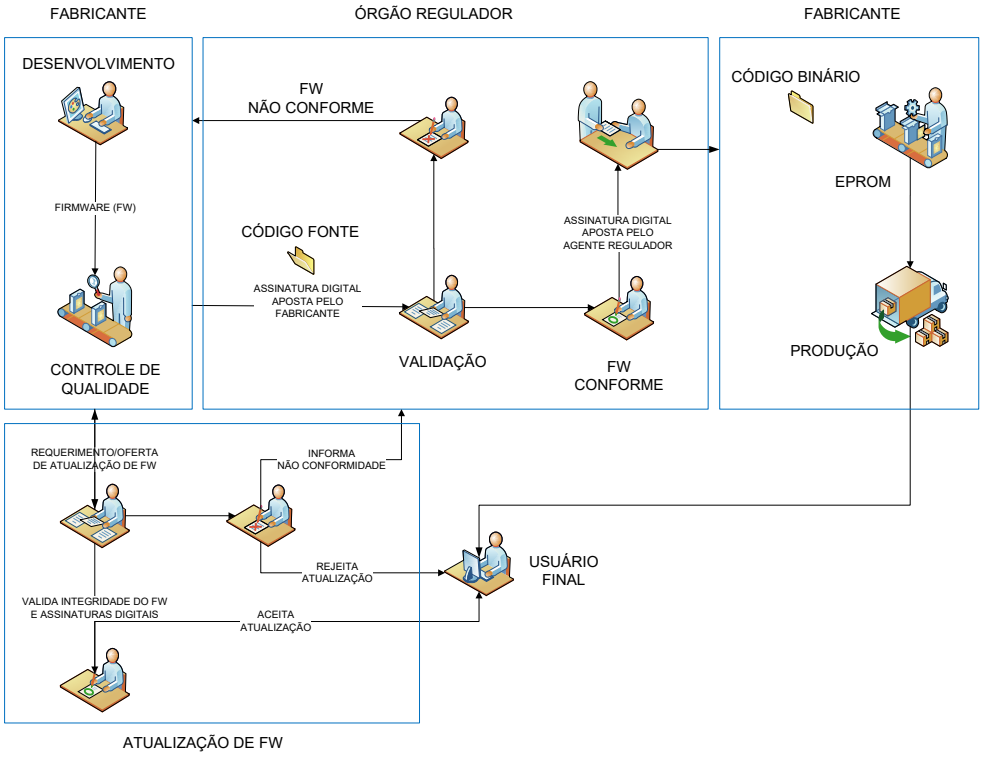


Figura 2 – Proposta de fluxo de processo de homologação de *firmware* por agência reguladora

que possam alcançar a criminalidade digital, exigindo cumprimento de leis e cláusulas contratuais severas que possam intimidar e penalizar de forma exemplar aqueles que usam das limitações alheias para a obtenção de vantagens ilícitas.

Pode parecer ingênuo, mas, no caso da Estônia, é provável que não desejem roteadores domésticos vulneráveis, visto que foi um dos primeiros países a passar por onda de "ataques" (Ruus, K., 2008) *Distributed Denied of Service* (DDoS) no mundo. A infraestrutura tecnológica do país teve que ser interrompida por conta de volume de acesso aos seus servidores. Pode ser justificativa para exigirem *appliances* menos suscetíveis ao mau uso por terceiros, evitando o "fogo amigo".

6. Considerações Finais

Do menor ao maior potencial de risco, podemos avaliar cenário simplista como o de uma câmera de vigilância tornada inoperante a um mais complexo como a tomada de controle de uma usina de força ou de uma aeronave ou de um míssil.

Meios para mitigar, temos: educação, disciplina e instrução. Se promovermos estas ações dentro de nossos lares e em nossos ambientes de trabalho, já nos encontraremos passo à frente diante aos atuais níveis de vulnerabilidade. Para isto, temos normas que

sugerem boas práticas para os diversos níveis de responsabilidade que envolvem as tecnologias das informações e meios computacionais: COBIT, coleção ISO/IEC 27000, CMMI, ISO/IEC 9126-1, ISO/IEC 25000, SWEBOK, dentre outras.

Negligenciar é algo facilmente inteligível quando definimos como "deixar de cuidar ou não dar a devida atenção", desde que o agente tenha conhecimento das possíveis adversidades imprimidas na qualidade daquilo que produz, adquire ou utiliza.

Educamos mal, formal e digitalmente. A educação formal carece de iniciação digital e de valores morais e éticos. Entregamos tecnologias e não transferimos conhecimento suficiente para que as manipulem com responsabilidade.

Sob o aspecto jurídico, temos que ser cautelosos, diante da inevitável digitalização do mundo e empreender formação adequada e de vanguarda a todos os envolvidos nos procedimentos investigatórios e interpretativos dos fatos e das leis, para que não incorramos em frequentes erros.

Firmwares, pequenos, mas eficientes sistemas operacionais, deveriam ser melhor tratados, ser foco constante de instâncias técnicas e motivação à Pesquisa e Desenvolvimento (P&D) nacionais, além de completar lista de ações de Segurança Nacional.

Expomo-nos, desnecessariamente, às vulnerabilidades importadas, sem que ocorra homologação lógica de equipamentos de uso profissionais e domésticos.

Se prestássemos mais atenção em nossos cientistas e no corpo técnico formal e informal, provido de imensurável capacidade e conhecimento, poderíamos utilizar o potencial deste capital humano aliado aos conhecimentos e experiências disponíveis em Vales da Eletrônica, unindo esforços para a construção de produtos de qualidade e menos vulneráveis.

Pensar em compartimentação, no viés contrário ao da origem da *Internet*, passa a plausível, visto a tendência de criação de fronteiras digitais, face a intervenções digitais desregradas contra nações e seus cidadãos.

Nesse meio-tempo, as Atividades de Inteligência merecem ser rotuladas de serviços de arapongagem e bisbilhotagem digitais, enquanto políticos, juristas e pensadores esboçam tentativas "*standalone*" de consenso sobre legalidade ou ilegalidade de tais ações, enquanto Agências de Inteligência desprezam e extrapolam suas linhas doutrinárias, violando a intimidade de cidadãos e soberanias nacionais.

É tema discutido tecnicamente ou politicamente. Não se percebe quaisquer movimentos que nos remetam a um ponto concreto e que contemplem a multidisciplinaridade de ações, visto que, praticamente, exauriram o assunto, isoladamente, nestas esferas.

Como regras não são definidas ações transfronteiriças perpetradas por organizações criminosas e terroristas, continuarão sem limites e ganhando larga dianteira contra aqueles que empreendem pelo cumprimento de regras sociais e princípios morais e éticos nos mundos real e virtual.

Referências

BRASIL. Decreto Nº 3.505 de 13 de junho de 2000. (2000) Institui a política de segurança da informação nos órgãos e entidades da administração pública federal. Brasília. Disponível em http://www.planalto.gov.br/ccivil_03/decreto/d3505.htm.

BRASIL. Senado Federal. (2013). CPI da Espionagem. Relatório Final. Comissão Parlamentar de Inquérito destinada a investigar a denúncia de existência de um sistema de espionagem, estruturado pelo governo dos Estados Unidos, com o objetivo de monitorar emails, ligações telefônicas, dados digitais, além de outras formas de captar informações privilegiadas ou protegidas pela Constituição Federal. Disponível em: http://www.senado.leg.br/atividade/rotinas/materia/getPDF.asp?t=148016&tp=1.

Cepik, M. (2001). Segurança nacional e segurança humana: problemas conceituais e conseqüências políticas. *Security and Defense Studies Review*. v.1. pp. 01-19. Disponível em <http://professor.ufrgs.br/marcocepik/files/cepik_-_2001_-_seg_nac_e_seg_hum_-_sec_and_def_review.pdf>.

Falliere N., Murchu L. & Chien E. (2011). *W32.Stuxnet Dossier*. Symantec.com. Disponível em https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

Girão, R. (2008). Analfabetismo digital e responsabilidade objetiva. *Jornal Estado de Minas*. Caderno Direito & Justiça, p. 8.

Girão, R. (2016). *Firmware*. Linkedin. Disponível em: https://pt.linkedin.com/pulse/firmwares-entrevista-concedida-%C3%A0-revista-security-report-gir%C3%A3o.

Girão, R. (2017). *Segurança digital em camadas – digital layered security*. Slideshare.net. Disponível em https://www.slideshare.net/bhackconference/palestra-regilberto-giro-segurana-digital-em-camadas-digital-layered-security.

Herold T., Verma, D., Lubert C., & Cloutier, R. (2009). *An obsolescence management framework for system baseline evolution—Perspectives through the system life cycle*. System Engineering, vol. 12, pp. 1–20. Disponível em https://pdfs.semanticscholar.org/bd53/bb33876e3aec683a97ba231818947dac24b9.pdf.

Mueller, P. & Yadegari, B. (2012). *The Stuxnet worm. CSc 466-566 Computer Security*. Disponível em http://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf.

Nohl, K. & Jakob, L. (2014). *BadUSB-On accessories that turn evil*. Black Hat USA. Disponível em: https://srlabs.de/wp-content/uploads/2014/07/SRLabs-BadUSB-BlackHat-v1.pdf.

NVD - CVE-2010-2568. (2010). Nvd.nist.gov. Disponível em https://nvd.nist.gov/vuln/detail/CVE-2010-2568.

NVD - CVE-2010-2772. (2010). Nvd.nist.gov. Disponível em https://nvd.nist.gov/vuln/detail/CVE-2010-2772.

NVD - CVE-2015-7754. (2015) Nvd.nist.gov. Disponível em https://nvd.nist.gov/vuln/detail/CVE-2015-7754.

NVD - CVE-2015-7755. (2015). Nvd.nist.gov. Disponível em https://nvd.nist.gov/vuln/detail/CVE-2015-7755.

NVD - CVE-2015-7756. (2015). Nvd.nist.gov. 2015. Disponível em https://nvd.nist.gov/vuln/detail/CVE-2015-7756.

Ruus, K. (2008). *Cyber War I: Estonia Attacked from Russia*. Europeaninstitute.org. Disponível em: https://www.europeaninstitute.org/index.php/42-european-affairs/winterspring-2008/67-cyber-war-i-estonia-attacked-from-russia?author=Kertu%20Ruus.

SANS Internet Storm Center. (2015). *The other Juniper vulnerability - CVE-2015-7756*. Disponível em https://isc.sans.edu/forums/diary/The+other+Juniper+vulnerability+CVE20157756/20529/.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 03/09/2017
Aceitação/Acceptance: 26/03/2018

Hacia la unificación de radares civiles y militares: Sistema de integración de la señal de radares de la Dirección General de Aviación Civil como apoyo a la Defensa y Seguridad del espacio aéreo ecuatoriano.

Juan Romero Mediavilla[1], Alex Jiménez Vélez[2]

ing.jcromero67@gmail.com; afjimenezv@gmail.com

[1] Comando de Operaciones Aéreas y Defensa, Departamento TIC-COAD, Guayaquil-Ecuador

[2] Centro de Investigación y Desarrollo FAE, Ambato-Ecuador

Pages: 66–75

Resumen: La topografía del Ecuador presenta zonas sin cobertura y se las denomina ciegas, en las cuales los radares primarios de la Fuerza Aérea Ecuatoriana (FAE) no disponen de cobertura; dificultando la vigilancia en estas áreas, causando un incremento de vuelos ilegales orientados al narcotráfico. Por tanto, se requiere complementar la información con las señales de los radares civiles en dichas zonas, específicamente los datos provistos por el Secondary Serveillance Radar (SSR), cuya identificación y seguimiento de blancos específicos se realiza gracias a equipos denominados transpondedores. En este trabajo se presenta un sistema piloto que integra la señal de los radares de la Dirección General de Aviación Civil (DGAC), complementando la de los radares militares, permitiendo ampliar la cobertura de la Defensa Aérea desde los Centros de Mando y Control (CMC) del Comando de Operaciones Aéreas y Defensa (COAD) de la FAE.

Palabras-Clave: telecomunicaciones; Eurocontrol; radar; SSR; Asterix.

Towards the integration of militars and civilian radar signals of the, in support of the defense and security of ecuadorian airspace

Abstract: The topography of the Ecuador presents areas without coverage called blind, in which the primary radars of the Ecuadorian Air Force (FAE) do not have coverage; making the surveillance in these areas, causing an increase of illegal flights aimed at drug trafficking. Therefore, it is required to supplement the information with the signals of the civil radars in these areas; specifically the data provided by the Secondary Serveillance Radar (SSR), whose identification and monitoring of specific targets is done thanks to computers named transponders. This work presents a pilot system that integrates the signal from the radar of the General Directorate of Civil Aviation (DGAC) with military radar, allowing to extend and complement the coverage of the Air Defense and Command and Control Center (CMC) of the Air Operations Command and Defense (COAD) of the FAE.

Keywords: telecommunications; Eurocontrol; radar; SSR; Asterix.

1. Introducción

Debido a los relieves del Ecuador y lugar de ubicación de los radares de la FAE, el control de Tránsito Aéreo presenta limitantes en la cobertura total, específicamente en la vigilancia de áreas ciegas. Este inconveniente ha ocasionado que se incrementen rutas aéreas ilegales en el territorio nacional en los tres últimos años; existiendo provincias con mayores incidencia como: Santa Elena, Guayas, Los Ríos y Manabí, consideradas la ruta de ingreso por su cercanía al perfil costanero.

La FAE, para cubrir estas áreas donde no se dispone de cobertura con los radares militares, requiere complementar la información con las señales de los radares secundarios de la Dirección General de Aviación Civil (DGAC), los cuales están ubicados en sectores que cubren algunas de las zonas ciegas. Estos radares secundarios son sistemas de radio-determinación basados en la comparación entre señales de referencia y señales radioeléctricas retransmitidas desde una posición a determina [1], donde las aeronaves en vuelo son identificadas en tierra por un interrogador conocido como: Secondary Serveillance Radar (SSR) [2], [3]such as one-dimensional (1-D quien solicita información de la aeronave, como su identidad y altitud, y cuyas peticiones son detectadas por equipos embarcados en las aeronaves conocidos como transpondedores, los cuales envían la información para facilitar su identificación en el control de tráfico aéreo.

2. Marco Conceptual

2.1. Sistemas Radáricos

La implementación y operación de Sistemas Radáricos, es una actividad en la que algunas leyes de la física son de mucha importancia y que involucran varias disciplinas tecnológicas y de ingeniería como: mecánica, eléctrica, electrónica, redes, telecomunicaciones y procesamiento de señales, donde se utiliza las ondas electromagnéticas para identificar la distancia, altitud, dirección y velocidad de movimiento de objetos que se encuentren en el espacio aéreo.

Con la finalidad de que las plataformas de control aéreo puedan integrarse entre los diferentes sistemas y dispongan de una interconexión remota, gran parte de fabricantes de sistemas radáricos están adoptando las recomendaciones de EUROCONTROL, organización civil y militar integrada por 41 estados europeos cuyo objetivo se centra en el desarrollo de un sistema seguro, eficaz y coordinado del tráfico aéreo europeo, para la utilización de interfaces, protocolos y categorías de acuerdo a las normas ASTERIX [4].

Asterix es un estándar que trabaja en las capas de presentación y aplicación definidos por la Interconexión de Sistemas Abiertos (OSI), donde pueden ser especificadas hasta 256 categorías de datos, siendo de nuestro interés la categoría 34 que es la nueva versión de la categoría 02 y sirve para decodificar los mensajes de servicio; y la categoría 48 que es la nueva versión de las categorías 01 y 16 y sirve para datos del radar primario y secundario.

1. *Radares Primarios*

   El funcionamiento básico de un radar primario, consiste en la emisión de una onda (Tx) al espacio (pulso continuo, señal modulada, impulso de corta duración), esta onda al alcanzar cualquier objeto o blanco, es reflejada o dispersada, creando un eco de la señal misma que recorren el camino de vuelta y se detectan de nuevo por el radar (Rx), tras un procesado de señales, se obtiene información de las características del objeto.

   En la actualidad los radares tres dimensiones (3D) son los más utilizados, ya que permiten medir varios parámetros de una aeronave en vuelo como: altura, distancia, dirección, velocidad y estos parámetros permiten localizar un objeto respecto a su posición geográfica.

   La energía que generan los radares, viajan en línea recta, aproximadamente a la velocidad de la luz, 300 000 Km/s o 162 000 NM/s y con variaciones mínimas ocasionadas por fenómenos atmosféricos y condiciones meteorológicas, para el cálculo de la distancia se utiliza la siguiente ecuación:

$$R=c.\frac{t}{2} \quad (1)$$

   c=velocidad de la luz

   t=tiempo

Las ondas electromagnéticas se reflejan sobre superficies conductoras; por lo tanto, si las ondas reflejadas retornan al punto de emisión de las ondas, se puede deducir que se encuentra un obstáculo en la trayectoria de propagación (ver Figura. 1), para cálculos se utiliza la Ecuación Básica Radar que permite determinar la potencia de pico recibida [5]:

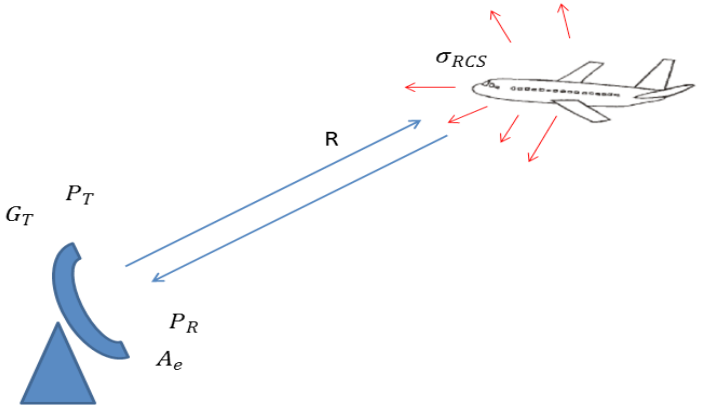


Figura 1 – Descripción del uso de la Ecuación Básica Radar
Fuente: Fundamentos de un Sistema radar INDRA

$$P_R = \frac{P_T G_T}{(4\pi)R^2} \frac{\sigma_{RCS}}{(4\pi)R^2} A_e \quad (2)$$

P_T=Potencia de pico transmitida

G_T=Ganancia de la antena

σ_{RCS}=Sección recta radar del blanco

A_e=Área efectiva de la antena

2. *Radares Secundarios*

Se utiliza para el control del tránsito aéreo, se lo conoce también como radar de interrogación (SSR), estableciéndose un canal entre el sistema y el transponder del blanco por el cual envía información como que solicita el interrogador como: identificación de matrícula o identificación de una aeronave, distancia, azimut, altura, emergencias, etc.

Los transponder que están en las aeronaves, tienen modos de operación, resumiéndoles de la siguiente manera:

- **Modo A:** Muestra la identificación de la aeronave.
- **Modo C:** Muestra la identificación de la aeronave y su altura.
- **Modo S:** Muestra la identificación de la aeronave y su altura pudiendo además codificarse señales aire-aire para evitar colisión (TCAS), reportes meteorológicos, alertas, servicio de vigilancia de tráfico. El código de identificación es único para cada aeronave (Aircraft Address). Evita la superposición en espacios congestionados.[6], [7]

2.2. Bandas de Operación de los Sistemas Radar

El espectro radioeléctrico ha sido dividido en subgrupos por rangos de frecuencias, esta extensa y completa gama tiene en cuenta las propiedades físicas de las ondas que lo componen y se la puede representar como se muestra en la siguiente figura (ver Figura 2)

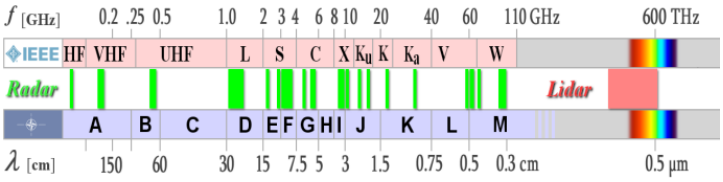


Figura 2 – Rangos de ondas y de frecuencias utilizadas por radares.
Fuente: www.radartutorial.eu

- **Banda L (1,0 a 2,0 GHz).-** Esta es la banda de frecuencias preferida para los radares de vigilancia aérea con base en tierra de largo alcance, como los radares de 200 NM. Es posible lograr un buen rendimiento en la Identificación

de un Objetivo en Movimiento (MTI) a estas frecuencias y obtener alta potencia con antenas de estrecha anchura de haz. El ruido externo es bajo. Radares 3D militares se pueden encontrar en banda L, pero también se encuentran en la banda S. Banda L también es adecuado para grandes radares que deben detectar objetivos a larga distancia [5]

- **Banda S (2,0 a 4,0 GHz).-** Radares de vigilancia aérea pueden ser de largo alcance en la banda S, pero por lo general es más difícil de lograr que en las frecuencias más bajas. Para largas distancias se producen áreas ciegas y es más numerosos cuando la frecuencia aumenta, lo que hace menos capaz de MTI, también es una buena frecuencia para aplicaciones de vigilancia del espacio aéreo de mediano alcance, como el radar de vigilancia de aeropuerto (ASR) que se encuentra en las terminales aéreas.[5]

3. Sistema prototipo de integración radares militares y civiles

En este contexto, los estudios están orientados en análisis teóricos y experimentales, a fin de implementar un Sistema Piloto para integrar las diferentes señales de los radares de la DGAC y transmitir la información a través de la tecnología WiMAX desde el Centro de Control de Área (ACC-Guayaquil) hacia el Centro de Mando y Control del Comando de Operaciones Aéreas y Defensa (CMC-COAD) y presentar los tracks de las aeronaves en vuelo utilizando un visualizador de ficheros Asterix.

El propósito de este sistema piloto, es desarrollar un sistema que permita visualizar las señales de los radares de la DGAC de manera individual pero simultánea y utilizarlos en apoyo a la Seguridad y Protección del Espacio Aéreo, complementando la cobertura de los radares militares.

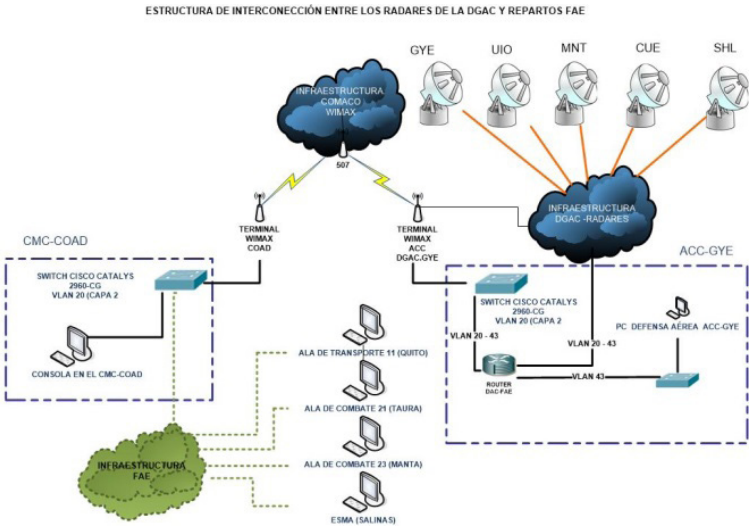


Figura 3 – Diagrama de red de la solución propuesta
Fuente: Elaboración propia

Además se tiene como proyección la réplica de la solución en otras unidades de Fuerzas Armadas, tanto Aéreas, Terrestres y Navales, utilizando la infraestructura propia de cada institución. El Diagrama de la solución propuesta se visualiza en la Figura 3.

Este sistema pretende tomar las señales de los radares de Galápagos, Manta, Cuenca, Quito y la Shell de la DGAC de manera individual y que convergen en un router en el cuarto de servidores del ACC- Guayaquil, y a través de la tecnología WiMAX, misma que permite prestar servicios en zonas de difícil acceso, cubriendo largas distancias y permitiendo materializar Puestos de Mando alternos en cualquier lugar dentro de la cobertura de la celda WiMAX, [8] mediante direccionamientos de canales de transmisión, capturar los datos de cada radar en forma individual y presentar en una consola utilizando el software VisualAST.

3.1. Fases de configuración del Software de visualización grafica de ficheros Asterix

Esta aplicación básicamente decodifica los mensajes Asterix y los presenta en forma de listas en una representación polar, el código está escrito para decodificar las categorías ASTERIX: 1, 2, 8, 10, 11, 21, 34 y 48, siendo estas dos últimas categorías, las que se utilizarían para datos de los radares secundarios [9][10].

El VisualAST, fue diseñado por la empresa INDRA para presentar los datos en laboratorio que emiten los radares primarios y secundarios, capturando la información de los mismos y decodificando los protocolos antes mencionados, siendo una herramienta de mantenimiento.

Fase 1

Para poder contar con el perfil del territorio ecuatoriano y de las aerovías, en el software se debe cargar plantillas en formatos .jue así como el posicionamiento en coordenadas sexagesimales de la ubicación de los radares, estos formatos se los ejecuto con personal técnico de la DGAC. (Ver figura 4)

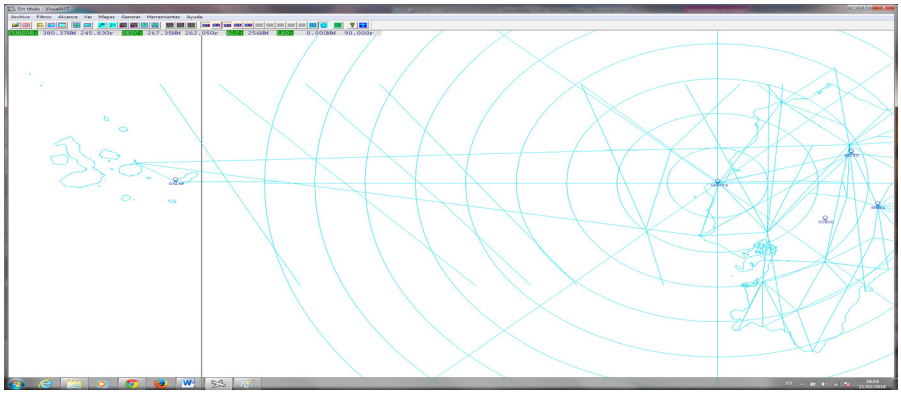


Figura 4 – Visualización del perfil ecuatoriano, las aerovías y ubicación de los radares de la DGAC

Fase 2

Para configurar los Parámetros del Canal de donde se obtendrán los datos, se utilizó un Analizador de Protocolos de Red "WireShark" [11], el mismo que permite reconocer el tráfico de la red, entender los protocolos utilizados y mostrar la manera como van viajando, y así facilitar el descubrir riesgos posibles como trafico malicioso, además me permite identificar las direcciones IP de origen, la IP Multicast y el Puerto de Destino, como se muestra en la Figura 5.

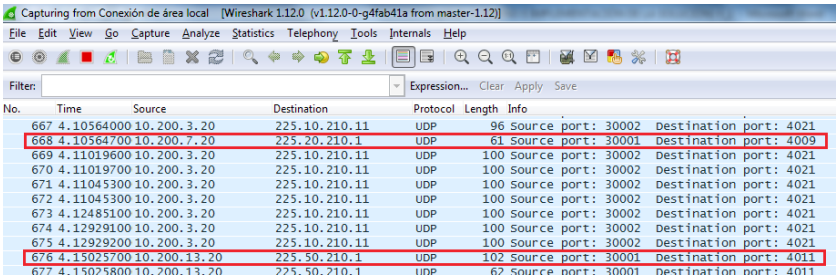


Figura 5 – Información de Protocolos de la Red.
Fuente: Elaboración propia

4. Análisis de Resultados

Para este proyecto se realizaron pruebas de Laboratorio y de Campo, para comparar los resultados y determinar la precisión de este sistema piloto, respecto a los sistemas que dispone actualmente la DGAC.

Para este ensayo, se analizó las capturas de información que se toma del radar de Manta, cada señal representa a una aeronave que en ese instante de tiempo se encontraba en vuelo, la información que presenta es la matrícula de la aeronave y la altura a la que se encuentra de acuerdo a su localización.

Las líneas, representan las aerovías, las mismas que permiten a los controladores de tránsito aéreo ver la trayectoria y destino de una aeronave, sin embargo existen muchas

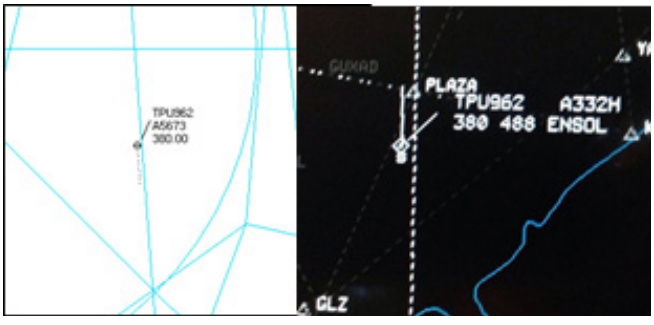


Figura 6 – Presentación de las aeronaves en vuelo radar de Manta
Fuente: Elaboración propia.

aeronaves que se salen de su trayectoria ya sea porque están circunvalando alguna nubosidad, o por algún otro motivo, es ahí cuando los controladores hacen contacto con la aeronave para preguntar la novedad y se lo enruta.

En la Figura 6, se puede observar en el lado izquierdo la presentación de una aeronave en vuelo en el VisualAST y en el lado derecho, la información de una consola de los radares de la DGAC, siendo preciso lo que eleva su confiabilidad.

En estas pruebas se compara al lado izquierdo las señales de las capturas realizadas con el software VisualAST que se encuentra en el CMC-COAD correspondiente al radar de Galápagos y a la derecha la presentación en una consola del ACC-DGAC, La información es igual y la presentación de las aeronaves en vuelo es precisa, (Ver Figura 7) es necesario recalcar que las consolas de la DGAC poseen más información como condiciones climatológicas, puntos de chequeo, áreas prohibidas y posee las señales integradas de todos los radares secundarios.

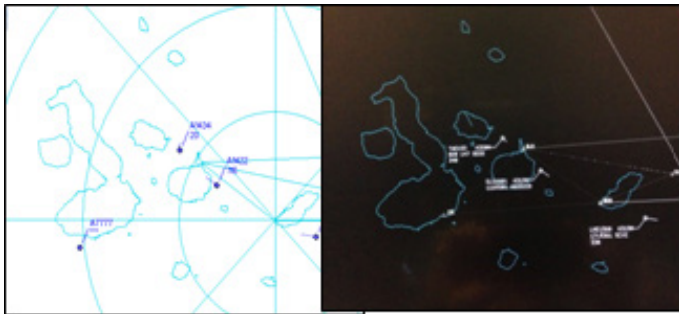


Figura 7 – Comparación del posicionamiento de una aeronave en vuelo con la señal del radar de Galápagos Fuente: Elaboración propia

Además, el software VisualAST, presenta la información que una aeronave emite a través del transponder como la distancia, el azimut, el código, la identificación; estos datos permiten identificarlos y presentar la información, pasando a ser un track que ha sido localizado.

Otra consideración es que más de un radar puede detectar una misma aeronave y los presenta de manera individual, teniendo como resultado que la plataforma me permite tener información de manera individual de cada radar operando simultánea en varias pantallas (Ver Figura 8)

5. Conclusiones

Las interfaces y protocolos en las categorías ASTERIX, facilitan la integración de sistemas e intercambio de datos radáricos entre diferentes regiones, ya que este protocolo es uno de los códigos abiertos más utilizados a nivel mundial, fortaleciendo la seguridad del control de tráfico aéreo.

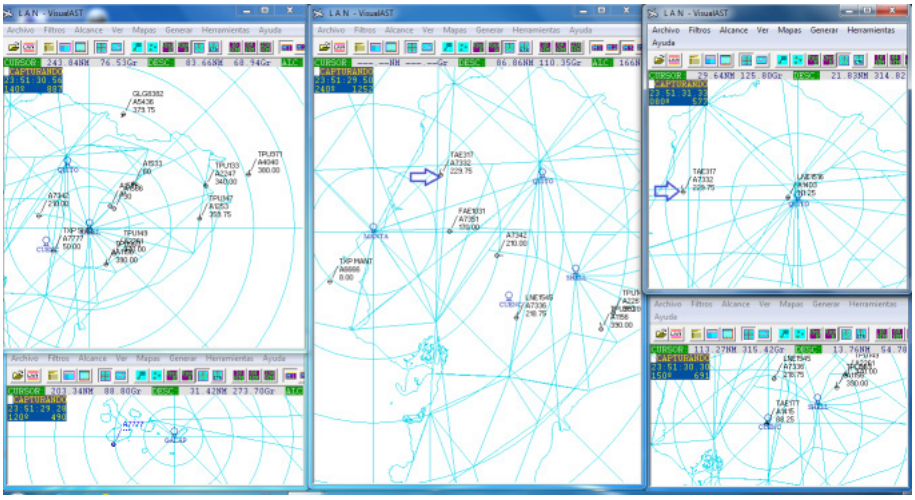


Figura. 8 – Señales de los radares trabajando de forma individual y simultanea
Fuente: Elaboración propia

El software VisualAST, trabaja en pantallas individuales por cada radar, ya que en los ensayos realizados se evidenció la limitación de trabajar de manera integrada con todos los radares en una sola pantalla, debido a que la plantilla del perfil del Ecuador al configurarlo inicialmente en las coordenadas, y al configurar para que capture los datos de todos los radares al mismo tiempo, presenta las aeronaves detectadas de forma aleatoria y en ubicaciones que no son las correctas.

El nivel de confianza de la información presentada es alto, ya que las pruebas de campo nos dieron información igual a la que se obtiene en las consolas propias del sistema de la DGAC.

Al haber obtenido buenos resultados en la implementación del plan piloto y que la información fue precisa, podemos concluir que es viable la replicación de la solución para otras Unidades de Fuerzas Armadas, utilizando la infraestructura propia de cada institución.

Agradecimientos

Al Comando de Educación y Doctrina de la Fuerza Aérea Ecuatoriana, al Comando de Operaciones Aéreas y Defensa y al personal de Oficiales y Aerotécnicos del Departamento TIC-COAD, al Centro de Investigación y Desarrollo de la FAE.

A la Escuela Politécnica del Litoral (ESPOL), por haber plantado los conocimientos y a través de los MSc. Cesar Yépez y PhD Freddy Villao guiado con sus experiencias y conocimientos.

Al Ing. Ángel de la Iglesia (INDRA), por haber orientado y compartido sus conocimientos y guía para la estructuración de este proyecto. Al Ing. Lenin Maldonado de la DGAC, por haber colaborado en las pruebas del proyecto.

Referencias

Senatel, “Plan Nacional de Frecuencias,” 2012.

D. Manolakis, “Aircraft geometric height computation using secondary serveillance radar ramge differences,” *Radar Sonar Navig.*, no. 1650, pp. 1–22, 2000.

F. Sagarra, “Control de tráfico aéreo y marítimo: Identificación de idiosincrasias y aportaciones al contexto de la seguridad marítima,” Politécnica de Cataluña, 2015.

EUROCONTROL, “Latest issues of ASTERIX Documents,” vol. 7, no. Part 3. .

M. Skolnik, *Radar Handbook*. 1970.

R. Bernal, “THE SYSTEM THAT HAS REVOLUTIONIZED THE CONCEPT OF AIR SAFETY,” *Cienc. y Tecnol.*, 2014.

R. M. Trim, “Mode S : an introduction and overview,” *Electron. Commun. Eng. J.*, vol. 2, no. 2, pp. 53–59, 1990.

I. Castro and J. Garcia, “Evaluación de desempeño de un enlace con tecnología WiMAX1,” *Entre Cienc. e Ing.*, vol. 9, no. 15, pp. 50–56, 2015.

EUROCONTROL, “EUROCONTROL STANDARD DOCUMENT FOR Part 8 : Category 011 Transmission of A-SMGCS Data,” *Released Issue*, no. May. 2008.

EUROCONTROL, “EUROCONTROL STANDARD DOCUMENT FOR Part 13 Transmission of TIS-B Management Messages,” no. April, 2007.

S. Alvernia, “WIRESHARK:Como herramienta de apoyo para el análisis de trafico maliciosoen una red local.,” Francisco de Paula Santander Ocaña, 2012.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 10/09/2017
Aceitação/Acceptance: 12/03/2018

Repensando los fundamentos de la gestión de riesgos. Una propuesta conceptual desde la incertidumbre y la complejidad

Jeimy J. Cano M.[1]

jeimy.cano@urosario.edu.co

[1] Universidad del Rosario, Calle 200 entre Autopista Norte y Carrera 7, Bogotá, Colombia.

Pages: 76–87

Resumen: La gestión de riesgos es una práctica gerencial consolidada en las organizaciones modernas. Adelantar este ejercicio permite a las empresas establecer marcos referentes de acción que la habilitan para avanzar en el desarrollo de sus estrategias de negocio. Para ello, se han utilizado de manera generalizada dos enfoques para su gestión: probabilidad vs impacto y frecuencia vs severidad. Cada uno de ellos, permite una forma ágil y concreta de atender los eventos adversos generalmente conocidos, con el fin de dar tratamiento a los mismos. Ahora en un contexto volátil, incierto, complejo y ambiguo, la gestión de los riesgos debe evolucionar y fundar una forma diferente de dar respuesta a la inestabilidad del entorno de negocios. En este sentido, se plantea una propuesta alterna basada en incertidumbre y complejidad, como una manera de atender aquellos eventos contrarios latentes y desconocidos, y sintonizar los enfoques previamente mencionados, con el fin de preparar a la organización para avanzar aún en situaciones inciertas para lograr sus objetivos de negocio.

Palabras-clave: Riesgos; probabilidad; complejidad; incertidumbre; negocios

Rethinking risk management fundamentals. A conceptual proposal based on uncertainty and complexity

Abstract: Risk management is a consolidated management practice in modern organizations. Advancing this exercise allows companies to establish benchmarks for action that enable them to advance in the development of their business strategies. For this purpose, two approaches to its management have been widely used: probability vs impact and frequency vs severity. Each of them, allows an agile and concrete way to attend generally known adverse events, in order to treat them. Now in a volatile, uncertain, complex and ambiguous context, risk management must evolve and form a different way of responding to the instability of the business environment. In this sense, an alternative approach based on uncertainty and complexity is proposed as a way to attend to those latent and unknown threats and to tune in the approaches previously mentioned, in order to prepare the organization to advance even in uncertain situations to achieve its business objectives.

Keywords*:* Risks; probability; complexity; uncertainty; business.

1. Introducción

La gestión de riesgos es parte fundamental del desarrollo de la vida empresarial y personal. Tanto las personas como las organizaciones, adelantan de manera formal o informal un análisis de las situaciones que pueden generar un incierto, con el fin de tratar de anticipar posibles consecuencias no deseadas (Aon, 2017). En este entendido, la práctica corporativa y la academia han fundado un marco general de dicha gestión basado en una propuesta que vincula dos conceptos: probabilidad e impacto.

Este marco de trabajo que se ha establecido como estándar, configura la manera natural como las empresas validan su ejercicio de valoración y priorización de riesgos, que les permite adelantar las acciones para mitigar los efectos no deseados de una posible materialización de los mismos (Freund & Jones, 2015, p.13). Si bien, esta propuesta permite un ejercicio que aumenta la sensibilidad de los participantes sobre el escenario, no se relaciona directamente con algunas exigencias ejecutivas que buscan no solo concientizar, sino conocer en detalle las implicaciones que se puedan anticipar de dichos eventos catalogados como adversos.

En este contexto, la industria de los seguros ha venido afianzando una lectura distinta y complementaria de los riesgos a lo que se conoce en el ámbito empresarial. Los especialistas en seguros conciben el riesgo como una relación entre frecuencia y severidad, dos elementos que hablan de "qué tantas veces se ha presentado el evento" y del "nivel de daño o compromiso" de la materialización de un evento respectivamente (Frapolli, 2015).

Mientras en el modelo tradicional de riesgo, la probabilidad se traduce como "una estimación de la materialización", generalmente basado en condiciones particulares o hipotéticas; en la apuesta de los seguros se habla de la frecuencia de "hechos concretos materializados", lo que permite analizar con claridad las causas raíces de los mismos. De igual forma, el modelo general de riesgos define el impacto como "las consecuencias que se pueden tener" de la materialidad del evento, mientras los especialistas en seguros validan la severidad como los "perjuicios que han tenido efectos concretos" que permiten tasar el valor a indemnizar.

Estas perspectivas han hecho carrera en dominios distintos, aportando luces tanto a los analistas de siniestros en los seguros, así como para los profesionales de riesgos en las empresas. En esta línea, poder visualizar una propuesta convergente que sume a la práctica de ambas posturas, puede potenciar un análisis riesgos más elaborado y plantear condiciones enriquecidas del mismo, que den cuenta de la inestabilidad del entorno y del reto de movilizarse en aún en medio de la volatilidad y ambigüedad de los sectores de negocio.

En consecuencia, se presenta este documento que analiza la gestión de riesgo tradicional y la propia de los seguros, para plantear una propuesta de gestión de riesgo basada en complejidad e incertidumbre como respuesta a la inestabilidad del entorno y la necesidad de las empresas para proponer nuevas propuestas de negocio, que cambien las reglas de juego en su sector específico y afecte la dinámica de la industria particular capitalizando las cambiantes expectativas de los clientes.

Por tanto, este artículo para dar cuenta de sus reflexiones se organiza de la siguiente manera: en la sección 2 se presenta una revisión de la gestión de riesgo actual detallando los elementos del modelo tradicional y el de seguros, para luego repensar en la sección 3 la gestión de riesgos desde la complejidad y la incertidumbre, el cual se ilustrará, en la sección 4, su aplicación en el contexto de la seguridad de la información y la ciberseguridad, para finalmente plantear algunas reflexiones finales y conclusiones en la sección 5.

2. La gestión del riesgo actual: modelo tradicional y modelo de los seguros

Los modelos de gestión de riesgos, sin perjuicio de los estándares disponibles a la fecha como pueden ser ISO 31000 y la AS/NZ 4360, en la actualidad responden a dos prácticas consolidadas. Una basada en *probabilidad e impacto*, de ahora en adelante modelo tradicional, donde el juicio de expertos y la posibilidad de valoración permiten una vista ágil de posibles eventos inesperados y una forma de tomar acción frente a ellos. Generalmente este ejercicio reviste de una actuación colegiada donde se concreta una visión o postura sobre el tratamiento de los riesgos particularmente conocidos, la cual termina informada a los ejecutivos de la empresa.

La otra, basada en *frecuencia y severidad*, de ahora en adelante modelo de los seguros, que ha sido ampliamente utilizada por la industria de los seguros para evaluar los siniestros, establece la cuantificación del daño para definir el monto de la indemnización a pagar por la materialización de los riesgos. Este ejercicio generalmente se encuentra asistido de estadísticas y modelos matemáticos que crean perfiles de eventos, comportamientos y prácticas, que permiten evaluar los impactos de los riesgos basados en simulaciones y correlaciones de posibles condiciones que generen los eventos adversos (Freund & Jones, 2015).

Estos dos modelos están fundados en premisas diferentes que pueden ser alineadas con el fin de aumentar la capacidad de los analistas de riesgos de las organizaciones y de las personas, para movilizar acciones no solo preventivas sino anticipativas que le permitan moverse con mayor celeridad en un entorno cada vez más inestable y complejo como el actual.

El modelo tradicional de riesgos se desarrolla bajo al menos tres premisas básicas:

- Reconocer las actividades o prácticas que no se están ejecutando adecuadamente.
- Sensibilizar a la organización de los impactos que se pueden tener del evento no deseado.
- Establecer una forma sencilla y expedita de valorar y priorizar los esfuerzos.

En este sentido, esta propuesta cotidiana está orientada al quehacer diario de la persona o empresa, que busca el aseguramiento de comportamientos y prácticas que lleven a la ejecución de procesos donde se puedan prever los resultados planeados y tener "control" de las condiciones en los cuales se ejecutan las actividades de las personas y las empresas.

La respuesta natural al modelo tradicional de riesgos son los sistemas de gestión de calidad, que buscan asegurar un resultado concreto, para lo cual el ciclo planear, hacer,

verificar y actuar, funciona como marco de acción que permite un camino cierto para tener un producto o servicio con unas características específicas y requeridas. En estos sistemas, cuando no se tiene el resultado esperado, se activa el concepto de análisis causa-raíz, que pregunta por aquellos elementos que no se han tenido en cuenta y que sacan el resultado obtenido de las especificaciones definidas para el producto o servicio (González & Arciniegas, 2016).

La ilusión del control es la limitación fundamental del modelo tradicional de riesgos. Esto es, entender el riesgo como una amenaza que se debe controlar y dilatar en el tiempo, habida cuenta que ella compromete alguna de las variables claves del negocio y puede afectar su continuidad en el mediano y largo plazo (Cano, 2015).

De otro lado, la propuesta de gestión de riesgos asociada con el modelo de los seguros se funda en al menos los siguientes tres interrogantes:

- ¿Realmente el riesgo materializado responde a un evento fortuito?
- ¿Se ha tenido el debido cuidado requerido para que el evento adverso no se presentara?
- ¿Los perjuicios evidenciados son cuantificables para ser resarcidos?

La respuesta a estos interrogantes busca comprender no solamente las prácticas actuales de la persona u organización, sino su nivel de prevención acerca de la exposición a situaciones no deseadas, la forma como mantiene la monitorización de su entorno y sobremanera, la responsabilidad particular y global para saber qué deben hacer y cómo indemnizar cuando los efectos de la materialización de los riesgos alcanzan sus grupos de interés internos y externos.

El modelo de los seguros se diferencia del modelo tradicional en el particular énfasis que tiene en las prácticas y estándares que usa la persona o las organizaciones, como quiera que las mismas establecen un patrón de comportamiento que puede ser validado y valorado respecto de eventualidades que se puedan presentar en el ejercicio de la gestión de los riesgos, las cuales pueden afectar la cultura, las operaciones y los comportamientos de los individuos.

De acuerdo con lo anterior, el modelo de riesgos de los profesionales de los seguros se encuentra ajustado con la práctica de cumplimiento, donde la organización mantiene al menos cuatro (4) elementos en ejecución permanente: a) desarrolla una cultura de prevención alrededor del cuidado del modelo de generación de valor, b) gestiona los riesgos propios de su práctica de negocio, c) asegura la operación de sus procesos de negocio y d) consulta las buenas prácticas nacionales e internacionales que le son pertinentes a su negocio (Cano, 2013; Interligi, 2010).

Esta visión desde la práctica de los seguros tiene como limitación el convencimiento que el cumplimiento de estándares, prácticas y regulaciones asegura un nivel de control adecuado y la responsabilidad de la empresa o persona frente a eventuales eventos adversos. Dicha perspectiva de la gestión de riesgo, entiende el riesgo como una falla en los comportamientos de las personas (sin considerar el contexto del evento), que deben ser ajustadas y adoctrinadas para cambiar sus acciones de cara a la prevención de un evento no deseados que aumente la confiabilidad de los resultados (Lanz, 2017).

Como se puede advertir, estos dos modelos, no refieren prácticas o preguntas sobre anticipar situaciones desconocidas (De Jong, 2015), explorar inestabilidades del entorno (Charan, 2015), simular eventos o tendencias identificadas, detectar riesgos latentes, focales o emergentes, ni propuestas para el desarrollo de habilidades y capacidades analíticas para las personas con el fin de contar con un marco de decisiones mejor informadas.

En este sentido, si bien cada perspectiva de la gestión de riesgos detallada ofrece ventajas y oportunidades evidentes, se hace necesario efectuar ajustes claves que permitan asumir el entorno volátil, incierto, complejo y ambiguo (Johansen, 2009) que se tiene a la fecha, como una forma de construir una "ganancia teórica" que enriquezca la práctica de gestión de riesgos disponible a la fecha y haciéndola más dinámica y resiliente frente a eventos contrarios o inesperados.

En este contexto, se plantea un modelo alterno, que conjugando las bondades tanto del modelo tradicional como del modelo de los seguros, permite concretar una vista más ajustada con la dinámica del entorno actual, con el fin de asegurar un ejercicio de gestión riesgos más cercano a las condiciones complejas e inciertas que se tienen a la fecha y motivar acciones proactivas que den cuenta de los escenarios posibles que amenacen la participación y estrategias de las empresas y las personas.

3. Repensando la gestión de riesgos: incertidumbre y complejidad

Una aproximación conceptual para fusionar estas dos vistas de la gestión de riesgos (modelo tradicional y modelo de los seguros) con el fin de darle mayor profundidad y dinamismo en las organizaciones y en la práctica de la persona recaba en tres fundamentos base a saber:

- Incluir tanto probabilidades como posibilidades como base de la exploración y comprensión del entorno.
- Aumentar la capacidad analítica y exploratoria de inestabilidades y rarezas que permitan adaptar y ajustar la lectura vigente del entorno.
- Plantear escenarios posibles y probables que prioricen los esfuerzos y capitalicen los intereses de la organización.

Estas tres declaraciones configuran un marco renovado de la gestión de riesgos que ahora tiene como base dos fundamentos: la incertidumbre y la complejidad. En este sentido, la propuesta metodológica entiende la incertidumbre como "el estado de indeterminación entre una causa y sus efectos" y la complejidad como el "resultado de la limitada capacidad para distinguir aspectos concretos de la realidad, que superan los saberes previos de los observadores" (Rosa, Renn, & McCright, 2014).

Así las cosas, se establecen cuatro (4) cuadrantes donde cada uno configura un escenario, que está compuesto de evento no deseado más un contexto. Lo anterior define cuatro lecturas como se observa en la figura 1:

Para los escenarios I y II donde la complejidad es baja, lo que se requiere de la organización o de la persona es responder, dado que se tiene conocimiento previo de la situación y es posible concretar acciones y explorar prácticas que se ajusten a los estándares vigentes para tratar el incierto que se puede generar frente a un evento en



Figura 1 – Visión extendida de la gestión de riesgos. Elaboración propia.

un contexto medianamente conocido. La respuesta se puede configurar siguiendo los referentes conocidos y las lecciones aprendidas previas que pueda tener la organización o la experiencia propia de una persona.

Para los escenarios III y IV donde la complejidad es alta, lo que se demanda de la empresa o la persona es aprender rápidamente, cuestionando los saberes previos que se tengan sobre las características de la situación en estudio. Para ello, se requiere probar con prototipos y simular con condiciones semejantes, con el fin de capitalizar ágilmente "errores brillantes" (Schoemaker, 2011), esos cuyo potencial de valor es muy alto y son de bajo costo para la empresa.

De esta manera la organización o la persona, tendrá mayores oportunidades de moverse con menos incierto y mayor confiabilidad, dado que han podido desarrollar pronósticos más confiables sobre los efectos o consecuencias de las acciones que pueden desarrollar. Sin perjuicio de este ejercicio, es claro que la inevitabilidad de la falla hará su aparición, por lo tanto la gestión de los incidentes será una práctica debidamente asegurada y probada para dar cuenta de la capacidad de respuesta que la organización tiene frente a eventos no planeados o inesperados (Kaplan, Bailey, O'Halloran, Marcus, & Rezek, 2015).

Así las cosas, la gestión de riesgos debe evolucionar de una práctica estándar que las organizaciones y las personas desarrollan frente a su entorno, a una capacidad organizacional y personal que le permita habilitar y mantener comportamientos: actividades, interacciones y decisiones (Hemerling, Bhalla, Dosik, & Hurder, 2016), para lograr movilizar los resultados de la empresa y la protección de su promesa de valor en el mediano y largo plazo.

Es decir, cambiar un ejercicio de procedimientos y formatos que transmiten conocimiento sobre la realidad que se estudia (práctica), a construir conocimiento y capitalizar "ganancias teóricas y prácticas" (capacidad) frente a un contexto siempre inestable y dinámico, que demanda aprender rápidamente para mantener a la organización fuera de su propio status quo.

4. Aplicando el nuevo marco riesgos propuesto en seguridad de la información y ciberseguridad

Para comprender esta propuesta de gestión de riesgos extendida, se tomarán tres eventos relevantes en seguridad de la información y ciberseguridad que han ocurrido recientemente y un nuevo pronóstico sobre usos inadecuados de la inteligencia artificial, con el fin de mirar algunas de las bondades y limitaciones de esta nueva aproximación.

El primer evento es el ciberataque que se realizó a la empresa *Target*. Los detalles de este caso establecen un contexto de alto nivel de volúmenes de transacciones para la empresa por temporada navideña a través de los sistemas POS (*Point of Sales*), donde se produce una brecha de seguridad a través de un punto de conexión configurado para efectuar mantenimientos de forma remota a los equipos de aire acondicionado, que habilita el ingreso de un código malicioso que termina con un robo masivo de información de tarjetas de crédito y débito que afectó a 70 millones de clientes aproximadamente (Radichel, 2014).

Frente a este caso, siguiendo la propuesta conceptual se puede advertir una complejidad baja, dado el conocimiento de la empresa respecto de la verificación de las prácticas y procedimientos de seguridad y control para conexiones remotas, y por otro lado, una incertidumbre baja dado que no es la primera vez que una temporada llega y el aumento de transacciones se tiene previsto dentro del ciclo operativo de la empresa (Escenario I). En este caso, el evento que materializa el ciberataque es una práctica inadecuada de seguridad y control de los terceros en sus conexiones remotas.

La falla en la práctica de aseguramiento de las conexiones remotas por parte del tercero obliga a Target, a actuar frente a la situación inesperada que se presenta, asegurar la gestión de la seguridad con los terceros de confianza y responder frente al incidente que se materializa. Esta situación que por demás es una falla en sí misma de la gestión, lleva un análisis de responsabilidades donde la frecuencia y la severidad de los hechos confirman la posible cuantificación del daño y los impactos sobre los grupos de interés para efectos de su indemnización.

El segundo evento es el caso de *Sony Corporation*, donde se plantea una compaña de seguimiento y toma de control de los recursos computaciones vía engaños como el phishing a personal clave de la empresa. Este tipo de actividades, trabajan de forma silenciosa, mientras avanzan en la conquista de la infraestructura tecnológica, hasta concretar un evento detonante que genere inestabilidad y caos en la operación de la empresa (Sánchez, 2015).

Este caso a la luz de la propuesta presentada, es un Escenario II, dado que la complejidad es baja, dado que el conocimiento sobre las técnicas iniciales para lograr el ataque son conocidas; con una incertidumbre alta, dado el lanzamiento inminente de la firma de un nuevo producto digital donde no se tenían claras las expectativas de operación del mismo ni existen antecedentes o experiencias de proyectos similares. En este caso, el malware implantado de manera silenciosa y su capacidad para producir daño y toma de control, es lo que determina la potencia y efectividad del ataque.

La capacidad destructora del malware y el éxito de la campaña de inteligencia que se efectuó sobre la empresa y sus productos, demanda de Sony responder al ataque en

curso, explorar y comprender las capacidades de los atacantes y sus motivaciones, para finalmente analizar su postura de seguridad vigente para establecer sus nuevos normales de operación. Esta situación lleva a revisar el detalle la cultura de seguridad y control de la organización, las prácticas de seguimiento y auditoría vigentes, que permitan conocer el debido cuidado de la organización como aspecto clave de la responsabilidad que asume frente sus grupos de interés internos y externos. Una postura que corresponde con las prácticas de cumplimiento organizacional.

El tercer evento para analizar es el ataque a las centrifugadoras de las plantas de uranio enriquecido de Irán. Una acción ofensiva que se concentra en estudiar detalladamente el funcionamiento de un controlador lógico programable de una marca conocida, para desarrollar un código capaz de tomar control de los objetos que este controla y causar una daño evidente a su operación. Este caso habla de una campaña de espionaje y desestabilización de una nación para demorar un programa de armas nucleares (Kushner, 2013).

Este ciberataque leído en la nueva propuesta de gestión de riesgo, exhibe una alta complejidad, dado el nivel de conocimiento que se tuvo que desarrollar para poder comprometer la operación del controlador y una incertidumbre baja, como quiera que el efecto del código malicioso siempre es comprometer y producir un daño sobre la infraestructura que afecta (Escenario III), particularmente en esta situación, afectar un objeto que se controla de forma remota con un flujo de control especializado.

La vulnerabilidad de la infraestructura crítica de la planta de uranio enriquecido, considerando las afectaciones devastadoras de un accidente radioactivo en el área, exige de Irán probar dicha infraestructura ante situaciones semejantes, adaptar sus sistemas de seguridad y control frente al aumento de la exposición de los sistemas de control industrial y aprender de las nuevas reglas de la geopolítica global que ahora se concretan a través de acciones cibernéticas conocidas y desconocidas. Este evento lleva a reconocer e incluir a los sistemas de control industrial como elementos susceptibles de prácticas de seguridad y control, para lo cual es necesario aumentar la resiliencia de dichas instalaciones y operaciones (Cano, 2016).

Finalmente se tiene un reciente pronóstico que habla del uso de la inteligencia artificial para crear ataques inesperados sobre las infraestructuras de las empresas y los países, que utilizando las características propias de su tráfico, logran simular su operación normal, evadiendo los sistemas de monitoreo, aumentado la efectividad del daño o compromiso sobre el sistema afectado. Este contexto, insinúa el mal uso de los algoritmos de aprendizaje profundo para superar las capacidades de detección y alerta vigentes en la actualidad (Yampolskiy, 2017).

Si se revisa este pronóstico a la luz de la propuesta de riesgos planteada, es un escenario IV, donde se tiene una situación de alta complejidad que supera por mucho los conocimientos que se tienen a la fecha sobre el uso de los algoritmos de aprendizaje profundo, creando una condición de alta incertidumbre, dado que no es posible anticipar o pronosticar los efectos que estos malos usos pueden tener. Así las cosas, los eventos que se materialicen por este escenario no son previsibles ni imaginables a la fecha, y sus impactos posiblemente serán muy altos y adversos.

Para dar cuenta de este escenario, el modelo sugiere que se debe simular una situación como la descrita, para comenzar a identificar patrones que permitan su detección, anticipar nuevas prácticas de monitoreo basados en confusión y suplantación de patrones de operación, con el fin de aprender rápidamente de las posibilidades que ofrecen estas nuevas tecnología cognitivas. Un ejercicio que podríamos llamar de contrainteligencia cognitiva que sea capaz de inferir usos inapropiados de los algoritmos sin despertar sospecha en el proceso de aplicación de los algoritmos de aprendizaje y detección.

Como se puede observar en el análisis de los tres eventos y el pronóstico, es posible contar con una vista enriquecida y extendida de la gestión de riesgos conectada con el entorno vigente. Incorporar a la lectura de los riesgos los elementos de incertidumbre y complejidad demanda de los analistas de riesgos una capacidad de valoración que no solo incluye frecuencia, severidad, probabilidad e impacto, sino la exigencia de calzarse los zapatos de los atacantes, recrear su habilidad para crear las condiciones del daño en escenarios específicos, que deben conectar la operación de la empresa, su contexto de negocio, así como sus objetivos estratégicos.

Este modelo alterno presentado si bien sugiere una forma diferente de asumir el reto de los riesgos, tiene limitaciones en su aplicación habida cuenta que requiere de información confiable de las estadísticas de eventos adversos, análisis de tendencias del entorno de negocio y laboratorios de simulación que permitan habilitar la ventana de aprendizaje que se demanda para concretar una gestión de riesgos que desconecta los supuestos vigentes de los eventos adversos, incorpora las nuevas condiciones del entorno y crea nuevas distinciones que cambian la forma de entender y aprovechar los riesgos.

5. Conclusiones

Cambiar la forma como se adelanta la gestión de riesgos establece un quiebre al status quo de la práctica actual, que incomoda y obliga tanto a las organizaciones como a las personas a un ejercicio permanente de pronóstico, capitalización de lecciones aprendidas y reconocimiento del error como ocasión de aprendizaje, en otras palabras, el desarrollo de una capacidad.

Actualizar la práctica actual de gestión de riesgos supone un reconocimiento de un entorno volátil, incierto, complejo y ambiguo, que debe retar los saberes previos alcanzados hasta el momento, para dar paso a la creación de escenarios más elaborados que permitan mirar con mayor detalle las posibilidades y así darle mayor sentido a las probabilidades. Es decir, superar los sesgos cognitivos particulares como son entre otras, mirar el corto plazo, olvidar rápidamente las lecciones del pasado, subestimar las posibilidades, mantener la condición actual, simplificar de forma selectiva y hacer selecciones basadas en observaciones de otros (Meyer & Kunreuther, 2017).

En este sentido, el modelo alterno de gestión de riesgo desarrollado en este documento, busca sugerir una forma diferente de estudiar y comprender los riesgos, más allá del tratamiento tradicional que se tiene bajo los estándares conocidos a la fecha. Una apuesta conceptual y académica que no busca desconocer los logros de la práctica actual, sino

complementar y aumentar la capacidad de acción de las mismas, para darle mayores elementos de actuación a las organizaciones y las personas.

La incertidumbre y las complejidad son dos conceptos que deben ser ahora parte natural de la práctica empresarial de las organizaciones, como quiera que son dos elementos que se encuentran constantemente en el proceso de toma de decisiones corporativas, que afectan su promesa de valor para sus grupos de interés y cambian los patrones de comportamiento de los diferentes actores del entorno de negocio donde ella participa.

Por tanto, la gestión de riesgos extendida que se plantea establece una base conceptual para repensar las actividades actuales frente a los diferentes escenarios que deben asumir las empresas, sin perjuicio de las necesarias preparaciones y procedimientos que se deben mantener para enfrentar y manejar la materialización de eventos inesperados o no planeados, como una forma natural de responder ante la inevitabilidad de la falla (Smith, 2017).

Los riesgos no deben ser ocasión de una revisión o carga negativa en sus análisis, sino una ventana de oportunidad que aumente la capacidad de la organización para aprender y/o desaprender de sus propias prácticas empresariales, y así fundar un escenario de armonía entre la inevitabilidad de la falla y las objetivos estratégicos, que la lleve al desarrollo de una resiliencia corporativa que la proyecte un paso adelante, a pesar de sus posibles eventos adversos materializados a lo largo de sus actuaciones en su ambiente de negocio.

En consecuencia, el modelo alterno de gestión de riesgos propuesto configura una nueva frontera para la gestión de riesgos que no solo vincula los resultados de los sistemas de gestión de la calidad y el aseguramiento de las buenas prácticas en la operación de las empresas, sino que abre la posibilidad para pensar hacia adelante y crear entornos de revisión y análisis que superen las sesión tradicionales de *feedback* o retroalimentación, necesarias para saber qué ha ocurrido, y se complementen con momentos de *feedforward* o alimentación hacia adelante, para explorar qué cosas pueden pasar y cómo actuar frente estos eventos.

Agradecimientos

El autor hace un especial reconocimiento a los doctores Javier González Rodríguez de la Escuela de Administración de la Universidad del Rosario y Jorge Ramio Aguirre de la Universidad Politécnica de Madrid, por sus acertados y valiosos comentarios que permitieron afinar las reflexiones planteadas en este artículo.

Referencias

Aon (2017) Aon's 2017 Global Risk Management Survey. Recuperado de: http://www.aon.com/2017-global-risk-management-survey/

Cano, J. (2013) La Inseguridad de la Información: Motivador de la Práctica de Cumplimiento Corporativo. *ISACA Journal*. (6). Recuperado de: https://www.isaca.org/Journal/archives/2013/Volume-6/Pages/Information-Insecurity-Motivator-of-Corporate-Compliance-Practice-Spanish.aspx

Cano, J. (2015) Entorno VICA. La incertidumbre y los bloqueos de un CISO. *Blog IT-Insecurity*. Recuperado de: http://insecurityit.blogspot.com.co/2015/05/entorno-vica-la-incertidumbre-y-los.html

Cano, J. (2016) Ciber ataques. La inestabilidad de lo que hemos aprendido en seguridad y control. *ISACA Journal*. (5). Recuperado de: https://www.isaca.org/Journal/archives/2016/volume-5/Pages/cyberattacks-the-instability-of-security-and-control-knowledge-spanish.aspx

Charan, R. (2015) *The attacker's advantage. Turning uncertainty into breakthrough opportunities*. New York, USA: Perseus Books Groups.

De Jong, R. (2015) *Anticipate. The art of leading by looking ahead*. New York, USA: AMACON.

Frappolli, M. (2015) *Managing cyber risk*. Malvern, Pennsylvania. USA: American Institute for Chartered Property Casualty Underwriters.

Freund, J. & Jones, J. (2015) *Measuring and managing information risk. A FAIR Approach*. Kidlington, Oxford. UK: Butterworth-Heinemann

González, O. & Arciniegas, J. (2016) *Sistemas de gestión de la calidad. Teoría y práctica bajo la norma ISO 2015*. Bogotá, Colombia: Ecoe Ediciones.

Hemerling, J., Bhalla, V., Dosik, D. & Hurder, S. (2016) Building capabilities for transformation that last. *Boston Consulting Group – BCG*. June. Recuperado de: https://www.bcgperspectives.com/content/articles/transformation-large-scale-change-people-organization-building-capabilities-transformation-that-lasts/

Interligi, L. (2010) Compliance culture: A conceptual framework. Journal of *Management & Organization*. 16. 235–249.

Johansen, B. (2009) *Leaders Make the Future: Ten New Leadership Skills for an Uncertain World*. San Francisco, USA: Berrett-Koehler Publishers.

Kaplan, J., Bailey, T., O'Halloran, D., Marcus, A. & Rezek, C. (2015) *Beyond cybersecurity. Protecting your digital business*. Hoboken, New Jersey. USA: Wiley

Kushner, D. (2013) The Real Story of Stuxnet. How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program. *IEEE Spectrum*. Recuperado de: https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

Lanz, J. (2017) Aligning cybersecurity strategy and performance with updated COSO ERM guidance. *CSO Online*. September. Recuperado de: https://www.csoonline.com/article/3227050/risk-management/aligning-cybersecurity-strategy-and-performance-with-updated-coso-erm-guidance.html

Meyer, R. & Kunreuther, H. (2017) *The Ostrich Paradox. Why we underprepare for disasters*. Philadelphia, USA: Wharton Digital Press.

Radichel, T. (2014) Case Study: Critical Controls that Could Have Prevented Target Breach. *SANS Institute*. InfoSec Reading Room. Recuperado de: https://www.

sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412

Rosa, E., Renn, O. & McCright, A. (2014) *The risk society revisited. Social theory and governance*. Philadelphia, Pennsylvania. USA: Temple University Press.

Sánchez, G. (2015) Case Study: Critical Controls that Sony Should Have Implemented. *SANS Institute*. InfoSec Reading Room. Recuperado de: https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-sony-implemented-36022

Schoemaker, P. (2011) *Brilliant mistakes. Finding success on the far side of failure*. Philadelphia, USA: Wharton Digital Press.

Smith, G. S. (2017) Emergency business management and internet connectivity. *Business Horizons*. 60. 353—361

Yampolskiy, R. (2017) AI is the Future of Cybersecurity, for Better and for Worse. *Harvard Business Review*. May. Recuperado de: https://hbr.org/2017/05/ai-is-the-future-of-cybersecurity-for-better-and-for-worse

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 09/09/2017
Aceitação/Acceptance: 24/03/2018

Guerras del Futuro: Causas y Estrategias

Marco Salinas Haro[1]

marsalin7@gmail.com

[1] Centro de Estudios Estratégicos-Marítimos, Academia de Guerra Naval, Guayaquil, Ecuador.

Pages: 88–99

Resumen: Este ensayo busca revisar el pasado y reconocer las posibles causas de las guerras futuras, enfocadas en el crecimiento poblacional, lo que ocasionará codicia de los recursos; así como los principios y procedimientos a ser utilizados por los estrategas de esa época. En tal virtud y considerando la realidad regional, propone la creación de una Fuerza de Tarea Regional Marítima, FTRM, "De llamada" que pueda neutralizar los impactos del escenario de la "Tormenta perfecta del 2030", respecto a la seguridad y protección marítima.

Palabras-clave: Guerras del futuro; estrategia; competencia por recursos.

Future Wars. Causes and Strategies

Abstract: This paper seeks to review the past and identify the possible causes of wars, focused on the population growth that will cause disputes over resources; as well as the principles and procedures to be used by the strategists of that time. In this virtue and considering the regional reality, it proposes the creation of a Maritime Task Force, FTRM, "On call" that can neutralize the impacts of the "perfect storm of 2030", regarding to maritime safety and security.

Keywords*:* Future wars; strategy; disputes over resources.

1. Introducción

En el marco de la teoría de las Relaciones Internacionales, el sistema internacional demuestra que algunos estados viven en una situación de tensión, respecto a la seguridad y defensa de intereses contrapuestos. Los mismos actores tratan de manejar las crisis, a través de acciones políticas, diplomáticas, económicas y militares; el mejor medio para el último componente es la Fuerza Naval, por su flexibilidad, capacidad de permanencia y proyección hacia áreas marítimas de interés en disputa. Cuando el manejo político de la crisis fracasa, empieza la fase del conflicto o guerra.

La evolución de la humanidad en cuanto a sociedad, trabajo y tecnología, ha configurado la Seguridad y Defensa de los reinos, imperios, estados-nación, o cualquier otra forma de organización política. El futuro proyecta incertidumbre en cuanto a los escenarios preferibles que se presenten a nivel mundial, regional y nacional. Todos los que somos

parte del estado tenemos la obligación moral de analizar el pasado, diagnosticar el presente y proyectar el futuro, de esta manera asegurar el bienestar de las nuevas generaciones. Seguridad y Defensa son conceptos fundamentales que todo ciudadano debería conocer, "(…) la Defensa es un componente del Sistema de Seguridad Pública y del Estado y de la Seguridad Integral esto supone que el objetivo de la defensa es contribuir en la consecución del bienestar de las ciudadanas y los ciudadanos y al desarrollo de la sociedad con sus medios y su contingente" (Ministerio de Defensa, 2014).

En Ecuador se está desarrollando la prospectiva estratégica, lo que permite aprovechar oportunidades y/o contener riesgos a tiempo "Por ello, los países latinoamericanos deben conocer y elaborar escenarios globales a largo plazo y avizorar el tipo y magnitud de los desafíos, riesgos y oportunidades que podrían enfrentar (…)" (Bitar, 2014).

El propósito del presente ensayo es reconocer académicamente, cuáles serían las causas de las guerras futuras, así como los principios y procedimientos de la estrategia, a ser aplicados, en base a la evolución del desarrollo de la tecnología, sociedad y trabajo, considerando los factores de riesgo y amenazas. Está concebido para aquellos lectores que no son especialistas o que no conocen la guerra y estrategia de manera profunda, especialmente para políticos, académicos y lectores en general, interesados en el tema.

2. Guerra y Futuro

Las variables más importantes del tema son "la guerra" y el "futuro", por lo que a continuación se definen sus conceptos:

Según el legendario estratega Chino Sun Tzu (2001) hace 400 años A.C dijo "La guerra es un asunto de importancia vital, para el estado, es la provincia de la vida o la muerte (…)". Para el general prusiano Clausewitz (1978) que nació en 1780 y murió en 1831 "La guerra es la continuación de la política por otros medios". Finalmente para el profesor Khan (2017) que nació en Estados Unidos en 1922 y falleció en 1983, indicó que "La guerra debe ser controlada, practicar la disuasión y evitar la escalada", fue un gran colaborador en el desarrollo de las estrategias nucleares de Estados Unidos.

La guerra es un concepto muy discutido entre "apologistas" y los "negadores" de la guerra, lo que sí es un hecho, que desde la paz de 1945 a la fecha, se han vivido aproximadamente 200 conflictos bélicos en más de sesenta países. Los apologistas de la guerra refuerzan sus convicciones a través del realismo y con datos como los siguientes. "(…) sin embargo, tendencialmente, y comparando con el período entre 2007 y 2013, se han registrado más enfrentamientos armados en los últimos tres años (…) 2016 fue el año más violento de las últimas tres décadas" (Aguirre, 2017).

Mientras tanto los negadores siguen confiando en la paz a través del idealismo y de organizaciones internacionales. En 2016 la Organización de las Naciones Unidas, ONU, estableció en la Agenda de Desarrollo Sostenible el Objetivo 16 para ser alcanzado en el 2030, que dice "(…) en la promoción de sociedades pacíficas e inclusivas para el desarrollo sostenible, la provisión de acceso a la justicia para todos y la construcción de instituciones responsables y eficaces a todos los niveles" (Gil, 2014).

La segunda variable por considerarse es el futuro, proviene del latín futūrus, el futuro es aquello que está por venir. En una hipotética línea del tiempo, el pasado se encuentra

detrás del presente, mientras que el futuro aparece adelante, es decir todavía no ha sucedido (definición.de, 2008). La prospectiva estratégica, enseña que pueden darse varios futuros entre los cuales están los posibles, probables y preferibles; constituyendo la visión, el escenario preferible que se desea alcanzar.

Un buen referente para analizar el "futuro" es Alvin Toffler (1980), a quién se le considera como el más influyente futurólogo de nuestros días, sus obras traducidas a más de 30 idiomas, han obtenido unánime reconocimiento internacional por sus importantes aportaciones a las ciencias sociales. Es pertinente aplicar el pensamiento de este sociólogo basados en su libro "La Tercera Ola", para reconocer la evolución de la sociedad, la tecnología y el trabajo; el estudio segmenta al tiempo en tres períodos: La primera ola llamada de la agricultura desde aproximadamente 8000 A.C hasta 1600 D.C. La segunda ola denominada industrial desde aproximadamente 1650, hasta 1950, y finalmente la tercera ola del conocimiento empieza a mediados de 1950, hasta nuestros días. En cada cambio de ola, se produjeron grandes guerras y revoluciones, hechos políticos, evolución tecnológica y desarrollo económico; produciendo cambios profundos en la sociedad, especialmente en su modo de trabajo y calidad de vida.

3. Evolución de la Estrategia

Existen varios niveles de estrategia, la primera se le llama "gran estrategia", o también conocida como "política"; el segundo nivel de la estrategia se denomina "estrategia general" y abarca a la estrategia: económica, diplomática, social, militar y marítima; en el tercer nivel se encuentran las "estrategias particulares" que son: terrestre, naval y aérea; finalmente en el escalón más bajo se encuentra la táctica. Con esta base teórica se trata de analizar la evolución de la Estrategia Militar y Marítima, que por su naturaleza compleja, podría ser susceptible a opiniones diversas muy respetables.

En la ola de la agricultura la guerra era eminentemente de concepción terrestre, aunque existían armadas respetables como la griega y romana, las guerras se decidían en tierra. En sus inicios los ejércitos lo conformaban mercenarios, luego fueron remplazados por personal profesional, a éstas guerras se las denomina de primera generación. El general Chino Sun Tzu podría ser uno de los estrategas terrestres en el contexto del tiempo, la esencia de su pensamiento se basa en el engaño, y en ganar las guerras sin combatir, muy discutible, pero la historia nos evidencia que sus principios fueron aplicados en la guerra de Vietnam por parte del Vietcong, la única guerra que ha perdido los Estados Unidos con un saldo de 51000 muertos (Jorge, 2016). En esta ola el uso del mar era utilizado como vía de comunicación, fuente de alimento y era unidimensional, solamente en la superficie. Se producen guerras navales de relevancia para la supervivencia de los imperios como la de Trafalgar, que marcó la supremacía inglesa en desmedro de la francesa y española.

Al iniciar la ola industrial, el Contralmirante Mahan de los Estados Unidos escribió sobre Estrategia Marítima, ya que anteriormente solo se conocía de Táctica Naval; con el desarrollo del avión se origina la Estrategia Aérea basada en el pensamiento de Dohuet. Con las tres estrategias se materializan, los conceptos de operaciones combinadas y conjuntas; así en la Segunda Guerra Mundial, se produce por parte de los Aliados la proyección estratégica más grande de la historia mediante el "Desembarco de

Normandía", que fue el preludio para el fin del nazismo. En la ola industrial la guerra en el mar es tridimensional con el empleo del submarino y avión. Los esfuerzos para la guerra y los productos que generan las grandes fábricas son transportados por grandes buques mercantes siguiendo líneas de comunicaciones marítimas que se enlazan con grandes ciudades portuarias. En esta etapa a la guerra se le llama de segunda y tercera generación, ya que el personal combatiente es permanente, profesional y las fuerzas militares tienen gran poder de fuego con gran velocidad de maniobra, respectivamente.

En la ola del conocimiento, la seguridad y defensa está completamente enmarcada por el Derecho Internacional; aparece una nueva dimensión en la guerra en el ciberespacio; los niveles estratégico, operacional y táctico, se basan en guerreros digitales, con conocimientos especializados en novedosas tecnologías de la información, TIC. Nuevamente los factores de alcance, velocidad y letalidad se elevan exponencialmente en relación a la primera y segunda ola. La letalidad de las armas nucleares es preocupante si se alcanza el nivel de destrucción mutua asegurada en una conflagración nuclear. Desde el punto de vista de la estrategia militar, es interesante y necesario tomar como referencia la guerra del Golfo Pérsico, enfrentando a Irak y una Coalición liderada por los Estados Unidos; el uso de la tecnología en esa guerra, fue de extraordinaria precisión alcance y velocidad, por lo que el empleo de los medios modernos con alta interoperabilidad, contribuyó de manera decisiva a favor de la Coalición. La difusión en directo de la CNN, marcó un hito para las operaciones de la información. En las primeras acciones, el Poder Aéreo de Estados Unidos lanzó más de 3.000 bombas guiadas de precisión y misiles sobre las defensas iraquíes, el efecto deseado era desactivar los sistemas de comando y control enemigo (Monge, 2003). Tiempo después, aparece la guerra llamada de cuarta generación o asimétrica, "(...) en un escenario de guerra contra el terrorismo iniciada por George W. Bush y un creciente antiamericanismo en la mayoría del mundo árabe" (Monge, 2003).

Históricamente los medios empleados en la guerra, han dependido de la evolución de la tecnología durante las tres olas, el factor acelerador ha sido definitivamente la energía; en la primera ola era el fuego en base a la madera; en la segunda ola fue el uso del carbón que disparó la Revolución Industrial con la máquina de vapor, posteriormente el uso del aceite de la ballena como energía para iluminar las nuevas ciudades, la caza de ballenas casi exterminó a esta especie; en 1901 el descubrimiento del primer pozo de petróleo en Texas permitió desarrollar la máquina de combustión interna que originó la industria automotriz, revolucionando el modo de vida y de hacer la guerra; hasta que en 1945 en Hiroshima se prueba la energía nuclear, desencadenando una carrera nuclear de las grandes potencias, a niveles desmesurados. En la actualidad, pese a los esfuerzos de uso de energía alternativa, el petróleo se mantiene como la fuente principal de energía a nivel global y los estados-nación muchas veces se han enfrentado por la guerra del petróleo.

Con estos antecedentes que contextualizan la evolución de la guerra, la mayor parte de analistas estratégicos validan que la "Estrategia Terrestre" busca la destrucción del enemigo y la conquista del territorio enemigo, consolidando de esta manera la victoria; la "Estrategia Naval" tiene como propósito el "control del mar" y sus objetivos naturales son la fuerza organizada, la posición y las líneas de comunicación marítimas y como servidumbre se le considera el territorio del enemigo; finalmente la "Estrategia Aérea"

busca el dominio del aire y la destrucción de objetivos estratégicos del enemigo y la defensa de los propios, es quién primero actúa en la cronología de las operaciones conjuntas y/o combinadas (Solís Oyarzún, 1991). Las tres estrategias son relevantes para la seguridad y defensa de un estado, que acorde a los intereses y objetivos nacionales deben ser fortalecidas y mantenidas con personal y medios eficaces y listos para actuar cuando se las requiera, no solamente en crisis y guerra, sino también de manera relevante para el apoyo en desastres naturales, humanitario y otras acciones de soporte al Estado, acorde a la Ley.

Depende de la actitud estratégica de los actores del conflicto para la concepción y planificación de las maniobras: estratégica, operacional y táctica. Los principios de la guerra clásicos, han sido aplicados desde las guerras A.C. hasta nuestros días, entre ellos tenemos: el objetivo, unidad de mando, ofensiva, concentración, sorpresa, economía de fuerzas, simplicidad y otros, estos han permanecido en el tiempo, son inmutables, lo que sí han cambiado con la evolución de la tecnología, sociedad y trabajo, son los procedimientos de empleo de los modernos medios con alta tecnología.

4. Causas de las Futuras Guerras y Estrategias

El escenario futuro mundial que se prevé para el 2030, se denomina "la tormenta perfecta", cuyas tendencias probablemente serán: la aparición de estados frágiles frente a los desastres naturales; estados con falta de gobernabilidad generando guerras civiles; un incremento de la población mundial y la continuación de guerras convencionales principalmente de origen: económico, teológico y territorial; la continuación de la guerra contra el terrorismo internacional y narcotráfico y la codicia de recursos vivos y no vivos; entre otros.

Es evidente que con este escenario el mundo necesitará producir: alrededor del 50% más de energía y alimentos; un 30% más de agua de bebida y sobre todo tener las capacidades para mitigar el cambio climático y desastres naturales. Sobre este tema diferentes actores privados y públicos han efectuado estudios como los del Pentágono que pronostican "(…) un hipotético futuro cuya base común denominador sería la escasez alimentaria, de agua o energía" (Gil, 2014). Las conclusiones de los estudios incluido el Vaticano, coinciden en que para el 2030, podría presentarse una "tormenta perfecta" a nivel mundial.

En el futuro, cualquiera sea la naturaleza de la guerra entre estados, los principios y procedimientos que se apliquen reflejará a la sociedad, la tecnología y la forma de trabajo de los actores en conflicto y de sus aliados, en otras palabras la forma de hacer la guerra de un estado demostrará la forma de trabajo del mismo. Sin duda el alineamiento de la trilogía del estratega terrestre Clausewitz, del Gobierno, la Población y las Fuerzas Armadas, impactará positiva o negativamente en los resultados de la crisis o la guerra. Las variables claves para el éxito o fracaso en el estado final deseado de la guerra serán: el presupuesto militar; el manejo de los medios de comunicación; el uso de las tecnologías de doble uso en cuanto a letalidad y precisión; la diferencia cuantitativa y cualitativa entre los recursos políticos y militares, y finalmente, la proliferación nuclear. Las guerras del futuro llevadas a cabo en el espacio y ciberespacio, serán factores a considerar en la concepción estratégica del empleo de los nuevos medios militares, especialmente los nuevos conceptos de "poder blando" y "ciberguerra", cuya armoniosa aplicación

corresponde a las guerras de quinta y cuarta generación, cambiarán la comparación de poderes oponentes en los niveles político, estratégico y operacional.

Los países con alto desarrollo tecnológico ya están preparándose para las guerras del futuro, así tenemos que la Agencia de Proyectos de Investigación Avanzada de Defensa, DARPA, de los EEUU "(...) presentó al Pentágono los cien proyectos que prepara para guerras cibernéticas y campos de batallas llenos de robots y sobre todo software y plataformas digitales" (Infobae, 2014). Estos serán los medios utilizados en las guerras del futuro; el moderno concepto de "big data", mediante la aplicación de algoritmos, marcará la diferencia entre vencedores y vencidos.

5. Organizaciones y Grupos Internacionales.

Desde las guerras del Peloponeso, hasta las guerras presentes y futuras, los poderes hegemónicos y sus aliados, se han apoyado y lo seguirán haciendo, mediante alianzas unidos por intereses comunes.

En la revista online Strategic Culture Foundation se manifiesta que luego de la caída del muro de Berlín en 1989, Washington pensó con extender su dominación en el mundo entero. China, Rusia e Irán, miraron con preocupación esa posibilidad y comprendieron que la unión y cooperación entre sí son las únicas herramientas para hacer frente a un "problema mutuo" (Pieraccini, 2017). "El nuevo Eje está dotado, igualmente, de un poderío militar, capaz de contrapesar, en las áreas de disputa, en el campo naval, terrestre y aéreo, a la Organización del Tratado del Atlántico Norte, OTAN (...)" (Leal, 2016).

En la región, Brasil tomó la iniciativa y lideró la conformación de la Unión de Naciones Suramericanas, UNASUR. Respecto a seguridad y defensa, a través del Consejo de Defensa Suramericano, CDS, vieron la necesidad de "(...) implementar políticas de defensa en materia de cooperación militar, acciones humanitarias y operaciones de paz, industria y tecnología de la Defensa, formación y capacitación" (UNASUR, 2017).

Las numerosas organizaciones internacionales y grupos a nivel mundial, regional y local, tienen diferentes visiones y propósitos, el problema está en el compromiso y responsabilidad para solucionar los grandes desafíos. Como evidencia, en el 2017 en la crisis de pesca ilegal del buque Chino en Galápagos, fue notorio el reclamo internacional y regional, ante la depredación de los recursos vivos en el "Patrimonio Natural de la Humanidad". Algunas organizaciones como la de Agricultura y la Alimentación, FAO y la Sociedad de Conservación Pastor del Mar, Sea Sheperd; se pronunciaron para buscar soluciones al problema, esta última se ofreció patrullar con sus medios en las áreas marítimas para evitar la pesca ilegal en Galápagos, ofrecimiento que no fue pertinente, ya que es responsabilidad del Estado la Soberanía e Integridad Territorial que dicta la Constitución. Un Oficial del Comando de Operaciones Navales de la Armada del Ecuador, manifestó que el área que cubría los aproximadamente 280 pesqueros chinos, en alta mar, era del tamaño de la Provincia del Guayas.

En el caso de América Latina y el Caribe, les une muchos factores de riesgo y amenazas que algunos ya fueron descritos anteriormente, bien podrían ser un elemento aglutinador efectivo respecto a seguridad y defensa, para neutralizar la codicia de los recursos.

La región posee abundantes recursos naturales como por ejemplo: posee el 20% de reservas de petróleo del planeta; concentra casi la mitad de reservas mineras a nivel global, respecto a litio, plata, cobre y estaño; alberga varios de los países más mega diversos del mundo, entre ellos Ecuador; cuenta con una quinta parte de bosques a nivel mundial; tiene el 12% de tierra cultivable del planeta; alberga un tercio de reservas de agua dulce del planeta y cuenta con el 25 % de reservas a nivel mundial en biocombustibles (Comisión Económica para América Latina y el Caribe, 2014).

6. Seguridad y Protección Marítima. Una propuesta

El mar puede ser el escenario de crisis y conflictos, en noviembre de 2017, el Departamento de Defensa de EEUU desplegó en el océano Pacífico tres portaaviones: el USS "Nimitz", USS "Reagan" y USS "Theodore Roosevelt", escoltados cada uno de ellos por sus respectivos grupos de combate, mismos que se han incorporado a la Séptima Flota, operando en aguas de la región Asia-Pacífico. "(…) la maniobra no está dirigida a ninguna amenaza en particular, pero es una demostración de que "podemos hacer algo que nadie más en el mundo puede", dijo la portavoz del Pentágono, Dana White" (Efe, 2017).

Si Mahan estuviera presente, se complacería en constatar el Poder Marítimo de los Estados Unidos con un potente Poder Naval, controlando desde el mar los intereses marítimos propios y de sus aliados, en el contexto de sus intereses nacionales. Independiente de las causas reales y aparentes de la presencia del Poder Naval de Estados Unidos en el mar meridional de China, es claro que el instrumento del Poder Militar más eficaz en una maniobra de crisis internacional, por su versatilidad, despliegue y presencia disuasiva, constituye la Fuerza Naval. El Poder Naval equivale al empleo de la Fuerza Naval, basado en posiciones estratégicas, más la voluntad estratégica. En otras palabras, la Fuerza de Portaviones y sus grupos de combate, se presentan en áreas de interés marítimo, con apoyo de bases aliadas y con la voluntad estratégica de los líderes políticos y militares, a fin de demostrar presencia, control local y temporal del área marítima y disuasión de los actores en disputa. Es indudable que el Poder Marítimo y Naval de Norteamérica y sus Aliados, juegan un rol preponderante y vital en el Control del Mar a nivel mundial, para la Seguridad y Protección de los Intereses Marítimos.

La población mundial para el 2030, estará navegando en un mar de incertidumbres, conflictos y oportunidades, en la misma nave, con la única diferencia, que en primera clase estarán los países que se encuentran en la ola del conocimiento, en segunda clase los países de la ola industrial y en tercera clase aquellos que se quedaron en la ola de la agricultura, sin descartar que se aparezcan polizones referidos a aquellos países considerados fracasados. La nave necesita quien la dirija, su Capitán podría ser un líder llamado "gobernanza mundial", con la suficiente autoridad y respaldo, para conducirla con responsabilidad y que garantice la supervivencia de la misma de manera integral. "(…) para que la opción de la integración internacional sea sostenible, el pueblo debe poder sacar un provecho, los Estados ponerse de acuerdo sobre sus objetivos, y las instituciones responsables ser consideradas legítimas (…)" (Pierre, Ferri, & Tubiana, 2016).

En el inicio de la segunda ola, solo Julio Verne pudo visualizar el futuro de la ciencia y la tecnología en el océano, imaginando viajar en el submarino Nautilus. Correlacionando, el Nautilus de hoy podría ser el submarino Alvin (DSV-2) es una embarcación sumergible

tripulada dedicada a la investigación oceánica profunda, propiedad de la Marina de los Estados Unidos. La investigación científica oceánica, puede ser otro factor aglutinador para que se formen alianzas o grupos internacionales para la preservación de los recursos en el mar y dar la esperanza de que tales estudios ayuden a cubrir el abismo que separa a los países que se encuentran en la primera ola y aquellos de la tercera ola.

Ecuador históricamente ha sido un país marítimo, sus áreas marítimas jurisdiccionales y de interés representan casi cinco veces el territorio terrestre, por lo que no está libre de enfrentar en el futuro crisis originadas por las tendencias mundiales descritas anteriormente. En el marco de la CONVEMAR es posible obtener grandes beneficios, tales como el reconocimiento internacional de los derechos de soberanía y jurisdicción sobre los recursos de las aguas, suelo y subsuelo hasta las 200 millas; además existe la posibilidad de extender los derechos de soberanía sobre la plataforma submarina ecuatoriana hasta las 350 millas náuticas. Con la voluntad política del estado ecuatoriano mediante Decreto Ejecutivo de enero de 2018, se crea el Comité de Límite Exterior de la Plataforma Continental Ecuatoriana, como instancia encargada de elaborar la propuesta para la determinación y definición del límite exterior de la plataforma submarina, más allá de las 200 millas náuticas.

Recordando la década del 60, Ecuador enfrentó la "Guerra del Atún", cuando pesqueros de California efectuaban sus maniobras de pesca en sus aguas jurisdiccionales. La pesca ilegal constituye un indicio de los escenarios para el 2030, cuando muchos países del mundo salgan a buscar recursos vivos y no vivos, en áreas marítimas especialmente sensibles como Galápagos. Donde solamente el Poder Naval que posea el Estado, darán Seguridad y Protección a sus recursos, llegando al uso de la Fuerza inclusive, lo que originaría maniobras de crisis que podrían desencadenar en conflictos internacionales, como históricamente ya han ocurrido. El tema de pesca ilegal es serio, "China es el mayor mercado del mundo de pescado y tiene la mayor flota pesquera de ultramar con 2.460 embarcaciones tras haber crecido rápidamente en las últimas (…) el tamaño de China y su crecimiento económico son dos de las claves de que América Latina esté en su punto de mira, también en lo que se refiere a la pesca" (García, 2016).

Siendo el ser humano el centro de gravedad de la Seguridad Integral del Estado, es de responsabilidad de la Gran Estrategia ecuatoriana, fortalecer con decisión su Poder Marítimo y Naval, el primero retomando una Secretaría Técnica del Mar profesional, con capacidad para aglutinar las diferentes instituciones públicas y particulares, para desarrollar la concepción estratégica marítima nacional, en base a los intereses marítimos y al fortalecimiento del Poder Naval para que proteja a los mismos. Brasil es un ejemplo a seguir con la "Amazonía Azul".

La modernización de la Fuerza Naval de Ecuador, es vital e impostergable, mediante la adquisición de unidades modernas con alta tecnología, que tengan gran capacidad de permanencia en las áreas marítimas jurisdiccionales y de interés, apoyadas con una fuerte exploración aeromarítima, inteligencia operacional y un eficaz comando, control, comunicaciones, inteligencia, vigilancia y reconocimiento. Esta Fuerza Naval será capaz de cumplir el rol militar para el control del mar, el rol diplomático para la presencia naval y el de autoridad marítima para la seguridad y protección marítima. Lógicamente estos mismos medios podrán cumplir eficazmente las tareas en apoyo a los desastres naturales y operaciones de apoyo humanitario, a nivel nacional e internacional.

Sin embargo, ningún país puede enfrentar solo los factores de riesgo y amenazas, el control del mar por su inmensidad es incompleto, relativo y temporal; ninguna Armada del mundo lo puede hacer, por lo que es indispensable constituir alianzas de seguridad y defensa regional, con intereses marítimos comunes, caso contrario sino se protegen los recursos, se pone en peligro el futuro de las nuevas generaciones. La propuesta de este trabajo es rediseñar una organización regional actual y plantear un objetivo estratégico, que a mediano plazo, permita conformar una Fuerza de Tarea Regional Marítima, FTRM, "De llamada", con la participación de estados voluntarios y regida por el Derecho Internacional; el reto consiste en el compromiso de trascender los intereses y posiciones particulares, responsabilizando a los mismos en sus obligaciones individuales y colectivas hacia la protección de los recursos de la región y de sus habitantes. La Armada del Ecuador con sus similares de Colombia y Perú, ya han tomado esta iniciativa en temas de actividades ilícitas en las fronteras marítimas comunes. Otro ejemplo, es la Fuerza de Paz Conjunta y Combinada "Cruz del Sur", compuesta por las Fuerzas Armadas de Argentina y Chile, a disposición de la ONU.

Tomando en cuenta lo anteriormente expuesto y los factores de riesgo y amenazas emergentes que se presentan en América Latina, tales como el narcotráfico; la pesca ilegal no declarada y no reglamentada, INDNR; los desastres naturales y sus consecuencias, considerando además los medios disponibles por parte de las armadas de los diferentes países, se puede dar inicio a la discusión del uso de estos medios para formar una Fuerza de Tarea Regional Marítima, FTRM, "De llamada", para afrontar las amenazas no tradicionales.

En este contexto, se requiere abordar aspectos de cooperación desde el nivel político hasta el nivel táctico; entendiendo que dichas operaciones pueden ser ejecutadas tanto en los espacios marítimos jurisdiccionales como en áreas marítimas de común interés fuera de ellos. En lo que se refiere al nivel político-estratégico, la demanda se define en la voluntad política de las autoridades, tanto en aceptar la cooperación como en entregar la misma a través de los medios navales disponibles. Por otro lado, a nivel estratégico-operacional, los representantes de las armadas deben incluir en la planificación y ejecución de sus operaciones la participación en ejercicios combinados, así como también en operaciones reales de presentarse el caso. Por su parte, en el nivel táctico, es necesario establecer procedimientos comunes a ser empleados, considerando que estos deben abarcar la total interoperabilidad de los medios disponibles.

Los estudios de riesgo, la frecuencia, vulnerabilidad e impacto generado por los factores de riesgo y amenazas determinarán los requerimientos; mientras que por su parte, la puesta a disposición de los medios por parte de los países participantes revelará el escenario para el diseño de la fuerza, misma que deberá ser temporal, en función de la disponibilidad, operatividad y mantenimiento de los medios. En cuanto a la planificación de los ejercicios y su materialización, es un reto alcanzable tomando en cuenta que ya existen en la región instituciones y mecanismos de cooperación multinacional que abarcan el tema de seguridad dentro de sus funciones principales, tal como son: la Organización de Estados Americanos, OEA, la Unión de Naciones Suramericanas UNASUR, y la misma Conferencia Naval Interamericana, CNI, entre otras instituciones multilaterales que pueden ser la base para la cooperación en este sentido.

Ahora bien, todas las buenas intenciones formuladas para la conformación de la Fuerza de Tarea Regional Marítima, FTRM, "De llamada", siempre serán dependientes de los recursos económicos asignados, lo que hace necesario que las autoridades estatales sean

involucradas en todos y cada uno de los pasos previos, con la finalidad que su intervención permita hacer conocer en el nivel respectivo la valoración y el impacto económico de no actuar frente a estas nuevas amenazas no convencionales, así como también que su decisión facilite su materialización (Chong, Garay, Mindiola, Palomeque y Rubio, 2018).

Coincidentemente al escribir estos párrafos, la región lamenta la pérdida de contacto y localización del submarino Argentino ARA "San Juan". Algunos países se han unido a la búsqueda y rescate entre ellos: Estados Unidos, Brasil, Chile, Colombia, Reino Unido y Uruguay. Diferentes medios de superficie y aeronavales con modernas capacidades se presentaron en el área de operaciones. El dispositivo marítimo de búsqueda y rescate, es un indicativo que cuando existe voluntad política y estratégica, es posible conformar una Fuerza de Tarea no solamente regional, sino también mundial, venciendo todo tipo de interferencias e intereses propios de los estados. Ecuador también puso a disposición de Argentina, un avión de exploración marítima de la Armada, con el único propósito y esperanza de salvar las 44 valiosas vidas de los submarinistas. Lo interesante del diseño emergente del esfuerzo combinado del ARA "San Juan", es que los medios participantes no solamente fueron militares, sino también civiles, sin que por ello se hable de la aplicación de la "privatización de la seguridad". El tema de la FTRM "De llamada", merece ser debatido y de ser posible materializado a corto plazo.

7. Conclusiones.

Las causas de las crisis y guerras futuras, ocurrirían principalmente por el crecimiento poblacional y la demanda de recursos vivos y no vivos, sin descartar los motivos que históricamente se han presentado; no se puede dejar de lado, los factores de riesgo y amenazas actuales como: La guerra económica, el narcotráfico vía marítima; el terrorismo internacional; guerras internas, actividades ilícitas en el mar; desastres naturales y otros.

En el escenario mundial todos somos actores, y es de responsabilidad de cada estado con sus aliados que comparten intereses comunes, visualizar la necesidad de diseñar una Fuerza de Tarea Regional Marítima, FTRM, "De llamada", que permita disponer de las capacidades estratégicas modernas, para que a través de alianzas internacionales, garantice y neutralice los impactos del escenario de la "tormenta perfecta del 2030", respecto a Seguridad y Protección marítima, de los recursos en disputa.

Es sorprendente y paradójico, que antes de la ola agrícola la supervivencia del hombre dependía de su habilidad para la caza de animales; mientras que miles de años después y en la plenitud de la ola del conocimiento, la supervivencia de la mayor parte de la humanidad corra peligro por la codicia de alimentos y energía.

Referencias

Aguirre, M. (3 de octubre de 2017). *Guerras, big data y desarrolo*. Recuperado el 13 de noviembre de 2017, de https://www.esglobal.org/guerras-big-data-desarrollo/

Bitar, S. (2014). *Las tendencias mundiales y el futuro de América Latina*. Santiago, Chile: CEPAL.

Chong, M.; Garay, F.; Mindiola, J.; Palomeque, L.; Rubio, X. (2018). *Las Armadas de la Región frente a las MOOTW y PSO*. Guayaquil. Academia de Guerra Naval.

Clausewitz, C. V. (1978). *De la Guerra*. Madrid.

Comisión Económica para América Latina y el Caribe. (27 de octubre de 2014). *Las tendencias mundiales y el futuro de América Latina*. Recuperado el 18 de enero de 2018, de https://www.cepal.org/es/publicaciones/35890-tendencias-mundiales-futuro-america-latina

definicion.de. (2008). *Definición de Futuro*. Recuperado el 2 de octubre de 2017, de definicion.de: https://definicion.de/futuro/

Efe. (27 de octubre de 2017). EEUU despliega tres portaaviones en el Pacífico. *Publico.es*. Recuperado el 15 de noviembre de 2017, de http://www.publico.es/internacional/eeuu-despliega-tres-portaaviones-pacifico.html

García, D. (21 de marzo de 2016). *La enorme operación ilegal de barcos pesqueros de China en aguas de América Latina*. Recuperado el 14 de noviembre de 2017, de BBC Mundo: http://www.bbc.com/mundo/noticias/2016/03/160316_enorme_operacion_ilegal_barcos_pesqueros_china_aguas_america_latina_dgm

Gil, I. (4 de agosto de 2014). *Iniciativa Minerva*. Recuperado el 13 de noviembre de 2017, de https://www.elconfidencial.com/alma-corazon-vida/2014-08-04/iniciativa-minerva-el-pentagono-se-prepara-para-el-colapso-del-sistema_147254/

Infobae. (22 de mayo de 2014). Así serán las guerras del futuro. *Infobae*. Recuperado el 12 de noviembre de 2017, de https://www.infobae.com/2014/05/22/1566589-asi-seran-las-guerras-del-futuro/

Jorge, J. (28 de abril de 2016). Resultados de la Segunda Guerra Mundial. Recuperado el 4 de octubre de 2017, de https://prezi.com/_dhqt47ty2ys/como-resultado-de-la-segunda-guerra-mundial-el-mundo-quedo-d/

Khan, H. (2017). Estrategia Escalada. Guayaquil.

Leal, P. (4 de septiembre de 2016). *Rusia-China-Irán; Una alianza destinada a romper hegemonías*. Obtenido de HispanTV. Nexo Latino: https://www.hispantv.com/noticias/opinion/286942/alianza-rusia-iran-china-occidente-eeuu

Ministerio de Defensa. (2014). *Agenda Política de la Defensa 2014-2017*. Quito: Ministerio de Defensa Nacional.

Monge, Y. (2 de marzo de 2003). ¿Qué aprendimos de la primera guerra del Golfo? *El País*. Recuperado el 13 de noviembre de 2017, de https://elpais.com/diario/2003/03/02/internacional/1046559610_850215.html

Pieraccini, F. (2017). How a United Iran, Russia and China are Changing The World - For the Better. *Strategic Culture Foundation. Online Journal*. Recuperado el 18 de noviembre de 2017, de https://www.strategic-culture.org/news/2017/01/01/how-united-iran-russia-china-changing-world-better.html

Pierre, J., Ferri, J., & Tubiana, L. (2016). *En busca de la Gobernanza Mundial*.

Solís Oyarzún, E. (1991). *Estrategia*. Valparaíso: Academia de Guerra Naval.

Toffler, A. (1980). La Tercera Ola. Bogotá: Plaza & Janes S.A. Editores.

Tzu, S. (2001). *El Arte de la Guerra*. Madrid: Arca de Sabiduría.

UNASUR. (2017). *Consejo de Defensa Sudamericano de UNASUR*. Recuperado el 18 de noviembre de 2017, de UNASUR: https://www.unasursg.org/es/consejo-defensa-suramericano-unasur

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 15/09/2017
Aceitação/Acceptance: 30/03/2018

Insertion in the Asia-Pacific the Economic Cooperation Forum: Challenges for the Countries of the South-East Pacific from the Security Perspective

Marfiu Rodríguez Jara[1], Teresa Guarda[2,3]

marfiurodriguez@yahoo.com, tguarda@gmail.com

[1] Armada del Ecuador, Guayquil, Ecuador

[2] Universidad de las Fuerzas Armadas-ESPE, Sangolqui, Quito, Ecuador

[3] Algoritmi Centre, Minho University, Guimarães, Portugal

Pages: 100–105

Abstract: The countries of the Southeast Pacific follow diverse national policies and initiatives to achieve the insertion to the region of the Pacific Rim, constituting the Forum of Asia-Pacific Economic Cooperation (APEC), like the main mechanism of access to the economies that represent a community of 2 800 million people who generate 47% of world trade in the present century. Faced with taking advantage of the opportunities to form part of APEC, it is also necessary to face the challenges of regional integration from a security perspective and formulate national strategies that include the strengthening of navies with oceanic capacities to protect maritime trade, to preserve the marine ecosystem , for assistance against natural disasters, for the application of the law against illegal activities at sea and to contribute to the regional cooperative security to achieve a safe Pacific Rim.

Keywords: APEC, Regional Integration; Regional Cooperative, Maritime Security.

1. Introduction

The Asia-Pacific Economic Cooperation is the regional economic forum that brings together 21 member countries to create prosperity in the region, including Chile and Peru, Southeast Pacific countries that promote the opportunities to be part of this Forum and assume the challenges of insertion into the Pacific Rim that guarantee the security and development of their national interests.

This article describes the importance of APEC for the countries of the Southeast Pacific, as a mechanism for insertion into the economies of the members of this Forum; the strategies and actions taken by these countries are identified to maximize the opportunities offered by being part of APEC; the risks and threats of the APEC region and the challenges from the perspective of security and defense of the State are analyzed, to finally draw conclusions on the subject.

2. APEC Importance for the Countries of the Southeast Pacific

APEC is a regional economic forum to promote trade, economic and technical cooperation, and investments in the Asia-Pacific region. It was created in 1989, at the urging of Australia and Japan to boost economic growth and prosperity of the community in the Asia-Pacific region.

Currently there are 21 APEC member countries (Fig. 1), distributed in the American region with 5 countries (Canada, USA, Mexico, Peru and Chile) and in the Asian region with 16 countries (Japan, South Korea, Taiwan, Hong Kong, Singapore, Malaysia, Thailand, Indonesia, Philippines, Brunei, China, Papua New Guinea, New Zealand, Australia, Russia and Vietnam).

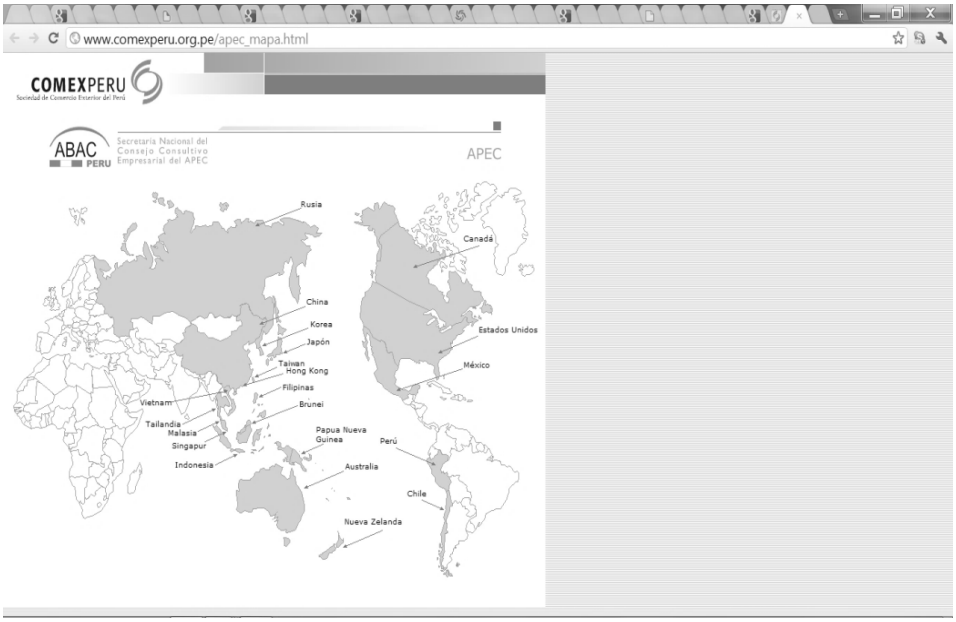


Figura 1 – APEC member countries.

The importance of APEC for the countries of the Southeast Pacific lies in the fact that this forum represents the integration mechanism to the block of economies that represent 2.8 billion people, 57% of the world GDP and 47% of world trade [1]. By comparison, the European Community represents 500 million people, 27 countries, 26% of world GDP and 40% of world trade.

The importance of the ocean as a way of commercial exchange for APEC is evidenced when we find that worldwide 80% of the foreign trade load is transported by this means. Of the 30 ports that transfer more containers in the world, 23 of them are located in this region, leading the list the port of Shanghai in China, with a volume of 36.54 million TEU in 2015 [2].

Peru was admitted as a member of APEC at the X meeting, held in November 1998 in Kuala Lumpur, Malaysia, and since then it has strengthened trade relations with Asian countries through bilateral treaties, such as China, Korea, Singapore and Thailand. A strategic objective of Peru is to become the hub of port and airport services for trade between Asia and South America [3], exploiting its geostrategic position of "Country Hinge" among the countries of Asia, Mercosur and the Andean Community of the Nations [4].

Only Peru's trade with the APEC block increased six times between 1998 and 2015, from US $ 7 million to US $ 44 million, with APEC representing 58% of Peru's exports to the world and 54% of the total of tourists who entered in 2015 [5].

Chile joined APEC as a full member during the APEC Summit in Jakarta, Indonesia, in November 1994, and since then has maintained an active participation in the promotion of trade in the Asia Pacific region, signing Free Trade Agreements with Malaysia, Vietnam, Hong Kong and an Investment Agreement with China. In 2012, Chile's trade with the APEC economies was US $ 96,434 million, of which US $ 50,207 million were exports, 64.1%. On the other hand, the direct investment of the APEC economies in Chile in 2012 was US $ 52,759 million, 58.3% of the total foreign investment in Chile) [6].

Colombia is not part of APEC but maintains presence and participation with observers in several APEC working groups; it also forms the Pacific Alliance bloc, together with Chile, Mexico and Peru, in its strategy of future insertion into APEC. Colombia's exports to the Asian region represent 8.7% of its total exports to the world [7].

Ecuador, is a country called to be maritime because of its geostrategic position in front of the Pacific Rim, with an ocean that communicates to the block of countries bordering APEC, considered one of the 17 most mega-diverse countries in the world [8], It has oceanic public policies issued by the Inter institutional Committee of the Sea, which promotes the strategic insertion of Ecuador in the Pacific Ocean and Antarctica [9], in accordance with the provisions of Article No. 276 of the Constitution of the Republic that indicates "... promote a strategic insertion in the international context, that contributes to peace ...", but that has not implemented a national strategy for the insertion in APEC, with an active participation in the economic, environmental, diplomatic and security in this forum.

The policies and strategies adopted by the Ecuadorian State for insertion into this Forum should be formulated under the principle of no renunciation of sovereignty or the rights of sovereignty acquired by international treaties signed by Ecuador, such as the Convention on the Rights of the Child. United Nations on the Law of the Sea, UNCLOS, make use of the right and right to the use of the international legal norms that assist it as a nation-state.

3. The Ocean, Fisheries and Aquaculture in the Pacific Rim

The Pacific Rim, formed by the Asian and American rivers, contains the largest ocean in the world that covers 46% of the planet, 4 continents converge over 25 thousand islands, and in the XXI century it is the most important ocean economic, political, strategic and environmental of the world.

APEC members generate about 80% of the world's aquaculture production and 65% of the world's fishing catches. The APEC region consumes fish products 65% higher than

the world average. Consistent with this reality, APEC formed the Oceans and Fisheries Working Group to delineate and execute actions to improve cooperation to combat illegal fishing, contribute to the conservation, protection and sustainable management of marine ecosystems, as well as implement improvements management practices in fisheries and aquaculture [10].

At the APEC meeting of Ministers of Oceans, on August 28, 2014 in China, the Xiamen Declaration was promulgated in recognition of the increasing fragility of the coastal marine environment and the reduction of fish stocks, prioritizing actions of cooperation in relation to the conservation of marine ecosystems, resilience to natural disasters, the promotion of the blue economy in the region, among other initiatives [11].

4. Challenges of Insertion into the Pacific Rim

In addition to the economic, environmental and social factors that are addressed in the different areas of cooperation among APEC members, lines of action and coordination are recognized and prioritized to build a safe Pacific Rim, but what are the risks and common threats to APEC members?

In the conference "Vision of Chile on the Pacific", the Minister of Defense of Chile pointed out as security problems for the Pacific Rim to the post-Cold War conflicts in the Korean peninsula, the maritime-territorial claims in Asia, the change climatic, natural disasters, sea level rise, overexploitation of marine resources, piracy, drug trafficking, organized crime, illegal trafficking, international terrorism, among others [12].

APEC adopted protection measures for maritime transport in the region, calling it the STAR initiative, Secure Trade in the APEC Region, reinforcing the measures adopted worldwide by the International Maritime Organization, such as the establishment of the Automatic Identification System, AIS, the Code International Ship and Port Security, ISPS, the Reformed Convention on the Safety of Human Life at Sea, SOLAS, or the 2005 Protocols for the Convention for the Suppression of Illegal Acts, SUA, becoming a commitment of the member countries.

In particular, the challenge that represents for the countries of the Southeast Pacific to reduce and neutralize the risks and threats respectively, comes from the same control of the extensive jurisdictional maritime spaces under sovereignty and sovereign rights of each State, whose areas are indicated in Table 1.

Country	Maritime Jurisdictional Space
Chile	3'681.989 Km^2
Colombia	928.660 Km^2
Ecuador	1'111.818 Km^2
Peru	855.475 Km^2

Table 1 – Jurisdictional Maritime Spaces of the Southeast Pacific Countries.

This implies planning and executing programs to strengthen the naval forces of the National Armed Forces, so that they carry out maritime security, understood as the activity to mitigate the risks and counteract the illegal activities in the maritime field, applying the law to protect the national maritime interests [13].

To achieve this purpose, the navy require technological infrastructure that allows them to access diverse sources of international and inter institutional information to achieve a clear and continuous Maritime Domain Awareness, which allows the Commanders and Joint Commands to analyze the information for the adequate decision-making in the conduct of maritime security operations with the naval resources assigned.

But to counteract the common risks and threats to the countries of the region in areas of interest beyond jurisdictional maritime spaces, it is necessary to establish cooperation agreements for the use of the Navy of War in a Combined Naval Force of the Pacific Rim, which contribute to maintaining peace and order under the international legal framework.

The exercises of the multinational naval forces of the Pacific Rim, called RIMPAC since 1971, demonstrate the capacity of coastal countries to contribute to regional cooperative security, promoting and maintaining cooperative relations that guarantee the safety of maritime routes and the protection of the Pacific Ocean. In the RIMPAC 2018 exercise, the Chilean Navy will conduct the Combined Force Maritime Component, constituting a relevant milestone since it is the first time that a Southeast Pacific Navy assumes this responsibility, recognizing its preparation and professionalism [14].

5. Conclusions

While the objectives of APEC are focused on cooperation for the economic growth of member countries through trade and investment, the inherently maritime nature of this regional trade must be considered, which implies challenges and opportunities for the countries of the Southeast Pacific, in the development of their maritime interests to maximize the advantages offered by being part of this regional block.

In the face of APEC opportunities, risks and threats in the maritime area also emerge that must be assessed and addressed through comprehensive maritime policies and strategies that include the strengthening of the security and defense sector, and in this way contribute to protecting maritime trade, to preserve the marine ecosystem from an irrational exploitation of the resources of the sea, and with the capacity to apply national and international laws against illicit activities at sea.

Finally, in order to successfully face the challenges of insertion into the Pacific Rim and its main integration mechanism such as APEC, it is a sine qua non requirement for the countries of the Southeast Pacific to strengthen their Armed Forces, with deterrent and action capabilities in oceanic zones, both in the jurisdictional maritime spaces of the respective countries and in the areas of interest, beyond their maritime limits, cooperating in the formation of a multinational naval force to execute combined operations, acting under the framework of regional cooperative security of the Pacific Rim.

References

APEC Secretariat, “Key APEC Documents 2017”, December 2017, http://www.apec.org

World Shipping Council, Top 50 World Container Ports, 2018, http://www.worldshipping.org

P. Pachas, ‘Desafíos para el Perú: APEC y TLC”, Revista de Investigación de la Universidad Nacional Mayor de San Marcos, Lima, Perú, Julio de 2006, pp. 36.

V. Giudice, “El Perú y la Cuenca del Pacífico”, 2008.

Acuerdos Comerciales del Perú, http://www.acuerdoscomerciales.gob.pe

Dirección General de Relaciones Económicas Internacionales de Chile, DIRECON, http://www.direcon.gob.cl

H. Laverde y L. Corredor, “Evaluación de las estrategias de ingreso de Colombia al Foro de Cooperación Económica Asia-Pacífico (APEC)”, 2016.

S. Burneo, “Megadiversidad”, 2009

Registro Oficial Nro. 383, del 26 de noviembre de 2012. El Comité fue creado creado mediante Decreto Ejecutivo Nro. 990, del 29 de diciembre de 2011.

Grupo de Trabajo de Océanos y Pesquería APEC, http://www.apec.org

APEC Secretariat, https://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Ocean-and-Fisheries.

Conferencia del Ministro de Defensa de Chile, 27-NOV-14, http://www.defensa.cl/discursos/vision-de-chile-sobre-el-pacifico-conferencia-del-ministro-de-defensa-nacional-en-ceseden/

Chiefs of European Navies Forum, “Developing a European interagency strategy for maritime security operations”, 2007.

Revista Infodefensa, “Chile liderará componente marítimo en el ejercicio naval más grande del mundo”, Mayo 2017, http://www.infodefensa.com

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 01/09/2017
Aceitação/Acceptance: 29/03/2018

Adoção de Políticas de Segurança de Sistemas de Informação nas Universidades Moçambicanas

Isabel Maria Lopes[1, 2, 3], Joaquina Rafael Monteiro

isalopes@ipb.pt, jmonteiro660@gmail.com

[1] Instituto Politécnico de Bragança, Bragança, Portugal.

[2] UNIAG (Applied Management Research Unit), Instituto Politécnico de Bragança, Bragança, Portugal.

[3] Centro ALGORITMI, Universidade do Minho, Braga, Portugal.

Pages: 106–117

Resumo: As universidades manipulam cada vez mais, grandes quantidades de informação em suporte tecnológico. Por isso, são imprescindíveis controlos de segurança cada vez mais rigorosos e abrangentes. De entre as medidas de segurança, as políticas assumem na literatura um papel central. Este trabalho foi realizado com recurso a um inquérito por questionário a 12 universidades moçambicanas, foram inquiridas 69 faculdades/escolas superiores que fazem parte da estrutura destas universidades. O principal objetivo do inquérito foi a obtenção de resposta à seguinte questão: As Universidades (faculdades/escolas superiores) tem posse de uma política de segurança da informação? Com base no levantamento efetuado concluiu-se que das 69 faculdades/escolas superiores, 43 (62%) indicaram dispor de políticas de segurança dos sistemas de informação e 26 (38%) indicaram não ter, mas têm intenção de adotar uma política. Os resultados são discutidos á luz dos dados recolhidos no inquérito e identificados trabalhos futuros.

Palavras-chave: Segurança da informação; segurança dos sistemas de informação nas universidades Moçambicanas; políticas de segurança de sistemas de informação.

Adoption of Information Sistems Security Policies in Mozambican Universities

Abstract: Universities are handle increasingly higher amounts of information in digital format. Therefore, more rigorous and comprehensive security controls are indispensable. In literature, security policies assume a paramount role among security measures. This work was carried out using a questionnaire survey of 12 Mozambican universities, in which 69 colleges that were part of the structure of these universities. Whose objective was to answer the main question related to the possession of a security policy based on the research carried out, it was found out that 43 (62%) have an information systems security policy and 26 (38%) do not have an information systems security policy. The results are discussed in light of the data collected in the survey and identified future work.

Keywords*:* Information security; information system security in Mozambican universities; information systems security policies.

1. Introdução

Nos dias de hoje as tecnologias e sistemas de informação tornaram-se, mais importante para a sobrevivência de qualquer organização. Os sistemas de informação devem permitir a recolha, armazenamento, processamento e facultar a informação relevante em tempo útil.

As universidades são instituições de ensino superior onde o número de utilizadores da rede de computadores é elevada. Para além dos funcionários, também temos um conjunto de estudantes, que usam os recursos disponíveis e têm acesso à informação da instituição a que pertencem. Independentemente da dimensão ou área de negócios das empresas ou organizações, é necessário que haja garantia de segurança da informação, e a respetiva estabilidade desta plataforma tecnológica. Para que isso aconteça é necessário levar em consideração os aspetos relacionados com a segurança da informação, dos seus sistemas e das tecnologias que manipulam essa informação.

Não são apenas as ameaças externas que representam riscos a uma instituição, os próprios funcionários e alunos representam alto risco, quando são mal-intencionados ou mesmo quando não estão conscientes dos riscos envolvidos na manipulação da informação (Vaz, 2014).

Vivemos na era digital, onde todos os tipos de informações são acessíveis eletronicamente a todo o momento, as organizações em todo o mundo lutam para manter seus ativos de informação seguros. Curiosamente, a maioria dos incidentes de segurança dos sistemas de informação organizacional são o resultado direto ou indireto de erros humanos (Haeussinger & Kranz ,2017).

Assim, devido a possíveis falhas humanas e riscos na troca de informação pela rede mundial de computadores é necessário gerir os sistemas de informação de um modo mais seguro, para que haja um bom desempenho dentro das organizações através das novas tecnologias de informação, para isso torna-se necessário que as organizações definam uma política de segurança, concebida de modo rigoroso e que ajude a regular o uso da sua plataforma tecnológica, a fim de proteger os seus ativos (Lopes & Oliveira, 2016).

A política de segurança da informação é um documento que deve conter um conjunto de normas, métodos e procedimentos, que devem ser comunicados a todos os funcionários, bem como a todos os estudantes (em suma a todos os utilizadores do sistema de informação), analisado e revisto criticamente, em intervalos regulares ou quando relevantes mudanças se fizerem no sistema de informação.

Após a definição, elaboração e aprovação de uma política de segurança, é necessária a sua implementação e, posteriormente, o recurso a auditorias internas e externas que verifiquem se as políticas de segurança estão a ser aplicadas de modo correto e adequado (Lopes & Oliveira, 2016).

É neste contexto que se enquadra o presente trabalho, que após a deteção de uma lacuna, no que concerne à existência ou não de políticas de segurança dos sistemas de informação nas universidades de Moçambique (uma vez, que não se identificaram estudos, que nos dessem essa informação), que se procedeu à elaboração de um inquérito, por forma a obtermos responda à nossa questão de investigação, que é até que ponto as universidades de Moçambique adotam estas políticas.

O presente trabalho estruturalmente após esta introdução, prossegue com uma abordagem às políticas de segurança. Em seguida na secção 3, apresenta-se o propósito da investigação. Na secção 4, abordamos a forma como foi feito o inquérito. Por último, apresentam-se os resultados e as conclusões à luz dos dados da pesquisa e propõem-se trabalhos futuros.

2. Políticas de Segurança dos Sistemas de Informação

Com a utilização massiva da Internet e com o constante crescimento do uso de meios tecnológicos pelas organizações a informação está cada vez mais exposta a ameaças, é aí que a segurança da informação entra, para garantir a integridade, confidencialidade e disponibilidade desses ativos (Lopes & Oliveira, 2015).

A tríade de ouro, conhecida também como CIA, do inglês - Confidentiality, Integrity and Availability – representa as propriedades convencionais que orientam a análise, o planeamento e a implementação da segurança da informação. Outras propriedades estão a emergir, como é o caso da legitimidade e a autenticidade, isto porque a utilização de transações comerciais em todo o mundo através de redes eletrónicas se massifica.

Os princípios clássicos da CIA podem ser explicados da seguinte forma (Dhillon & Backhouse, 2000):

- Confidencialidade – acesso a informação somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.
- Integridade – a informação manipulada deve manter todas as características originais estabelecidas pelo proprietário da informação, garantindo que o conteúdo não é alterado de forma não autorizada.
- Disponibilidade – a informação está sempre disponível para o uso legítimo, sempre que dela se necessite.

A reforçar este ponto de vista, outro autor (Peltier, Peltier & Blackley, 2005), afirma que a segurança da informação deve ser vista como um triângulo, em que um vértice é ocupado pela confidencialidade e os outros dois pela integridade e pela disponibilidade, respetivamente.

Ao se falar em segurança da informação, deve-se levar em consideração estes três princípios básicos, pois toda ação que venha a comprometer qualquer um desses princípios estará atentando contra a sua segurança.

Para obter a segurança da informação, torna-se necessário implementar um conjunto de medidas adequadas, com o intuito de garantir a segurança desse ativo. Uma das medidas é a criação de um conjunto de normas e recomendações normalmente vertidas no documento designado por política de segurança dos sistemas de informação.

Tendo em conta que a segurança não é só o aspeto tecnológico, a política de segurança deve incluir um conjunto de referências que podem ir desde a concordância e consciencialização dos utilizadores para a problemática da segurança até à aprovação do documento pela direção da empresa, pois é fundamental para que a mesma seja efetiva, sem a presença deste apoio e aprovação, iniciar qualquer ação neste sentido é algo inviável.

As políticas de segurança dos sistemas de informação devem:

- Definir o que é a segurança da informação, quais são os seus principais objetivos e a sua importância dentro da organização.
- Mostrar o empenho da direção com a problemática da segurança.
- Definir a filosofia relativamente ao acesso aos dados.
- Estabelecer responsabilidades.
- Estabelecer a base para a elaboração de regras e procedimentos relacionados com:
  - Organização da segurança;
  - Classificação e controle de dados;
  - Segurança das pessoas;
  - Segurança física e ambiental;
  - Plano de contingência;
  - Prevenção e deteção de vírus;
  - Administração de computadores.

A segurança da informação engloba tecnologia, processos e pessoas. As medidas técnicas, tais como passwords, dados biométricos ou firewalls, por si só não são suficientes para atenuar as ameaças à informação. Uma combinação de medidas é necessária para garantir e proteger os sistemas de informação contra eventuais riscos ou ameaças (Da Veiga & Eloff, 2007).

Para Dantas (Dantas, 2011), pode-se definir a política de segurança como um documento que estabelece princípios, valores, compromissos, requisitos, orientações e responsabilidades sobre o que deve ser feito para alcançar um padrão desejável de proteção para as informações.

3. Propósito de Investigação

É notória a falta de estudos empíricos no âmbito das políticas de segurança dos sistemas de informação. Embora as críticas à falta de investigação sobre estas políticas e à inexistência de estudos empíricos sobre essa área sejam frequentes (Lopes, 2012), da revisão que se efetuou da literatura parece assistir-se a dificuldades no sentido de inverter esta situação.

Na sequência desta constatação, este trabalho visa contribuir para colmatar essa falha, procurando-se desenvolver investigação que tenha em conta aquelas críticas, designadamente no que respeita à condução de estudos empíricos e à contextuação da aplicação das políticas de segurança.

Neste sentido, esta investigação centra a sua atenção nas universidades Moçambicanas, que para além de ser um sector que importa e interage com um número elevado de cidadãos (funcionários, alunos, etc.), é notória a inexistência de estudo sobre a temática das políticas de segurança.

4. Inquérito

Com vista a caracterizar empiricamente a adoção de políticas de segurança dos sistemas de informação por parte das universidades Moçambicanas, entendeu-se apropriado

aplicar a técnica de Inquérito, uma vez que potencia uma resposta clara, direta e objetiva às questões apresentadas aos inquiridos.

Os inquéritos foram feitos em Moçambique no período entre o dia 20 de julho a 8 de setembro do ano 2016 foram inquiridas 12 das 14 universidades existentes, bem como, as suas respetivas faculdades e/ou escolas superiores que delas fazem parte. Foram efetuados 69 questionários, tendo obtido 69 respostas. O inquérito foi presencial em todas as faculdades/escolas superiores. Para a obtenção da informação necessária o inquérito foi direcionado e efetuado aos responsáveis da área da informática das diferentes universidades (faculdades/escolas superiores).

Como o número de faculdades que cada universidade tem é elevado, mencionam-se só as universidades, estas dividem-se em públicas - Universidade Eduardo Mondlane (UEM), Universidade Pedagógica (UP), Universidade Uni Zambeze (UNI ZAMBEZE), Universidade Uni Lúrio (UNI LURIO) e em universidades privadas - Universidade Católica de Moçambique (UCM), Universidade Wutivi (WUTIVE), Universidade Adventista de Moçambique (UAM), Universidade Técnica de Moçambique (UDM), Universidade São Tomas de Moçambique (USTM), Universidade A Politécnica (A POLITECNICA), Universidade Jean-Piaget (UNIPIAGET), Universidade Mussa BinBique (UMBB), Universidade Nachimgwya (UNA), Universidade Methodista Unida de Moçambique (UMUM).

A estrutura do inquérito resultou da revisão de literatura sobre políticas de segurança de sistemas de informação, que culminou com a utilização de um já existente e que se enquadrava perfeitamente após pequenas alterações nas instituições em estudo (Lopes, 2012). As questões do inquérito, de resposta individual e de natureza confidencial, estavam organizadas em quatro grupos.

O primeiro grupo visava obter uma breve caracterização da Universidade e do respondente, seguindo-se os grupos de questões atinentes às características gerais das políticas de segurança dos sistemas de informação, as quais eram antecedidas pela questão fundamental: "A universidade/faculdade possui uma política de segurança dos sistemas de informação?".

Após a pergunta principal, e caso a resposta fosse negativa, passava-se para o grupo de questões onde se questionava os inquiridos se estavam a pensar formular uma política de segurança, uma vez que ainda não possuíam nenhuma, e caso estivessem a pensar formular alguma, se a mesma já estava em processo de elaboração. Se não estivessem a pensar formular uma política de segurança, eram questionados se essa opção seria por não considerarem a segurança dos sistemas de informação importante.

Caso a resposta à questão principal fosse positiva, passava-se aos grupos de questões em que se procurava focar as políticas enquanto produto e se centrar a atenção nos processos de formulação e implementação das mesmas.

Relativamente às políticas enquanto produto, as questões colocadas prendiam-se com a forma como são apresentadas; o que abordam; dimensão em número de páginas; quem tem conhecimento da política; onde se encontra disponível; se estão definidos os papéis,

as responsabilidades e as sanções para o seu não cumprimento e se os utilizadores assinaram um termo de aceitação da política.

Em relação aos processos, as questões colocadas relacionavam-se com o tempo de vida das políticas, por quem foi desencadeado o processo de formulação, por quem foi desenvolvida, se foi aprovada superiormente, quem a implementou e quem supervisiona o seu cumprimento, se foi bem aceite pelos utilizadores, se está em vigor, se é revista, se existe uma única política ou várias, e a quem se destina.

Uma última questão formulada aos inquiridos relacionava-se com a existência e identificação de outros mecanismos de proteção da informação.

5. Resultados

A questão principal do inquérito prendia-se com o apuramento da existência de políticas de segurança nas universidades Moçambicanas.

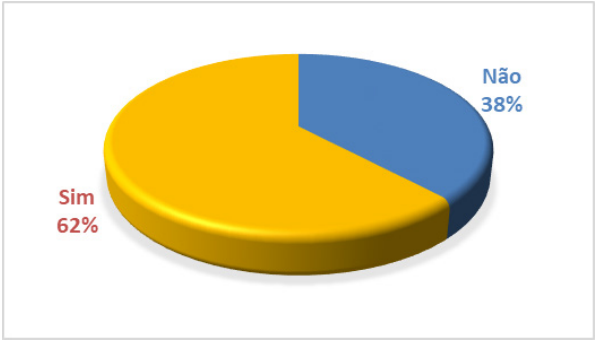


Figura 1 – Posse de uma Política

Como se pode observar na Fig. 1, dos 69 inquiridos 62% responderam possuir uma política de segurança dos sistemas de informação que corresponde a um total de 43 faculdades/ escolas superiores que fazem parte das 12 universidades, e 26 (38%) informaram não dispor de uma política de segurança.

Questionados sobre o que a política aborda, dos 43 casos que responderam possuir uma política de segurança, as políticas abordam e focam os temas que se podem observar na Fig. 2. Tratando-se de uma questão com possibilidade de escolha múltipla o total não tem que somar 43. De referir que por "comportamentos" entende-se o modo de atuação dos funcionários, ou seja, as suas ações concretas.

Questionados sobre quem elaborou a política, a resposta obtida no universo dos 43 inquiridos, foi que em todos os casos a política de segurança dos sistemas de informação foi elaborada pelo pessoal interno ou por especialistas ou técnicos de informática, das faculdades/escolas superiores.

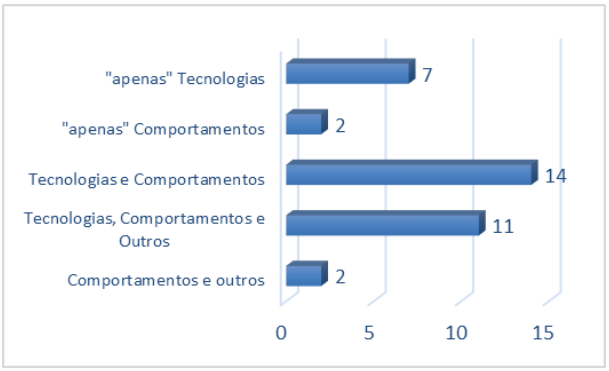


Figura 2 – Temas Abordados pelas Políticas

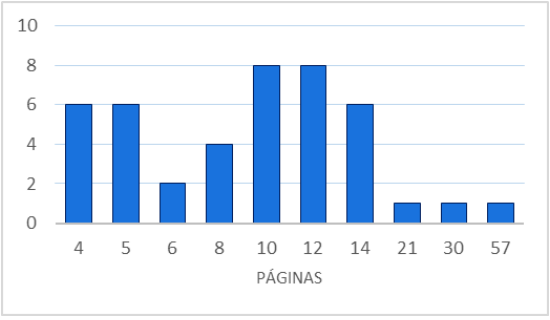


Figura 3 – Dimensão do Documento da Política

Relativamente a quem tem conhecimento da política de segurança, as respostas foram: Direção (43), Chefias (43), Funcionários (43), e Estudantes (8).

Relativamente à dimensão das políticas, em termos de número de páginas, varia muito no universo das 43 faculdades/escolas superiores, sendo a média de 11 páginas por documento, com o máximo de 57 páginas e o mínimo de 4 páginas, como se observa na Fig. 3.

Dos 43 casos que afirmaram possuir uma política de segurança dos sistemas de informação, questionados sobre se estão definidos os papéis e as responsabilidades, foram unânimes em responder que sim.

Relativamente ao facto de estarem ou não definidas sanções para o caso de um determinado utilizador não cumprir o estipulado na política, 21 (49%) afirmaram que as políticas tem definidas as sanções para o não cumprimento e 22 (51%) não têm definidas as sanções no documento da política.

Como advém da literatura sobre a implementação de políticas de segurança é imperioso que todos os utilizadores dos sistemas de informação tenham conhecimento da política, e que preferencialmente assinem um documento como a receberam, ou seja um termo de aceitação. Questionados a esse respeito, 18 (42%) responderam positivamente e os restantes 25 (58%) negativamente.

A quantidade de anos em que a política de segurança está implementada em cada faculdade/escola superior é, como se compreende variável, a média das respostas obtidas situa-se em cinco anos, as políticas mais antigas foram elaboradas há 8 anos e as mais recentes foram há dois anos. Estes resultados são apresentados na Fig. 4.

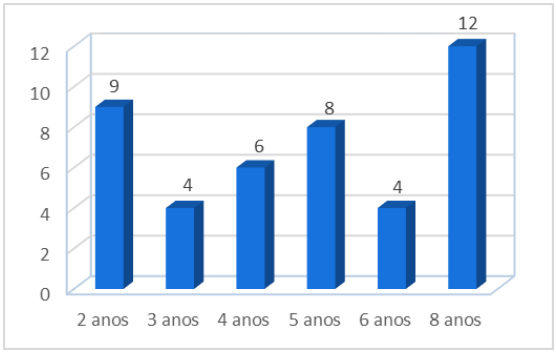


Figura 4 – Anos de Existência da Política

Em relação à questão sobre quem desencadeou o processo de formulação da política de segurança dos sistemas de informação, as 43 respostam vão no mesmo sentido, indicando o departamento das tecnologias de informação e comunicação responsável por esse facto.

Foi também sobre o departamento das tecnologias de informação das faculdades/ escolas superiores que recaiu a responsabilidade de implementar a política formulada, bem como, a responsabilidade pela observância ou cumprimento da política. Pois não basta implementar uma política de segurança, a sua observância é igualmente imperiosa pois se não estiver adotada de nada serviu a sua implementação.

Quanto à aprovação da política, verificou-se que foi aprovada superiormente nos 43 casos.

Como nem sempre as mudanças sem bem aceites pelos utilizadores do sistema de informação, essa questão foi colocada, ou seja, questionou-se se a implementação da política foi bem aceite pelos utilizadores e as respostas forma positivas em 28 (65%) dos casos, contra 15 (35%) onde a política não foi bem aceite. A Fig. 5 apresenta os valores agregados das respostas a esta questão.

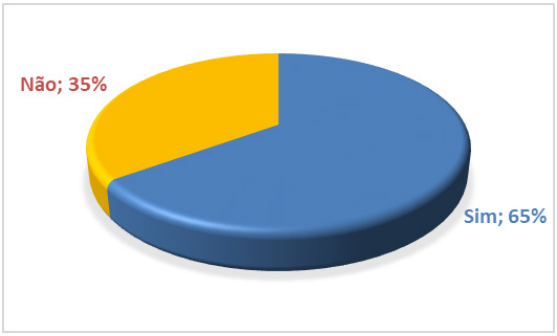


Figura 5 – Aceitação da Política

Nas 43 faculdades/escolas superiores que responderam possuir uma política de segurança dos sistemas de informação, a mesma está implementada, ou seja, encontra-se em vigor.

Questionados sobre como foi implementada a política, responderam que foram disponibilizados os documentos em todos os sectores de atividade. Em 27 (63%) casos a distribuição foi em formato de papel e nos restantes 16 (37%) dos casos foi via Internet.

Relativamente à questão se a política de segurança dos sistemas de informação, já sofreu alguma revisão, em 9 (21%) das faculdades/escolas superiores fizeram uma vez uma revisão, nos restantes 34 (79%) dos casos nunca fizeram qualquer revisão à política implementada. Esta verificação pode ser vista na Fig. 6 que se segue.

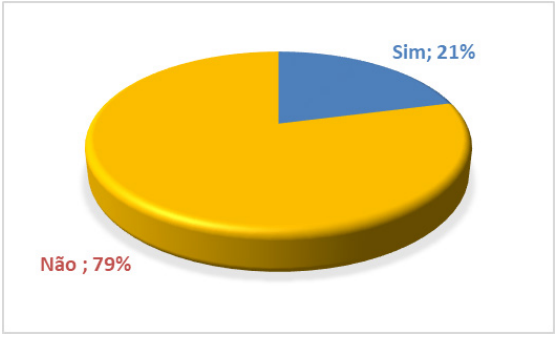


Figura 6 – Revisão da Política

Embora tenham afirmado que é difícil definir um intervalo de tempo em que a política deve ser revista, definiram esse intervalo entre dois ou cinco anos, contudo, o que se verifica é que já têm políticas implementadas há vários anos e a taxa de revisão é muito baixa.

As respostas anteriores foram todas relacionadas com faculdades/escolas superiores que afirmaram possuir uma política de segurança. Relativamente às 26 faculdades/escolas superiores que não têm implementada uma política, também lhes foram colocadas algumas questões.

A primeira delas é se não têm uma política, têm intenção de adotar uma? Está em processo de formulação essa política? ou Não têm intenção de adotar uma política de segurança? A esta questão a resposta foi unânime em afirmarem que têm intenção de adotar uma política de segurança dos sistemas de informação.

As 26 universidades que afirmaram não possuírem uma política de segurança dos sistemas de informação, mas que segundo a questão anterior pretendem adotar uma, são as constantes na Fig. 7.

Uma outra questão, uma vez que do universo de faculdades/institutos superiores inquiridos que foi de 69, observou-se que 26 não possuem uma política de segurança, a questão que lhe foi colocada é se "não consideram a segurança da informação importante?", a resposta foi consentânea pois obtiveram-se 100% de respostas positivas, o que está de acordo com a intenção de todas em formularem uma política de segurança.

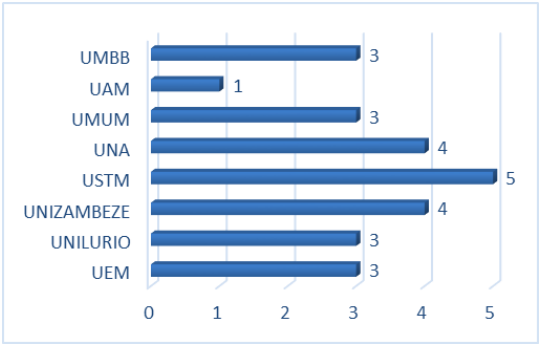


Figura 7 – Universidades que não têm uma Política

Questionados sobre a existência de outros mecanismos de proteção da informação e dos sistemas informáticos, a resposta foi unânime e todas as faculdades/institutos superiores possuem em maior ou menor número estes mecanismos, embora não se tenha procedido à sua quantificação no âmbito deste estudo. O mecanismo de proteção mais comum é a existência de software anti-vírus, as firewalls são dispositivos igualmente existentes em grande número, os filtros anti-spam e os backups diários da informação são também muito utilizados, assim como, active directory e anti-malware.

Relativamente à questão sobre os fatores que condicionam a adoção de uma política de segurança, obtiveram-se as seguintes respostas: falta de capacidade do pessoal para a elaboração de uma política; falta de sensibilização por parte dos órgãos decisores sobre esta temática; falta de legislação sobre crime informáticos em Moçambique e os serviços

informáticos serem coordenados diretamente pela reitoria das faculdades/escolas superiores.

Por fim, foram questionados sobre que benefícios considerem espectáveis com a adoção de uma política, e as respostas foram as seguintes: melhor segurança e maior credibilidade ao nível da informação; garantia dos direitos e deveres de cada utilizador do sistema de informação; melhoria na gestão da informação e maior controlo da invasão de hackers.

6. Conclusões

Com vista às organizações alcançarem um determinado nível de segurança dos seus sistemas de informação, a literatura tem apontado as políticas de segurança dos sistemas de informação como o meio mais adequado e indispensável para o lançamento e sustentação do programa de segurança dos sistemas de informação das organizações.

Assim, este trabalho teve como objetivo, estudar a adoção de políticas de segurança dos sistemas de informação pelas universidades Moçambicanas, para esse efeito foi realizado um inquérito dirigido às faculdades/escolas superiores.

Com este estudo procurou-se contribuir para o conhecimento da realidade em Moçambique no que diz respeito à adoção de políticas de segurança dos sistemas de informação e para o enriquecimento da literatura de sistemas de informação, deficitária em estudos empíricos sobre a temática versada.

Das 69 faculdades/escolas superiores inquiridas, 43 (62%) indicaram possuir uma política de segurança e 26 (38%) referiram não terem qualquer política, contudo, foi mencionado por unanimidade que ponderam adotar uma política de segurança dos sistemas de informação.

Diante do que foi analisado, pode-se afirmar que este trabalho alcançou o seu objetivo, pois conseguir-se dar resposta à questão de investigação que lhe estava inerente, que era até que ponto as universidades de Moçambique têm ou não adotadas políticas de segurança dos sistemas de informação.

Uma dificuldade inicial com que se debateu na condução do inquérito relacionou-se com a falta de um entendimento claro e universal por parte dos respondentes para o conceito de política de segurança dos sistemas de informação. Foi com alguma dificuldade que diversos respondentes associaram esse conceito ao conjunto de regras que estabelecem o regime de utilização dos sistemas de informação das universidades. Para tal, poderá contribuir a enorme profusão de "roupagens" formais de normas e regras de procedimento existentes nas universidades, em virtude das mesmas se acharem vertidas por uma disparidade de documentos, tais como regulamentos internos, normas, despachos e até mesmo sob a forma de avisos no espaço de trabalho.

Contudo, a preocupação com a segurança dos ativos de uma empresa é visível e esperada em organizações, seja de pequena, média ou grande dimensão. A implementação de mediadas e ferramentas concretas que visam garantir essa segurança ou mesmo minimizar os possíveis incidentes são, no mínimo, ações que precisam de ser adotadas e consequentemente executadas por todos os utilizadores do sistema de informação.

Como trabalho futuro propõe-se a ampliação deste estudo sobre segurança da informação nas universidades Moçambicanas, partindo das políticas de segurança existentes nestes organismos analisando as suas características e componentes.

Agradecimentos

UNIAG, R&D unit funded by the FCT – Portuguese Foundation for the Development of Science and Technology, Ministry of Science, Technology and Higher Education. . Project n. º UID/GES/4752/2016

Referências

Dantas, M. (2011). Segurança da informação: uma abordagem focada em gestão de riscos. Edição nº1, Olinda: Livro rápido.

Dhillon, G. & Backhouse, J. (2000). InformationSystem Security Management in the New Millennium, Communications of ACM, 43 (7), 125–128.

Haeussinger, F. & Kranz, J. (2017). Antecedents of employees' information security awareness – Review, synthesis, and directions for future research. In Proceedings of the 25th European Conference on Information Systems.

Lopes, I. (2012). Adopção de Políticas de Segurança de Sistemas de Informação na Administração Pública Local em Portugal, Tese de Doutoramento, Universidade do Minho, Guimarães.

Lopes, I. & Oliveira, P. (2015). Implementation of Information Systems Security Policies: A Survey in Small and Medium Sized Enterprises. Álvaro Rocha et al (eds.). New Contributions in Information Systems and Technologies, Advances in Intelligent Systems and Computing, Volume 1. Springer International Publishing, 553, 459–468.

Lopes, I. & Oliveira, P. (2016). The Security Policies Application Process: Action Research. Álvaro Rocha et al. (eds.). New Advances in Information Systems and Technologies, Advances in Intelligent Systems and Computing, Volume 2. Springer International Publishing, 445, 353–362.

Peltier, T. R., Peltier, J. & Blackley, J. (2005). Information security fundamentals: Auerbach Publications – CRC Press Company.

Vaz, E. (2014). Segurança dos Sistemas de Informação Estudo de Caso INPHARMA. Dissertação do Mestrado, Universidade Jean Piaget, Cabo Verde.

Da Veiga, A. & Eloff, J. H. P. (2007). An Information Security Governance Framework, Information Systems Management, 24(4), 361–372.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 17/09/2017
Aceitação/Acceptance: 24/03/2018

Aplicabilidade do Regulamento Geral sobre Proteção de Dados em Clínicas de Saúde

Isabel Maria Lopes[1, 2, 3], Pedro Oliveira[1]

isalopes@ipb.pt, pedrooli@ipb.pt

[1] Instituto Politécnico de Bragança, Bragança, Portugal.

[2] UNIAG (Applied Management Research Unit), Instituto Politécnico de Bragança, Bragança, Portugal.

[3] Centro ALGORITMI, Universidade do Minho, Braga, Portugal.

Pages: 118–129

Resumo: O Regulamento Geral sobre Proteção de Dados (RGPD) visa assegurar a coerência da proteção das pessoas singulares no seio da União Europeia (UE). O RGPD compreende regras inovadoras muito importantes que serão aplicadas em toda a UE e afetarão de forma direta todos os Estados Membros. Além disso, o seu objetivo é superar os regulamentos fragmentados existentes e modernizar os princípios da privacidade na UE. É já em maio de 2018 que este regulamento entra em vigor, trazendo consigo vários desafios tanto aos cidadãos, como às empresas e outras organizações privadas e públicas. A proteção de dados pessoais é um direito fundamental. O RGPD considera uma "categoria especial de dados pessoais" e inclui aqui os dados relativos à saúde, pois são dados pessoais sensíveis, sujeitos, por isso, a especiais reservas quanto ao seu tratamento e acesso por terceiros. Dada esta premissa é aqui que este trabalho se vai debruçar, analisando a aplicabilidade do RGPD em clínicas de saúde em Portugal. Os resultados são discutidos á luz dos dados recolhidos através de um inquérito e identificados trabalhos futuros.

Palavras-chave: Regulamento (EU) 2016/679; regulamento geral sobre proteção de dados; dados pessoais, clínicas de saúde.

Applicability of the General Data Protection Regulation in Health Clinics

Abstract: The GDPR aims to ensure the coherence of natural persons' protection within the European Union (EU), comprising very important innovative rules that will be applied across the EU and will directly affect every Member State. Furthermore, it aims to overcome the existing fragmented regulations and to modernise the principles of privacy in the EU. This regulation will come into force in May 2018, bringing along several challenges for citizens, companies and other private and public organisations. The protection of personal data is a fundamental right. The GDPR considers a 'special category of personal data', which includes data regarding health, since this is sensitive data and is therefore subject to special conditions regarding treatment and access by third parties. This premise provides the focus of this research work, where the applicability of the GDPR in health clinics

in Portugal is analysed. The results are discussed in light of the data collected in the survey and possible future works are identified.

***Keywords**:* Regulation (EU) 2016/679; general data protection regulation; personal data, health clinics.

1. Introdução

O Regulamento 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril, que entrou em vigor a 25 de maio de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, que revoga a Diretiva 95/46/CE, de 24 de outubro de 1995, vem colocar inúmeros desafios a todas as empresas cujas atividades envolvam o tratamento de dados pessoais.

Embora a entrada em vigor tenha acontecido a 25 de maio de 2016, as empresas têm de implementar as alterações necessárias, de forma a garantir a plena conformidade do tratamento dos dados realizados com as novas determinações impostas pelo RGPD até 25 maio de 2018.

Assim, empresas e entidades públicas devem começar já a preparar internamente a sua organização para a aplicação do RGPD. É essencial conhecer as novas regras, analisar as novas obrigações, verificar o nível atual de cumprimento e adotar as medidas necessárias durante este período de transição para assegurar que tudo está pronto atempadamente (Comissão Nacional de Proteção de Dados, 2017).

Apenas através do conhecimento das regras versadas nesse documento de proteção de dados pessoais se poderá definir os procedimentos e adotar medidas que permitam, por uma lado, evitar os riscos de incumprimento da lei e, por outro, retirar maiores benefícios dos dados recolhidos.

Uma vez que a data final para a aplicabilidade do regulamento se aproxima do teu termo, é premente saber se as empresas já identificaram as alterações necessárias, para estarem em conformidade com o regulamentado da UE, bem como, se já estão a implementar essas alterações.

É neste contexto que se enquadra o presente trabalho, que estruturalmente após esta introdução, prossegue-se com a revisão da literatura sobre o regulamento geral de proteção de dados. Em seguida, a secção 3, centraliza-se na metodologia de pesquisa, identificando-se a população alvo e a estrutura do inquérito. Os resultados do estudo são discutidos na secção 4. Por último, apresentam-se as conclusões à luz dos resultados, identificam-se as limitações deste estudo e propõem-se trabalhos futuros.

2. Regulamento Geral sobre Proteção de Dados

O GDPR declara que as organizações precisam implementar medidas tecnológicas e operacionais adequadas para garantir a salvaguarda dos dados, incluindo a criação de fortes controlos de privacidade. As organizações devem por defeito, adotar medidas internas que respeitem os princípios da proteção de dados na fase de desenvolvimento. O que significa na prática é que a proteção de dados e a privacidade devem ser consideradas desde o início do processo de planeamento de segurança (Lei nº67/98, 1998).

Para um melhor entendimento, é conveniente definir o que se entende por "dados pessoais", o RGPD no artigo 4, define esses dados como informação relativa a uma pessoa singular identificada ou identificável ("titular dos dados"); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.

A lei de proteção de dados pessoais (Tankard, 2016), acrescenta à definição anterior a referente aos dados pessoais no sector da saúde que podem ser, historiais clínicos, historial e características de doenças e perfis de utilizadores/utentes.

O RGPD expande o propósito da proteção de dados para que qualquer pessoa ou qualquer organização que recolha e processe informação relacionadas com os cidadãos da UE, independentemente de onde eles se baseiam ou onde os dados são armazenados. O armazenamento em cloud não é uma exceção. A definição de dados pessoais também foi expandida. Afirma que os dados pessoais incluem informações a partir das quais uma pessoa poderá ser identificada, direta ou indiretamente. Sob a nova definição, identificadores como endereços IP e cookies são incluídos como informações pessoais (Lei nº67/98, 1998).

Tal como acontece com a diretiva de 1995 (EU Data Protection Directive) bem como, em outras diretivas e regulamentos, o GDPR não é prescritivo nas tecnologias que devem ser utilizadas para alcançar a conformidade. Isso não é nada fora do comum, uma vez que qualquer legislação que seja demasiado prescritiva corre o risco de tornar-se

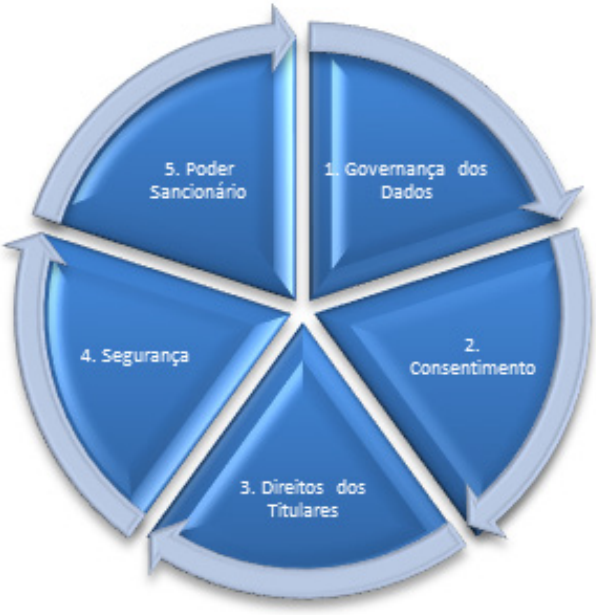


Figura 1 – Principais vetores de mudança

rapidamente obsoleta, especialmente devido ao rápido ritmo de mudanças tecnológicas no mundo de hoje. Como prescritivo podemos apontar a criptografia e a pseudonimização (pseudonymisation), que são apontadas como proteção adequada para os dados.

Contudo, é necessário garantir a capacidade de uma rede ou de um sistema informático de resistir, com um dado nível de confiança, a eventuais acidentais ou a ações maliciosas ou ilícitas que comprometam a disponibilidade, a autenticidade, a integridade e a confidencialidade dos dados pessoais não só dos clientes, mas também dos colaboradores/funcionários.

As organizações têm até 25 de maio de 2018 para se prepararem para as exigências decorrentes do regulamento, que se podem agrupar em cinco vetores de mudança principais, conforme se observa na Fig. 1 (SPMS, 2017):

No primeiro vetor "governança dos dados", o RGPD estabelece que todas as organizações devem implementar um conjunto alargado de medidas com vista a reduzir o risco de incumprimento das regras de privacidade e proteção de dados pessoais, demonstrando, assim, o seu compromisso relativamente a estas matérias e comprovando, sempre que solicitado, o cumprimento das regras aplicáveis. Ou seja traduz-se nas seguintes medidas (SPMS, 2017):

- Implementação dos conceitos de "privacidade desde a conceção" e "privacidade por defeito".
- Realização de "avaliação de impacto da privacidade" e consulta prévia à Comissão Nacional de Proteção de Dados.
- Designação de um encarregado da proteção de dados.
- Realização de auditorias de conformidade e adoção de políticas.
- Registo das atividades de tratamento.
- Maior responsabilização na escolha de entidades externas.
- Códigos de conduta e certificação.

O segundo vetor "Consentimento", o RGPD vem clarificar as condições que devem ser verificadas para que o consentimento do titular dos dados seja considerado válido e, como tal, um fundamento legal para o tratamento de dados.

O responsável pelo tratamento tem de demonstrar que o titular dos dados deu o seu consentimento (livre, específico, informado e agora também explícito).

Relativamente aos "dados sensíveis", como os dados relativos à saúde, têm de ser tratados ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional, ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade.

Para além disso, em relação aos "dados sensíveis" ou transferência de dados para fora da União Europeia, o consentimento tem de ser explícito. O silêncio, opções pré-validadas ou omissões do titular não constituem consentimento.

No terceiro vetor "direitos dos titulares dos dados", o RGPD alarga os direitos dos titulares, passando a existir o direito à limitação do tratamento e o direito à portabilidade, bem como novos requisitos quanto ao direito à eliminação dos dados e quanto à notificação de terceiros sobre retificação ou apagamento ou limitação de tratamento solicitados pelos titulares.

O quarto vetor intitulado "segurança", o RGPD apresenta um reforço das medidas de segurança dos dados, nomeadamente com a adoção de medidas técnicas como a pseudonimização (os dados não podem ser atribuídos a uma pessoa) e a encriptação dos dados pessoais e pela capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência durável dos sistemas e dos serviços de tratamento.

Para além disso as organizações têm de comunicar até 72 horas após ter acontecido uma violação de dados e de incidentes de segurança essa ocorrência à Comissão Nacional de Proteção de Dados.

No quinto e último vetor "poder sancionatório", o RGPD reforça os poderes das autoridades e aumenta o valor das coimas. Essas sanções são mais gravosas do que o atual quadro legal, podendo ascender os 20 milhões de euros ou 4% do volume de negócios global do exercício anterior.

Para além disto é necessário assegurar que os recursos humanos da empresa estejam conscientes das implicações do RGPD e tenham formação sobre as novas regras que dele advêm.

3. Metodologia de Pesquisa

A transformação digital nos últimos anos é notória em vários sectores, o da saúde não foge à regra e é hoje uma realidade incontornável.

Associado a esta revolução digital, surgem naturalmente preocupações ao nível da segurança, privacidade e proteção dos dados dos utentes, em particular dos dados de saúde e informação clínica (SPMS, 2017).

Com vista a caracterizar a aplicabilidade do RGPD pelas clínicas médicas, entendeu-se apropriado aplicar a técnica de inquérito, uma vez que potencia uma resposta clara, direta e objetiva às questões apresentadas aos inquiridos. Além disso, uma vez que o universo em estudo compreende milhares de clínicas, das quais 190 foram inquiridas, julgou-se que este número inviabilizava ou desaconselhava a adoção de técnicas de investigação alternativas.

O objetivo do inquérito é caracterizar o estado atual das clínicas de saúde, quanto à aplicabilidade do RGPD, ou seja, o nível de conhecimento e preparação para o tema da proteção e privacidade dos dados pessoais.

3.1. População

O inquérito foi remetido a 190 clínicas, contudo só 57 tiveram uma resposta efetiva o que corresponde a uma taxa de resposta de 30%. Para a seleção recorreu-se a uma amostragem aleatória, com base no tipo de clínica e distribuída pelos 18 distritos de Portugal mais os arquipélagos da Madeira e dos Açores.

Dos 190 contactos efetuados, em 35 obtiveram-se as respostas por via telefónica e em 22 casos via correio eletrónico, na sequência de um contacto telefónico prévio.

Tentou-se no maior número de casos possíveis que o respondente a este inquérito fosse o responsável pela informática, caso não existisse contactou-se o responsável pela clínica.

O estudo foi realizado entre os meses de outubro e dezembro de 2017.

3.2. Estrutura

A estrutura do Inquérito resultou da revisão de literatura sobre proteção de dados pessoais e do enquadramento legal com o estudo do Regulamento UE 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril – Regulamento Geral sobre Proteção de Dados.

As questões do inquérito, de resposta individual e de natureza confidencial, foram organizadas em três grupos.

O primeiro grupo visava obter uma breve caracterização da clínica e do respondente, seguindo-se os grupos de questões atinentes à aplicabilidade do RGPD, as quais eram antecedidas pela questão fundamental: "A clínica já implementou as medidas impostas pelo RGPD?".

Após a pergunta principal, e caso a resposta fosse negativa, passava-se para o grupo de questões onde se questionava os inquiridos se estavam a pensar implementar essas medidas, uma vez que ainda não estão em conformidade com o regulamento, e caso estivessem a pensar adota-las, se as mesma já estava em processo de implementação. Se não estivessem a pensar adotar qualquer medida, eram questionados se têm conhecimento das coimas que podem pagar, pelo incumprimento do regulamentado e o porquê para a não adoção dessas medidas.

Caso a resposta à questão principal fosse positiva, passava-se aos grupos de questões direcionadas para as empresas que já estão em conformidade com o regulamento ou que estão a implementar as mediadas por ele impostas. Algumas das questões colocadas neste grupo foram: Está a implementar as medidas vertidas no regulamento? Já identificou ou nomeou alguém para responsável pelo tratamento de dados? Já foram feitas ações de formação e sensibilização dos colaboradores sobre as novas regras? A proteção de dados pessoais é uma prioridade nessa clínica? O plano para estar em conformidade com o regulamento como foi feito?

O inquérito foi bastante abrangente, contudo para este estudo, o foco recaiu só no nível da caracterização, ou seja, do estado atual das clínicas de saúde em relação ao cumprimento das medidas impostas pelo RGDP.

4. Resultados

As organizações estão neste momento a usufruir de um intervalo de dois anos de adaptação, tempo que pode e deve ser utilizado para conhecer as novas regras e analisar as novas as exigências decorrentes do regulamento, adotando as medidas necessárias, para assegurar que tudo está em conformidade no término deste período.

O primeiro grupo de questões recaiu sobre a caracterização da clínica e da pessoa que respondeu ao inquérito, como essas dados são confidenciais, caracteriza-se na Tabela 1 o tipo de clínicas às quais foi remetido o inquérito e o número de clínicas que respondeu, em função do seu tipo. Como já foi anteriorme nte referido, foram contactadas 190 clínicas de áreas diferentes e geograficamente dispersas pelo País, das quais de conseguiu obter resposta efetiva de 57.

Tipo de Clínica	Clínicas contactadas	Clínicas inquiridas
Enfermagem	49	12
Médicas Dentárias	36	16
Oftalmológicas	12	4
Médicas e de Diagnóstico	39	15
Ortopédicas	11	3
Fisioterapia	43	7

Tabela 1 – Clínicas Inquiridas

Questionados sobre se iniciaram ou concluíram o processo de implementação das medidas previstas no RGDP, 43 (75%) responderam que não e 14 (25%) responderam que já iniciaram ou terminaram a adoção dessas medidas (Fig.2).

Das 14 clínicas que responderam afirmativamente, só 4 clínicas é que consideram que já estão em conformidade com o previsto no regulamento. As restantes 10 clínicas ainda estão a implementar essas medidas.

Este número parece residual quando vemos que das 57 clínicas inquiridas, só 7% é que têm o RGDP implementado.

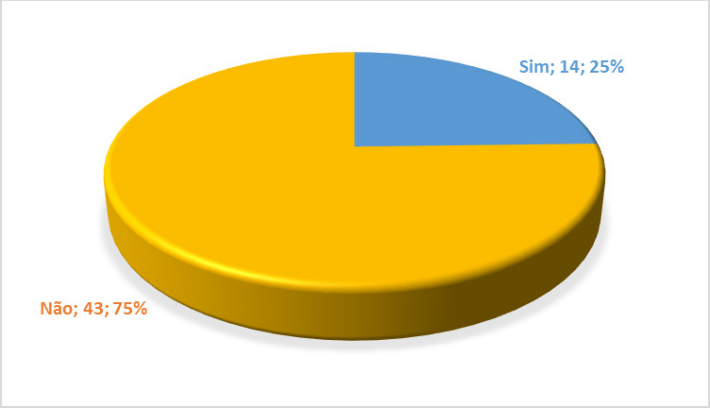


Figura 2 – Clínicas que estão a implementar o RGPD

A maioria das clínicas inquiridas está consciente sobre as obrigações e desafios do novo regulamento geral de proteção de dados, embora pareça um contrassenso pois só 25% é que adotaram ou estão adotar as medidas impostas pelo regulamento.

Para um melhor entendimento podemos agrupar as clínicas em três clusters, conforme se observa na Fig.3:

- Cluster 1 – Clínicas em conformidade com o regulamento;
- Cluster 2 – Clínicas que estão a implementar as medidas impostas pelo regulamento;
- Cluster 3 – Clínicas que não estão em conformidade com o regulamento.

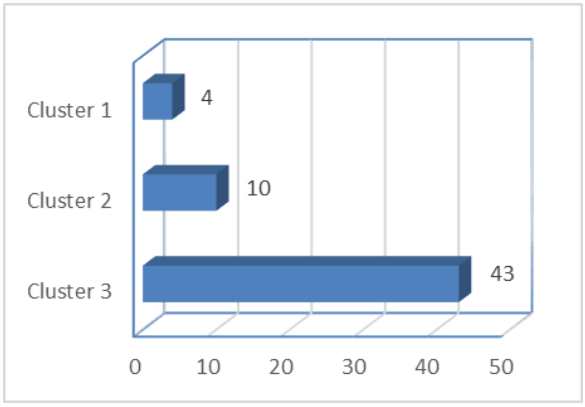


Figura 3 – Clusters em função da implementação do RGPD

Relativamente ao Cluster 1, questionados sobre como implementaram as novas regras, as quatro clínicas responderam de igual forma, que não tinham ninguém na empresa que tivesse conhecimento suficiente para a sua implementação. Verificou-se que recorreram a empresas externas para os orientarem, de forma, a ficarem de acordo com as medidas impostas pelo RGPD.

Verificou-se também que das quatro clínicas que responderam estar em conformidade com o regulamento, só uma tem identificada e nomeada a pessoa que ficará responsável pelo tratamento dos dados.

Genericamente, observou-se a sensibilidade e importância para a formação dos dirigente e funcionários, contudo ainda não foi feita qualquer ação de formação ou sensibilização sobre as novas regras a adotar, embora estejam previstas essas ações para breve. É premente assegurar que os colaboradores estejam conscientes das implicações do RGPD e para isso a formação será o meio mais eficaz.

Questionados se consideram totalmente finalizado este processo, a resposta foi unânime em responder que não. Consideram que têm de garantir a continuidade da conformidade com o regulamento. Para o efeito, deverão ser efetuadas com alguma regularidade, auditorias para avaliar o estado de conformidade da clínica. Por outro lado, irão surgir necessidades de adaptação dos processos e procedimentos devido a novas necessidades do negócio as quais deverão ter sempre medidas que cumpram os requisitos de proteção "desde a conceção" e proteção "por defeito".

Em relação às clínicas que se enquadram no Cluster 2, que neste caso são 10, pois encontram-se a implementar as medidas definidas pelo RGDP, questionadas sobre

como está a ser feita a implementação, duas clínicas responderam que é uma empresa de informática que já dava apoio à clinica a vários níveis, três responderam que as alterações estão a ser feitas por pessoal interno e as restantes cinco clínicas, responderam que são empresas que prestam serviços de consultadoria especializada que os estão a orientar, para garantir a conformidade das clínicas com este regulamento.

Maioritariamente, as empresas estão a recorrer a empresas externas para a implementação de práticas efetivas, que as coloque em conformidade com o regulamento (Fig.4).

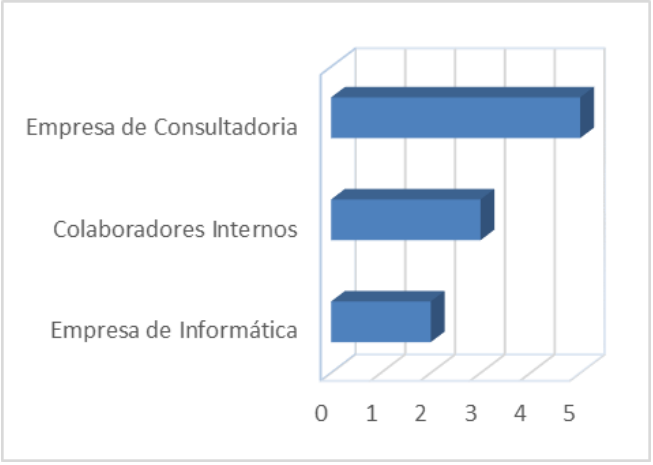


Figura 4 – Quem está a implementar o regulamento

Questionados se vão estar preparados em Maio de 2018, uma vez que são empresas que incluímos no Cluster 2, pois neste momento têm implementadas ações pontuais em áreas específicas, 40% afirmaram que sim, 50% pensam conseguir e 10% das clínicas entendem que não vão conseguir ter o regulamento adotado até essa data.

Questionados se sabem da existência de penalizações e coimas no caso de incumprimento, a resposta foi unânime em afirmar que sim, embora desconheçam os detalhes e os montantes que podem ser aplicados.

Para além das coimas que possam ser aplicadas às clínicas, também está contido no regulamento, que as empresas responsáveis pelo tratamento de dados respondem pelos danos causados por um tratamento que viole o regulamento, sendo obrigado a indemnizar a pessoa que tenha sofrido danos materiais ou imateriais devido a essa violação, tratando-se de clínicas de saúde essa responsabilidade é acrescida.

Quanto às empresas inseridas no Cluster 3 – Clínicas que não estão em conformidade com o regulamento, foram questionadas se consideram a proteção de dados pessoais uma prioridade para a sua empresa? E a resposta foi positiva nas 43 clínicas, o que

denota consciencialização das empresas, para a implementação de procedimentos de proteção dos dados pessoais dos seus clientes, dirigentes e colaboradores.

Naturalmente, não basta apenas existir consciência sobre a importância da aplicação do regulamento, é imperativo que as empresas materializem esta consciência em ações concretas que conduzam à conformidade com o RGDP. Esta consciencialização manifestada não se reflete nos resultados, uma vez que só 9% das clínicas inquiridas responderam estar em conformidade com o novo regulamento de dados pessoais.

Seguidamente, dada a consciencialização relativa à proteção de dados, foram questionadas se vão implementar o regulamento. Das 43 clínicas pertencentes ao Cluster 3, 25 (58%) responderam que vão iniciar brevemente esse processo, 8 (19%) não estão a pensar implementar o regulamento e 10 (23%) desconhecem a existência do regulamento aprovado pelo Parlamento Europeu em maio de 2016, por isso não têm opinião (Fig.5).

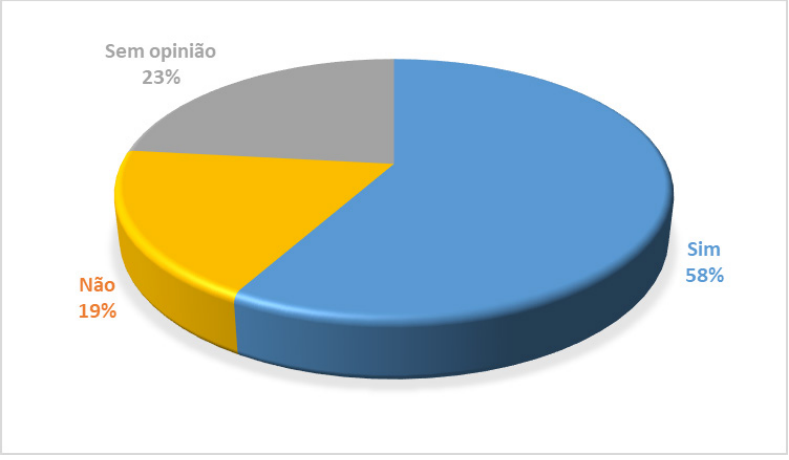


Figura 5 – Clínicas que vão iniciar ou não a adoção do RGPD

Relativamente às 8 clínicas que não estão a pensar adotar as medidas do RGDP, as razões são: falta de recursos financeiros, a dimensão da clínica não justifica, consideram o que têm suficiente e não sabem como adotar essas medidas.

Genericamente, verifica-se algum desconhecimento sobre o RGPD principalmente nos seus detalhes, embora haja uma perceção da elevada importância a atribuir à proteção dos dados pessoais, não estão na maioria das empresas reunidas as condições para estarem em conformidade com o regulamento.

Questionados sobre se têm conhecimento das penalizações e coimas de que podem ser alvo, pelo não cumprimento do regulamento, 28 clínicas ou seja 65% não tem conhecimento e 15 clínicas (35%) afirmaram saber dessas penalizações e coimas (Fig. 6).

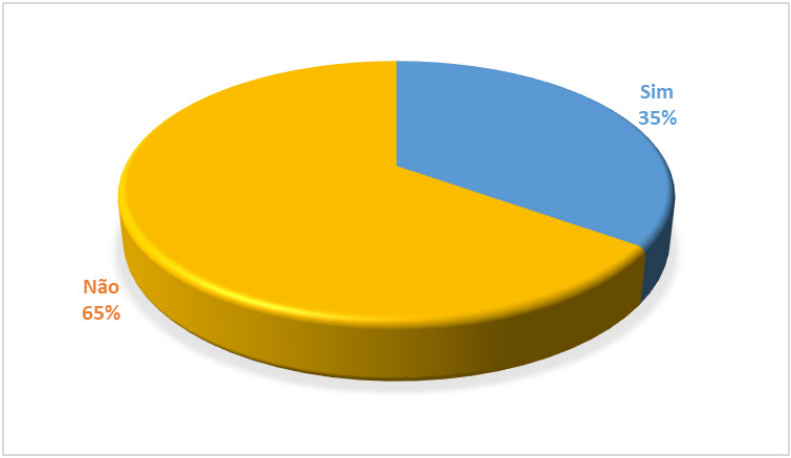


Figura 6 – Conhecimento sobre as coimas aplicar

Do total das empresas que responderam ao inquérito, a maioria consideram o período estipulado de dois anos para a adaptação das empresas ao novo RGPD insuficiente, distribuindo-se esses resultados da seguinte forma: 10 (31,5%) consideram suficiente, 29 (50,8%) consideram insuficiente e as restantes 10 clínicas (17,6%) não têm opinião formada.

A duração da implementação do RGDP irá sempre depender da complexidade da atividade da empresa, do volume e variedade de dados pessoais utilizados, do estado de maturidade da empresa em termos organizacionais, da adequabilidade e flexibilidade dos sistemas de informação e da disponibilidade de todos os intervenientes. Não é fácil definir o tempo que demora a garantir a conformidade com o regulamento, como muitas empresas só agem no término dos prazos, acredita-se, que a grande maioria das empresas estará preparada para garantir essa conformidade no prazo exigido, tendo também em consideração, que as coimas que lhe podem ser aplicadas são elevadas.

5. Conclusões

A maioria da informação que, presentemente, é partilhada digitalmente anteriormente era partilhada em papel, suscitando assim, novos desafios e ameaças digitais ao nível da segurança e privacidade, nomeadamente em relação à proteção dos dados pessoais numa sociedade cada vez mais digital (SPMS, 2017).

Atualmente existem 28 leis de proteção de dados baseados na EU Data Protection Directive de 1995, ou seja, implementada há 20 anos e que gradualmente está a ser substituída pelo novo RGPD (Rys & Grest, 2016). Com os avanços das tecnologias de informação e comunicação, nestes dois últimos séculos, as mesmas só podem estar completamente desajustadas para poderem proteger os dados dos indivíduos e das empresas.

O RGPD introduz não só novas regras como também um sistema sancionatório, com a aplicação de coimas em caso de incumprimento, o que exige uma atenção cuidada das organizações que lidam e possuem à sua guarda dados pessoais.

Este regulamento coloca o ónus de responsabilidade dos dados pessoais (tratamento e conformidade) nas organizações, ao contrário do que se verificava anteriormente, que era responsabilidade da Comissão Nacional de Proteção de Dados, que agora lhe vai caber a obrigação de inspecionar o cumprimento do regulamento.

Este regulamento prevê novas obrigações, até aqui não obrigatórias, nomeadamente um registo com todas as operações de dados pessoais.

Na implementação do RGPD haverão desafios que não serão fáceis de ultrapassar, em muitos casos é de uma mudança cultural que se trata mas, para muitas empresas poderá ser uma oportunidade para finalmente documentarem os seus processos e procedimentos, implementarem os seus valores, consolidarem a sua ética empresarial e demonstrarem ao mercado, aos seus clientes, parceiros e colaboradores uma coerência convincente e motivadora.

A recente aprovação do RGPD mantém perspetivas positivas para o futuro da proteção de dados na Europa. A existência de um quadro jurídico sólido e uniforme em toda a Europa que tenha sido atualizado para atender às necessidades da tecnologia, não só permitirá libertar o potencial do mercado digital, para a promoção da inovação, para a criação de emprego e geração de riqueza, mas também para proteger o direito fundamental da proteção de processamento de dados para cidadãos ou residentes na Europa (Díaz, 2016).

Agradecimentos

UNIAG, R&D unit funded by the FCT – Portuguese Foundation for the Development of Science and Technology, Ministry of Science, Technology and Higher Education. Project n. º UID/GES/4752/2016

Referências

Comissão Nacional de Protecção de Dados. (2017). 10 Medidas para preparar a aplicação do regulamento europeu de proteção de dados.

Díaz, Díaz, E. (2016). The new European Union General Regulation on Data Protection and the legal consequences for institutions, Church, Communication and Culture, 1, 206–239.

Lei n.º 67/98 de 26 de outubro, Lei da Proteção de Dados Pessoais, Diário da República n.º 247/1998, Série I-A de 1998-10-26.

Ryz, L. & Grest, L. (2016). A new era in data protection, Computer Fraud & Security, v. 2016, 3, 18–20.

SPMS (2017) – Serviços Partilhados do Ministério da Saúde, Privacidade da informação no setor da saúde.

Tankard, C. (2016). What the GDPR means for business, Network Security, v. 2016, 6, 5–8.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 14/09/2017
Aceitação/Acceptance: 17/03/2018

Detección de anomalías con selección negativa y gráfos de perfiles de comportamiento del usuario

César Byron Guevara Maldonado[1], Janio Jadán-Guerrero[2]

cesargue@uti.edu.ec, janiojadan@uti.edu.ec

[1] Centro de Investigación en Mecatrónica y Sistemas Interactivos (MIST) de la Universidad Tecnológica Indoamerica, Quito, Ecuador.

[2] Centro de Investigación en Mecatrónica y Sistemas Interactivos (MIST) de la Universidad Tecnológica Indoamerica, Quito, Ecuador.

Pages: 130–143

Resumen: Este trabajo propone la aplicación de Grafos y sistemas inmunes artificiales con Selección Negativa para el desarrollo de un algoritmo de Detección de Anomalías basado en el comportamiento de usuarios dentro de sistemas informáticos. El desarrollo de este algoritmo permite identificar actividades anómalas durante la ejecución de las tareas, como también al finalizar la sesión de usuario. Las principales contribuciones de este trabajo son: creación de un perfil de usuario basado en grafos para la detección y predicción de anomalías en ejecución tareas. Además, la generación de comportamientos anómalos para la detección de irregularidades al finalizar la sesión de usuario. El artículo presenta de forma detallada el desarrollo y el aceptable resultado en la detección de tareas fraudulentas, mostrando una óptima precisión y un bajo porcentaje de falsos positivos.

Palabras-clave: Grafos, Detección de Anomalías, Sistemas Informáticos, Selección Negativa.

Anomaly Detection with Negative Selection and Graphs of User Behavior Profiles

Abstract: This work proposes the application of a Negative Selection Algorithm inspired in Artificial Immune Systems and the use of Graphs. This approach allows to identify anomalous activities based on user's behavior, during the execution of tasks, as well as at the end of the user session. The main contributions of this work are: creation of a graph-based user profile for the detection and prediction of anomalies in execution tasks. In addition, the generation of anomalous behaviors for the detection of irregularities at the end of the user session. The article presents in detail the development and the acceptable result in the detection of fraudulent tasks, showing an optimum precision and a low percentage of false positives.

Keywords*:* Graphs, Artificial Immune Systems, Negative Selection Algorithm, anomaly detection, user behavior.

1. Introducción

La detección de anomalías es un área de investigación de vital importancia con un sin fin de aplicaciones de alto impacto en distintas disciplinas como la economía, ciberseguridad, las finanzas, la medicina, entre otras. En la actualidad se han desarrollado varias técnicas y algoritmos para identificar valores atípicos y anomalías en los conjuntos de datos multidimensionales no estructurados. El presente trabajo presenta el desarrollo de un algoritmo detección de anomalías en un sistema informático aplicando teoría de grafos y la selección negativa basado en el comportamiento único de cada uno de los usuarios de un sistema informático. La detección de anomalías de los datos en secuencias de ejecución de tareas es un tema importante de investigación en la ciber defensa ya que existen muchos trabajos sobre tema.

La aplicación de la teoría de grafos en la detección de anomalías se ha convertido una de las técnicas que ha brindado nuevo enfoque en su estudio e implementación en múltiples áreas de la ciencia. Una de las principales ventajas en la detección de anomalías es la alta correlación entre los datos y un largo alcance en su representación gráfica, además de brindar un eficiente análisis.

Un ejemplo de la aplicación de grafos es el trabajo de (Messinger, 2011), el cual realiza un algoritmo de detección de anomalías para el procesamiento de imágenes espectrales, que en lugar de aplicar un modelo de datos han utilizado el concepto de un grafo tridimensional. Este grafo espectral contiene varias métricas que se pueden calcular relacionando la conectividad global de la imagen debido a la conectividad entre píxeles individuales (métrica para la detección de anomalías). Los resultados presentados en este trabajo para una imagen hiperespectral han demostrado ser bastante buenos y casi similares al algoritmo RX.

En el trabajo de (Le, 2011) se propone un método para detectar anomalías en el tráfico de red basado en los conceptos de teoría de grafos como la distribución de grado máximo y la distancia DK-2. El principal enfoque aplicado es la aplicación de los grafos de dispersión de tráfico (TDG) para modelar el tráfico de red en el transcurso del tiempo. Se realiza un análisis de las diferencias entre los grafos TDG en series de tiempo para detectar anomalías e introducir un método para identificar patrones de ataque en el tráfico anómalo, con resultados óptimos y una tasa de detección bastante alta.

Otro ejemplo es el trabajo presentado por (Fontugne, 2010) busca identificar objetos o tareas anormales que son diferentes de las normales en el tráfico de red. El trabajo propone una metodología basada en la teoría de grafos que relaciona las salidas de múltiples algoritmos teniendo en cuenta toda la información recopilada. El método propuesto identifica de forma eficiente las anomalías en el tráfico de la red. La aplicación de este estudio mostró que la teoría de grafos es una herramienta con sin fin de aplicaciones y con un alcance bastante eficiente en termino implementación.

Por otra parte, el algoritmo de selección negativa ha sido en los últimos años muy utilizado para desarrollar novedosas soluciones a problemas técnico – específicos de varias disciplinas, como, por ejemplo: detección de virus informáticos, detección de malware, diagnóstico de fallas, detección de fraude en tarjetas de crédito, entre otras.

Uno de estos trabajos es el que presenta (Aydin, 2010), donde se propone un nuevo algoritmo de selección negativa que utiliza mapas caóticos para la selección de parámetros. Este trabajo se ha realizado una mejora en la aplicación de selección negativa con generadores de números caóticos para la mutación y generación de la población inicial. El algoritmo propuesto utiliza la selección clonal para obtener detectores óptimos.

Otro trabajo en esta misma línea es el de (Gong, 2012) que presenta una mejora algoritmo de selección negativa para la detección de anomalías mediante la integración de una nueva metodología de formación de detectores en la etapa de entrenamiento. El principal proceso de formación continua es la generación detectores self y una reducción de muestras self no compatibles para reducir el coste computacional en fase de pruebas. El algoritmo propuesto obtiene una tasa de detección alta y una baja tasa de falsas alarmas en la mayoría de los casos.

En el trabajo desarrollado por (Bhuyan, 2014), presenta un algoritmo con múltiples fases para la detección de anomalías de red, que clasifica aplicando técnicas y métodos existentes basados en las aplicaciones computacionales que utilizan varios conjuntos de datos. Esta propuesta ha obtenido resultados eficientes y con una tasa de falsos positivos bastante baja.

El algoritmo propuesto se enfoca en la detección de anomalías en secuencias discretas para encontrar posibles intrusiones, fraudes, fallos o posibles fugas de información. La detección de anomalías para las secuencias discretas no es una tarea fácil, ya que implica el análisis de secuencias normales de datos para detectar posibles irregularidades.

El documento está organizado de la siguiente manera: en la sección 2, muestra los métodos y materiales utilizados como la teoría de grafos, algoritmo de selección negativa y el algoritmo de búsqueda local de secuencias. En la sección 3, se detalla el desarrollo del algoritmo propuesto, es decir, la estructura de los datos que sirven de base para la investigación, el modelamiento matemático y el proceso del algoritmo. Sección 4 describe los resultados del experimento realizado en este trabajo. Por último, las conclusiones que se han extraído de esta investigación.

2. Materiales y Métodos

Los datos con los que se ha realizado este trabajo fueron proporcionados por una entidad de gobierno de la República de Ecuador, dicha información corresponde a un sistema informático real. La información se ha codificado para salvaguardar la confidencialidad y proteger su integridad. El conjunto de datos fue recabado mediante captura de ejecuciones de operaciones de los usuarios a la base de datos, mediante la utilización un sistema informático con fines de auditoría. La información pertenece al período comprendido entre los años 2011 a 2013, con 15.571 registros de sesiones normales y 5312 de registros de sesiones anómalas, además, estos datos fueron producidos por diez usuarios que han permanecido realizando ejecuciones de forma regular en el sistema durante ese periodo de tiempo.

Este conjunto de datos contiene todo el comportamiento normal de cada uno de los usuarios dentro del sistema, desde inicio hasta el fin de cada sesión incluyendo todas las ejecuciones de tareas que realicen los usuarios.

El sistema informático con el que se va a trabajar contiene siete tablas principales en la base de datos ($Tb_1, Tb_2, \ldots, Tb_7$), donde es posible ejecutar las cuatro operaciones sql que son Insertar, Modificar, Eliminar y Buscar. La estructura de datos de una sesión de usuario está conformada por un login (acceso al sistema) y una o varias tareas ejecutadas en forma secuencial, es decir, no tiene un tamaño fijo. Las tareas fueron codificadas en 28 tareas genéricas, es decir, las cuatro operaciones para cada una de las tablas, además, no se toma en cuenta el inicio ni el fin de cada sesión de usuario. Se define a cada tarea genérica como T_n, donde n es el número de la tarea. El conjunto de tareas ejecutadas por un usuario U se define como $T^U = \{T_1, T_2, T_3, \ldots, T_m\}$ donde m es el número de tareas ejecutadas por el usuario. Una sesión se define como $S^U = \{T_1^U, T_2^U, T_3^U, \ldots, T_l^U\}$, donde l es número de tareas de usuario dentro de una sesión. El conjunto de sesiones históricas se define como $Hs^U = \{S_1^U, S_2^U, S_3^U, \ldots, S_r^U\}$, donde r es el número sesiones que contiene el histórico. Una nueva sesión de usuario es llama Sesión Activa As^U, la cual contiene una o varias tareas T_n han sido ejecutadas por el usuario, la cual va ser objeto de análisis en la fase de pruebas. Esta estructura es bastante dinámica como se muestra en la Figura 1.

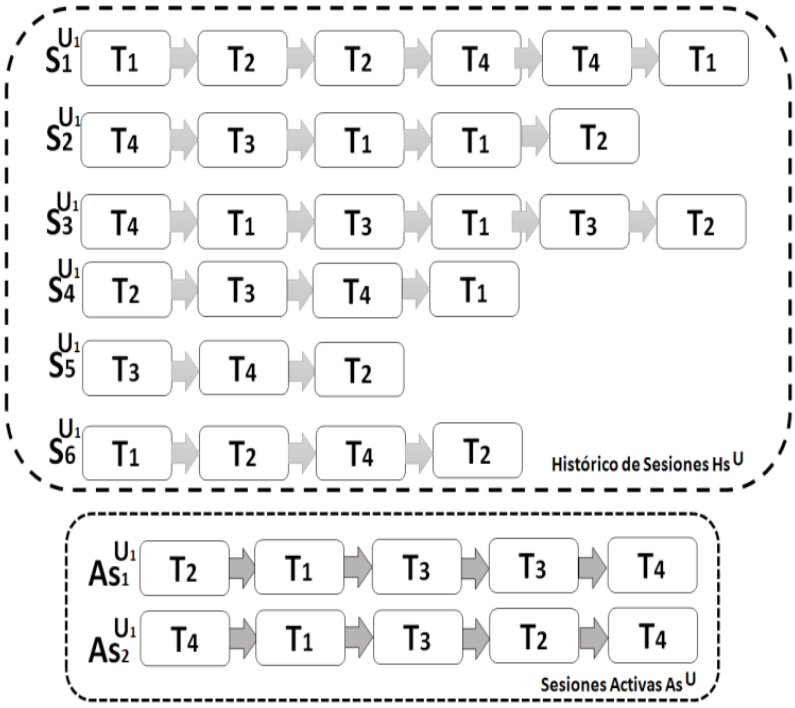


Figura 1 – Estructura de datos de sesiones Históricas Hs^U y sesión activa As^U, del comportamiento de usuario en un sistema informático.

El comportamiento de cada usuario es dinámico y diferente de otro usuario, esto permite definir de una manera más real la conducta individual de cada usuario dentro

del sistema. Aplicando esta estructura de datos se desarrolla el algoritmo de detección de anomalías.

A continuación, se presentarán los algoritmos utilizados los cuales son la base fundamental para el desarrollo del algoritmo propuesto de detección de anomalías.

2.1. Teoría de grafos

La teoría de grafos es una rama de las matemáticas discretas que utiliza una multitud conceptos de diversas áreas como combinatorias, álgebra, probabilidad, geometría de polígonos y aritmética, que analiza las propiedades de los grafos y sus estructuras. El conocimiento profundo de la teoría de grafos junto con los algoritmos de implementación son la base fundamental para conseguir el mayor rendimiento de las operaciones con datos, sobre todo si éstos son complejos en su organización. Los grafos, definidos como *G* constan de dos partes: el conjunto de vértices definido como *V*, nodos o puntos y el conjunto de aristas definidas como *A* (líneas o lados) (Noble, 2003; Akoglu, 2015).

La teoría de grafos es posible solucionar una amplia gama de problemas como por ejemplo la síntesis de circuitos secuenciales, análisis de anomalías, etc. Los grafos son aplicables a varias áreas de la informática e ingeniería (Messinger, 2010; Fontugne, 2010; Le, 2011).

2.2. Selección Negativa

La Selección Negativa es un sistema inmunológico artificial el cual es aplicado en una multitud de áreas de conocimiento, pero en su gran mayoría a sistemas computacionales, como discriminador de objetos o elementos ajenos y dañinos para este sistema. Por ejemplo, la detección de virus computacionales, detección de intrusos y detección de anomalías. Este algoritmo realiza una tarea de filtro o discriminador entre los elementos normales (propios) y anormales (impropios) del sistema durante un periodo normal de funcionamiento. El objetivo principal es detectar un posible intruso o una acción fraudulenta de cualquier secuencia subsecuente que debe ser similar al perfil normal de un usuario o equipo, y cualquier irregularidad es identificada como un posible archivo o actividad maliciosa. Entre los trabajos más importantes son los de (Aydin, 2010), (Gong, 2012) y (Laurentys, 2010).

2.3. Algoritmo Shift-Or

El algoritmo Shift-Or trabaja con un conjunto de letras o caracteres desarrollando un alfabeto propio el cual utiliza una máquina de estados. El alfabeto generado lo conforman todos los caracteres diferentes del texto y del patrón. Los estados existentes en el algoritmo son la comparación de las diferentes partes de un patrón base con diferentes partes, en donde se utilizan dos operaciones: el desplazamiento (SHIFT), el cual da paso de un estado a otro y la operación lógica OR para calcular el siguiente estado. En la actualidad existen varios trabajos que aplican este algoritmo a la detección de intrusos como lo presenta (Oh, 2012) y en la búsqueda de patrones como lo detalla (Wang, 2012).

3. Desarrollo del algoritmo de Detección de Anomalías

El algoritmo propuesto en este trabajo contempla el análisis (detección) y predicción en tiempo real (online) de ejecución de las tareas de usuario (Mehnaz, 2016), como también, el análisis de las tareas ejecutadas por el usuario al finalizar la sesión (offline) y comprobación del resultado con el algoritmo UCS. La aplicación de esta metodología para la detección de anomalías permite que el algoritmo sea más eficiente y dinámico en el momento de identificar tareas irregulares o posiblemente fraudulentas.

3.1. Detección de Anomalías en tiempo real (online)

En esta parte del algoritmo se describe la creación de un modelo matemático aplicando grafos dirigidos a la estructura de datos anteriormente descrita en la sección 2. El grafo G del comportamiento de usuario está construido por varios sub-grafos SG que utilizan las tareas T^U como vértices de origen y vértices de destino del sub-grafo dirigido. Cada sub-grafo SG se construye dependiendo de la posición p de la tarea ejecutada en la sesión S_n^U, es decir, todas las tareas T^U que se ejecutaron en la posición p=1 serán vértices origen y las tareas T^U que se ejecutaron en la posición p=2 serán vértices destino. La arista del sub grafo está definida como $C_{T_i^p, T_j^{p+1}}$, donde T_i es la tarea inicial y T_j es la tarea final. El valor de la arista es calculado por el número de veces que se repite la combinación (i, j) en la posición p y $p+1$. Este proceso se realiza varias veces dependiendo del tamaño máximo de tareas T^U de las sesiones S^U existentes en el histórico de sesiones Hs^U. Por ejemplo, utilizando la estructura de datos de la Figura 1 se obtiene el siguiente grafo en la Figura 2, donde, el valor de la arista entre los vértices T_4 y T_1 en la posición inicial $pi = 1$ y posición final $pf = 2$ es $C_{T_4^{pi=1}, T_1^{pf=2}} = 1$.

Una vez generado el grafo G es necesario crear $p-1$ número de matrices $M^{p,p+1}$de dimensiones (mxm) donde m es el número total de tareas ejecutadas por el usuario (vértices del grafo SG en la posición p), donde el valor de las aristas es C_{T_i,T_j} de los vértices. Las matrices $M^{p,p+1}$se muestran a continuación:

$$M^{p,p+1} = \begin{pmatrix} C_{T_1,T_1} & \cdots & C_{T_1,T_m} \\ \vdots & \ddots & \vdots \\ C_{T_m,T_1} & \cdots & C_{T_m,T_m} \end{pmatrix}$$

En el ejemplo del histórico de sesiones de la Figura 1 se obtienen las siguientes matrices $M^{p,p+1}$ con posiciones $p = 6$:

$$M^{1,2} = \begin{pmatrix} 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}; M^{2,3} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} M^{3,4} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix};$$

$$M^{4,5} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}; M^{5,6} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Una vez obtenidas las matrices $M^{p,p+1}$ se va a aplicar el siguiente proceso evaluando una a una las combinaciones de tareas T_i y T_j de la nueva sesión As^U. En el algoritmo existen dos funciones las cuales tienen como objetivo calcular el valor de las aristas de los vértices T_i y T_j. Dichas funciones son las siguientes:

- Buscar Valor Matriz en P: Esta función busca los valores de las aristas de los vértices T_i y T_j en la matriz $M^{p,p+1}$,dependiendo de su posición p en la que fueron ejecutadas las tareas. Es decir, busca las tareas (T_i, T_j) en la misma posición que fueron ejecutadas en el histórico Hs^U.

  El resultado debe ser un número entero (si la combinación fue ejecutada al menos una vez) o vacío (si no fue ejecutada en esa posición).
- Buscar Valor Matrices Sin P: Esta función busca los valores de las aristas de los vértices T_i y T_j en todas las matrices $M^{p,p+1}$ sin tomar en cuenta la posición p. Es decir, busca las tareas (T_i, T_j) que fueron ejecutadas en el histórico Hs^U en todas las posiciones existentes.

  El resultado debe ser un número entero (si la combinación fue ejecutada al menos una vez) o vacío (si no fue ejecutada).

El funcionamiento del algoritmo se describe en el siguiente pseudocódigo:

$$C_{T_i,T_j} = \text{Bucar\_Valor\_Matriz\_en\_P}(T_i, T_j, p);$$

If $C_{T_i,T_j} \neq 0$ **then**

$$result = normal;$$

Else

$$C_{T_i,T_j} = \text{Bucar\_Valor\_Matrices\_sin\_P}(T_i, T_j);$$

If $C_{T_i,T_j} \neq 0$ **then**

$$result = normal;$$

Else

$$result = anormal;$$

End If

End If

Si el resultado de este procedimiento es igual a '*normal*' el usuario puede seguir ejecutando tareas ya que este análisis es continuo hasta que finalice la sesión. Caso contrario si el resultado obtenido es '*anormal*', se envía una alerta al administrador del sistema y se evita que el usuario pueda realizar más ejecuciones dentro del sistema, además, es detectado como posible anomalía y se almacena en el sistema para futuros análisis.

La implementación del algoritmo de detección de anomalías en una capa intermedia entre la interfaz del usuario y la ejecución de las operaciones en la Base de datos permite que las todas actividades del usuario queden bloqueadas si han sido detectadas como anómalas.

Como ejemplo de este procedimiento se presenta la sesión activa $As_1^{U1} = \{T_2, T_1, T_3, T_3, T_4\}$, la cual presenta los siguientes resultados:

(T_2, T_1): El valor $C_{T_2,T_1} = 0$ en la posición pi=1 y pf=2, donde el resultado de la detección es ***'anormal'***.

(T_1, T_3): El valor $C_{T_1,3} = 1$ en la posición pi=2 y pf=3, donde el resultado de la detección es ***'normal'***.

(T_3, T_3): El valor $C_{3,T_3} = 0$ en la posición pi=3 y pf=4, donde el resultado de la detección es ***'anormal'***.

(T_3, T_4): El valor $C_{3,T_4} = 1$ en la posición pi=4 y pf=5, donde el resultado de la detección es ***'normal'***.

Con estos resultados las secuencias (T_2, T_1) y (T_3, T_3) han sido detectadas como anormales y se procederá a bloquear dichas tareas además de alertar al administrador del sistema.

En la sesión activa $As_2^{U1} = \{T_4, T_1, T_3, T_2, T_4\}$, la cual presenta los siguientes resultados:

(T_4, T_1): El valor $C_{T_4,T_1} = 1$ en la posición 1 y 2, donde el resultado de la detección es ***'normal'***.

(T_1, T_3): El valor $C_{T_1,3} = 1$ en la posición 2 y 3, donde el resultado de la detección es ***'normal'***.

(T_3, T_2): El valor $C_{3,T_2} = 1$ en la posición 3 y 4, donde el resultado de la detección es ***'normal'***.

(T_2, T_4): El valor $C_{2,T_4} = 1$ en la posición 4 y 5, donde el resultado de la detección es ***'normal'***.

Los resultados de esta sesión activa han sido detectados como normal, y el usuario podrá proseguir con su trabajo de forma habitual.

En la siguiente etapa del algoritmo se detectará anomalías en las sesiones activas luego de que hayan salido del sistema utilizando selección negativa.

3.2. Detección de anomalías en fin de sesión (offline)

En esta sección se va desarrollar un nuevo modelo de datos para aplicar la selección negativa y generar detectores anómalos para aplicar el algoritmo Shift-Or a una sesión As^U, de esta manera identificar si contiene tareas anómalas.

Como primer paso, se va a identificar las tareas más ejecutadas por el usuario y se crea una tabla que defina si existe esa tarea en el sesión S^U en el histórico Hs^U. En este trabajo se ha comprobado que cada uno de los usuarios no realizan más de 13 tareas de las 28 existentes para su comportamiento normal, pero si en el caso de existiese un número mayor o menor de tareas al establecido en el modelo de datos se adapta al comportamiento de cada uno de los usuarios. Por esta razón se ha tomado ese valor como máximo de tareas ejecutadas para este nuevo modelo. El modelo de datos identifica si existe una o varias tareas T^U en una sesión S^U y asigna un valor de "1" al casillero correspondiente de cada tarea y caso contrario "0" al no existir dicha tarea. Un ejemplo del modelo de datos basado en el histórico de la Figura 1 está presentado en la Tabla 1.

	T_1	T_2	T_3	T_4
S_1^{U1}	1	1	0	1
S_2^{U1}	1	1	1	1
S_3^{U1}	1	1	1	1
S_4^{U1}	1	1	1	1
S_5^{U1}	0	1	1	1
S_6^{U1}	1	1	0	1

Tabla 1 – Modelo de Datos para la aplicación de selección negativa.

Para la implementación de selección negativa es necesario utilizar el modelo de datos de la Figura 1 anteriormente descrito, como también el algoritmo de búsqueda local de secuencias Shift-Or. Este proceso se puede resumir en los siguientes pasos:

Paso 1. Generación de secuencias anormales

En este paso lo que se propone utilizar un sistema inmune artificial aplicando el algoritmo de selección negativa, el cual a partir de un conjunto de datos del modelo propuesto

genere combinaciones binarias de tareas anómalas (T_i, T_j) para poder ser comparadas en el siguiente paso con una sesión activa. Este paso consta de tres fases las cuales son:

- Fase 1: Generación aleatoria de la población inicial B_0 utilizando el modelo de datos anteriormente descrito con detectores r. donde $r \in B_0$. Estos detectores se basan en las secuencias históricas de tareas T^U de S^U. En la generación de la población inicial el número de elementos B_0 se calcula con la formula $B_0 = f^m$, donde f es el número de bits de posibilidades y m es la cantidad de tareas que ejecuta el usuario.
- Fase 2: Con los datos de entrenamiento B_0 una porción del espacio se define como normal (itself) utilizando el algoritmo Shift-Or. El algoritmo de búsqueda local analiza cada registro de B_0 buscando similitudes con los las sesiones del modelo de datos de cada uno de los usuarios, si existe una similitud los marca como normales D_n, caso contrario los marca como anómalos denominados D_{an}.
- Fase 3: Se elimina todos los detectores que se superponen con la región definida en itself, dejando el resto como detectores anormales D_{an}. El algoritmo de selección negativa obtiene detectores de comportamiento anómalo para ser utilizados en el siguiente paso del sistema de detección.

Paso 2. Detección de Intrusos en Secuencias Activas

En este último paso se analiza la sesión activa As^U y se compara con todo el conjunto de detectores anómalos D_{an}, para determinar la similitud aplicando el algoritmo Shift-Or. Si la similitud (umbral de estimulación *sth*) es $\alpha > sth$, donde $\alpha = 10\%$, el detector se activa y el algoritmo lo clasifica como anómalo, de lo contrario, se clasifica como normal. Para calcular el valor del porcentaje *sth* de detectores anómalos en la sesión activa, el cual deberá comparado con un umbral a fijado por el experto. El umbral se define como el porcentaje máximo de combinaciones binarias de tareas anómalas (T_i, T_j) en la sesión activa. Basándonos en trabajos previos se ha definido un umbral a=10%, cual ha brindado óptimos resultados. La formulación del umbral es la siguiente:

$$num = \sum_{r \in D_{an}} (r, As^u)$$

$$sth = (num/|As^u| - 1) * 100;$$

If $sth < \alpha$ **then**

'Anormal'

Else

'Normal'

End If

Un ejemplo sobre esta etapa de la detección se realiza con la sesión activa As_1^{U1} con los siguientes resultados:

$As_1^{U1}: \{T_2, T_1, T_3, T_3, T_4\}$

$\text{num} = \left(D_{an}, As_1^{U1}\right) = 2$

$\text{sth} = \left(\frac{2}{5}\right) * 100 = 33.33\% \qquad \alpha = 10\% \alpha = 10\%$

$\textbf{If}(\text{sth} > \alpha)$ **then** 'Anormal'

Experto: 'Anormal'

Otro ejemplo se puede presentar con la sesión activa As_2^{U1} con los siguientes resultados:

$As_2^{U1}: \{T_4, T_1, T_3, T_2, T_4\}$

$\text{num} = \left(D_{an}, As_1^{U1}\right) = 0$

$\text{sth} = \left(\frac{0}{5}\right) * 100 = 0\% \qquad \alpha = 10\%$

$\textbf{If}(\text{sth} > \alpha)$ **then** 'Normal'

Experto: 'Normal'

En la siguiente sección se presentan los resultados obtenidos en la fase de pruebas donde se demuestra el desempeño del algoritmo tanto en detección como en rendimiento.

4. Desarrollo del algoritmo de Detección de Anomalías

En esta sección se presentan los resultados de las pruebas de detección de anomalías en fase online y offline de manera conjunta. Para estas pruebas se utiliza la información diez usuarios de un sistema informático real. Durante el presente estudio se evidenció muchas características que hacían de la propuesta tener resultados de detección eficiente, una de estas es el modelo de datos, algoritmo de grafos y la aplicación de selección negativa del comportamiento normal de cada uno de los usuarios.

El resultado de las pruebas de la aplicación del algoritmo muestra una tasa de clasificado correctamente (%CC), tasa clasificado incorrectamente (%IC). También presenta la detección tiempo promedio (segundos) para cada usuario del estudio como se muestra en la Tabla 2.

Para valorar el desempeño adecuado detector de anomalías es necesario presentar valores de Precisión (PR), Tasa de Detección (DR) y Tasa de Falsas alarmas (FA) las cuales se presentan a continuación en la Tabla 3.

USR	%CC	%IC	Tiempo
1	96.69	3.31	10.045
2	94.172	5.828	13.432
3	95.89	4.11	9.616
4	96.113	3.887	14.003
5	95.447	4.553	14.196
6	94.609	5.391	8.784
7	95.523	4.477	13.524
8	95.69	4.31	11.761
9	95.465	4.535	14.018
10	95.058	4.942	12.601
Media	95.466	4.534	12.198

Tabla 2 - Resultados de Detección de Anomalías propuesto en clasificado correctamente (CC), clasificado incorrectamente (CC).

USR	%PR	%DR	%%FA
1	96.69	97.942	4.049
2	94.172	95.117	6.154
3	95.89	91.202	2.747
4	96.113	93.253	3.058
5	95.447	87.533	2.635
6	94.609	87.831	3.867
7	95.523	93.285	3.692
8	95.69	89.714	2.303
9	95.465	92.525	3.446
10	95.058	91.089	2.743
Media	95.466	91.949	3.469

Tabla 3 – Resultados del Detección de anomalías propuesto en valores de Precisión, Tasa de Detección y Tasa de Falsas Alarmas.

Como se pudo apreciar los resultados obtenidos a través del Detector de Anomalías propuesto son bastante eficientes para pruebas iníciales con una tasa clasificado correctamente alta y podemos ver que la precisión de 96,466%, la tasa de detección de 91.949%, y la tasa de falsas alarmas son inferiores al 4%, lo que significa que la detección tiene identificación aceptable.

Dicho desempeño del Detector de Anomalías en una estación de trabajo es bajo lo que es un punto a favor a la propuesta. El tiempo promedio para detectar relativamente mínimo ya que con solo registros de 2 años facilita que la rapidez de la detección,

pero no se puede obtener un perfil totalmente eficiente. El costo del entrenamiento no es un factor de riesgo porque el entrenamiento se realiza solo una vez en períodos semanales o mensuales lo que hace al sistema se pueda adaptar al comportamiento del usuario.

5. Conclusiones y trabajos futuros

Este trabajo se ha propuesto y validado un sistema de detección de anomalías con un enfoque basado en Grafos de comportamientos de usuario de manera online y la aplicación en la detección offline con Sistemas inmunes artificiales implementado en un sistema informático, lo que permitió que el trabajo pueda describir de una forma aproximada la creación de perfiles de usuario representados por el modelo de datos. Una de las ventajas de nuestro modelo es la generación de comportamientos anómalos, aplicando selección negativa, a partir de comportamientos normales de cada uno de los usuarios. Esto permite que el perfil de cada usuario sea único y dinámico. El desarrollo de perfiles de usuario de forma dinámica y real para determinar comportamientos irregulares y predecir si la futura ejecución de una tarea es normal.

El sistema de detección se aplicó para comprobar el análisis de sensibilidad y definir el mejor rendimiento de parámetros de detección. Esta forma ofrece un mejor equilibrio entre la tasa de detección y tasa de falsas alarmas, también comprueba su adaptabilidad al comportamiento humano para la detección aplicando el enfoque propuesto.

El desempeño del algoritmo en pruebas no ha sido evaluado debido a que únicamente el objetivo del estudio es comprobar la eficiencia del algoritmo en una fase de pruebas, para posteriormente implementarlo en un sistema informático real.

Como líneas de trabajos fututos serán la implementación de identificación de comportamientos anómalos en secuencias temporales de las tareas ejecutadas por el usuario aplicando redes bayesianas u otras técnicas de inteligencia artificial. También, algoritmos de optimización y big data para mejorar el desempeño de las detecciones y reducir el tiempo de procesamiento y respuesta para ser implementado de manera online y con varios sistemas a la vez. Además de realizar la aplicación a diferentes áreas como la medicina y detección de problemas en sistemas industriales.

Referencias

Akoglu, L., Tong, H., & Koutra, D. (2015). Graph based anomaly detection and description: a survey. Data Mining and Knowledge Discovery, 29(3), 626–688.

Aydin, I., Karakose, M., & Akin, E. (2010). Chaotic-based hybrid negative selection algorithm and its applications in fault and anomaly detection. Expert Systems with Applications, 37(7), 5285–5294.

Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2014). Network anomaly detection: methods, systems and tools. Ieee communications surveys & tutorials, 16(1), 303–336.

Fontugne, Romain, et al. “Uncovering relations between traffic classifiers and anomaly detectors via graph theory.” Traffic Monitoring and Analysis. Springer Berlin Heidelberg, 2010.101–114.

Gong, Maoguo, et al. “An efficient negative selection algorithm with further training for anomaly detection.” Knowledge-Based Systems 30 (2012): 185–191.

Laurentys, C. A., et al. “Design of an artificial immune system for fault detection: a negative selection approach.” Expert Systems with Applications 37.7 (2010): 5507–5513.

Le, Do Quoc, et al. “Traffic dispersion graph based anomaly detection.” Proceedings of the Second Symposium on Information and Communication Technology. ACM, 2011.

Mehnaz, S., & Bertino, E. (2016, December). Building robust temporal user profiles for anomaly detection in file system accesses. In Privacy, Security and Trust (PST), 2016 14th Annual Conference on (pp. 207-210). IEEE.

Messinger, David W., and J. Albano. “A graph theoretic approach to anomaly detection in hyperspectral imagery. “Hyperspectral Image and Signal Processing: Evolution in Remote Sensing (WHISPERS), 2011 3rd Workshop on. IEEE, 2011.

Noble, C. C., & Cook, D. J. (2003, August). Graph-based anomaly detection. In Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining (pp. 631-636). ACM.

Oh, Sung-Il, Inbok Lee, and Min Sik Kim. “Fast filtering for intrusion detection systems with the shift-or algorithm.” Communications (APCC), 2012 18th Asia-Pacific Conference on. IEEE, 2012.

Wang, Taowei David, AmolDeshpande, and Ben Shneiderman. “A temporal pattern search algorithm for personal history event visualization.” Knowledge and Data Engineering, IEEE Transactions on 24.5 (2012): 799–812.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 11/09/2017
Aceitação/Acceptance: 28/03/2018

Seguridad Informática para Pequeñas y Medianas Empresas de la Provincia de Santa Elena

Julio Reyes[1], Carlos Muñoz[1], Teresa Guarda[1]

emmanuel_492@hotmail.es, barcemunoz13@gmail.com, tguarda@gmail.com

[1] Universidad Estatal Península de Santa Elena, La Libertad, Ecuador

Pages: 144–152

Resumen: En la actualidad el crecimiento acelerado del internet, las pequeñas y grandes empresas (Pymes) es evidente. Por lo tanto, son sometidos a nuevos y potencialmente altas amenazas y vulnerabilidades que atentan contra su sistema de información y muchos otros ámbitos de importancia. El presente artículo se enfoca en el uso de los controles de la norma ISO 27000, dedicada a especificar requerimientos necesarios para: establecer, implantar, mantener y mejorar un sistema de seguridad de la información. Sin embargo, la mayoría de las pequeñas y grandes empresas no consideran como una inversión importante el hecho de implantar políticas y mecanismo para el correcto funcionamiento de la empresa. Por lo que se desarrollara una guía de seguridad informática, para que posteriormente pueda ser implementado en las empresas. Nuestra propuesta busca fomentar técnicas existentes para vencer la inseguridad y la desconfianza que pueda causar, los hackers, los crackers y otras potenciales amenazas. Así como también concientizar en las personas que estas vulnerabilidades tienen efectos devastadores, y que generan indisponibilidad al momento de acceder a la información cuando es vital y necesaria para la toma de decisiones.

Palabras-clave: Pymes, vulnerabilidades, amenazadas, información. ISO 27000, seguridad de la información, inseguridad, desconfianza, personas.

Computer Security for Small and Medium-Sized Enterprises of the Province of Santa Elena

Abstract: Currently the accelerated growth of the internet, small and large companies (SMEs) is evident. Therefore, they are subject to new and potentially high threats and vulnerabilities that threaten their information system and many other important areas. This article focuses on the use of the controls of ISO 27000, dedicated to specify requirements necessary to: establish, implement, maintain and improve an information security system. However, most small and large companies do not consider as an important investment the fact of implementing policies and mechanisms for the proper functioning of the company. Therefore, a computer security guide will be developed, so that it can later be implemented in companies. Our proposal seeks to encourage existing techniques to overcome the insecurity and distrust that may cause, hackers, crackers and other potential threats. As well as to

make people aware that these vulnerabilities have devastating effects, and that they generate unavailability when accessing information when it is vital and necessary for decision making.

***Keywords**:* SMEs, vulnerabilities, threats, information. ISO 27000, information security, insecurity, distrust, people.

1. Introducción

El desarrollo de las actividades comerciales en la península de Santa Elena ha crecido considerablemente, si comparamos la cantidad de negocios que se encontraban antes de convertirse en provincia con los que existen actualmente. Muchas de estas empresas comenzaron siendo pequeños puestos en los que a veces no se podía atender a la cantidad de clientes que incluso por curiosidad se acercaban a observar los productos que ofrecía el negocio. Actualmente la mayoría de los mismos han crecido hasta el punto de ofrecer servicios propios de su firma, incrementando así, la competencia. Pero muchas veces esta competencia es desleal ya que existe gente mal intencionada, que busca corromper los sistemas y bases de datos de las empresas para copiar patentes, información de productos, información de proveedores y clientes.

Los sistemas de seguridad han contribuido a que la información que posee una empresa se quede mucho tiempo únicamente en la base de datos de las mismas. Un sistema de seguridad robusto y consistente permite a las personas que están a cargo de una empresa confiar en su base de datos sin temor a que la información sea robada y utilizada en su contra.

Para que un sistema sea considerado robusto debe cumplir con los cinco pilares fundamentales de la seguridad de la información: Integridad, que nos valide que la información sea la adecuada y que no haya alteraciones desde su punto de creación (Thomson, 2009). Confidencialidad, garantizar que solo los usuarios tengas permisos para acceder a la información almacenada. Disponibilidad, asegurar el respetivo correcto funcionamiento de los sistemas de datos y a su vez van a estar disponibles a los diferentes usuarios cuando requieren en cualquier momento. Evitar el rechazo, que nos certifique que no haya ningún rechazo al momento de solicitar una información en particular. Autenticación, que nos permita que solo los usuarios autorizados puedan acceder a la información almacenada.

El rápido desarrollo de la tecnología y de la informática y la importancia que ésta ha alcanzado en la mayoría de las actividades cotidianas del ser humano han provocado que éste se encuentre condicionado e interesado es estos avances. En la actualidad son pocas las personas que pueden evitar mantenerse en contacto directo con la tecnología, lo cual evidencia la importancia que ésta ha obtenido en el desarrollo del ser humano y de las actividades que a diario realiza. (Ojeda-Pérez, 2010).

El uso de las herramientas que el internet ofrece se ha convertido en esenciales para cualquier negocio o actividad en la actualidad. De manera muy particular el uso de mensajería instantánea y de correo electrónico han contribuido para que las empresas se mantengan con continuo contacto con sus clientes y para mantenerse informado acerca de las tendencias tecnológicas y del desarrollo de sus competidores. (Molina, Meneses, & Silgado, 2009).

Con él internet las empresas se han visto en la obligación de interconectar diferentes técnicas para publicar servicios a los usuarios, para conservar un nivel óptimo de competitividad y de rendimiento económico. Por lo tanto, con el manejo del internet se han encontrado expuestas a múltiples riesgos y amenazas con respecto a la ejecución de transacciones comerciales. Por lo tanto, esta dificultad impacta de forma negativa en las empresas (Tur, 2015).

Gracias a diversas investigaciones realizadas por expertos han dado a notar que la seguridad informática es una disciplina del conocimiento que busca disminuir el impacto que pueden tener eventos inesperados y que puedan comprometer los procesos normales de una organización para así contar con estrategias y procedimientos que permitan avanzar ante cualquier eventualidad. (Cano, 2007).

El avance de la tecnología y del crecimiento del internet ha derivado también en la aparición de ataques de tipo distribuido y un creciente número de virus en la red, estos aspectos aumentan la posibilidad de un inminente black out informático. Es así que surgen los primeros sistemas ideados de manera particular a la protección de la infraestructura como los routers y otros sistemas convencionales de conexión. (Leone, 2003).

La principal ventaja que tienen las personas es el fácil acceso a la información desde sus dispositivos inteligentes, el acceso a los datos es inmediato, es decir basta tener una conexión a internet para realizar un sinfín de actividades, pero es ahí donde nace el conflicto de mantener una conexión segura a través de internet, también conocida como la red de redes que tiene usuarios a nivel mundial, nunca se conoce que encontraremos detrás de esta red (Entonado, 2001).

Para neutralizar los peligros tecnológicos se han desarrollado varias alternativas de soluciones informáticas de seguridad que trabajan de manera autónoma, tales como son los firewalls, antivirus, anti-spam, etc. Sin embargo, el crecimiento de amenazas puede ocasionar que las diferentes soluciones asuman un alto costo operativo y administrativo.

En el documento se detallan los antecedentes, la metodología a utilizar, así como también las teorías de diferentes autores que nos contribuyeron con información que consideramos importante para tomarse en cuenta en lo que debe ser un sistema de seguridad robusto. Las tecnologías utilizadas para llevar a cabo un delito informático y las que se deben utilizar para contrarrestar su funcionamiento e impacto.

2. Antecedentes

En el área de la informática la seguridad de la información es un ámbito muy importante que tiene como objetivo la protección de todo lo relacionado con los servicios que la tecnología y las redes ofrecen. Debido a esto los expertos en el área han considerado un sinnúmero de protocolos y herramientas con la plena intención de minimizar los riesgos y posibles amenazas que puedan afectar la información y todo lo que un sistema puede considerar.

Es importante mencionar que dependiendo del negocio la información que manejan las empresas puede significar de mucha importancia para sus intereses, y por tanto, es imperante que ésta información se quede en la base de datos de la empresa incluso evitando los riesgos de que la información sea robada.

La seguridad informática no surgió de la nada, tiene un precursor, fue en 1980 en que las investigaciones y trabajos de James P. Anderson quien, para cumplir una orden gubernamental, estableció uno de los primeros escritos que tenían relación con el tema. El documento al que se refería el investigador fue llamado "Computer Security Threat Monitoring and Surveillance" en el que se hace hincapié al enfoque de lo que debe considerase como seguridad de la información (Anderson, 1980).

Pero para cubrir una necesidad es importante primero que exista un problema, fue en 1972 en que se produjo uno de los primeros ataques informáticos, se trataba de un virus el mismo que fue bautizado como Creeper, desarrollado por Robert Thomas Morris consistía en presentar de manera periódica en pantalla el mensaje: "Son una enredadera, agárrame si puedes" (Erquiaga, 2011). Es así que se crea el primer programa antivirus, Reaper. Sin embargo, los "virus" propiamente definidos aparecieron desde mucho antes, en los laboratorios de Bell Computers, mediante un juego llamado Core Wars, el mismo que basaba su funcionamiento en ocupar la totalidad de la memoria RAM del equipo contrario en el menor tiempo posible.

La criptografía es uno de los principales métodos que en lo últimos años ha alcanzado importancia, se puede mencionar que como todo método surgió para proteger pequeños sistemas como un simple correo, sin embargo, enfocándolo en el tema de estudio de éste documento sabemos lo importante que puede llegar a ser proteger información que una empresa utilice para llevar a cabo sus funciones o principales negocios.

3. La Evolución de la Tecnología.

Retrocediendo en el tiempo por el año 90 aproximadamente, el acceso tecnológico era prácticamente limitado, nuestros padres, abuelos, tíos para poderse comunicar se lo realizaba por medios de cartas, ir a visitar a los familiares, realizar llamadas telefónicas convencional, etc. de tal forma es como se conservaba una comunicación a la antigua (Trasobares, 2003).

Con el pasar del tiempo todo el sistema fue evolucionando, de tal forma comenzaron aparecer las computadoras, teléfonos celulares y el internet que al principio solo fue líneas de texto. Desde entonces la tecnología no conforme comenzaron a implantar interfaces gráficas, juegos novedosos hasta equipos inteligente tales son los Smartphone. Por lo tanto, nos cambió la forma de ver el mundo, que ya no es necesario recurrir a las bibliotecas, o un diccionario para ver el significado de una palabra en particular.

Con todo lo que está avanzando la tecnología no es suficientes para nosotros. Sin embargo, nos estamos olvidado de progresar junto con ella. Por lo tanto, cada cambio tecnológico implica que debemos informarnos del pro y contra de las tendencias actuales. Por lo que lograríamos a minimizar los diferentes riesgos al momento de exponer nuestros criterios en redes sociales.

3.1. ¿Pasará esto en la Provincia De Santa Elena?

Las vulnerabilidades en la seguridad de la información pueden producirse en cualquier parte del mundo, ya que existen muchas personas que pasan su tiempo intentando robar información que puedan usar para beneficio propio y perjuicio a terceros.

En la provincia de Santa Elena se han encontrado casos en los que una página ha sido *hackeada*, sin embargo, en aquella ocasión la intención del delincuente informático no fue la de substraer información, sino solo de modificar la presentación de la página y subir la evidencia a una página en la que se ganan puntos por hackeos exitosos. Este caso se produjo en el 2015 en la página de la facultad de Sistemas y Telecomunicaciones de la Universidad Estatal Península de Santa Elena (UPSE) (Mouh, 2015).

El usuario o grupo de usuarios que se atribuyeron el *hackeo* fueron Admirale_Mouh, a continuación, se muestra la captura de pantalla que fue subida a la página en la que publican los haceos realizados para sumar puntos.



Figura 1 – Captura de pantalla subida a zone-h para referenciar el hackeo de la página de la UPSE

Como mencionamos anteriormente en todos los lugares del mundo y todas las páginas del mundo se pueden hacer intromisiones a las páginas web de otras instituciones, uno de los objetivos de nuestro trabajo es brindar información a las personas de la Provincia de Santa Elena acerca de las diferentes opciones que se ofrecen actualmente para contribuir con la seguridad de la información y que pueda servir para mantener la información de sus empresas lejos de las manos de personas que puedan utilizarla para perjudicarlos.

4. La fuga de información

Como datos estadísticos de años anteriores podemos mencionar que el 63% de las empresas, sean éstas públicas o privadas se vieron perjudicadas al perder sistemas de archivos los cuales eran muy importantes para sus intereses y funcionamiento procedimental. Sin embargo, solo el 23% puede considerar que sus sistemas de información y banco de datos fue vulnerado para robar información.

Del total de información intervenida se puede mencionar que solo el 75% de la información se produce por la pérdida de dispositivos electrónicos, tales como computadores

personales, teléfonos celulares, discos portátiles, memorias extraíbles y UBS. Por otra parte, el otro 25% se debe a la intromisión deliberada por parte de *hackers* los mismos que utilizan diferentes técnicas de violación de seguridad informática para acceder y utilizar la información para fines lucrativos e incluso en ocasiones ilegales.

4.1. ¿Qué es fuga de información?

Se puede considerar la fuga de la información como la salida de la información de tal manera que no pueda ser controlada por parte de quien la posee hacia alguien que no está en el mismo lugar y que no debería conocer de la misma. Muchas veces una fuga no debe ser considerada grave, sino hasta cuando se comprueba que la información que ha sido desviada sea de verdadera confidencialidad y que se considere un peligro que caiga en manos equivocadas o que sea divulgada de manera deliberad en la red (Sebastián, 2010).

Por lo general puede suceder por accidente ya sea interno como externo, hasta el caso que sea intencional o no. Detallaremos un ejemplo de fuga o perdida de información ya que puede producirse con un empleado entregando datos muy valiosos a la competencia, cuando una secretaria por error pierde documentos en un sector público mediante dispositivos electrónicos como laptop, USB, etc. Por último, se puede considerar el acceso externo a una base de datos de la empresa o un equipo informático infectado que les permita enviar información al cyber-delicuente.

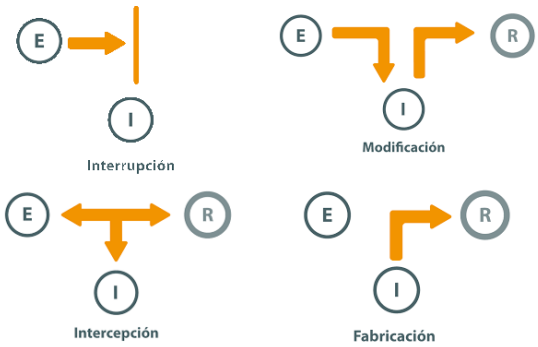


Figura 2 – Tipos de amenazas para la fuga de la información

Podemos mencionar algunos de los procesos que son considerados amenazas para el buen flujo de la información. Como se muestran en la figura 2. La Interrupción, la modificación, la intercepción y la fabricación en muchas ocasiones pueden producir que los sistemas de información tengan inconsistencias que afecten a los procesos de producción de las diferentes empresas.

La Interrupción. - Básicamente consiste en que la información no llegue al destino, es interceptada por algún otro medio presente en el camino, y robada.

La Modificación. - Consiste en que la información es interceptada en el camino, llevada a otro destino en el que es modificada, y luego es enviada a destino principal, pero con información diferente.

La Intercepción. - La información es interceptada en el camino, llevada a otro destino, no es modificada y luego es enviada al destino principal.

Finalmente, la Fabricación consiste en que sin necesidad de que un Emisor, se genera información para que sea enviado a un destino, en muchas ocasiones éste tipo de procesos es utilizado para robar información de los bancos de datos.

Se debe tener claro de igual manera que existen ataques informáticos que se basan en el robo de la información a los cuales se definen como Activos, y también los que son pasivos los cuales se identifican por el NO robo de la información.

5. Políticas de seguridad de un sito.

Cuando nos referimos a una organización, podemos mencionar que ésta puede tener muchos sitios, y cada uno contar con sus propias redes. En este caso sí la organización es grande, existen muchas posibilidades de que los sitios tengan diferente administración de red, cada uno con metas y objetivos diferentes (Cañavate, 2012). Por otra parte, si esos sitios no se encuentran conectados a través de una red interna, cada uno de ellos puede tener sus propias políticas de seguridad de red. El caso contrario es que, si los equipos si se encuentran conectados mediante una misma red interna, es muy importante que las políticas de seguridad de red deban cumplir con todos los objetivos de los sitios que se encuentren interconectados.

En líneas generales, un sitio puede definirse como cualquier parte de la organización en el que se encuentren computadoras y todos los recursos que éstos puedan interconectarse y relacionarse mediante la red. Éstos podrían ser unos cuantos:

- Servidores de terminal.
- Software para conexión de red y de aplicaciones.
- Cables de red
- La información de archivos y bases de datos.
- Estaciones de trabajo.
- Computadoras host y servidores.
- Dispositivos de interconexión Gateway, routers, bridges, repetidores.

La política o políticas de seguridad del sitio deben considerar la seguridad y protección de todos estos recursos. Esto debido a que el sitio puede estar conectado a otras redes, es importante que las políticas de seguridad consideren las necesidades y requerimientos de todas las redes que se encuentren interconectadas.

5.1. Planteamiento de la política de seguridad.

Definir una política de seguridad de red significa elaborar procedimientos y planes que salvaguarden los recursos de la red contra perdida y daño. Uno de los enfoques posibles para elaborar dicha política es examinar lo siguiente:

- ¿Qué recursos está usted tratando de proteger?
- ¿De quiénes necesita proteger los recursos?

- ¿Qué tan posibles son las amenazas?
- ¿Qué tan importante es el recurso?
- ¿Qué medidas puede implementar para proteger sus bienes de forma económica y oportuna?
- Examine periódicamente su política de seguridad de red para ver si han cambiado los objetivos y las circunstancias de la red.
- La figura siguiente muestra una hoja de trabajo que puede ayudarle a canalizar sus ideas conforme estos lineamientos.
- La columna "Número de recursos de red" es un numero de red de identificación interna de los recursos que van a ser protegidos (sí se aplica).
- La columna "Nombre del recurso de red" es la descripción en lenguaje común de los recursos. La importancia del recurso puede estar en una escala numérica del 0 al 10, o en expresiones "Vagas" de lenguaje natural como bajo, alto, medio, muy alto, etcétera.
- La columna "Tipo de usuario del que hay que proteger al recurso" puede tener designaciones como interno, externo, invitado o nombres de grupos como usuarios de contabilidad, asistentes corporativos, etcétera.
- La columna "Posibilidad de una amenaza' puede estar en una escala numérica del 0 al 10, o en expresiones 'Vagas" de lenguaje natural como baja, alta, media, muy alta, etcétera.
- La columna "Medidas que se implementarán para proteger el recurso de red" puede tener valores tales como 'permisos de sistema operativo" para archivos y directorios; pistas/alertas de auditoria' para servicios de red; "routers de selección" y "firewalls" para host y dispositivos para conectividad de red; y cualquier otra descripción del tipo de control de seguridad.

En general, el costo de proteger las redes de una amenaza debe ser menor que el de recuperación en caso de que se viera afectado por una amenaza de seguridad. Si usted no tiene el conocimiento suficiente de lo que está protegiendo y de las fuentes de la amenaza, puede ser difícil alcanzar un nivel aceptable de seguridad.

6. Conclusiones

La seguridad de la información no solo se basa en la capacidad que puede tener un sistema de información a recibir la mayor cantidad de datos posibles, sino también a la robustez con la que ésta pueda defenderse de amenazas y ataques informáticos. Existen muchas formas en las que las personas pueden proteger los datos de sus sistemas de información, depende muchas veces de la programación con la que han sido elaborados los sistemas visuales y de base de datos. En la provincia de Santa Elena existen muchas empresas que se dedican al desarrollo de sistemas de información, los cuales durante su proceso de formación conocen los diferentes medios de hackeo y de igual manera muchas formas de evitarlos. Las empresas que laboran en la provincia de Santa Elena en muchas ocasiones son dirigidas por personas que no conocen acerca de los problemas que enfrentan los sistemas de información, y simplemente se hacen de un sistema sin conocer si es robusto o no.

Referencias

Anderson, J. P. (1980). *Computer security threat monitoring and surveillance*. Technical Report, James P. Anderson Company.

Cañavate, A. M. (2012). *www.upf.edu*. Obtido de https://www.upf.edu/ hipertextnet/ numero-1/sistem_infor.html

Cano, J. J. (2007). Inseguridad Informática: Un Concepto Dual en Seguridad Informática. In *Revista de Ingeniería, nº No. 19* (pp. pp. 40-44).

Entonado, F. B. (2001). Sociedad de la informácion y educación . Mérida: Junta de Extremadura .

Erquiaga, M. J. (2011). Botnets: Mecanismos de control y de propagacion. *In XVII Congreso Argentino de Ciencias de la Computación*.

Leone, S. B. (2003). e-commerce security issue. In v. V. Notiziario Tecnico Telecom Italia.

Molina, K. J., Meneses, J. P., & Silgado, I. Z. (2009). Firewall - Linux: Una Solución De Seguridad Informática Para Pymes (Pequeñas Y Medianas Empresas. *Revista UIS Ingenierías*, 155–165.

Mouh, A. (2015). *http://www.zone-h.org*. Obtido de http://www.zone-h.org/mirror/ id/24914628

Ojeda-Pérez, J. E. (2010). Delitos informáticos y entorno juridico vigente en Colombia. In *Cuaderno de Contabilidad* (pp. pp. 41-66.).

Sebastián, B. (2010). *www.welivesecurity.com*. Obtido de ¿Qué es la fuga de información?: https://www.welivesecurity.com/la-es/2010/04/13/que-es-la-fuga-de-informacion/

Thomson, F. (2009). Todas las entradas etiquetadas como integridad. https://infosegur.wordpress.com/tag/integridad/.

Trasobares, A. H. (2003). Los sistemas de información: evolución y desarrollo. Proyecto social. *Revista de relaciones laborales,*, 149–165.

Tur, A. (2015). *Facultad de Diseño y Comunicación*. Obtido de Internet, ¿oportunidad o amenaza para los negocios?: http://fido.palermo.edu/ servicios_dyc/ publicacionesdc/vista/detalle_articulo.php?id_libro=501&id_articulo=10417

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 30/09/2017
Aceitação/Acceptance: 09/03/2018

Gobernanza y nuevos medios en la radiotelevisión pública europea. Panorámica sobre las pruebas de valor público

Marta Rodríguez-Castro[1], Francisco Campos-Freire[2]

m.rodriguez.castro@usc.es, francisco.campos@usc.es

[1] Universidade de Santiago de Compostela, Av. de Castelao, s/n, 15782, Santiago de Compostela, España

[2] Universidade de Santiago de Compostela, Av. de Castelao, s/n, 15782, Santiago de Compostela, España

Pages: 153–162

Resumo: Los avances de las radiotelevisiones públicas europeas en los nuevos medios a lo largo de los últimos años no han estado exentos de polémica. La necesidad de legitimar estas nuevas actividades de los medios públicos derivó en la implantación de una prueba de valor público que evalúa las propuestas de nuevos servicios contraponiendo su valor público a su impacto de mercado. En este artículo se contextualizan y se describen las 10 pruebas existentes hasta el momento en países de la Unión Europea, prestando atención a los puntos en común y las diferencias que emanan de los distintos contextos nacionales.

Palavras-chave: pruebas de valor público; Comunicación de 2009; Public Service Media; nuevos medios; gobernanza.

Governance and new media in European Public Service Media. An overview around Public Value Tests.

Abstract: The progress of European public service broadcasters in the field of digital media during the last years have been surrounded by controversy. The need to legitimize these new activities led to the implantation of a public value test that assesses new proposals of the public service media organizations, counterbalancing its public value and its market impact. This paper approaches and contextualizes the tests implemented in 10 member States of the European Union, focusing on the similarities and differences that arise from the national contexts.

Keywords*:* Public Value Test; Communication of 2009; Public Service Media; New Media; Governance.

1. Introducción

Las tensiones entre los medios de comunicación públicos y los privados han derivado en una serie de medidas de control e intento de legitimación de los medios públicos a nivel europeo. Desde que el Reino Unido fuese pionero en el diseño de su

Public Value Test en 2007 hasta la recomendación de la Comisión Europea a los Estados Miembros de introducir un mecanismo de evaluación *ex ante* en la Comunicación de 2009, estas pruebas han generado todo un debate en torno a su pertinencia, su utilidad y su ambivalencia, al usarse tanto a favor como en contra de los medios de comunicación públicos.

Este debate continúa aún abierto, después de que un total de doce países -diez de ellos pertenecientes a la Unión Europea (UE) y dos extracomunitarios enmarcados en el Espacio Económico Europeo (EEE)- hayan incorporado una prueba *ex ante* que evalúe los nuevos servicios que sus medios de comunicación públicos deseen llevar a cabo. Estos procesos de adaptación del test, junto con la situación de *stand-by* en la que se encuentra España en cuanto a la incorporación de la Comisión Europea merece que se revise lo que está sucediendo ahora mismo en Europa con las pruebas de valor público. En este artículo se traza un estado de la cuestión alrededor de estos mecanismos *ex ante*. Para ello, se ha realizado una revisión de la legislación de los diez países analizados, así como de los documentos sobre el desarrollo de las distintas pruebas que han sido publicados. De forma complementaria se ha consultado también la literatura científica producida hasta el momento en torno a estas pruebas.

2. Antecedentes: el *Public Value Test* y la Comunicación de 2009

Es en un contexto marcado por las protestas del sector privado y la demanda de la sociedad por una mejor rendición de cuentas de los organismos públicos en el que se comienza a hablar de la necesidad de introducir algún mecanismo de evaluación que permita tanto controlar como legitimar las actividades de las radiotelevisiones públicas en los nuevos medios. La British Broadcasting Corporation (BBC) es pionera en el diseño de este mecanismo, que los británicos denominaron *Public Value Test*. Tras tres años de desarrollo, el primer *Public Value Test* se llevó a cabo en 2007.

El *Public Value Test* es un instrumento de regulación utilizado para decidir sobre la introducción de un nuevo servicio dentro de las actividades de una radiotelevisión pública. Para ello, la prueba contrasta dos aspectos diferentes: por una parte, se evalúa el valor público de una propuesta, vinculándolo con su misión de servicio público; por otra, se estudia el impacto de mercado que conllevaría la introducción de la propuesta. La valoración conjunta de estas dos cuestiones derivará en la decisión sobre la aprobación del nuevo servicio propuesto.

Este es el concepto del que parten las directrices que en 2009 recomendará Bruselas en la «Comunicación de la Comisión sobre la aplicación de las normas en materia de ayudas estatales a los servicios públicos de radiodifusión» (Comisión Europea, 2009). En el párrafo 84 de la Comunicación se recomienda un procedimiento de evaluación previa basado en una consulta pública abierta, con el objetivo de decidir si los nuevos servicios "satisfacen las necesidades democráticas, sociales y culturales de la sociedad, teniendo en cuenta debidamente sus efectos potenciales en las condiciones comerciales y en la competencia" (Comisión Europea, 2009).

3. Las pruebas de valor público en Europa: estado de la cuestión

Desde la recomendación de la Comisión Europea, y contando con el antecedente de la radiotelevisión pública británica, un total de diez Estados miembros cuentan con un procedimiento *ex ante* para la valoración de nuevos servicios (Reino Unido, Alemania, la región belga de Flandes, Irlanda, Austria, los Países Bajos, Dinamarca, Suecia, Finlandia y Croacia). La Comunicación de 2009 es pertinente a efectos del EEE, por lo que Noruega e Islandia también han optado por desarrollar su propia prueba.

3.1. Reino Unido

El *Public Value Test* es la prueba más popular de las existentes. Desde su implantación en el año 2007, tras la modificación de la Royal Charter (Department for Culture, Media and Sport, 2006) -que también incluía la creación del organismo supervisor BBC Trust-, se han llevado a cabo cinco *Public Value Tests* que han evaluado los siguientes servicios: televisión bajo demanda, televisión de alta definición, un canal de televisión digital orientada a la comunidad de hablantes de gaélico, un servicio de vídeo local y un paquete de cambios relativos a los servicios televisivos y online de la BBC. Tan sólo el servicio de vídeo local suspendió la prueba y no pudo ser llevado a cabo, mientras que el paquete de cambios fue aprobado parcialmente, al considerarse que una de las cuatro modificaciones propuestas contaba con un escaso valor público que no justificaba su alto impacto de mercado.

El *Public Value Test* consta de una evaluación del valor público (PVA), a cargo del BBC Trust, y de una evaluación del impacto de mercado (MIA), realizada por la Ofcom. Ambas se realizan de forma simultánea durante un plazo de 3 meses, constituyendo la mitad de la duración global de la prueba, seis meses. El PVA se estructura en torno al análisis de la calidad, el alcance, el impacto individual y social y el coste de la propuesta. El BBC Trust puede emplear como fuentes del estudio predicciones de demanda, resultados de pruebas o pilotos, recomendaciones de expertos independientes o estudios de mercado y consumo. En cuanto MIA, la Ofcom recurre a una combinación de pruebas empíricas y consultas a expertos, centrándose en el impacto directo que la implantación del servicio propuesto pudiese tener en los consumidores y en los productores de servicios similares a corto plazo, así como su influencia, tanto positiva como negativa, en la competencia y en el desarrollo del mercado. Finalizadas las dos evaluaciones, el BBC Trust se encarga de contraponer los resultados para valorar si el valor público de la propuesta de nuevo servicio justifica su impacto de mercado, aprobando o rechazando entonces su aprobación.

3.2. Alemania

El *Drei-Stufen-Test* alemán (prueba de los tres pasos) fue fruto de las negociaciones entre el gobierno alemán y la Comisión Europea a raíz de la financiación del sistema alemán de radiotelevisión pública. La prueba de evaluación previa alemana cuenta con dos particularidades con respecto a los mecanismos homólogos de otros países, ambas relativas a las propuestas que deberán someterse a la evaluación: su alcance no se limita a nuevos servicios o modificaciones significativas, sino que los servicios preexistentes

vinculados a los nuevos medios también tuvieron que ser evaluados; y se trata del único contexto nacional que cuenta con una lista de servicios vetados a los medios públicos por su carencia de valor democrático, cultural o social (Dorr, 2011). El gran alcance de servicios a evaluar, junto con el sistema federal de la radiotelevisión pública alemana (tanto las emisoras nacionales como las regionales deben aplicar la prueba) convierten al *Drei-Stufen-Test* en el procedimiento *ex ante* más utilizado de Europa, con un total de 45 aplicaciones desde su introducción.

Los tres pasos a los que se refiere la prueba son los tres aspectos clave de las propuestas que serán evaluados: 1) la relación del servicio con las necesidades democráticas, sociales y culturales de la sociedad; 2) la contribución de la propuesta a la competencia editorial, y 3) el gasto financiero necesario para llevar a cabo la propuesta

Durante la recogida de toda la información necesaria para evaluar estos tres aspectos, el *Rundfunkrat* encarga el informe de mercado a una consultora externa, escogida por concurso público, que contará con un plazo de dos meses para llevar a cabo la evaluación del impacto de mercado, para la cual deberá tener en cuenta, además de otras fuentes, las opiniones de terceros expresadas en la consulta pública. Una vez recopilada toda la información necesaria, el *Runkdfunkrat* estará capacitado para aplicar los tres criterios que vertebran el *Drei-Stufen-Test* y decidir si aprobar o no el nuevo servicio o cambio propuesto. El *Rundfunkrat* toma esta decisión en un pleno donde el resultado debe ser aprobado por una mayoría de dos tercios de los miembros presentes. Tras la pronunciación del *Rundfunkrat* se procede al cierre del proceso, con la publicación de toda la documentación relevante empleada durante el transcurso de la prueba y la justificación de la decisión. La duración total del proceso es de seis meses.

3.3. Bélgica (Flandes)

En el año 2009, la Región Flamenca belga aprobó el *Mediadecreet* (Departement Cultuur, Jeugd, Sport en Media, 2009), la nueva ley de radio y televisión, tras cinco años de negociaciones con la Comisión Europea a raíz de las protestas que los medios de comunicación privados presentaron contra la Vlaamse Radio- en Televisieomroep (VRT). Esta ley incluye una de las principales exigencias de la Comisión al gobierno flamenco: una mejor definición de su misión de servicio público y un procedimiento de evaluación previa necesario para aprobar nuevos servicios. De forma complementaria, el gobierno de Flandes también añadió al contrato de gestión de la televisión pública vigente una lista que enumeraba todos los servicios existentes (incluyendo proyectos de innovación a dos años vista) que, por lo tanto, quedaban exentos de la necesidad de ser evaluados mediante un mecanismo *ex ante*. Esta limitación del alcance de la prueba fue muy criticada por el sector privado.

Hasta el momento no se ha llevado a cabo ninguna prueba de valor público, aunque según se recoge en el *Mediadecreet* su funcionamiento seguiría de forma bastante fiel la recomendación de la Comisión Europea. El organismo encargado de llevar a cabo tanto la evaluación del valor público como la relativa al impacto de mercado sería el Consejo Estratégico de Cultura, Juventud, Deportes y Medios de Comunicación (SARC), a pesar de que su independencia fue cuestionada por el potencial carácter imparcial de sus miembros (pertenecientes al sector mediático) y por no contar con recursos económicos propios, dependiendo del Ministerio.

A pesar de no haber realizado ningún *ex ante test*, el SARC ha desarrollado una evaluación similar en relación a la posición de la VRT, incluyendo una encuesta al público flamenco, un análisis de los comentarios de distintos *stakeholders*, y un estudio del impacto de mercado de la VRT –cada estudio con un coste de 60.000€ (Van den Bulck, 2011:159)- que podría servir como antecedente a la hora de aplicar una prueba de valor público propiamente dicha.

3.4. Austria

Tras numerosas quejas por parte de la prensa y los medios de comunicación privados, Austria aprobó en el año 2010 la nueva ley de la ORF (Bundeskanzleramt, 2010), que introducía una prueba de evaluación previa de nuevos servicios (*Auftragsvorprüfung*). La prueba austríaca tiene como objeto todas las propuestas que la radiotelevisión pública Österreichischer Rundfunk (ORF) quiera llevar a cabo. Esto abarca canales o servicios que se desarrollen por primera vez, así como modificaciones considerables de servicios ya existentes (cambios en sus contenidos, accesibilidad o audiencia objetivo, así como cualquier otro cambio que implique un aumento de los costes de más del 2% del presupuesto total de la emisora).

Hasta el momento, se han completado cuatro procedimientos, referidos a los siguientes servicios: *Ö1 Macht Schule*, un portal web con material didáctico para profesores y alumnos de secundaria (2011), *Focus Sendungsarchiv*, un programa de contenidos dedicados a una mejor comprensión de la vida actual (2012), *ORF III – Kultur und Information*, un canal temático de información y cultura (2013), y *TVthek.ORF.at*, el portal web de la ORF, en el que se puede seguir su programación en directo a través de *streaming* o acceder a su archivo bajo demanda (2013). Todos los servicios fueron aprobados a través de la prueba, aunque en dos casos la aprobación estuvo sujeta a condiciones. Además, otras cuatro pruebas están abiertas en el momento de la redacción de este trabajo.

El *Auftragsvorprüfung* se inicia cuando la ORF redacta y entrega al Kommunikationsbehörde Austria (KommAustria, la Autoridad de Comunicaciones independiente) una propuesta de nuevo servicio. Ésta debe incluir el concepto detallado del servicio, argumentos que apoyen su relación con los objetivos y la misión de servicio público de la ORF, información relativa a su financiación y una primera valoración sobre el posible impacto que la aprobación de la propuesta tendría en la competencia del mercado correspondiente y en la diversidad de servicios ofrecidos a la audiencia. Toda esta información deberá ser entregada también al Wirtschaftskammer Österreich (WKÖ, la Cámara Federal de Economía de Austria) y al Kammer für Arbeiter und Angestellte (AK, la Cámara de Trabajo de Austria), a la vez que se publicará en la web de la ORF.

La publicación de la información en la web de la ORF marca el inicio de la consulta pública para terceros interesados, de seis semanas de duración. Finalizada la consulta, la ORF deberá entregar sus resultados a KommAustria, para que este organismo decida sobre la pertinencia de continuar adelante con la prueba. En caso afirmativo, KommAustria tomará el mando en la gestión del *Auftragsvorprüfung* y remitirá la documentación que recibió de la ORF al Consejo Asesor del Valor Público y a la Autoridad Federal de Competencia (BWB), para que ambos organismos desarrollen en las siguientes seis semanas sus respectivos informes.

El Consejo Asesor se encarga de la evaluación del valor público de la propuesta en relación con la misión de servicio público y los principios de la ORF. Por su parte, la BWB lleva a cabo el estudio sobre el impacto del servicio propuesto sobre otras actividades mediáticas del mismo sector del mercado en Austria. Una vez terminadas estos informes, serán entregados a KommAustria, que se encargará de contraponer toda la información para tomar una decisión sobre la propuesta de la ORF. La aprobación de la propuesta por parte de KommAustria puede estar sujeta a compromisos por parte de la ORF, normalmente relacionados con el diseño técnico del servicio, su accesibilidad, o sus contenidos. La ORF, por su parte, deberá publicar en su página web y de forma fácilmente accesible y permanente el concepto que ha sido analizado y la aprobación pertinente de KommAustria. La duración total del proceso es de cinco meses.

3.5. Irlanda

La prueba de valor pública irlandesa ha sido utilizada para aprobar seis nuevos servicios: el canal en alta definición RTÉ Two HD Select (2011), el canal de información 24 horas RTÉ News Now (2011), el canal infantil RTÉjr (2011), RTÉ Plus, para la redifusión de contenido de RTÉ1 (2011), el servicio de teletexto digital RTÉ Aertel Digital (2011) y Oireachtas TV, un canal temático centrado en el Parlamento irlandés (2016).

El mecanismo de evaluación ex ante en Irlanda cuenta con la particularidad de estar dirigida desde el propio Ministerio de Comunicación, Acción Climática y Medio Ambiente. El proceso gira en torno a la provisión de información al Ministro de Comunicación, ya que éste será el encargado de tomar la decisión final relativa a la aprobación del servicio propuesto. Tras una consulta pública abierta a los grupos de interés, la realización de un análisis del valor público de la propuesta y el estudio del impacto de mercado corren a cargo de la Broadcasting Autority of Ireland. Tras un proceso de seis meses de duración, el Ministro de Comunicación será el encargado de decidir sobre la pertinencia de aprobar o no el nuevo servicio propuesto, por lo que la prueba de valor público irlandesa está marcada por su fuerte dependencia política.

3.6. Países Bajos

La prueba de evaluación previa de los Países Bajos es una *rara avis* dentro del panorama europeo, por dos motivos. En primer lugar, las bases de la introducción de esta prueba se encuentran tanto en el la Ley de Medios de 2008 (Minister van Justitie, 2008) como en el derecho administrativo general, donde se detallan las características del proceso. Por otra parte, resulta llamativo que el *ex ante test* neerlandés prescinda del informe de uno de los aspectos fundamentales del procedimiento recomendado por la Comisión Europea: el análisis del impacto de mercado. El gobierno neerlandés, sin embargo, está estudiando la futura inclusión de un impacto de mercado en futuras pruebas.

Actualmente se han completado dos pruebas de valor público. En 2009 se aprobó un paquete de propuestas para el presupuesto 2008/2009, que incluía 12 radios temáticas digitales, tres canales de vídeo para móviles, información complementaria sobre la programación accesible a través del mando a distancia y servicios audiovisuales en el transporte público y las estaciones de tren. De igual forma, en 2010 se aprobó la propuesta para el plan estratégico 2010-2016, que consistía en la prolongación hasta enero de 2012 de la autorización del paquete de nuevos servicios anterior.

La prueba neerlandesa se inicia cuando el Ministro de Comunicación pide su opinión al Consejo de Cultura (*Raad vor Cultuur*) y a la Autoridad de Medios (*Commissariaat vor de Media*) sobre las propuestas de nuevos servicios. Estos dos organismos valorarán las propuestas en función de su conexión con la misión de servicio público de la NPO y su plan estratégico. A partir de sus conclusiones, el Ministro tomará una decisión provisional, sobre la cual los distintos grupos de interés podrán realizar comentarios en una consulta pública de 6 semanas. Los resultados de esta consulta serán revisados por el Ministro, quien, en función del valor público y del posible impacto de mercado de las propuestas, decidirá sobre su aprobación o no. La decisión del Ministro podrá ser apelada por la vía administrativa.

3.7. Dinamarca

En Dinamarca el *ex ante test* cuenta con un precursor, ya que desde 2007 se habían realizado ya tres pruebas de valor público –servicios de Danmarks Radio (DR) en el espacio público, la web con información sobre salud *dr.dk/sundhed,* y la web para consultas gratuitas para jóvenes *dr.dk/tvaers*. Sin embargo, estas primeras pruebas no incluían una valoración del impacto de mercado. Esta parte fue añadida a partir de la Comunicación de la Comisión Europea de 2009, así como de las presiones del sector privado.

La base legal de la actual prueba se plasmó en el *Mediepolitisk aftale 2011-2014* (Kulturministeriet, 2010), el contrato de servicio público que ha sido actualizado para el periodo 2015-2018. El proceso danés se inicia cuando la radiotelevisión pública DR propone un nuevo servicio o una modificación importante ante el Consejo de Radio y Televisión (*Radio-og tv-naevnet*). Este será el encargado de evaluar el valor público de la propuesta, al mismo tiempo que encarga a una consultora externa la elaboración del informe sobre el impacto de mercado (con una duración máxima de doce semanas) que después se encargará de comentar y valorar. Este proceso incluye también una consulta pública de 3 semanas. Una vez recabada toda la información, el Consejo contrapondrá el valor público de la propuesta con su impacto de mercado para decidir sobre la pertinencia o no de su aprobación. En total, el proceso está calculado para realizarse en veinte semanas.

3.8.Suecia

La prueba de valor público sueca ha estado rodeada de polémica en el país nórdico, por no gozar de la simpatía ni del público ni de la propia televisión pública. A pesar de que la radiotelevisión sueca incorporó una prueba de evaluación previa a su contrato de servicio público en el año 2011, hasta el momento no se ha llevado a cabo ningún proceso.

Sobre el papel, sin embargo, el proceso debería iniciarse con la elaboración de una propuesta de nuevo servicio por parte de la emisora pública, que será entregado al gobierno. Este, a su vez, se lo entregará a la Autoridad de Medios (*Myndigheten för radio och tv*) si considera que la prueba es necesaria. Tras la publicación del resumen del concepto, se abriría una consulta pública durante tres semanas. La Autoridad de Medios deberá realizar tanto la evaluación del valor público como el estudio del impacto de mercado, para el cual podría contar con la ayuda de la Autoridad de Correos

y Telecomunicaciones (*Post- och telestyrelsen*). Una vez valorados los dos aspectos que componen la prueba, la Autoridad de Medios se pronunciará a favor o en contra de la introducción del servicio propuesto. Sin embargo, la decisión final recae en manos del Gobierno.

El hecho de que la prueba no haya sido empleada no ha sido bien recibido por el sector privado. Su molestia se plasma en el encargo realizado por la Asociación de Editores de Periódicos (*Tidningsutgivarna*, TU) a la consultora Copenhaguen Economics, consistente en la aplicación independiente de la prueba de valor público a los últimos cuatro servicios aprobados por la *Sveriges Television* (SVT): *SVT Nyhetsappen,* una aplicación que incluye contenido informativo levemente diferente de lo emitido en televisión, *SVT Edit,* con contenido no relacionado con su programación radiotelevisiva, *SVT Opinion, SVT Recept*. Todos estos servicios habían generado controversia entre el sector privado, por considerarlos dañinos para la competencia del mercado. Copenhaguen Economics (*Förhandsprövning av fyra digitala SVT-tjänster)* concluía que, de haberse sometido a la prueba de valor público, dos de los cuatro servicios –*SVT* Nyhetsappen y *SVT Edit*) no habrían podido ser aprobados, ya que su elevado impacto de mercado no estaría justificado por su valor público (Copenhaguen Economics, 2015).

3.9. Finlandia

El caso finlandés es particular porque la única prueba de valor público llevada a cabo hasta el momento se completó antes de su introducción oficial en la legislación en 2013 (Liikenne- Ja Viestintäministeriö, 2013). Esta prueba tuvo lugar en 2010 y puede considerarse como la reacción a las críticas del sector privado del mercado finlandés. El *ex ante test* finlandés corre a cargo del Consejo Administrativo de la *Yleisradio* (YLE), formado por miembros del Parlamento y encargado tanto de la decisión final como de realizar las evaluaciones, aunque contando con ayuda: para el estudio del valor público se apoya en un experto en servicio público, mientras que para la evaluación del impacto de mercado se recurre a una consultora externa. Una vez recopilada toda la información, es el propio Consejo Administrativo quien decide si aprobar o rechazar la propuesta de la YLE.

3.10. Croacia

La introducción de una prueba de valor público en la Ley de la Radiotelevisión croata (Hrvatski Sabor) en 2010 se enmarca en la preparación de Croacia para su adhesión a la Unión Europea en 2013. Todavía no se ha llevado a cabo ningún procedimiento, aunque las generalidades de la prueba se recogen en el artículo 15 de la Ley de Radiotelevisión de Croacia: serán objeto de una prueba de valor público todos los nuevos servicios o modificaciones importantes que quiera introducir la HRT, que además cuenta con una lista de actividades prohibidas para la radiotelevisión pública, al igual que sucedía con Alemania. El proceso corre a cargo del Consejo de Medios Electrónicos (*Vijice za Elektronické medije*), después de recibir la propuesta detallada de la HRT. La prueba consta de una consulta pública de 45 días, de la evaluación del Consejo de Programación de la HRT sobre el valor de la propuesta y del estudio del impacto de mercado, a cargo de la Autoridad de Competencia. Una vez recogida toda la información, el Consejo de Medios Electrónicos decidirá sobre la aprobación o no de la propuesta de HRT.

4. Conclusión: un modelo, múltiples interpretaciones

Como se puede deducir de la descripción de las pruebas de cada Estado miembro, el ex ante test propuesto por la Comisión Europea ha dado lugar a múltiples interpretaciones en cada contexto nacional, derivadas, en parte, del tamaño de los mercados audiovisuales de cada país y de la posición en la que se encuentra cada radiotelevisión pública dentro de ese mercado.

De forma general, todos los países, salvo los Países Bajos, estructuran su prueba en torno a la evaluación del valor público y del impacto de mercado, siguiendo de forma directa la base esencial propuesta por la comisión. En todos los casos se incluye un periodo de consulta pública abierto a la opinión de los distintos grupos de interés, cuya duración puede oscilar entre las 3 y las 6 semanas.

En la duración y el presupuesto requerido para cada prueba sí que se encuentran diferencias más notables. Reino Unido y Alemania apuestan por mecanismos que se alargan hasta los 6 meses y que requieren de un gran desembolso económico. Otros países, sin embargo, optan por procesos más económicos y fijan su duración en tres meses, como es el caso de Suecia. Limitar el proceso a tres meses añade dinamismo y rapidez a la toma de decisiones, por lo que el diseño de procesos de esta duración sería recomendable siempre y cuando no fuese en detrimento de la calidad y validez de sus resultados.

Los agentes encargados del desarrollo de la prueba también difieren en cada país: mientras que en algunos casos se opta por organismos independientes (como el BBC Trust, en Reino Unido), en otros países la prueba corre a cargo de instituciones conformadas por distintos grupos de interés (como los Rundfunkrat alemanes), pasando por aquellos en los que un agente político cuenta con mayor peso (como Irlanda, los Países Bajos o Suecia). La independencia constituye una característica muy deseable a la hora de diseñar y llevar a cabo una prueba de valor público, ya que sólo así podrá derivar en resultados justos que contribuyan a legitimar el papel de la radiotelevisión pública y su avance en los nuevos medios.

A modo de conclusión, se percibe que donde mejor acogida ha tenido este procedimiento de evaluación previa ha sido en los países que ya contaban con un sistema de medios de comunicación públicos fuerte y consolidado en su mercado –algo que se puede percibir teniendo en cuenta las diferencias en la duración y el presupuesto de las pruebas en distintos países. La puesta en marcha de este procedimiento ex ante en España parece no ser prioritaria en la actualidad, pero es necesario mantenerse alerta ante las posibles novedades que se planteen en el panorama europeo.

Referencias

Bundeskanzleramt (2010). Bundesgesetz über den Österreichischen Rundfun. Recuperado de https://goo.gl/inMm63

Comisión Europea (2009). Comunicación de la Comisión sobre la aplicación de las normas en materia de ayudas estatales a los servicios públicos de radiodifusión. Recuperado de https://goo.gl/VSttJP

Copenhaguen Economics (2015). Förhandsprövning av fyra digitala SVT-tjänster. Mångfaldshotande eller samhällsberikande? Recuperado de https://goo.gl/EGH8VN

Departement Cultuur, Jeugd, Sport en Media (2009). Decreet van 27 Maart 2009 Betreffende Radio-Omroep en Televisie. Recuperado de https://goo.gl/VBktFr

Department for Culture, Media and Sport (2006). Royal Charter for the continuance of the British Broadcasting Corporation. Recuperado de https://goo.gl/Zua215.

Dorr, R. (2011). The ZDF three-step test. A dynamic tool of governance. En: K. Donders, K. & H. Moe (eds.), *Exporting the Public Value Test: The Regulation of Public Broadcasters's New Media Services Across Europe*, pp. 69-82. Gotemburgo: Nordicom.

Hrvatski Sabor (2010). Zakon O Hrvatskoj Radioteleviziji. Recuperado de: http://www.hrt.hr/uploads/media/Zakon_o_HRT_2010.pdf

Kulturministeriet (2010). Fokus på kvalitet og mangfoldighed. Mediepolitisk aftale for 2011-2014. Recuperado de https://goo.gl/KeS9Nb

Liikenne- Ja Viestintäministeriö (2013). Act on Yleisradio Oy. Recuperado de https://goo.gl/ekVJCu

Minister van Justitie (2008). Wet van 29 december 2008 tot vaststelling van een nieuwe Mediawet. Recuperado de https://goo.gl/8gVsPz.

Reconocimientos de la investigación

Los resultados de este artículo corresponden al proyecto de "Indicadores de gobernanza, financiación, rendición de cuentas, innovación, calidad y servicio público de las RTV europeas aplicables a España en el contexto digital" (Referencia CSO2015-66543-P) del Programa estatal de Fomento de la Investigación Científica y Técnica de Excelencia, subprograma estatal de Generación de Conocimiento del Ministerio de Economía y Competitividad de España, cofinanciado por el Fondo Europeo de Desarrollo Regional (FEDER) de la Unión Europea. Así como de la actividad de la Red Internacional de Investigación de Gestión de la Comunicación (REDES 2016 G-1641 XESCOM) apoyada por la Consellería de Cultura, Educación e Ordenación Universitaria de la Xunta de Galicia (referencia ED341D R2016/019). La autora Marta Rodríguez-Castro es beneficiaria de un contrato de Formación de Profesorado Universitario (FPU16/05234) del Ministerio de Educación, Cultura y Deporte.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 19/09/2017
Aceitação/Acceptance: 23/03/2018

La promoción de la diversidad lingüística en las radiotelevisiones públicas europeas

Sara Pérez-Seijo[1], Francisco Campos-Freire[2]

s.perez.seijo@usc.es, francisco.campos@usc.es

[1] Universidade de Santiago de Compostela, 15782, Santiago de Compostela, España

[2] Universidade de Santiago de Compostela, 15782, Santiago de Compostela, España

Pages: 163–173

Resumo: Diversidad es un concepto amplio, un término que engloba diferentes dimensiones: cultura, sociedad, lengua, orientación sexual, género, edad, etcétera. Y diversa es la Unión Europea de Radiodifusión (UER). Como ente de servicio público y, por tanto, al servicio del público, la UER debe velar por garantizar la representación de todos los colectivos de la sociedad, sin excluir o marginalizar. En este sentido, este estudio se centra en apreciar cómo en los últimos años, concretamente entre el 2013 y el 2015, las radiodifusoras públicas europeas han desarrollado, implementado y gestionado sus medidas y políticas de programación a favor de la diversidad lingüística y cuáles han sido sus principales apuestas.

Palavras-chave: diversidad lingüística; lenguas minoritarias; lenguas cooficiales; radiodifusoras públicas europeas; Unión Europea de Radiodifusión.

The promotion of linguistic diversity on the European public broadcasters

Abstract: Diversity is a broad concept that covers different dimensions: culture, society, language, sexual orientation, gender, age, and so on. And the European Broadcasting Union (EBU) is also diverse. As a public service entity and therefore at the service of society, the UER should ensure that all social groups are represented without being excluded and/or marginalized. In this regard, this study focuses on how the European public broadcasters have developed, enforced and managed their programming measures and policies in support of linguistic diversity between 2013 and 2015. Furthermore, the aim is to identify their main stakes in this respect.

Keywords*:* linguistic diversity; minority languages; co-official languages; European public broadcasters; European Broadcasting Union.

1. Introducción

Diversidad, del latín *diversitas*, es un término que significa variedad, diferencia o abundancia de elementos distintos. No obstante, bajo esta palabra se engloban multitud de grupos, categorías y clases. Tal amplitud conlleva que la diversidad se entienda como

"un concepto multidimensional" (León, 2007) y que por ello se distingan distintos tipos de diversidades.

Las variedades más frecuentes son: cultural, que refleja la multiplicidad de culturas o grupos culturales a nivel global, regional o local y su convivencia o interacción; étnica, que se refiere a las acciones de visibilidad de los diferentes pueblos en una misma sociedad; sexual, que engloba los distintos tipos de orientación o identidad sexual -por lo general se emplea la clasificación de heterosexuales, homosexuales, bisexuales y transexuales, y en la actualidad (2017) ha ganado fuerza el colectivo LGBTI (lesbianas, gais, bisexuales y personas transgénero e intersexuales)-; funcional, un término alternativo al de discapacidad y que significa "la diferencia de funcionamiento de una persona al realizar las tareas habituales (desplazarse, leer, agarrar, ir al baño, comunicarse, relacionarse, etc.) de manera diferente a la mayoría de la población" (Romañach & Lobato, 2015); biológica, que abarca la amplia variedad de seres vivos del planeta y al resto de elementos que conforman el medioambiente; y lingüística, que hace referencia a la existencia de múltiples lenguas en un mismo espacio geográfico -a veces, lengua y comunidades étnicas o migrantes van de la mano-.

Aunque estos seis tipos de diversidades sean los más frecuentes en las clasificaciones, existen otros menos comunes pero igualmente recurridos: cinematográfica (Manfredi, 2015), social, de género, generacional/de edad y profesional, entre otras.

1.1. La diversidad como concepto: el caso de las radiotelevisiones públicas europeas

El 12 de febrero de 1950 nace en Devon, Reino Unido, la Unión Europea de Radiodifusión, más conocida por sus siglas UER. Como "asociación de organizaciones de radiodifusión" (European Broadcasting Union, 2015) de servicio público, su misión era y es la de servir a todos los ciudadanos, un hecho que a priori parece descartar la discriminación y la marginalización. Sin embargo, la tendencia de los medios de comunicación es a "conferir estatus y legitimidad a ciertos sectores de la sociedad, así como a sus comportamientos y actividades", mientras que "las prácticas y significados de los demás grupos son excluidos o marginalizados en el campo semántico social" (Pontes, 2013).

Para cumplir la meta de la UER como un servicio público para todos, sin exclusión (European Broadcasting Union, 2015), a principios de siglo se procedió a un reajuste de una política multicultural, en boga en los años noventa, a una de diversidad cultural. Con esta modificación, paulatinamente las radiodifusoras públicas europeas comenzaron a optar por la inclusión en vez de separar la programación dirigida a minorías, grupos sociales o comunidades lingüísticas del territorio (Hultén & Horsti, 2016).

En 2005, en el marco de la 33ª Conferencia General de la UNESCO, se celebró la Convención sobre la protección y la promoción de la diversidad de las expresiones culturales. Este encuentro tenía como finalidad alentar a los diferentes países europeos a promover la diversidad en sus territorios mediante la implementación y creación de políticas y medidas estrechamente ligadas a los objetivos del acuerdo. Entre estas se encontraban la inversión en creación local audiovisual, el apoyo a la producción cinematográfica independiente, la imposición de obligaciones de programación o iniciativas de cooperación cultural internacional, entre otras (García, 2015).

De este tratado se derivaron sucesivos documentos a favor de la integración social y cultural. Uno de ellos fue la Agenda Europea para la Cultura, aprobada por el Consejo de la Unión Europea en 2007. Este texto señala tres objetivos generales para la comunidad europea: la diversidad cultural y el diálogo intercultural; la cultura como herramienta catalizadora para la creatividad; y la cultura como elemento vital en las relaciones internacionales. En síntesis, el escrito sacaba a flote la diversidad cultural como eje central de las políticas comunitarias, entre las que presentan un papel decisivo las relativas al sector audiovisual público. En este sentido, la UER ha demandado reiteradamente que sus miembros proporcionen "programación variada y equilibrada para todos los sectores de la población, incluyendo programación dedicada a los intereses de las minorías" (Horsti, 2014) Con todo, los servicios públicos de radiodifusión europeos tienen la responsabilidad legal de incluir las minorías étnicas y colectivos sociales en su oferta programática, bien como temas o como profesionales.

Si bien el servicio de radiodifusión pública insiste en una gama dispar de programación, no precisa cómo esa diversidad es supervisada y seguida (Horsti, 2014). La UER se refiere a la diversidad como parte de los deberes del servicio público de los entes que lo conforman. Por lo tanto, es tarea de cada estado europeo el fomento de la diversidad en su territorio (León, 2007), comprometiéndose o no así con todos los miembros de la sociedad a la que informa.

2. Metodología

La presente comunicación tiene como objetivo obtener una visión detallada del nivel de promoción de la diversidad lingüística –en cierta medida también cultural y regional-, entre los años 2013 y 2015, por parte de las radiotelevisiones que conforman la Unión Europea de Radiodifusión (UER). Para contextualizar el concepto de diversidad y su pasado y presente en el sector audiovisual público europeo, se procedió en primer lugar a una revisión teórica para sentar una base antes de avanzar en la investigación.

Posteriormente, se procedió a la selección de la muestra de análisis, que en este caso se correspondió con las radiodifusoras públicas de los países miembros de la UER: *Radio Televizioni Shqiptar* (Albania), *Radio Télévision Belge Francophone* (Bélgica), *Vlaamse Radio- en Televisieomroep* (Bélgica), *Danmarks Radio* (Dinamarca), *Yleisradio* (Finlandia), *France Médias Monde* (Francia), *France Télévisions* (Francia), *Radio France* (Francia), *Ríkisútvarpið* (Islandia), *TG4* (Irlanda), *Raidió Teilifís Éireann* (Irlanda), *Israel Broadcasting Authority* (Israel*), Radiotelevisione Italiana* (Italia*), Public Broadcasting Services Limited* (Malta), *Teleradio-Moldova* (Moldavia), *Rádio e Televisão de Portugal* (Portugal), *Norsk Rikskringkasting* (Noruega), *Romanian Radio Broadcasting* (Rumanía), *Societatea Română de Televiziune* (Rumanía), *Radiotelevisión Española* (España), *Sveriges Radio* (Suecia), *Sveriges Television* (Suecia*), Sveriges Utbildningsradio* (Suecia), *Schweizerischen Radio- und Fernsehgesellschaf* (Suiza), *British Broadcasting Television* (Reino Unido).

Una vez identificados los entes televisivos públicos, se seleccionaron los informes oficiales publicados por los mismos entre los años 2014 y 2016, con el fin de obtener los datos más recientes en el tiempo. De ellos se debían extraer y recoger datos que

dieran cuenta de los niveles de diversidad lingüística en cada radiodifusora pública europea, por lo que para realizar esta tarea fue necesario el empleo de técnicas de carácter cuantitativo. Tras obtener la información necesaria para la investigación, se elaboraron tablas clasificatorias para, posteriormente, establecer unas conclusiones sólidas y probadas. El fin era advertir qué recursos, medidas y/o tiempo ha dedicado cada ente a la promoción y fomento de las lenguas cooficiales o minoritarias del territorio.

3. Resultados

Europa es un continente variado, dispar y diverso. Por ese motivo, las radiodifusoras públicas se han autoimpuesto la meta de mostrar cuán distinto es cada estado con respecto a los demás y cuánto lo es en su propio territorio y sociedad. Así, valiéndose de la propia programación, estos entes tratan de trasladar al espectador la idea de que las macrocategorías o macroetiquetas no albergan mayorías, sino que se componen de múltiples minorías. Y, para alcanzar este objetivo, han desarrollado en los últimos años políticas en favor de la diversidad.

Los principales esfuerzos de las radiodifusoras públicas se centran en visibilizar, sobre todo la diversidad cultural del territorio. Así lo ha demostrado el 80% de entes radiodifusores que entre 2013 y 2015 han apostado por políticas que velen, respalden y protejan las diferentes culturas de cada territorio. El 76% también ha abogado por apoyar por medio de políticas de programación inclusivas la diversidad funcional. Por su parte, un 68% ha concentrado sus esfuerzos en promover la diversidad lingüística existente en su área geográfica. Otras diversidades que también cuentan con un respaldo considerable teniendo en cuenta el total de radiodifusoras serían: la diversidad social (64%), donde entrarían los colectivos en riesgo de exclusión y las personas en situación de pobreza; la diversidad generacional o de edad (60%); la diversidad étnica (60%); y la diversidad de género (60%). Con menos representación y apoyo en las políticas y planes de programación se encontrarían las diversidades: profesional (40%), sexual (24%) y medioambiental (24%).

País	Ente	Cult.	Func.	Étn.	Gén.	Sex.	Bio.	Ling.	Soc.	Ed.	Prof.
PT	*RTP*	x	x	x	x		x		x		
IS	*RÚV*		x		x					x	x
IE	*RTÉ*	x	x		x			x			
IE	*TG4*	x						x			
DK	*DR*	x	x	x				x	x	x	
CH	*SRG-SSR*	x	x	x	x		x	x	x	x	x
BE	*RTBF*	x	x	x		x			x	x	x
BE	VRT		x	x	x				x	x	x
ES	*RTVE*	x	x		x	x	x	x	x		x

País	Ente	Cult.	Func.	Étn.	Gén.	Sex.	Bio.	Ling.	Soc.	Ed.	Prof.
MT	*PBS*										
IT	*RAI*	x	x		x		x	x	x	x	
RO	*ROR*	x		x				x		x	
RO	*TVR*	x	x	x				x			
FI	*YLE*	x	x	x				x	x	x	
MG	*TRM*	x		x				x	x		
FR	*FTV*	x	x	x	x	x	x	x	x	x	x
FR	*RF*	x	x		x				x	x	
FR	*FMM*	x	x		x			x			x
NO	*NRK*	x	x	x	x			x	x	x	x
IL	*IBA*										
SE	*SR*	x	x	x	x			x	x	x	
SE	*SVT*	x	x	x	x	x		x	x	x	x
SE	*UR*	x	x	x	x	x		x	x	x	x
UK	*BBC*	x	x	x	x	x	x	x	x	x	x
AL	*RTSH*										
T O T A L		80 %	76 %	60 %	60 %	24 %	24 %	68 %	64 %	60 %	40 %

Tabla 1 – Tipos de diversidades que las radiodifusoras públicas europeas contemplaron en sus políticas y acciones entre los años 2013 y 2015. Elaboración propia [1]

Las radiodifusoras públicas europeas prestan especial atención a la diversidad cultural, regional y/o lingüística de su propio territorio. Para dar cuenta de la dispar realidad cultural que presenta cada sociedad, las radiotelevisiones dedican programas o secciones a narrar, visibilizar o explicar la historia, tradiciones, músicas y costumbres de cada uno de los colectivos y regiones que conforman el país.

En este sentido, el 80% de las radiodifusoras púbicas europeas han promocionado de alguna manera la diversidad cultural entre 2013 y 2015, situándose esta como la diversidad con mayor apoyo y visibilidad en las políticas programáticas de dichos entes. A su vez, también consideran que el apoyo a las lenguas cooficiales o minoritarias del territorio es crucial para llegar a todos los públicos. Así lo ha ejemplificado el 68% de los entes. Pero no solo se trata de hablar de su existencia, sino que estos medios reservan o dedican anualmente horas de programación para emitir contenido en las diferentes lenguas habladas en cada estado.

[1] Las siglas significan: Cult. de cultural; Func. de funcional; Étn. de étnica; Gén. de género; Sex. de sexual; Bio. de biológica; Ling. de lingüística; Soc. de social; Ed. de edad; Prof. de profesional.

Ente	Lenguas del territorio		Lenguas foráneas	
BBC	Inglés Galés Gaélico escocés Escocés de Ulster Irlandés		Árabe Kirguís Nepalí Azerbaiyano Portugués brasileño Birmano Chino Francés Hausa Ucraniano Urdu Uzbeko Vietnamita	Hindi Indonesio Pastún Persa Español Ruso Cingalés Somalí Suajili Tamil Tailandés Turco Etcétera
FMM	Francés		Inglés Camboyano Chino Español Hausa Suajili Persa	Portugués Portugués brasileño Romaní Ruso Vietnamita Khmer
FTV	Francés Bretón Alsaciano	Otros dialectos del suroeste	-	
TRM	Rumano Ruso Búlgaro	Gagaúzo Ucraniano Romaní	-	
RTÉ	Irlandés Inglés	Gaélico de Gaeltacht	-	
YLE	Finés Sueco	Sami (northern, inari, kolt)	Ruso Romaní Inglés	Latín Etcétera
VRT	Neerlandés		Inglés Alemán	Francés
ROR	Rumano Griego Tártaro Turco Armenio Ruso Húngaro Romaní	Alemán Checo Eslovaco Croata Serbio Italiano Romanche Etcétera.	Español Chino Inglés Portugués	
TVR	Ucraniano Rumano Alemán Húngaro Croata Búlgaro	Esloveno Serbio Romaní Romanche Etcétera.	-	
SRG-SSR	Sueco Romanche		Italiano Alemán	Francés
SR	Sueco Finés Romaní	Sami Yidis Meänkieli	Inglés Ruso Alemán Árabe	Kurdo Persa Somalí

Ente	Lenguas del territorio		Lenguas foráneas
SVT	Sueco Finés Sami	Meänkieli Romaní	-
UR	Sueco Finés Meänkieli	Romaní Sami Yiddish	-
RAI	Italiano Ladino Alemán	Francés Esloveno	Inglés
NRK	Noruego Finés	Kven Sami	-
RTVE	Castellano Catalán	Gallego Euskera	Inglés

Tabla 2 – Lenguas por las que las radiotelevisiones emprendieron medidas de diversidad lingüística entre los años 2013 y 2015. Elaboración propia

British Broadcasting Corporation. La *BBC* apuesta por la difusión de contenidos en lenguas minoritarias del territorio. Por ese motivo, en 2014 destinó 14,1 millones de libras a la producción de productos íntegramente en gaélico escocés a través de *BBC Radio nan Gaidheal*, una cifra que incrementó en 2015: 14,2 millones de libras. Al galés también dedicó recursos en *BBC Radio Cymru*, aunque en menor medida: 3,9 millones de libras en 2015 y 3,7 millones en 2014. A través de *BBC Alba* también ofreció contenido para los gaélico-parlantes, pero en este caso la inversión fue menor: 5,5 millones de libras en 2015 y 6 millones en 2014. Al resto de lenguas minoritarias, como es el caso del irlandés y del escocés de Úlsers, la *BBC* dedicó en 2015 un total de 261 horas de programación a través de *la BBC Radio Ulster* y de la *BBC Radio Foyle*. En cuanto a lenguas foráneas al territorio se refiere, produce contenido en alrededor 30 lenguas distintas a través de su servicio de noticias internacionales.

France Médias Monde. *FMM* difundió en 2014, a través de *Radio France International*, contenidos en más de 12 lenguas, incluido el francés. No obstante, prestó atención a varias lenguas minoritarias: diariamente emitió alrededor de 13 horas de programación en khmer, 11 en romaní y 2 horas y media en hausa. En resumidas cuentas, mantuvo una clara política multilingüe.

France Télévisions. La radiodifusora francesa *FTV* apostó en 2015 por la difusión de magazines en las lenguas minoritarias de las regiones de Bretaña, Alsacia y el Suroeste.

Teleradio-Moldova. *TRM* reserva alrededor del 93% de las emisiones totales al idioma oficial, el rumano, una cifra que suele equivaler a, aproximadamente, 8.050 horas. El 7% restante lo destina a las lenguas de las comunidades nacionales del territorio, es decir, unas 600 horas de emisión anuales. Con todo, los resultados finales del 2015 resultaron positivos para los idiomas minoritarios: *TRM* difundió el 8,09% de su programación en lenguas de las comunidades nacionales, el equivalente a 702 horas, mientras que en rumano difundió el 91,01%, exactamente 7.966 horas.

Yleisradio. *YLE* aboga por un servicio de información multilingüe a través de sus canales televisivos y radiofónicos. De hecho, en 2015 produjo noticias en 11 idiomas distintos. La principal vía de difusión lingüística es el canal de radio *Yle Mondo*, por el cual emitió en 2013 8.760 horas en lenguas foráneas, 24 más que en 2012. En diciembre de 2013 dio un paso adelante en favor de las lenguas minoritarias de Finlandia. El canal radiofónico *Yle Oddasar*, que por aquel entonces ya emitía también contenido en romaní, pasó a añadir a su programación el sami, que ya se incluía en otros programas de la radiodifusora. De este modo, en 2013 se emitieron alrededor de 1.590 horas en esta lengua minoritaria, 20 más que el año anterior.

Vlaamse Radio- en Televisieomroeporganisatie. *VRT* aboga por el uso del estándar neerlandés en su programación, la misma que no destaca por la diversidad lingüística. No obstante, en la web sí dispone de plataformas en otros idiomas: francés, alemán e inglés.

Romanian Radio Broadcasting. Como servicio de radio público de Rumanía, *ROR* apuesta notoriamente por una política lingüística en beneficio de las lenguas minoritarias del territorio. Por esa razón, las seis estaciones de radio regionales producen y emiten programas semanales en los diferentes idiomas minoritarios.

Televiziunea Română. La televisión pública de Rumanía también aboga por la inclusión y difusión de contenidos en lenguas minoritarias del territorio. Solo en 2015, a través de *TVR1* y *TVR2*, el ente emitió 145 minutos semanales de contenido en alemán y 35 minutos mensuales en *TVR3*. Por su parte, *TVR Cluj* fue la cadena que más idiomas adoptó en su programación: en húngaro transmitió alrededor de 559 horas, mientras que para el resto de lenguas minoritarias destinó cerca de 130 horas en ese mismo canal y aproximadamente 50 horas en *TVR3*.

Schweizerischen Radio- und Fernsehgesellschaf. El ente de radiodifusión público de Suiza *SRG-SSR* dispone de un canal de radio en alemán y romanche y otro de televisión de redifusiones solamente en alemán; una oferta de contenidos en idiomas extranjeros que complementa con la publicación en la web de contenidos en francés.

Sveriges Radio. *SR* apuesta por el fomento de la lengua oficial, el sueco, y de los idiomas minoritarios de su territorio, prestando especial atención al sami (1.390 horas de emisión en 2015 y 1.393 en 2014), al meänkieli (830 horas en 2015 y 803 en 2014), romaní (395 horas en 2015 y 391 en 2014) y finés (7.390 horas en 2015 y 7.319 en 2014). Junto a estas, también les dedicó tiempo, aunque en menor medida, al yidis (2 horas en 2015 y 1 hora en 2014), al kurdo (3.302 horas en 2015 y 392 en 2014), al somalí (122 horas en 2015 y 156 en 2014) y al árabe (325 horas en 2015 y 392 en 2014). Sin embargo, también respalda la publicación de contenido internacional en la página web: en inglés todos los días (325 horas en 2015 y 392 en 2014) y en ruso y alemán de lunes a viernes.

Sveriges Television. *SVT* enfatiza y prioriza la variedad lingüística de su territorio, apoyando así las lenguas minoritarias de su territorio en estrecha colaboración con *Sveriges Radio* para la planificación lingüística. De este modo, en 2015 permitió que un 25% de la programación, alrededor de 655 horas (559 en 2014), pudiera ser difundido en idiomas no reconocidos como oficiales en país. Si se desglosa el tiempo total dedicado, se obtiene que se emitieron: en finés 325 horas (314 en 2014), en meänkieli

19 (17 en 2014), en somalí 109 (84 en 2014), en romaní 27 (23 en 2014) y en lengua de signos sueca 175 (121 en 2014). En total, *SVT* logró difundir contenido en 40 idiomas diferentes.

Sveriges Utbildningsradio. *UR* emitió en 2015 un total de 99,8 horas de programas en sami, finés y meänkieli, lo que supuso un aumento del 25% con respecto al 2014, con 80 horas solamente. Con todo, la evolución semeja positiva a lo largo de los años, teniendo en cuenta que en 2013 solo se dedicaron 75 horas de programación a estas lenguas minoritarias.

Radiotelevisione Italiana. La *RAI* apostó en 2015 una vez más por sus minorías lingüísticas y aprovechó sus redacciones regionales para potenciarlas desde allí con la emisión de programas en los diferentes idiomas.

Norsk Rikskringkasting. En 2015 *NRK* se marcó el objetivo de emitir el 25% de su contenido siguiendo el estándar nynorsk del idioma noruego, pero cerró el año con solo un 24%. Además, la empresa también transmite en kven, finés y sami.

Radiotelevisión Española. *RTVE* apuesta notablemente por el empleo del catalán, de tal forma que en 2014 dispuso de una franja de programación diaria en este idioma en *La 2*. En total, emitió alrededor de 140 horas de contenidos. Cabe destacar y señalar la existencia de *Rádio 4*, la emisora en catalán de *Radio Nacional Española*. Junto a esto, existen otras políticas lingüísticas de inclusión que obligan a emitir todas las declaraciones de los telediarios nacionales en la lengua oficial en la que estén (gallego, catalán, euskera), siendo subtituladas en castellano a la par. Por otra parte, en 2013 *RTVE* puso en marcha *Let's Clan*, un programa infantil avalado por el British Council que permitió la emisión en dual en inglés del 80% aproximadamente.

Danmarks Radio. *DR* incluye en sus últimos informes que al idioma principal, el danés, ha destinado en 2015 un total de 19.485 horas y en 2014 19.202. No obstante, ha dejado espacio para programación en otras lenguas, aunque no especifica cuáles: 23.164 horas en total.

4. Conclusiones

Concluido el análisis, se puede afirmar que entre el año 2013 y el 2015, periodo analizado en este estudio, las radiotelevisiones públicas europeas centraron sus esfuerzos, recursos y programación en fomentar la diversidad. Con todo, se trata de un concepto muy amplio y que abarca múltiples tipologías, por eso es necesario desglosarlo.

Las diversidades más apoyadas durante los tres años analizados fueron, por orden: la diversidad cultural (80%), la diversidad funcional (76%), la diversidad lingüística (68%) y la diversidad social (64%), donde entrarían las minorías en riesgo de exclusión o en situación de pobreza. Muy de cerca, con prácticamente el respaldo de la mitad de entes radiodifusores públicos, estaría la diversidad generacional o de edad, la diversidad étnica y la diversidad de género. La diversidad profesional, es decir, de igualdad de oportunidades y responsabilidades para todas las personas –independientemente de sus diversidades funcionales, género, cultura, etnia u orientación sexual- es una de las metas que paulatinamente las radiotelevisiones tratan de mejorar, aunque hasta

2015 -este incluido- solo 11 empresas públicas mencionan en sus informes sus medidas o políticas para contribuir a la inclusión e igualdad laboral.

La diversidad cultural y la lingüística van, en numerosos países, de la mano. Ejemplo de ello son las comunidades samis de Noruega, país donde la televisión pública, *Norsk Rikskringkasting*, incluye en su programación tanto contenidos sobre la cultura sami como programas en la propia lengua sami. Mediante las políticas a favor de la diversidad cultural y lingüística, los gobiernos tratan así de dar cuenta de la disparidad cultural que presenta cada sociedad. Y lo hacen, por un lado, mostrando las tradiciones, costumbres, historias y demás rasgos de cada uno de los colectivos regionales o culturales del país y, por otro, mediante el apoyo a las lenguas cooficiales o minoritarias habladas en el territorio para, de este modo, llegar a todos los públicos.

La diversidad lingüística supuso, entre 2013 y 2015, el tercer tipo de diversidad con más apoyo, promoción y atención por parte de las radiodifusoras públicas europeas en términos de políticas y medidas de programación. Dos entes de los que más apoyo dan a los diferentes colectivos lingüísticos de sus respectivos países son la *British Broadcasting Company* –al gaélico escocés, al galés y al irlandés y escocés de Úlsers- y *Sveriges Radio* –al sami, meänkieli, romaní, finés, yidis, etcétera-. Esta última, junto con *Sveriges Television*, ha seguido en los años mencionados un plan lingüístico encaminado a visibilizar los idiomas minoritarios por medio de su programación.

Romanian Radio Broadcasting también supone un buen ejemplo de aplicación de políticas lingüísticas de cara a la programación orientadas a fomentar los idiomas minoritarios hablados en el territorio. Sus seis estaciones de radio regionales han emitido entre 2013 y 2015 programas semanales en las lenguas minoritarias del país.

Reconocimientos

Los resultados de este artículo corresponden a los proyectos de, por un lado, "Indicadores de gobernanza, financiación, rendición de cuentas, innovación, calidad y servicio público de las RTV europeas aplicables a España en el contexto digital" (Referencia CSO2015-66543-P) del Programa estatal de Fomento de la Investigación Científica y Técnica de Excelencia, subprograma estatal de Generación de Conocimiento del Ministerio de Economía y Competitividad de España, cofinanciado por el Fondo Europeo de Desarrollo Regional (FEDER) de la Unión Europea; y, por otro, al de "Usos y preferencias informativas en el nuevo mapa de medios en España: modelos de periodismo para dispositivos móviles" (Referencia: CSO2015-64662-C4-4-R), del Ministerio de Economía y Competitividad. Este proyecto está cofinanciado por el fondo estructural FEDER. También se incluye dentro del programa de actividades de la Red Internacional de Investigación de Gestión de la Comunicación (REDES 2016 G-1641 XESCOM) apoyada por la Consellería de Cultura, Educación e Ordenación Universitaria de la Xunta de Galicia (referencia ED341D R2016/019). Además, la autora Sara Pérez Seijo es beneficiaria del programa de Formación del Profesorado Universitario (FPU16/06156) financiado por el Ministerio de Educación, Cultura y Deporte (Gobierno de España).

Referencias

European Broadcasting Union (2015). Statutes of the European Broadcasting Union. *Ebu.ch*. Recuperado de: https://goo.gl/L13Rgj

García, M. T. (2015). España y la Convención sobre Diversidad Cultural: consecuencias de su ratificación para las políticas de comunicación y cultura. *Trípodos*, 36, 167–183.

Horsti, K. (2014). The cultural diversity turns: policies, politics and influences at the European level. En Horsti, K., Hultén G. & Titley G. (eds.) *National conversations: public service media and cultural diversity in Europe*. Bristol: Intellect.

Hultén, G. & Horsti, K. (2016). In case of diversity: dilemmas of sharing good practices across borders in European broadcasting. En Edide, E & Nikunen, K. (eds.. *Media in motion. Cultural complexity and migration in the Nordic region*. New York: Routledge.

León, B. (2007). Commercialization and Programming Strategies of European Public Television. A Comparative Study of Purpose, Genres and Diversity. *Observatorio Journal*, 2, 81–102.

Manfredi, J. L. (2006). El reto digital de las televisiones públicas en Europa. Las estrategias de la BBC y de RTVE. *Telos: Cuadernos de comunicación e innovación*, 68, 45–51.

Pontes, L. (2013). Promovendo a diversidade? A representação das mulheres migradas na televisão pública da Catalunha (TV3). *Diálogo*, 23, 77–91.

Romañach, J. & Lobato, M. (2015). Diversidad funcional, nuevo término para la lucha por la dignidad en la diversidad del ser humano. *Foro de Vida Independiente*. Recuperado de: https://goo.gl/ogG8EX

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 31/12/2017
Aceitação/Acceptance: 01/03/2018

Telemedicina en la Salud para la Provincia de Santa Elena

Carlos Lindao[1], Evelyn Castillo[1], Teresa Guarda[1]

carlos.junior.dj@hotmail.com, eve_c.ml10@hotmail.com, tguarda@gmail.com

[1] Universidad Estatal Península de Santa Elena, La Libertad, Santa Elena, Ecuador

Pages: 174–180

Resumen: Este artículo se basa en aprovechar la tecnología que poseemos en la actualidad para integrarlas en el área de la medicina, de tal manera obtener una mejor y eficiente atención a los pacientes que soliciten el servicio en algún centro de salud público de nuestro país. El uso de la tecnología ha sido muy eficiente en todos los ámbitos. La sociedad que habita en la provincia de Santa Elena no posee un seguimiento de su salud por medio de aparatos electrónicos y no tiene conciencia del buen uso que le puede dar, no se lleva un riguroso control de cada persona en los centros de salud públicos. La telemedicina ayudará a mejorar la forma de monitorear el estado de salud de los pacientes en tiempo real evitando las consultas médicas tradicionales.

Palabras-clave: Telemedicina; aparatos electrónicos; salud pública

Telemedicine in Health for the Province of Santa Elena

Abstract: This article is based on taking advantage of the technology that we currently possess to integrate them in the area of medicine, in order to obtain a better and efficient service to patients who request the service in a public health center in our country. The use of technology has been very efficient in all areas. The society that lives in the province of Santa Elena does not have a follow-up of their health through electronic devices and is not aware of the good use that it can give, it does not take a strict control of each person in public health centers. Telemedicine will help improve the way of monitoring the health status of patients in real time avoiding traditional medical consultations.

Keywords*:* Telemedicine; electronic devices; public health.

1. Introducción

Con el pasar del tiempo se impusieron nuevas y modernas técnicas de estudios y de investigación aplicada a la medicina, con el fin de obtener iniciativas enmarcadas a mejora la salud organizacional y equipamiento adecuado de cada área de algún centro médico y hospital. Como dice (Rabanales J., Párraga I., López H., Pretel F.& Navarro B., 2011) "Desde hace años, los sistemas sanitarios buscan nuevas estrategias de organización y

alternativas a los modos tradicionales de proporcionar servicios sanitarios. La aparición de las tecnologías de la información y las comunicaciones ha facilitado la viabilidad de modelos organizativos, como la continuidad asistencial o el acercamiento de la atención al paciente. Posteriormente, la evolución de estas nuevas tecnologías ha permitido aplicar los conceptos de globalidad e interoperabilidad a las organizaciones sanitarias, dando lugar a nuevos entornos organizativos y de trabajo en los que aquel primer concepto de telemedicina asociado, exclusivamente, a la superación de barreras geográficas ha perdido vigencia".

El avance tecnológico a través del tiempo ha ido evolucionando abarcando todas las áreas de la salud, incorporando artefactos o equipos tecnológicos para poder mejorar la atención, cuidados, y seguimientos de los pacientes, con base en (Rabanales J., Párraga I., López H., Pretel F.& Navarro B., 2011) "Describe que el uso de tecnologías de telecomunicación para la provisión de servicios médicos desde los años 60, es en las dos últimas décadas (desde los años 90) cuando aparece un verdadero interés por la necesidad de encontrar procedimientos alternativos de atención médica que respondan al incremento observado tanto en los costes sanitarios como en las expectativas de los pacientes. Este reciente impulso de la telemedicina ha colaborado en el incremento de los beneficios para el profesional de salud y para los usuarios de los servicios médicos". Según (Kopec A. , Salazar A., 2002) "La aparición de las tecnologías de la información y las comunicaciones ha facilitado la viabilidad de modelos organizativos, como la continuidad asistencial o el acercamiento de la atención al entorno del paciente. Posteriormente, la evolución de estas nuevas tecnologías ha permitido aplicar los conceptos de globalidad e interoperabilidad a las organizaciones sanitarias, dando lugar a nuevos entornos organizativos y de trabajo en los que aquel primer concepto de telemedicina asociado, exclusivamente, a la superación de barreras geográficas ha perdido vigencia".

Según (Rabanales J., Párraga I., López H., Pretel F.& Navarro B., 2011) "Son muchas las áreas que se han visto influidas en los últimos años por estas nuevas tecnologías, entre otras las consultas de los pacientes a profesionales, la comunicación entre profesionales y el seguimiento de pacientes con problemas de salud de carácter crónico". Según (Ronald C., Merrell M. y Charles R.) "Las aplicaciones de telemedicina juegan un papel cada vez más importante en la atención médica. Ofrecen herramientas indispensables para la atención domiciliaria, la monitorización remota de pacientes y la gestión de enfermedades, no solo para la salud rural y la atención en el campo de batalla, sino también para hogares de ancianos, instalaciones de vida asistida y entornos marítimos y de aviación."

Teniendo en cuenta a (Rabanales J., Párraga I., López H., Pretel F.& Navarro B., 2011) "La asistencia prestada a través de telemedicina brinda la posibilidad de un mejor seguimiento de las enfermedades crónicas y facilita la educación sanitaria del paciente en medicina preventiva y salud pública. Su utilización facilita la accesibilidad de los pacientes a los servicios sanitarios, sin necesidad de tener que realizar desplazamientos, desde su propio domicilio. El actual desarrollo de las TICs (Tecnología de la Información y la Comunicación) permite la obtención de una amplia información de una manera rápida y sencilla".

Como señala (Rabanales J., Párraga I., López H., Pretel F.& Navarro B., 2011) "En la actualidad nos podemos plantear la posibilidad de una utilización más provechosa de todo el potencial que ofrece la nueva generación de sistemas de telemedicina personal

y móvil en diferentes ámbitos sanitarios. La disponibilidad de soportes adecuados facilitará el desarrollo mantenido de la Atención Primaria. La implantación de las nuevas tecnologías de telemedicina en Atención Primaria podría formar parte de la estrategia de mejora del modelo actual de prestación de servicios sanitarios a una población que ha cambiado sus características sociodemográficas en los últimos años".

2. Aplicación de la Telemedicina en las Diferentes Áreas de Salud

Desde el punto vista de (Monteagudo J., Serrano L. & Hernández C., 2005) "El cambio tecnológico se ha producido simultáneamente con cambios sanitarios importantes. Desde hace varios años los modelos sanitarios de los países desarrollados se encuentran en revisión continua en un intento de dar respuesta a las exigencias de satisfacer una mayor demanda de servicios de salud, con mejor calidad, haciéndolo compatible con las limitaciones existentes de recursos. Este cambio está guiado por principios tales como poner al paciente en el eje de todas las actuaciones, mejorar la continuidad en la asistencia y la equidad en el acceso. Entre los criterios que guían la actuación se encuentran sobre todo la continuidad de la asistencia; la gestión integrada de procesos y la búsqueda de eficiencia operacional para facilitar la ausencia de errores".

3. Importancia de la Telemedicina

Teniendo en cuenta a (Monteagudo J., Serrano L. & Hernández C., 2005) "Los sistemas de telemedicina plantean la integración de las tecnologías de red con los procesos sanitarios. La interoperabilidad es una de las cuestiones principales ya que las diferentes formas y modalidades de asistencia descansan en general sobre entornos informáticos heterogéneos. Ligado a la ausencia de normas se identifican problemas tales como: fragmentación del mercado; florecimiento de aplicaciones diferentes; alto coste soluciones particulares; corto ciclo de vida de los sistemas; falta de compatibilidad e integración con el resto de los sistemas y aplicaciones. El entorno de estandarización en información sanitaria es complejo e involucra múltiples iniciativas de distintas organizaciones. A pesar del reconocimiento de la conveniencia de tener un espacio normalizado hay que constatar un nivel de adopción relativamente bajo y con problemas de convergencia" (Monteagudo J., Serrano L. & Hernández C., 2005).

Como expresa (González M. & Herrera O. , 2007) "La telemedicina también es usada para la interacción entre profesionales, para la educación médica y de los pacientes. Las aplicaciones de la telemedicina se expanden en un nuevo contexto por lo que las organizaciones de la salud deben fijar la atención en la búsqueda de formas específicas para eliminar las barreras de la comunicación que acompañan el uso de esta tecnología".

Como expresa (Monteagudo J., Serrano L. & Hernández C., 2005) "Al igual que en otros dominios de aplicación, la telemedicina ha adoptado diferentes modelos de servicio para adquirir, distribuir, y procesar datos multimedia que en general se han construido orientados a una solución particular usando tecnologías propietarias a veces combinadas con componentes siguiendo normas limitadas o incompatibles".

De acuerdo con (González M. & Herrera O. , 2007) "La Telemedicina sólo debe constituir una herramienta de apoyo que ayude a aumentar la calidad del servicio de salud integral,

en ningún momento debe sustituir la experiencia subjetiva que el médico de base obtiene en la relación cara a cara con su paciente, como tampoco se debe deshumanizar el servicio de salud".

4. Tendencias y perspectivas de la telemedicina en la actualidad

Como expresa (Monteagudo J., Serrano L. & Hernández C., 2005) "La profundidad del cambio tecnológico está superando las previsiones de apenas hace unos años y el progreso de las tecnologías digitales y de la globalización de la economía también afecta a los servicios de salud. El sector sanitario es intensivo en el uso de tecnología. De cara a la identificación de escenarios de futuro se deben considerar de forma especial algunos vectores de tendencias tecnológicas actuales en sanidad":

1. "El uso extendido de historia clínica electrónica y otras herramientas haciendo descansar el trabajo de los profesionales sobre sistemas digitales, favoreciendo la proliferación de ordenadores en todas partes incluyendo sistemas portátiles y de uso personal" (Monteagudo J., Serrano L. & Hernández C., 2005).
2. "El desarrollo intensivo de redes inalámbricas (WLAN) para voz y datos así como para biotelemetría, señalización, alarma y localización. Este hecho, ligado a la difusión de los sistemas de comunicaciones móviles (GSM, GPRS, UMTS), está obligando a considerar las cuestiones de compatibilidad electromagnética y gestión del espacio radioeléctrico en los entornos sanitarios" (Monteagudo J., Serrano L. & Hernández C., 2005).
3. "El desarrollo creciente de nuevos sistemas de adquisición de imágenes diagnósticas (PET, SPECT, RM, escáner helicoidal, eco 3D) y la digitalización con archivo y comunicación (PACS) haciendo factible el acceso a las imágenes en cualquier momento en cualquier parte" (Monteagudo J., Serrano L. & Hernández C., 2005).
4. "Robotización y automatización de laboratorios centrales mientras se multiplican nuevos dispositivos de uso periférico y personal, con interfaz normalizada para intercambio de datos y telecontrol" (Monteagudo J., Serrano L. & Hernández C., 2005).
5. "Nuevas instalaciones quirúrgicas con desarrollo de cirugía mínimamente invasiva incorporando soportes de imágenes avanzados y de robótica" (Monteagudo J., Serrano L. & Hernández C., 2005).
6. "Sistemas de monitorización avanzada en las unidades de cuidados intensivos, cabecera de camas de paciente y llevables personales con tecnologías de comunicación de corto alcance (Bluetooth, Zigbee, RF, etc)" (Monteagudo J., Serrano L. & Hernández C., 2005).
7. "Difusión de sistemas de videoconferencia personal y en grupo. Necesidad de instalaciones dedicadas a teleconsulta. Proliferación de sistemas de telemedicina" (Monteagudo J., Serrano L. & Hernández C., 2005).
8. "Sistemas de teleformación y de realidad virtual y simulación para formación" (Monteagudo J., Serrano L. & Hernández C., 2005).

Actualmente en la provincia según el censo realizado en el 2014 existen alrededor de 205.969 habitantes. De acuerdo con (Monteagudo J., Serrano L. & Hernández C., 2005)

"Los cambios tecnológicos influyen y se imbrican con los cambios organizativos y de concepción de los servicios sanitarios. Es evidente que los recursos tecnológicos que exhiben los hospitales de hoy día son muy diferentes a los de apenas una década y con toda seguridad a los de dentro de unos años. Ligado a la evolución general de la sociedad, se están planteando propuestas de rediseño de las instituciones sanitarias como empresas basadas en el conocimiento haciendo uso intensivo de tecnologías de la información y desarrollando el trabajo en red con otros recursos sanitarios y los pacientes, no sólo en su área de inscripción geográfica sino hasta allí donde alcance la necesidad".

Los proyectos iniciados en los actuales gobiernos han surgido como una nueva iniciativa para la inclusión de nuevas personas con discapacidad y personas que no poseen los recursos necesarios para ser atendidos en centro hospitalarios. El (Meza D., 2010) expresa que "Por otra parte, el proyecto Manuela Espejo, busca la identificación de personas con discapacidades en el territorio nacional, se encuentra en fase de diagnóstico y permitirá a la Vicepresidencia de la República emprender una respuesta interinstitucional para brindar calidad de vida a este sector de conciudadanos. El proyecto está llegando a zonas a donde nadie ha llegado, se ha logrado identificar a más de 20.000 de estas personas para quienes una única visita es muy poco ya que necesitan monitoreo constante de su estado de salud, y no sólo eso sino, que las personas quienes están a su cargo requieren o.. Estas experiencias de otros países evidencian que la tele-salud domiciliaria permitiría no dejar desatendido a este grupo tan vulnerable y apoyaría en la reducción de los costos en los centros de salud. Basándonos en experiencias de otros países como Colombia, Venezuela y España, en donde este servicio tiene un papel preponderante en aspectos como calidad, control y rapidez. La telemedicina nos ayudará a implementar servicios preventivos, mediante programas de educación continua para escuelas rurales, con el fin de disminuir diferentes tipos de enfermedades y sus complicaciones".

Según (González M. & Herrera O. , 2007) "Estudios sobre la eficacia de la Telemedicina en diversos países indican que es un recurso que contribuye significativamente a la mejoría de la calidad de la asistencia médica y a la reducción del tiempo que media entre diagnóstico y terapia, así como a la extensión de servicios médicos a distancia a localidades en que no existen. Se reducen los costos de asistencia, la necesidad de hospitalización, los gastos de transportación del paciente y del personal especializado. Además, permite poner en práctica asistencia médica en casos de catástrofe y en eventos de gran afluencia de público".

Como expresa (Jorge M. & Mérida R., 2010) "La Telemedicina ya no puede ser observada como un invento de la Ciencia Ficción. Es una realidad que se aplica cada día con mayor provecho, aunque tendrá que sortear algunos inconvenientes propios del manejo remoto de la información". En la provincia de santa Elena los métodos tradicionales de comunicación han quedado atrás y todos los centros de atención hospitalarias están incorporando nuevos dispositivos de comunicación.

5. Monitorización de pacientes a distancia.

Según (Alvez R., 2011) "Como se ha mencionado en el apartado anterior, el desarrollo de las redes de alta velocidad abre un abanico de posibilidades para la mejora de los servicios médicos. Dentro de estas mejoras que se pueden realizar se encuentra el sistema de

monitorización a distancia. La monitorización a distancia permite que los pacientes sean controlados las veinticuatro horas, los siete días de la semana. En el presente trabajo se enfocará a un tipo de pacientes especiales, los cuales serán quienes saquen más beneficios a este sistema, ellos son los pacientes con enfermedades cardíacas. Las fallas cardíacas constituyen las causas más frecuentes por las que los pacientes son internados. Esto no solo afecta a los pacientes, a los que hay que proveerles formas más rápidas de detectar las fallas, sino que también afecta a las instituciones médicas. Es claro que se deben minimizar los costos en los hospitales y que se debe mejorar la atención a los pacientes con estas enfermedades, para ello se propone un sistema en el cual los pacientes estén siendo constantemente monitoreados y cualquier anormalidad detectada a tiempo. Todo ello contribuirá a tener una asistencia sanitaria más personalizada y más eficiente, siendo capaz de evitar muchas muertes al año por estos problemas. Por último, es preciso remarcar que este sistema puede ser extendido para tratar todo tipo de enfermedades, para ello bastará con proveer al paciente del hardware necesario para detectar los parámetros relevantes a su enfermedad.".

6. Conclusión

La salud en el ecuador no es la mejor del mundo ya que posee algunos problemas a la hora de atender a un paciente en algún centro de salud, el proceso que se realiza es registrar al paciente y solicitar a que especialista desea que lo atienda ya sea este un médico general o un especialista. En nuestro país no se cambia el método de atención a los pacientes que asisten a estos centros de salud, se trató de mejorar este sistema con los nuevos gobiernos pero no se logró, por ello se trató de buscar unos nuevos métodos de asistencia hospitalarias para mejorar el proceso de atención.

Referencias

Alvez R. (2011). Aplicación de Telemedicina para la mejora de los sistemas de emergencias y diagnósticos clínicos. *Memoria de trabajos de difusión científica y técnica*(9), 8.

Fernández M. & Mérida R. (2010). Telemedicina: futuro o presente. *Habanera de Ciencias Médica, 9*(1).

González M. & Herrera O. . (2007). Bioética y nuevas tecnologías: Telemedicina. *Revista Cubana de enfermería, 23*(1).

Jorge M. & Mérida R. (2010). Telemedicina: futuro o presente. Revista Habanera de Ciencias Médicas. *Habanera de Ciencias Médicas, 9*(1).

Kopec A. , Salazar A. (2002). Aplicaciones de Telecomunicaciones en salud en la subregión andina: Telemedicina, Organización Panamericana de la Salud, Washington D.C. *Telemedicina*.

Lusignan S., Wells S., Johnson P., Meredith K., Leatham E. (s.d.). Compliance and effectiveness.

Meza D. (2010). *Telemedicina en el Ecuador: un mundo de desafíos y oportunidades*.

Monteagudo J., Serrano L. & Hernández C. (2005). La telemedicina:¿ ciencia o ficción?. *Anales del Sistema Sanitario de Navarra*, No. 3, pp. 309–32.

Ochoa G. , Daza M., Archila M., Montilla G., De la Torre M. & Ubacius V. (1998). Las telecomunicaciones, la telemedicina y la reingeniería de la salud. Ingeniería UC. (1), 5.

Rabanales J., Párraga I., López H., Pretel F.& Navarro B. (2011). Tecnologías de la información y las telecomunicaciones: telemedicina. Revista Clínica de Medicina de Familia. *Revista Clínica de Medicina de Familia*, 4(1),42–4.

Roldán H. (2016). Desarrollo de un modelo de gestión de servicios de TI para aplicaciones de Telemedicina en el Ecuador.

Ronald C., Merrell M. y Charles R. (s.d.). *Mary ann liebert, Inc. publishers*. Obtido de http://www.liebertpub.com/overview/telemedicine-and-e-health/54/

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 09/12/2017
Aceitação/Acceptance: 27/03/2018

Análisis de las Tecnologías de Redes Heterogéneas (HetNet) en los Sistemas Móviles

Dayana Tigrero [1], Jimmy González [1], Teresa Guarda [1]

dtigrerosuarez@gmail.com, jimmygonzalez19920@gmail.com, tguarda@gmail.com

[1]Universidad Estatal Península de Santa Elena, La Libertad - UPSE, Santa Elena, Ecuador.

Pages: 181–186

Resumen: El presente artículo describe cómo actualmente los estudios tecnológicos que se realizan constantemente han solucionado los problemas que se presentan en las conexiones inalámbricas. Un ejemplo evidente es el ambiente móvil, que ha brindado las mejores soluciones para satisfacer las necesidades del usuario. Todos sabemos que el avance móvil ha causado una gran demanda espectral, y cómo esto ha representado una problemática importante para los operadores móviles. Tal motivo ha llevado a la realización de un análisis de las tecnologías de las redes heterogéneas para buscar soluciones a las dificultades que presentan las redes de banda ancha móvil, así mismo mostrar las necesidades de los cambios respectivos en el paradigma de arquitectura de red.

Palabras-clave: Inalámbrico; móvil, redes heterogéneas; banda ancha; paradigma; arquitectura; femtoceldas; IEEE, y viabilidad.

Analysis of Heterogeneous Network Technologies (HetNet) in Mobile Systems

Abstract: This article describes how technological studies that are constantly being carried out have solved the problems that arise in wireless connections. An obvious example is the mobile environment, which has provided the best solutions to meet the needs of the user. We all know that the mobile advance has caused a great spectral demand, and how this has represented an important problem for mobile operators. This reason has led to an analysis of heterogeneous network technologies to find solutions to the difficulties presented by mobile broadband networks, as well as to show the needs of the respective changes in the network architecture paradigm.

Keywords*:* Wireless; mobile; heterogeneous networks; broadband; paradigm; architecture; femtocells; IEEE; and viability.

1. Introducción

La proliferación de dispositivos móviles conectados a Internet continuará impulsando el crecimiento del tráfico de datos de manera exponencial, forzando a los operadores

de red a aumentar drásticamente la capacidad de sus redes. Para hacer esto de manera rentable, se está produciendo un cambio de paradigma en el despliegue de la infraestructura de la red celular lejos de las estaciones base tradicionales montadas en torres de alta potencia y hacia elementos heterogéneos. Los elementos heterogéneos incluyen picoceldas, macroceldas, microceldas, femtoceldas y sistemas de antena distribuida, que se distinguen por sus potencias de transmisión, tamaño físico, red de retroceso y características de propagación.

La implementación de redes heterogéneas ha tenido una acogida favorable a nivel de redes, ayudando a mejorar la cobertura y la capacidad de la red basándose en mezclar diferentes tipos de tecnología de radio y hacer uso de nodos o pequeñas celdas.

En la actualidad existe el incremento de usuarios de banda ancha móvil, por lo que se considera fundamental para los operadores móviles especialmente en la tecnología LTE-A.

Mediante el actual crecimiento del tráfico de datos, se ha considerado usar estrategias directamente en los pequeñas celdas, femtoceldas, microceldas, macroceldas y picoceldas, añadiéndolas en las celdas macro generando y creando las redes heterogéneas o también conocidas como HetNet, sus términos en inglés.

La creación de esta industria, ha hecho que esta red heterogénea sea más compleja tanto en cobertura interferencias, haciendo que todo tipo de planificación, gestión de canales de radio y traspaso de celdas o handover, sea más complicado que las redes homogéneas, sin embargo para ellos existen robustas herramientas de gestión y control. (Tuckler, 2015)

El objetivo y enfoque de este tipo de red, es mejorar la eficiencia espectral mediante operaciones en las bandas del espectro, estas operaciones han sido comprobadas, realizadas y utilizadas por celdas macro, no obstante así también se han realizado uso de técnicas efectivas en cuestión a la reducción de interferencias y la coordinación entre las capas macro y pequeñas celdas llegando a obtener un aumento en la capacidad de la red.

De esta manera, las redes heterogéneas han ayudado de forma efectiva, ser un medio interesante para expandir la capacidad de la red móvil, brindando además que las rede de una estación base o nodo puedan conectarse a micros, pico, femtoceldas y unidades remotas de radio, para disponer de una red sobrepuesta a la macro. (Tuckler, 2015)

El presente artículo se desglosará en 5 secciones, siendo estas las siguientes: introducción, antecedentes, metodología, tecnologías de las redes heterogéneas, conclusiones y recomendaciones.

2. Antecedentes

Las redes heterogéneas o HetNet han estado presentes en nuestro medio como una red de conexión de ordenadores y otros dispositivos con diferentes sistemas operativos y/o protocolos. Esta palabra es muy utilizada en las redes inalámbricas que utilizan diferentes tecnologías de acceso, por ejemplo, una red inalámbrica que proporciona un servicio a través de una LAN inalámbrica y que es capaz de mantener el servicio cuando se cambia a una red celular. (Delphinanto, Hillen, Passchier, van Schoonhoven, & den Hartog, 2009)

Las redes heterogéneas o HetNet indican el acceso a una red inalámbrica a través de múltiples tipos de nodos. Ofrecer una red con área amplia con mayor y gran cobertura, genera que se haga la utilidad de macro celdas, pico celdas y/o femtoceldas, todo esto aplicándolo a entornos con variedad de zonas de coberturas de red inalámbricas, es decir se aplica en entornos al aire libre, abierto a los edificios de oficinas, hogares y así mismo el lugares y espacios subterráneos. (Huidobro, 2013)

Todo el concepto de redes heterogéneas ha ido mucho más allá para los operadores móviles, pues a raíz que incrementa la base de usuarios de banda ancha móvil, han incrementado todo tipo de dispositivos tales como son los Smartphone y tabletas, lo que ha generado gran demanda económica a través de los clientes obtenidos con sus dispositivos en espera que el incremento sea el doble para realizar el uso de otras tecnologías de acceso que no pertenezcan a la familia 3GPP, como Wi-Fi. (Huidobro, 2013)

El aumento rápido de los puntos de accesos dentro de las redes heterogéneas han sido las pequeñas celdas, por lo cual varios operadores han realizado ofertas de algún tipo de backhaul (fibra, cobre, inalámbrico, entre otros). (Huidobro, 2013)

Gracias a las redes heterogéneas en específico a las pequeñas celdas que implica a las femto y pico celdas, han permitido a los operadores móviles, realizar un despliegue de todos los dispositivos basados en IP, haciendo el uso de la misma infraestructura IP existente, hasta que proporcione una evolución suave a IMS (IP Multimedia Subsystem). (Huidobro, 2013)

3. Metodología

El desarrollo del artículo está basado en el análisis de redes heterogéneas con respecto a estudios y trabajos previos. Las etapas que se detallan a continuación son parte de un caso de estudio denominado “Tecnologías lightRadio TM”:

La búsqueda de información de varios conceptos de telecomunicaciones fue necesario conocerlos, sobre todo los conceptos actualizados, por ejemplo la topología de la red de telefonía tanto fija como móvil en nuestro país, además es de mucha importancia conocer cada una de las generaciones de la telefonía celular y todos los parámetros de importancia relevantes en la parte de redes móviles y entre otros conceptos importantes. La consulta de libros, artículos científicos y proyectos han sido de gran ayuda para el proceso de la primera etapa. (Picado, 2012)

La segunda etapa, se basó a la recopilación de la información necesaria, sobre todo sobre los términos de femtoceldas y redes heterogéneas, sobre todo la parte fundamental ha sido los artículos científicos de la IEEE.

Sin embargo el uso de las páginas web y documento de desarrollos móviles, también fue una solución para conocer los conceptos de redes heterogéneas. (Picado, 2012)

Y como última etapa de este artículo, es realizar el informe de manera formal, para brindar el conocimiento del estudio de un nuevo paradigma de red como lo es la red heterogénea o también conocida como HetNet, sobre todo mostrar sus características principales, viabilidad económica, desafíos que enfrentan en la actualidad y sobre todo

el incremento de usuarios que ha tenido y todos los beneficios que se obtendrían al implementarla. (Picado, 2012)

4. Tecnologías de las Redes Heterogéneas

Una topología HetNet desafía fundamentalmente muchos aspectos tradicionales del diseño y análisis de sistemas celulares. Los modelos obsoletos son el uso de una cuadrícula hexagonal uniforme para modelar las ubicaciones de las estaciones base, y la suposición de que un móvil generalmente debe conectarse a la estación base que proporciona la señal más potente, lo que en una HetNet no es la mejor velocidad o rendimiento en toda la red (Jo, Sang, Xia, & Andrews, 2012).

4.1. Femtoceldas

Una femtocelda es una estación base celular pequeña y de baja potencia, diseñada típicamente para su uso en un hogar o una pequeña empresa. También se llama femto AccessPoint (AP). Se conecta a la red del proveedor del servicio a través de banda ancha (como DSL o cable). Es conocida también como un punto de acceso radio 3G que se colocan en edificios para brindar coberturas a las personas que se encuentran en el lugar, es decir, gracias a las femtoceldas, pueden los usuarios recibir llamadas móviles o telefónicas, entre otros. Todo esto a través de la conexión de banda ancha a las líneas o cable que permite la conexión (Lopez-Perez, Guvenc, G., Quek, & Zhang, 2011). Los diseños actuales suelen admitir de cuatro a ocho teléfonos móviles activos simultáneamente en un entorno residencial, según el número de versión y el hardware femtocelda, y entre ocho y dieciséis teléfonos móviles en entornos empresariales (Ghosh, et al., 2012). Una femtocelda permite a los proveedores de servicios ampliar la cobertura del servicio en interiores o en el borde de la cedula, especialmente cuando el acceso estaría limitado o no estaría disponible (Fig.1).

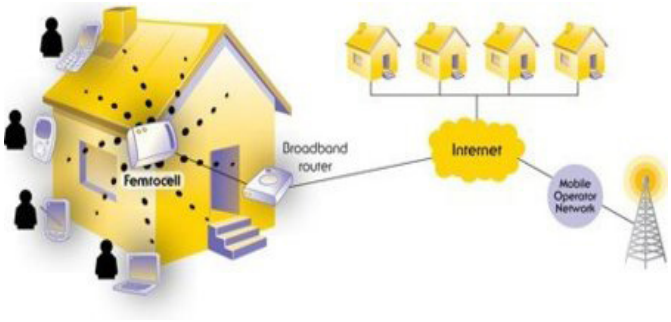


Figura 1 – Diseños actuales de Femtoceldas

4.2. Macroceldas

Se la define como un circuito de bloques que contén compuertas OR para sumar productos de una AND, estas compuesta de flip-flops, un buffer tres estados, y varios multiplexores para seleccionar señales de control, beneficiando a realizar un control de pruebas en las señales (Picado, 2012).

4.3. Picoceldas

Una picocelda es una estación base celular pequeña que generalmente cubre un área pequeña. En las redes celulares, las picoceldas pueden utilizarse para extender la cobertura a áreas interiores donde las señales exteriores no alcanzan bien, o para agregar capacidad de red en áreas con un uso muy denso del teléfono, como estaciones de tren o estadios. Las Picocelda proporcionan cobertura y capacidad en áreas difíciles o costosas de alcanzar utilizando el enfoque de macroceldas más tradicional (Ghosh, et al., 2012).

4.4. Microceldas

Las microceldas son nodos intermedios para el acceso móvil, es decir que son pequeñas estaciones base, como su nombre lo indica, tanto en tamaño como en potencias de emisión. Ayudan a conectar terminales móviles de telefonía convencional a las redes de operadoras utilizando lo que actualmente se conoce como lo es: banda ancha, ADSL, cable o fibra óptica y las redes móviles que existen hoy en día, por ejemplo las 3G o LTE (Ghosh, et al., 2012).

4.5. Pequeñas celdas

Las celdas pequeñas son nodos de acceso de radio celular de baja potencia que operan en un espectro licenciado y sin licencia que tiene un alcance de 10 metros a unos pocos kilómetros. Son pequeñas en comparación con una macrocelda móvil, porque tienen un rango más corto y normalmente manejan menos llamadas o sesiones concurrentes. Aprovechan al máximo el espectro disponible reutilizando las mismas frecuencias muchas veces dentro de un área geográfica (Delphinanto, Hillen, Passchier, van Schoonhoven, & den Hartog, 2009).

Generalmente, las macroceldas proporcionan una cobertura mayor que la microceldas. Las antenas para macroceldas están montadas en mástiles de tierra, tejados y otras estructuras existentes, a una altura que proporciona una vista clara de los edificios y el terreno circundantes. Las estaciones base de macroceldas tienen salidas de potencia de típicamente decenas de vatios. El rendimiento de las macroceldas se puede aumentar aumentando la eficiencia del transreceptor (Ghosh, et al., 2012).

El término macrocelda se usa para describir el rango más amplio de tamaños de celda. Macroceldas se encuentran en áreas rurales o a lo largo de carreteras. En un área de celda más pequeña, se usa una microcelda en un área urbana densamente poblada. Las Picoceldas se utilizan en áreas más pequeñas que las microceldas, como una oficina grande, un centro comercial o una estación de tren. Actualmente, el área de cobertura más pequeña que puede implementarse con una femtocelda es una oficina pequeña.

5. Conclusiones y Recomendaciones

Las investigaciones que se han realizado en este artículo han sido de gran beneficio para la aportación tecnológica y para los usuarios que hace uso de las redes heterogéneas que existen en la actualidad, desde telefonía móvil, fija, y radio.

Las comunicaciones que se establecen en la actualidad son muestras de que las redes heterogéneas tienen grandes ventajas sobre ellas, mostrando que si se realizan más

investigaciones, se puede ir mejorando con el paso del tiempo hasta brindar redes de excelente calidad para el mundo entero.

La preparación e investigación en este artículo sobre las redes heterogéneas permite concluir que al trabajar con este tipo de redes, se mejora la comunicación en diferentes áreas, brindando comodidad al usuario.

El artículo realizado debe continuar investigando, consultando mejoras en las redes heterogéneas, experimentando en diferentes lugares de poco acceso, para llegar a obtener más conocimiento sobre ellas hasta conocer sus límites, ya que estas en la actualidad han brindado mejoras en el ámbito de comunicación tecnológica.

Referencias

Delphinanto, A., Hillen, B., Passchier, I., van Schoonhoven, B., & den Hartog, F. (2009). *Remote Discovery and Management of End-User Devices in Heterogeneous Private Networks.* 6th IEEE Consumer Communications and Networking Conference.

Ghosh, A., Mangalvedhe, N., Ratasuk, R., Mondal, B., Cudak, M., Visotsky, E., et al. (2012). Heterogeneous cellular networks: From theory to practice. *IEEE communications magazine, 50(6).*

Huidobro, J. M. (2013). Redes Heterogéneas. La solución para LTE. *Antena de Telecomunicación, 1*(1), 4.

Jo, H. S., Sang, Y. J., Xia, P., & Andrews, J. G. (2012). Heterogeneous cellular networks with flexible cell association: A comprehensive downlink SINR analysis. *IEEE Transactions on Wireless Communications, 11(10),* 3484–3495.

Lopez-Perez, D., Guvenc, I. D., G., K. M., Quek, T. Q., & Zhang, J. (2011). Enhanced intercell interference coordination challenges in heterogeneous networks. *IEEE Wireless Communications, 18(3).*

Picado, E. A. (2012). *Análisis de las tecnologías de Redes Heterogéneas.*

Tuckler, H. R. (10 de Octubre de 2015). *La Prensa.*

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 06/12/2017
Aceitação/Acceptance: 10/03/2018

OWITest: Metodología de test de penetración en redes inalámbricas

Luis David Narváez[1], Stalin Marcelo Arciniegas[1], Laura Guerra[1], Francklin Rivas Echeverría[2]

ldnarvaez@pucesi.edu.ec, smarciniegas@pucesi.edu.ec, lrguerra@pucesi.edu.ec, rivas@ula.ve

[1] Pontificia Universidad Católica del Ecuador Sede Ibarra/Av. Jorge Guzmán Rueda y Av. Aurelio Espinosa Pólit, Ciudadela La Victoria/100112/Ibarra, Ecuador.

[2] Universidad de los Andes/Avenida 3, Independencia/ Mérida, Venezuela.

Pages: 187–200

Resumen: La particularidad de las redes inalámbricas en ambientes de gran afluencia, como es el caso de las instituciones de Educación Superior o lugares de acceso público, radica en la forma abierta o libre con la que son desplegadas. El objetivo por el cual se crea una red inalámbrica es el de brindar servicios de acceso a Internet, además en una misma organización pueden desplegarse varios tipos de redes con diferentes niveles de seguridad, desde las redes abiertas sin ningún mecanismo de seguridad hasta los tipos con técnicas de autenticación avanzadas y cifrado. La vulnerabilidad principal radica en la modalidad de red abierta, donde los accesos no autorizados son un grave problema, porque pueden desembocar en ataques de escalada de privilegios y comprometimiento total de las comunicaciones. Estos antecedentes motivaron el diseño de una metodología de test de penetración denominada OWITest para potenciar la seguridad ofensiva de una red inalámbrica.

Palabras-clave: OWITest; test de penetración; redes inalámbricas; Seguridad en Internet.

OWITest: Penetration test methodology in wireless networks

Abstract: The feature of wireless networks in high influx of people environments, such as higher education institutions or public access places, lies in the open or free connection in which they are deployed. The purpose for creating a wireless network is to provide Internet access services. In addition, in organizations can be deployed several types of networks with different security levels, from open networks without any security mechanism to Advanced authentication techniques and encryption. The main vulnerability is undoubtedly due to the open network mode, where unauthorized access is a serious problem, because it can lead to privilege escalation attacks and total compromise of the communications infrastructure. This situation led to a penetration test methodology design called OWITest to enhance the offensive security of a wireless network.

Keywords*:* OWITest; Pentesting; Wireless network; Internet security.

1. Introducción

El presente trabajo de investigación tuvo como fin el desarrollo de una metodología de test de penetración para redes inalámbricas en campus universitarios o lugares públicos de gran afluencia de personas, la cual se la denominó OWITest (Open Wireless Test). Para lograr tal fin, se partió de un estudio de las metodologías de auditoría técnica OWISAM (Open Wireless Security Assessment Methodology) (Tarlogic Security, 2013), OSSTMM (Open Source Security Testing Methodology Manual) (Herzog P., 2010) y OWASP (Open Web Application Security Project) (Muller A. & Meucci M., 2014); luego se entabló un acercamiento con los modelos de despliegue de redes de instituciones de Educación Superior, donde se identificó los requisitos reales de una red inalámbrica de este tipo; de esta forma se dio inicio al diseñó de la metodología abierta para test de penetración OWITest.

Se ha estructurado la metodología en un marco similar al de las metodologías OWISAM, OSSTMM y OWASP, para tener una mejor visión del entorno en el que se desarrolla la presente propuesta de metodología. El objetivo principal es mantener la simplicidad y fácil adaptación del modelo a un entorno académico o de acceso público (Estrada, 2011). Para lo cual se han definido las siguientes fases del proceso de auditoría bajo test de penetración:

- Fase 1. Acuerdos y planificación del test.
- Fase 2. Análisis y explotación de vulnerabilidades.
- Fase 3. Resultados e Informes.

En la figura 1 se presenta un condensado de las fases de la metodología propuesta a modo de diagrama de flujo:



Figura 1 – Fases de la metodología OWITest (Narváez D., 2017)

2. Fundamentación Técnica

2.1. OWISAM (Open Wireless Security Assessment Methodology)

Es una metodología de evaluación de la seguridad de la información, que se enfoca principalmente en las redes de comunicación inalámbrica. Proporciona un conjunto

de elementos de forma abierta a los administradores y gestores de TI, orientados a la identificación de los riesgos y la minimización de los posibles impactos frente a intrusiones no autorizadas que se catalogan como ataques; además prevé el reforzamiento de la seguridad ofensiva de las infraestructuras inalámbricas Wi-Fi, bajo el estándar IEEE 802.11 (Whitaker & Newman, 2005).

El análisis del riesgo de la seguridad de la información que propone la metodología OWISAM, se basa en controles de verificación técnica a la infraestructura de comunicación inalámbrica dentro de la periferia de la organización, dichos controles se encuentran organizados en secciones de acuerdo a la tabla I (Tarlogic Security, 2013).

#	Código	Tipo de control	Descripción de los controles
1	**OWISAM-DI**	Descubrimiento de dispositivos	Recopilación de información sobre las redes inalámbricas
2	**OWISAM-FP**	Fingerprinting	Análisis de las funcionalidades de los dispositivos de comunicaciones.
3	**OWISAM-AU**	Pruebas sobre la autenticación	Análisis de los mecanismos de autenticación
4	**OWISAM-CP**	Cifrado de las comunicaciones	Análisis de los mecanismos de cifrado de información
5	**OWISAM-CF**	Configuración de la plataforma	Verificación de la configuración de las redes
6	**OWISAM-IF**	Pruebas de infraestructura	Controles de seguridad sobre la infraestructura Wireless
7	**OWISAM-DS**	Pruebas de denegación de servicio	Controles orientados a verificar la disponibilidad del entorno
8	**OWISAM-GD**	Pruebas sobre directivas y normativa	Análisis de aspectos normativos que aplican al uso de las redes de Wi-Fi
9	**OWISAM-CT**	Pruebas sobre los clientes inalámbricos	Ataques contra clientes inalámbricos
10	**OWISAM-HS**	Pruebas sobre host spots y portales cautivos	Debilidades que afectan al uso de portales cautivos.

Tabla 1 – Secciones de controles OWISAM

2.2. OSSTMM (Open Source Security Testing Methodology Manual)

Es un conjunto de procedimientos organizados en un manual técnico, que fue creado por la organización dedicada a las metodologías de la seguridad de la información ISECOM (Institute for Security and Open Methodologies). En la actualidad se lo considera

como uno de los estándares más completos y de mayor utilización en el quehacer de la Auditoría de Seguridad, gracias al enorme conglomerado de profesionales (más de 150 expertos) que colaboran y perfeccionan dicho manual (Whitaker & Newman, 2005).

El alcancel del manual OSSTMM comprende cualquier entorno de seguridad operativo que ejecute una interacción con cualquier tipo de activo, incluido los mismos componentes de las medidas de seguridad adoptadas. Un activo es un bien, servicio o persona que tenga valor para el propietario, pueden ser propiedad física como: equipos computacionales, planos de diseños, recurso humano, entre otros; o propiedad intelectual como: logos, marcas, procesos de negocio, datos personales, entre otros (Ramilli, 2013).

OSSTMM ha definido dentro de su alcance tres clases, y un total de cinco canales, en base a la actualidad de la industria de la seguridad, el gobierno y el ámbito militar. Las clases definen específicamente áreas de estudio, investigación u operación; mientras que los canales se establecen como los medios específicos de interactuar con los activos. Las clases y canales son los siguientes que se muestran en la tabla II (Herzog P., 2010).

Clase	Canal	Descripción
Seguridad Física (PHYSSEC)	Humana	Comprende el elemento humano de la comunicación donde la interacción es física o psicológica.
	Física	Pruebas de la seguridad física en las que el canal es de naturaleza física y no electrónica. Comprende el elemento tangible de seguridad donde la interacción requiere esfuerzo físico o un transmisor de energía para la ejecución de las actividades.
Seguridad del espectro (SPECSEC)	Wireless	Comprende todas las comunicaciones electrónicas, señales y emanaciones que tienen lugar sobre el espectro electromagnético conocido.
Seguridad de las comunicaciones (COMSEC)	Telecomunicaciones	Comprende todas las redes de telecomunicaciones, digitales o analógicas, donde el medio de transmisión son las líneas telefónicas.
	Redes de datos	Comprende todos los sistemas electrónicos y redes de datos donde el medio de transmisión es el cableado estructurado.

Tabla 2 – Secciones de controles OSSTMM

2.3. OWASP (Open Web Application Security Project) Testing Project

Es una iniciativa que en la última década ha colaborado en el desarrollo de guías de aplicación y compresión para evaluar de mejor manera las aplicaciones web. El proyecto

se ha enfocado en brindar un marco muy completo de pruebas junto a técnicas que permitan poner en práctica las diferentes propuestas, de forma abierta para el acceso de cualquier usuario. Todo esto integrado en el ciclo de desarrollo de software mediante pruebas de penetración (Johansen, Allen, Heriyanto, & Ali, 2016).

El marco de pruebas OWASP Testing Project ofrece un modelo de referencia para la aplicación de técnicas y herramientas en todas las fases del ciclo de vida de desarrollo de software SDLC, un modelo flexible para que cada organización lo adapte a su entorno de negocio, normas y cultura; teniendo en cuenta que el marco de pruebas debe abarca de extremo a extremo el desarrollo del software para elevar los niveles de seguridad de la aplicación final (Sillitti, Martin, Wang, & Whitworth, 2010).

Es importante establecer que las pruebas de penetración conforman solo una parte del conjunto total de medidas de evaluación que deben aplicarse durante las fases de desarrollo de software. En otras palabras la seguridad debe ser probada en las fases de definición, diseño, desarrollo, implementación y mantenimiento; y no limitarse a pruebas cuando la aplicación esté finalizada. Conforme al marco OWASP se detallan las siguientes fases, donde deben aplicarse las evaluaciones de seguridad (Muller A. & Meucci M., 2014).

- Antes de iniciar el desarrollo
- Durante el proceso de definición y diseño
- Durante la fase de desarrollo
- Durante la implementación
- Mantenimiento y operaciones (producción).

3. Identificación de requisitos

El modelo de distribución del espacio es muy común para todos los campus universitarios de las instituciones de Educación Superior, donde se puede identificar claramente la conjugación de sitios para clases, laboratorios y oficinas administrativas; por lo que los tipos de redes inalámbricas que se despliegan para satisfacer las necesidades de comunicación y acceso al Internet se las agrupa de la siguiente forma:

- WLANs de acceso masivo, para usuarios autorizados.
- Redes federativas de acceso global.
- Redes para la conexión de las aulas y laboratorios.
- Redes temporales.

3.1. Topología de acceso a Internet

La topología genérica de la red para acceso a Internet es básicamente estrella (donde básicamente existe un nodo central y nodos en el extremo como puntos de acceso), con un conmutador de núcleo y varios conmutadores de distribución, para el acceso se emplean puntos de acceso inalámbrico con soporte al protocolo IEEE 802.11 g/n, mismos que están supervisados por una Controladora inalámbrica para la administración y gestión de las redes virtuales creadas.

La autenticación de los usuarios autorizados es mediante un portal cautivo, que inmediatamente después de enlazarse el cliente con el punto de acceso se hace a través de un sitio web bajo el protocolo HTTPs, mismo que se presenta a modo de formulario con dos campos de ingreso (usuario y contraseña), estos datos viajan al servidor RADIUS y a su vez se replican al servidor del Directorio Activo donde se permite o deniega el acceso.

Como mecanismo de protección de borde puede existir un firewall, por ejemplo, un CISCO ASA más la debida configuración de iptables. En la figura 2 se muestra el detalle de una red inalámbrica genérica para el acceso a Internet en campus universitarios.

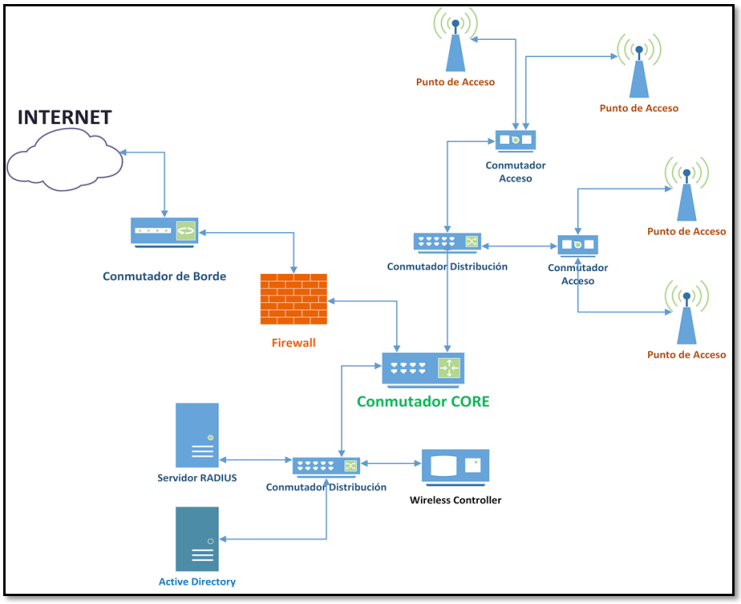


Figura 2 – Topología de una red inalámbrica para el acceso a Internet (Narváez D., 2017)

4. Fases de la Metodología OWITEST

La metodología OWITest persigue un modelo simple pero que integre cada una de las actividades que se deben desarrollar en un test de penetración; un proceso activo de análisis de una red, que busca identificar aquellas vulnerabilidades que puedan disminuir las prestaciones de la infraestructura o servicios soportados y que posiblemente comprometan la información sensible que circule por la misma.

4.1. Fase 1. Acuerdos y planificación del test

El éxito de la ejecución de las pruebas de penetración depende de una adecuada planificación previa, así como el fijar los alcances o límites de cada evaluación, al ser un entorno de ataque controlado los responsables de la organización deben permitir su ejecución y conocer cada de una de sus fases, por su puesto hay que mencionar que

este tipo de metodología busca potenciar la seguridad de una red a través de un enfoque ofensivo, y no perjudicar a una organización.

Esta fase es el inicio de la metodología OWITest y tiene como fin el establecimiento de acuerdos entre los analistas y los propietarios de la red inalámbrica, como: (ver figura 3)

- Restricciones y la parte contractual.
- Objetivos y alcance.

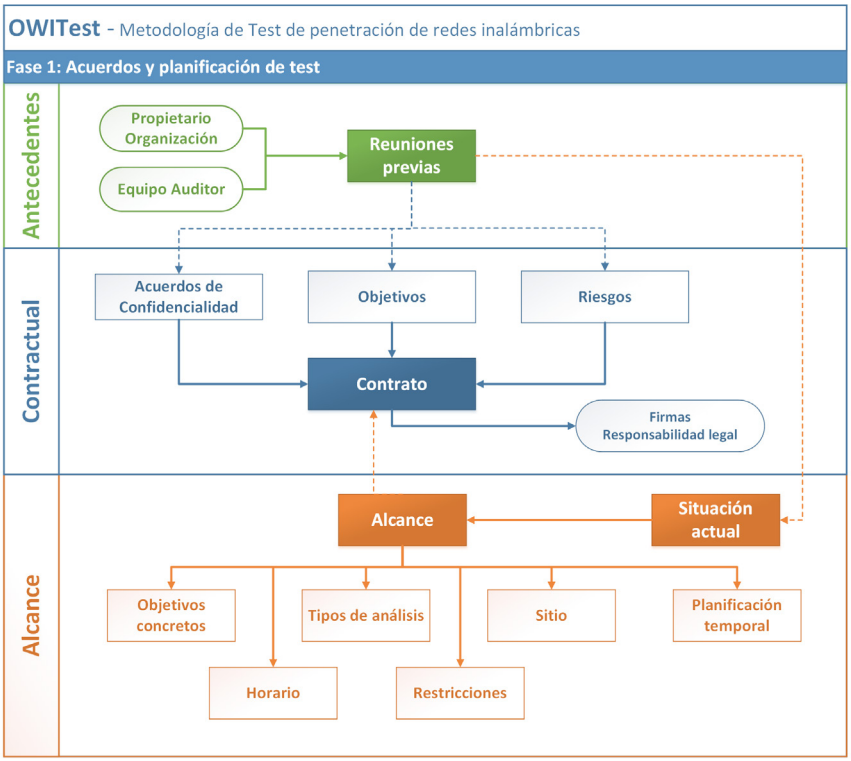


Figura 3 – Fase 1. Acuerdos y Planificación del Test (Narváez D., 2017)

4.2. Fase 2. Análisis y explotación de vulnerabilidades

La fase de análisis y explotación de vulnerabilidades se la puede considerar como la etapa donde realmente se da inicio a las evaluaciones de auditoría de forma técnica, para cubrir todos los aspectos que se han definido en la fase 1 acuerdos y planificación del test. Las actividades que se realizarán en esta fase se dividen en las siguientes etapas:

- Recopilación y organización de la información.
- Ataque.

El obtener un panorama claro del objetivo a auditar, es uno de los fines principales de la recopilación de la información, para que de esta forma el analista de seguridad se familiarice con el funcionamiento, la forma como está implementada la red, además de reconocer el matiz completo de los mecanismos y controles de seguridad que se encuentren configurados, para así encontrar de mejor forma un camino para realizar los ataques, con el afán de recolectar la mayor cantidad de información.

Dentro de esta etapa se reconocen dos actividades importantes denominadas Footprinting (recopilación de información del objetivo del ataque de forma pasiva) y Fingerprinting (recopilación de la información de forma activa para la identificación de los sistemas operativos del objetivo del ataque), mismas que se detallan en la figura 4.

Al tener toda la información recopilada y organizada de acuerdo a los aspectos, se procede a determinar las vulnerabilidades de los diferentes objetivos a ser evaluados, para lo cual se emplearán diferentes técnicas y herramientas tomando en cuenta los límites y alcances del test de penetración determinados en la fase inicial.

A continuación se procede con la explotación de las vulnerabilidades inventariadas, cuyo objetivo es la eliminación de falsos positivos, para proceder con la penetración de la red inalámbrica, mediante técnicas de escalamiento de privilegios; de este modo medir el nivel de impacto del ataque simulado, es decir obtener un panorama real de la seguridad de la red inalámbrica de la organización. Dentro de esta etapa se reconocen dos actividades importantes denominadas Análisis de vulnerabilidades e Intrusión (ver figura 5).

4.3. Fase 3. Resultados e Informes

La fase final de la metodología OWITest es la de Resultados e Informes, donde se plasma un resumen de todo el proceso de evaluación realizado, destacando principalmente los resultados y el nivel de impacto alcanzado en la infraestructura o sistemas de la red inalámbrica, las conclusiones y las posibles medidas de mitigación a los fallos o vulnerabilidades encontradas. Es importante que los hallazgos sean presentados de una forma muy clara, ordenada y con el lenguaje adecuado para el entendimiento total de los interesados por parte de la organización.

El éxito de esta fase radica en el hecho de que la documentación se desarrolle en cada fase o etapa de la metodología, para no sobrecargar el trabajo final del equipo auditor y además no perder información valiosa por olvido u omisión. Es una buena práctica presentar un borrador previo a la organización auditada para obtener aspectos de retroalimentación que mejoren la calidad del informe final.

Esta fase final de Resultados e Informes se divide en la generación de dos tipos de informes, con más detalle se observa en la figura 6:

- Informe ejecutivo.
- Informe técnico.

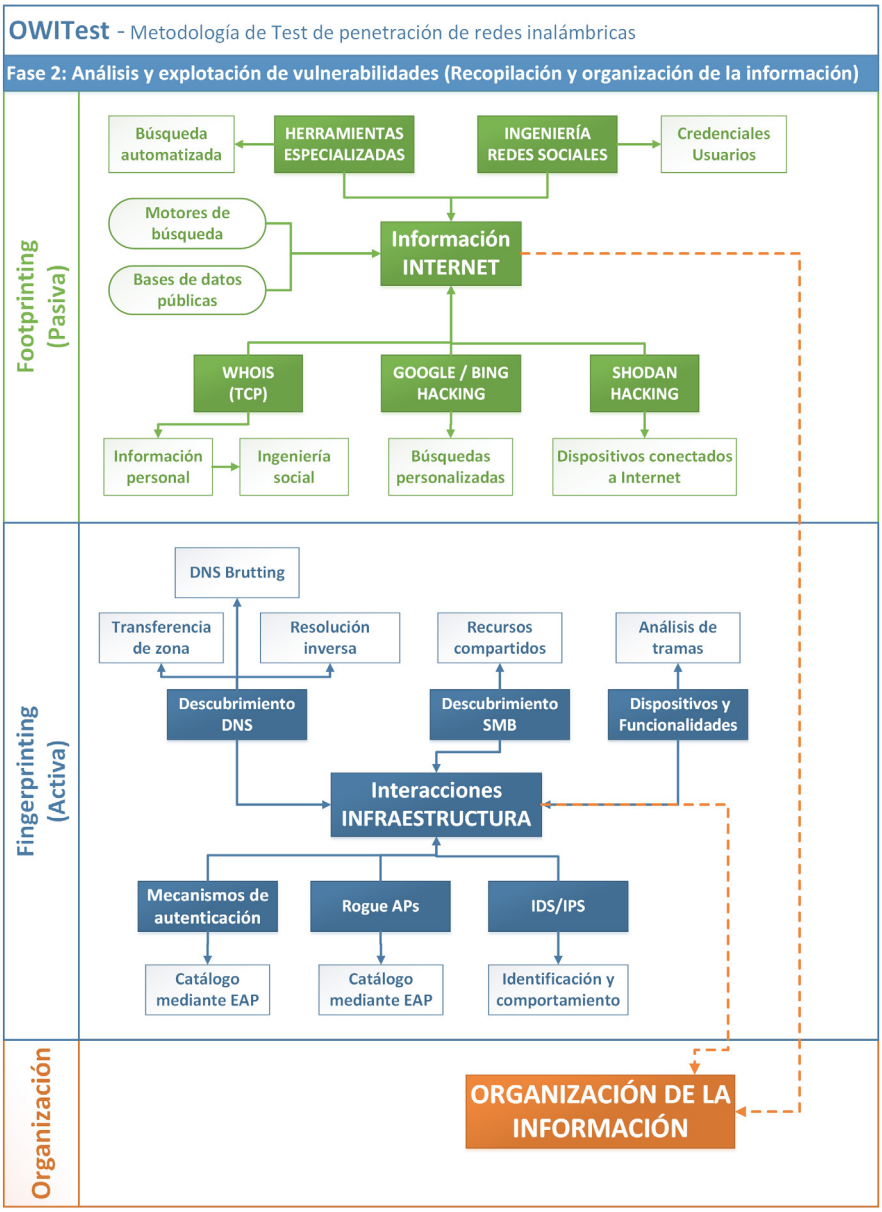


Figura 4 – Fase 2. Recopilación y organización de la información (Narváez D., 2017)

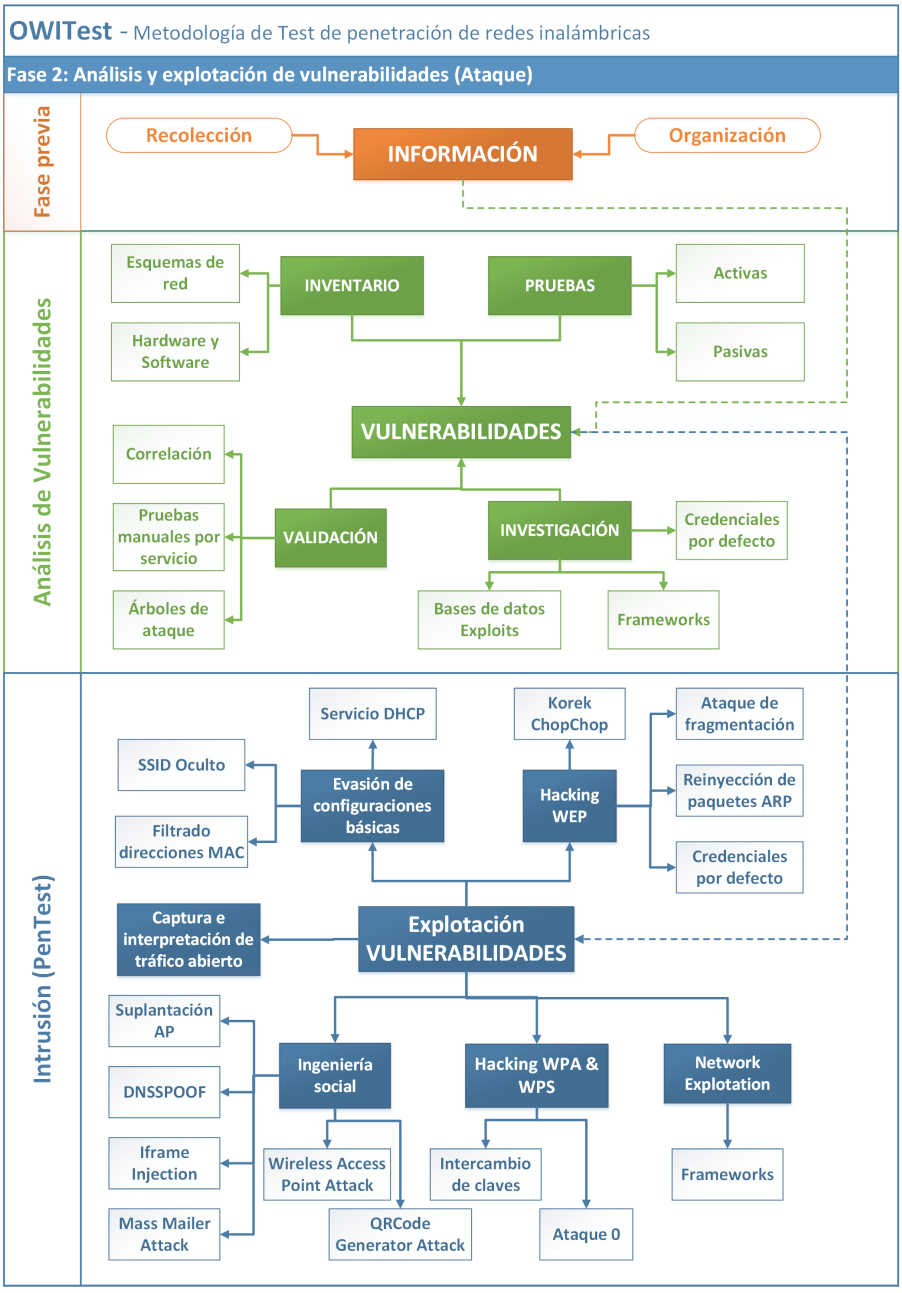


Figura 5 – Fase 2. Ataque (Narváez D., 2017)

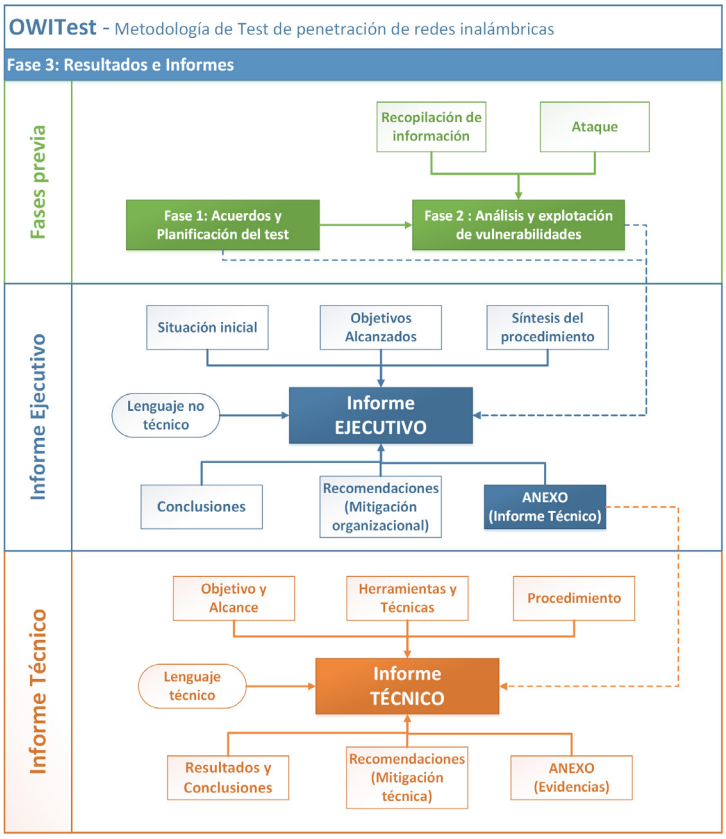


Figura 6 – Fase 3. Resultados e Informes (Narváez D., 2017)

5. Análisis de resultados

El principal objetivo de la metodología OWITest es potenciar la seguridad ofensiva de la red inalámbrica desplegada en campus académicos de Instituciones de Educación Superior, a través de procesos, herramientas y técnicas plasmadas en una auditoría de test de penetración o intrusión; por lo cual el resultado principal fue el establecer las principales formas de despliegue de las redes inalámbricas en el campus universitario, mismo que permitió proponer un prototipo de validación de la metodología.

- Red de acceso para usuarios autorizados: Red con SSID conocido similar al nombre de la institución (ej. WIFIPUCESI) con mecanismo de autenticación mediante portal cautivo (HTTP o HTTPS) y credenciales (usuario y contraseña), misma que abarca todo el campus universitario.
- Red federativa interinstitucional: Red que permite el acceso a servicios de Internet, con mecanismos de autenticación basados en credenciales de dominios @xxx.edu.ec, y control de acceso bajo WPA 2 Infraestructure.

- Red para laboratorios y aulas de clase: Red que permite el acceso a servicios de Internet para equipos que se encuentran en los laboratorios de informática o aulas de clase, con acceso restringido solo para los usuarios que el Departamento de TI de la institución disponga, bajo WPA 2 Personal.
- Red temporal abierta: Red temporal con duración muy corta creada para eventos especiales con casi ningún mecanismo de protección. Una práctica existente para nada recomendable.

En base a las consideraciones anteriores se propuso un esquema (infraestructura y servicios) que el prototipo de validación debe contener para evaluar los requisitos de la metodología OWITest. La selección específica de los elementos (marcas y características) se considerará a futuro en otras investigaciones.

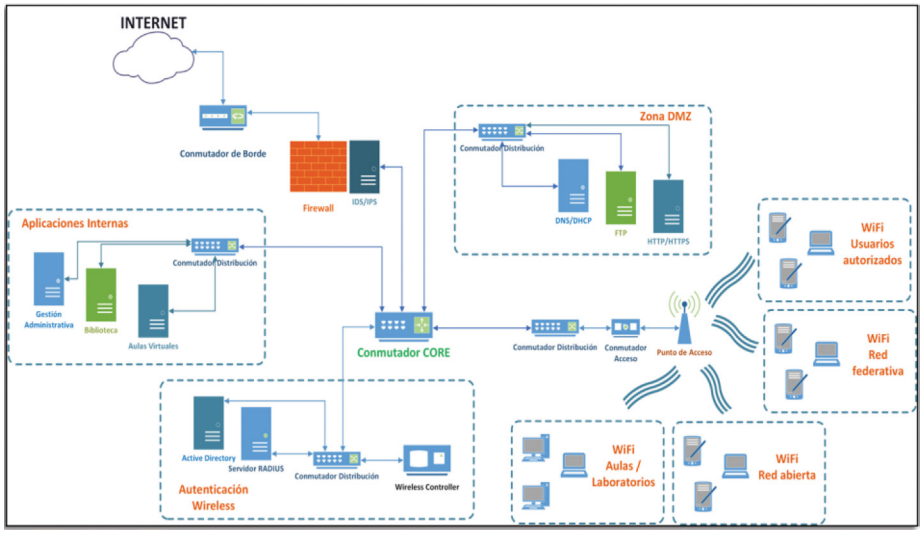


Figura 7 – Prototipo de validación (Narváez D., 2017)

6. Conclusiones

La creación de una metodología abierta de test de penetración brinda flexibilidad al equipo auditor, para poder realizar las adecuaciones, de acuerdo al escenario al que se enfrente, utilizando su experiencia y los recursos técnicos o logísticos con los que cuente. Es importante mencionar que las herramientas o aplicaciones propuestas en cada fase son sugerencias más no un camisa de fuerza o elementos obligatorios. Por otro lado abre las puertas a futuras investigaciones que tomen como base la metodología OWITest de forma libre.

La etapa más crítica dentro de las fases de la metodología OWITest es la intrusión que consiste en las explotación de las vulnerabilidades detectadas en etapas previas,

a través de herramientas automatizadas y manuales; el hecho de ser critica es porque el analista de seguridad no debe perder en ningún momento el control del ataque ya que debe respetar los acuerdos pactados, y además no afectar el rendimiento de los servicios, sistemas y accesibilidad a la red inalámbrica. Esto se logra sólo a través de un buen nivel de experticia, por lo que la organización debe asegurarse de que el equipo auditor responda en este sentido y no perder de vista la supervisión de todos los procesos.

Agradecimientos

Un especial agradecimiento al Departamento de Tecnologías de Información de la Pontificia Universidad Católica del Ecuador Sede Ibarra por permitir el acceso a la información.

Referencias

Estrada, A. C. (2011). Seguridad por niveles: Seguridad de acuerdo al modelo de capas TCP/IP. Alejandro Corletti.

Herzog P. (2010). OSSTMM 3 – The Open Source Security Testing Methodology Manual (3.ª ed.). España: ISECOM. Recuperado a partir de http://www.isecom.org/mirror/OSSTMM.3.pdf

Jang, M. (2010). Security Strategies in Linux Platforms and Applications. Jones & Bartlett Publishers.

Johansen, G., Allen, L., Heriyanto, T., & Ali, S. (2016). Kali Linux 2 – Assuring Security by Penetration Testing. Packt Publishing Ltd.

Learning, L. J. & B., & Harwood, M. (2011). Security Strategies in Web Applications and Social Networking. Jones & Bartlett Publishers.

Long, J. (2004). Google Hacking for Penetration Testers. Syngress.

Muller A., & Meucci M. (2014). OWASP Testing Project 4.0 (4.ª ed.). The OWASP Foundation. Recuperado a partir de https://www.owasp.org/index.php/OWASP_Testing_Project

Narváez D. (2017, septiembre 21). Metodología de test de penetración para redes inalámbricas en campus universitarios. Universidad Internacional de La Rioja, Ibarra.

Ramilli, M. (2013). A Design Methodology for Computer Security Testing. Lulu.com.

Sillitti, A., Martin, A., Wang, X., & Whitworth, E. (2010). Agile Processes in Software Engineering and Extreme Programming: 11th International Conference, XP 2010, Trondheim, Norway, June 1-4, 2010, Proceedings. Springer Science & Business Media.

Tarlogic Security. (2013, abril 9). OWISAM. Recuperado 10 de junio de 2017, a partir de https://www.owisam.org/es/P%C3%A1gina_principal

Whitaker, A., & Newman, D. P. (2005). Penetration Testing and Network Defense. Cisco Press.

Wilhelm, T. (2013). Professional Penetration Testing: Creating and Learning in a Hacking Lab. Newnes.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 11/12/2017
Aceitação/Acceptance: 21/03/2018

Gestión de correspondencia física a través de aplicación móvil y códigos QR

Yuri V. Nieto A.[1], José F. López Q.[2], Carlos E. Montenegro M.[3]

Yuri_nieto@cun.edu.co, cemontenegrom@udistrital.edu.co, jflopezq@hotmail.com

[1] Facultad de Ingeniería, CUN, Bogotá, Colombia

[2] Facultad de Ingeniería, Universidad Distrital FJC, Bogotá, Colombia

[3] Facultad de Ingeniería, Bogotá, Colombia

Pages: 201–213

Resumen: Este artículo presenta la explicación y la descripción de la arquitectura interna del desarrollo de una aplicación de elementos web y móvil para la gestión de la correspondencia física a través de códigos QR, además de las herramientas utilizadas para desarrollo y modelado para satisfacer las necesidades del usuario, que se mostrará como un requisito y entonces los casos de uso serán considerados, el proyecto se ejecutará a través de una metodología que se compone de dos partes, la primera de la investigación y la segunda del desarrollo complementan entre sí para finalmente obtener una aplicación que le da la notificación oportuna de la información contenida en la correspondencia física.

Palabras claves: Códigos QR, aplicaciones móviles, aplicación web, correspondencia física, desarrollo, ciclo de vida, modelado.

Physical correspondence management through mobile application and QR codes

Abstract: This article presents the explanation and description of the internal architecture of the development of an application with web elements and mobile elements for the management of physical correspondence through QR codes, in addition to the tools used for development and modeling To satisfy the needs of the user, which will be shown as a requirement and then the use cases will be considered, the project will be executed through a methodology that is composed of two parts, the first of research and the second of development that complement each other to finally obtain an application that gives timely notification of the information that is contained in the physical correspondence.

Keywords: QR codes, mobile application, web application, physical correspondence, development, lifecycle, modeling.

1. Introducción

En la actualidad es necesario dar solución a ciertos problemas comunes que se dan a diario pero no se les presta mucha atención, en este caso, y con ayuda de la tecnología se realizará la implementación y desarrollo de una aplicación para gestionar la correspondencia física y evitar que la información de esta se pierda o que no se vea a tiempo.

El artículo está compuesto por una metodología en donde se realizará y mostrará la forma en que se obtuvieron los datos y como se realizó el análisis de estos para obtener las necesidades del usuario, también se mostrará la forma en que fue desarrollado el proyecto para cumplir con los requerimientos planteados por los desarrolladores y aprobados por el cliente, luego se realizará un marco teórico donde se hablará de la historia de los códigos QR y de los sustentos del por qué estos son tan importantes para la sociedad actual. Para complementar esta información, se mostrarán algunos ejemplos de estos códigos y como última parte del marco teórico se compararán las aplicaciones web con las aplicaciones móviles para determinar el tipo de aplicación necesario para el proyecto.

Adicionalmente, se presenta una sección de desarrollo e implementación, en la que primero se muestra la estructura de la aplicación donde se evidencia el ambiente de desarrollo utilizado, el sistema operativo para realizar la ejecución de la aplicación y el funcionamiento de la base de datos, luego se mostrarán y se hará una descripción de las tecnologías a utilizar para el desarrollo y en la última parte dentro de la implementación y el desarrollo se mostrará el modelamiento del sistema comenzando por los requerimientos y sus consecuentes casos de uso, esta parte del artículo será gráfica, donde se mostrarán ciertos diagramas y su correspondiente descripción y explicación, el primero de estos diagramas es el diagrama de clases para mostrar la estructura de la lógica de lo desarrollado, seguido del diagrama de secuencia para mirar los procesos a lo largo del tiempo, el diagrama de colaboración para ver la interacción entre los roles y el diagrama de componentes para mostrar los distintos elementos que son necesarios para el funcionamiento de la aplicación.

2. Metodología

El proceso de investigación aplicado para este proyecto se dividió en dos partes, la primera de ellas, el uso de un enfoque de investigación y por otro lado el uso de una metodología de desarrollo.

Como metodología de investigación se decidió el uso del enfoque cuantitativo, esta decisión se tomó debido a la forma en que se quiere adquirir la información. Para este caso, es necesario la obtención y el análisis de datos a nivel de encuestas, por lo que el enfoque cuantitativo brinda suficientes bondades para que al asignar números a estos resultados se puedan generalizar resultados a nivel poblacional.

Para llevar a cabo de forma correcta el análisis de datos a través del enfoque cuantitativo es necesario cumplir con ciertos pasos, primero se debe plantear y delimitar el problema, donde se especifique una pregunta a resolver, luego se debe realizar la revisión de la literatura, es decir, la revisión de trabajos o estudios anteriores relacionados con el tema que se está investigando, como siguiente paso, se construye el marco teórico para poder

realizar la hipótesis de la investigación, la cual a partir del marco teórico y de la revisión de la literatura se pueden consolidar consistentemente, o por el contrario, descartarlas por falta de evidencia.

Con ayuda del procedimiento mencionado anteriormente, se escoge el enfoque cuantitativo para apoyar la investigación, de tal forma, que los resultados obtenidos arrojen características que se puedan tener en cuenta para el correcto desarrollo del proyecto.

Por otro lado, se tiene la metodología de desarrollo, en la cual se escogió el ciclo de vida iterativo (Campderrich Falgueras, 2013) por las bondades que brinda. Este ciclo de vida está basado en el modelo de cascada, (Maller, Ochoa, & Silva, 2004), (Hossein & Natsu, 1997) el cual se separa en cuatro fases, comenzando por un análisis, seguido de un diseño, se hace la correspondiente codificación y se sigue para realizar las pruebas. Luego de completadas cada una de las 4 fases, se obtiene un resultado también llamado liberable que será entregado al cliente para su correspondiente aprobación y realización de sugerencias para empezar con el siguiente ciclo; este proceso se realiza cuantas veces sea necesario hasta cumplir con los requerimientos acordados al principio del proyecto. (Carnegie Mellon, 2008)

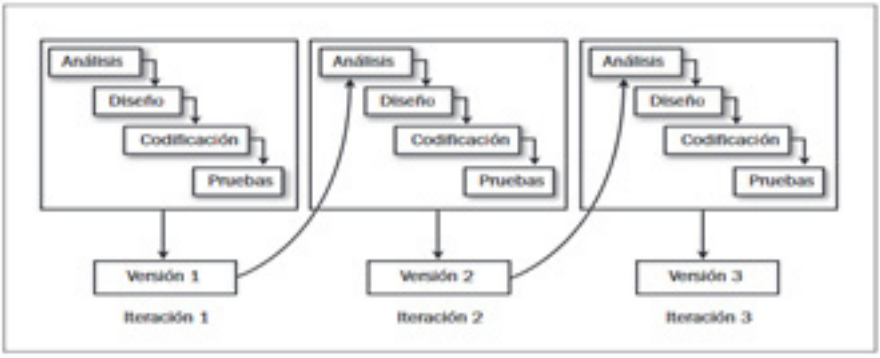


Figura 1 – Ciclo de Vida

En la figura anterior, se puede ver de forma gráfica el funcionamiento del ciclo de vida iterativo, para el caso de la imagen se realizan tres iteraciones y por lo tanto se obtienen tres entregables que son las versiones y se debe tener en cuenta que la cantidad de versiones (liberables) debe corresponder a la misma cantidad de iteraciones.

3. Marco teórico

3.1. Historia

A lo largo de la historia de la humanidad la tecnología ha jugado un papel muy importante para la optimización de tiempos y recursos en ciertas tareas, en la década de 1960, para realizar el registro de productos para la venta era necesario el registro y búsqueda manual de los productos, esta tarea llevaba mucho tiempo y el uso de mucho más personal que se veía afectado debido al alto nivel de trabajo.

Por esta razón, en el año 1952, se inventaron los códigos de barras y fueron usados comercialmente hasta 1966 (Meneses Fernández, Martín Gutiérrez, & Álvarez Martínez, 2014), los cuales son una serie de líneas de distinto grosor que almacenan cierta información, con esta invención se realizó el desarrollo del sistema POS en la década de 1970 (Gutiérrez, 2012), en dónde se almacenaba este código de barras se adhería al producto, en el código estaba almacenado la información correspondiente al precio y al realizar la lectura esta información se obtenía instantáneamente.

Denso Wave, en 1994, anunció el lanzamiento de un nuevo código con muchas más bondades que las brindadas por el código de barras, este nuevo código era capaz de almacenar 7.000 caracteres y podía ser leído 10 veces más rápido, por esto mismo se le denominó código de Respuesta Rápida, del inglés Quick Response, al cual llamaron simplemente código QR. (Leiva-Aguilera, 2012)

Luego de esto, el código QR se empezó a utilizar como estándar para muchas empresas y asociaciones, la primera de ellas fue la AIM (Automatic Identification Manufacturer), para la identificación automática de la fabricación a nivel industrial, luego de ello, se estandarizó en otras empresas japonesas, para que finalmente en el año 2000, fuera aprobado por la ISO (International Organization for Standardization) encargada de regir los estándares de la industria a nivel mundial.

Otro detalle que ayudó a la difusión del código QR fue la decisión de Denso Wave de liberar el código fuente para el uso de este nuevo método de almacenamiento de información, por esta misma razón en 2002, los teléfonos móviles se empezaron a comercializar con la opción de leer códigos QR (Villoldo, Salom, Pons Chaigneau, Rubio Montero, & Vallés Navarro, 2012) que permitían el acceso a páginas web, de esta forma la cantidad de información que se podía obtener sobre algún producto o servicio era mucho mayor.

3.2. Ejemplos códigos QR

Actualmente existe una gran variedad de códigos QR a lo largo del mundo (Luque Ordóñez, s.f.), los ejemplos que se mostrarán a continuación son estándares de alguna empresa o asociación que a través de estos han optimizado o mejorado alguna característica dentro de ellas.



Figura 2 – Aztec Code

El primero de ellos es el Aztec Code, apareció en el año de 1995, inventado por inventado por Andrew Longacre, Jr. y Robert Hussey, su nombre se debe a la similitud con las pirámides aztecas, tiene la ventaja de mejorar el uso del espacio porque no necesita de una zona para determinar el sentido del código.



Figura 3 – Micro QR Code

El siguiente de ellos, es el código QR micro, que es una representación minimizada del código QR estándar, a pesar de que minimiza el uso del espacio la cantidad de caracteres que puede almacenar también se ve reducida.



Figura 4 –Datamatrix

Como bien lo dice su nombre, este código QR, se asemeja a una matriz de datos, este tipo de código puede almacenar muchas más caracteres que otros, es capaz de almacenar hasta 2.335 caracteres alfanuméricos, es mayormente usado en los dispositivos electrónicos de menos tamaño como lo recomienda la Alianza de Industrias Electrónicas (EIA – Electronic Industries Alliance).



Figura 5 – Microsoft Tag

El último de los ejemplos, es el Microsoft Tag, que como se evidencia en su nombre, pertenece a la multinacional Microsoft. Este fue un servicio creado en el año 2010, con el objetivo de que cualquier persona promoviera algún servicio en la web por medio de este y que con una aplicación del mismo proveedor se pudiera interpretar, sin embargo, en 2013, Microsoft cerró este proyecto debido a la falta de popularidad de este tipo de código.

3.3. Aplicación Web vs. Aplicación Móvil

Para determinar el tipo de aplicación sobre el que se iba a desarrollar, fue pertinente realizar una comparación entre las ventajas que brindan las aplicaciones web y las

aplicaciones móviles, para realizar esta comparación se mostrarán las características de cada una de ellas y luego se define la que brinda la mayor cantidad de ventajas para este proyecto.

En primer lugar, se tienen las aplicaciones web las cuales se ejecutan desde un navegador, tienen las ventajas de ser utilizadas sin necesidad de una instalación previa, dentro de las ventajas que se tienen dentro de este tipo de aplicaciones está la posibilidad de almacenar cierta información en servidores que pueden ser accedidos cuando se tiene internet, con una conexión de este tipo y un navegador la información puede ser consultada desde cualquier parte del mundo.

Algunos ejemplos de aplicaciones web que se usan a diario están las aplicaciones de correo electrónico de las distintas empresas proveedoras de este servicio en el mundo como lo son Google, Yahoo o Microsoft; otros ejemplos, son la variedad de redes sociales que hay actualmente dentro de las cuales están Facebook, Twitter, entre otras.

Con información general de que son las aplicaciones web y algunos ejemplos de estas, es pertinente hablar de las ventajas, este tipo de aplicaciones tienen una compatibilidad multiplataforma, es decir, que sin importar el sistema operativo en el que se encuentre o el dispositivo se podrá acceder a la aplicación.

Por otro lado, se tienen las aplicaciones móviles que hoy en día, son importantes para el desempeño de la cotidianidad de las personas, debido a la gran cantidad de aplicaciones que existen en el mercado se pueden realizar diferentes actividades y esto es lo que ha aumentado la popularidad de estas, las principales categorías con las que se interactúan son juegos, educación, negocios, estilo de vida y entretenimiento.

El uso de aplicaciones móviles o “apps” está desplazando el uso de aplicaciones web dado que en ocasiones es necesario realizar acciones fuera de línea y a veces no se tiene acceso a internet desde el dispositivo móvil lo que permite que las ventajas de este tipo de aplicaciones aumenten.

Al analizar las distintas ventajas que brinda cada uno de los tipos de aplicaciones se puede concluir que cada una es pertinente en su contexto, es decir, que dependiendo de la necesidad del usuario se utilizará una sobre la otra, para este caso se realizará uso de los dos tipos de aplicación para satisfacer los requerimientos del proyecto.

4. Desarrollo e implementación

4.1. Estructura de la aplicación

1. *Ambientes de desarrollo:* Para desarrollar esta aplicación es necesario de dos ambientes, el primero de ellos, Java para el desarrollo de la parte móvil de la aplicación y HTML5 (Xuelei, Shulin, Guyang, & Liping, 2013) con uso de Javascript (Elliott, 2014) para la parte web de la aplicación.

Comenzando por la parte móvil, se usa Java por el soporte multiplataforma que brinda, porque este es un lenguaje de programación orientado a objetos, tiene una gran oferta de librerías para el desarrollo de distintas aplicaciones incluidas algunas para complementar el desarrollo para aplicaciones Android. Además, es un lenguaje fácil de aprender, de

leer y de entender, y adicionalmente con ayuda de las plataformas de desarrollo (IDE) se facilita el trabajo y se reducen la cantidad de errores que se puedan cometer.

Por otra parte, se tiene el desarrollo web con HTML5 (Harris, 2014) y Javascript, con estas herramientas se puede realizar un despliegue liviano de información hacia cualquier dispositivo, además de ello los diseños se pueden optimizar de tal forma que la visualización sea buena en cualquier tamaño de pantalla, a pesar de las ventajas el desarrollo web para ser ejecutado desde dispositivos móviles presenta algunas dificultades como el acceso al hardware como lo es la cámara.

2. *Sistema operativo:* Se realizará uso del sistema operativo Android el cual está basado en Linux, en este sistema operativo se puede realizar la ejecución de aplicaciones móviles sin ningún problema. A pesar de que este sistema operativo brinda grandes ventajas en tema de seguridad para la instalación y ejecución de aplicaciones por parte de fuentes desconocidas, también se tiene la opción de omitir esta parte del sistema de seguridad con el objetivo de ejecutar aplicaciones propias.

3. *Base de datos:* El almacenamiento de datos se debe realizar de una forma en la que estos estén relacionados y agrupados de una forma estructurada, para esto, es necesario el uso de base de datos, además de ello la seguridad de la información aumenta junto con la cantidad de funcionalidades que se pueden hacer sobre esta.

Existen varios modelos para realizar una base de datos, para este caso, se utilizará el modelo relacional. Para este tipo de modelo, es necesario realizar el modelamiento para que cumpla con las especificaciones del cliente.

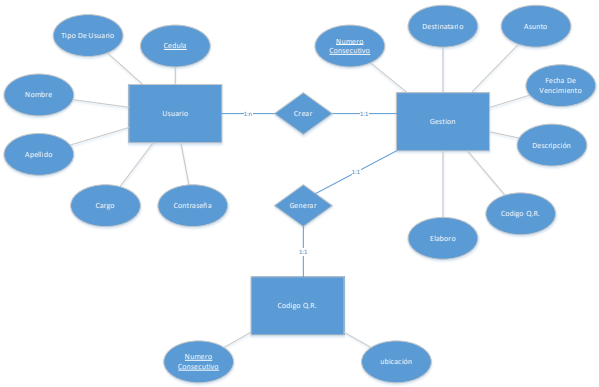


Figura 6 – Diseño físico de la base de datos

El anterior diagrama entidad relación, es el obtenido para el desarrollo y diseño físico de la base de datos donde se tienen tres entidades: usuario, gestión y código QR, que a su vez, tienen cierta cantidad de atributos para guardar la información, cabe resaltar que no todas las entidades se relacionan, usuario se relaciona con gestión y gestión con código QR, pero las entidades usuario y código QR nunca se relacionan, esto se hace para evitar la alteración de datos por parte del usuario.

4.2. Tecnologías a utilizar

1. *Android Studio:* (Van Drongelen, 2015) Es un entorno de desarrollo integrado (IDE) para desarrollar aplicaciones móviles del sistema operativo Android, fue el reemplazo de Eclipse y su primera versión estable fue publicada en diciembre de 2014, tiene características que permiten la optimización de recursos, entre las cuales se encuentran la renderización en tiempo real, plantillas para la creación de diseños comunes además de la posibilidad de crear estos con la opción de agarrar y soltar, y la ejecución virtualizada de la aplicación para realizar las pruebas pertinentes a las aplicaciones.
2. *MySQL (PHPMyAdmin):* (Rochkind, 2013) Con esta herramienta desarrollada en PHP se realiza la administración de la base de datos en MySQL a través de una página web, dentro de esta aplicación se pueden importar y exportar datos desde y hacia diferentes formatos, creación de consultas complejas utilizando Query-by-Example (QBE) y la posibilidad de monitoria las actividades y recursos asignados a la base de datos.
3. *Visio 2013:* Es una aplicación de Microsoft Office para realizar diagramas y gráficas, con ayuda de esta herramienta se buscan realizar los distintos diagramas como lo son los diagramas de caso de uso, el modelo entidad relación para la base de datos y los diagramas de arquitectura: diagrama de clases, diagrama de secuencia, diagrama de colaboración y diagrama de componentes.
4. *Dreamweaver:* Dreamweaver es un programa de estudio de Adobe para la construcción, diseño y edición de sitios y aplicaciones web, actualmente con ayuda de Dreamweaver es posible la realización de páginas sin necesidad de conocer HTML, además soporta herramientas que complementan la funcionalidad como los son las hojas de estilo (CSS) y la realización de lógica con Javascript, esta herramienta está disponible en Windows y en MAC, aunque también es posible utilizarlos en UNIX con simulador de herramientas de Windows como Wine.
5. *Sublime Text:* Es un editor de texto y editor de código que soporta una gran cantidad de idiomas y tiene varias bondades dentro de las que se encuentran la multiplicidad de la selección, la multiplicidad del cursor, búsqueda dinámica, auto completado y marcado de llaves, uso de pestañas para la edición de varios archivos al mismo tiempo, resaltado de paréntesis para la identificación de bloques.
6. *Selenium:* Con esta herramienta se tiene un entorno de pruebas de software principalmente para aplicaciones basadas en la web, estas pruebas se pueden realizar sin necesidad de escribirlas en un lenguaje de scripting, además de ellos se pueden realizar depuración y puntos de verificación (breakpoints).
7. *JMeter:* (Erinle, 2014) Esta última herramienta desarrollado por Apache brinda la posibilidad de hacer pruebas de desempeño en tiempo real de servicios especializados en aplicaciones web, además de ello tiene la opción de monitorear los recursos que se están utilizando, la primera versión de JMeter fue lanzada el 9 de marzo de 2001.

4.3.Modelamiento del sistema

1. *Requerimientos:* Para realizar los requerimientos fue necesario realizar una encuesta para conocer las necesidades que tiene la empresa respecto a la correspondencia física, al realizar un análisis de los datos y estadísticas obtenidas por medio del enfoque cuantitativo se levantaron cuatro requerimientos.

El primero de ellos, con identificador RF-001, llamado “Acceso a la aplicación”, este tiene una prioridad alta y consta en que la aplicación será accesible por medio de un usuario y contraseña previamente configurados en el sistema. En segundo lugar, está el requisito de “Administración de usuarios”, con identificador RF-002 y con prioridad alta, en donde la aplicación estará en la capacidad de realizar la creación, modificación y eliminación de usuarios; el tercer requerimiento, “Documentos”, identificado con RF-003 y con alta prioridad, también es en donde la aplicación estará en la capacidad de realizar la creación, modificación y eliminación de documentos que contengan la información relevante de la correspondencia recibida, y el último requerimiento, “Notificaciones”, con identificador RF-004 y alta prioridad, de las misma forma que los otros requerimientos, tiene como descripción que la aplicación estará en la capacidad de realizar la creación, modificación y eliminación de las alarmas que servirán.

2. *Casos de Uso:* A partir de los requerimientos levantados anteriormente, se procede a realizar la elaboración de los casos de uso, de los cuales se obtienen 5, los cuales serán realizados por 3 actores y su resultado se evidencia en el siguiente diagrama, en el que se aprecia quien tiene asignado el caso de uso y las precondiciones para poder realizarlo.

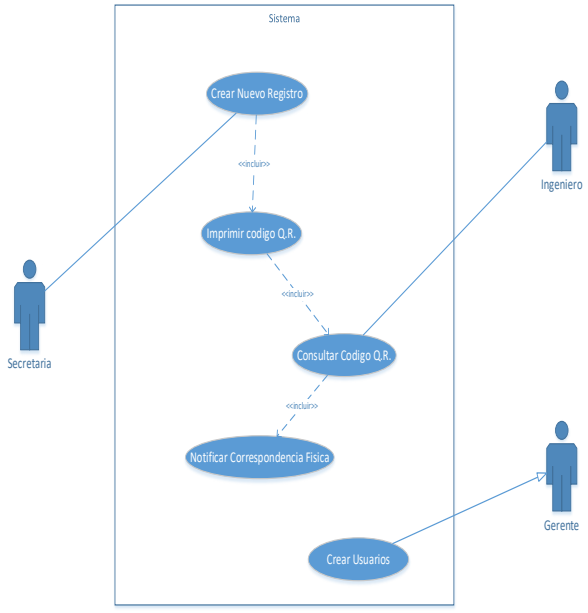


Figura 7 – Casos de uso

3. *Diagrama de clases:* En el siguiente diagrama de clases, se representa la estructura de la lógica realizada en Java a través del Android Studio, es relevante recordar que los diagramas de clases según UML (Unified Model Language) están compuestas por tres secciones horizontales, la primera de ellas lleva el nombre de la clase, la segunda los atributos y la tercera los métodos dentro de la clase.

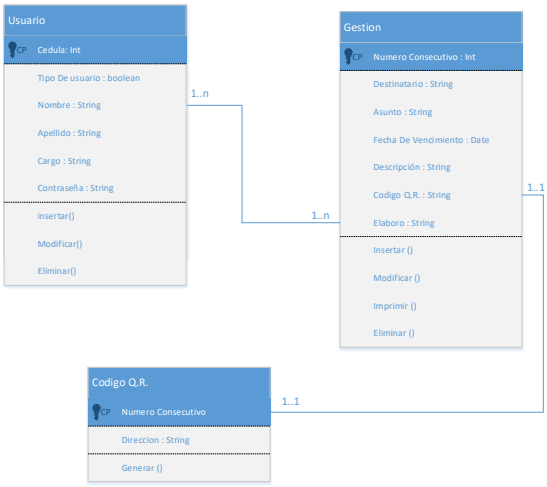


Figura 8 – Diagrama de Clases

En este diagrama, se puede ver que el desarrollo de la aplicación móvil se realizó en tres (3) clases, la primera de ellas “usuario”, compuesta por 5 atributos y 3 métodos que correspondiendo con lo planteado en los requerimientos son insertar, modificar y eliminar; la segunda clase es “Gestión”, en donde fuera de insertar, modificar y eliminar, tiene la opción de imprimir, y finalmente, está la clase código “QR” en dónde únicamente se puede realizar la generación del código y solo tiene como atributo la dirección en donde está almacenada la imagen.

4. *Diagrama de secuencia:* Para visualizar la interacción de los objetos a través del tiempo se tienen los diagramas de secuencia, en el diagrama a continuación, se evidencia la existencia de 5 objetos: Secretaria, Formulario, Generador Códigos QR, Destinatario y Android, en la primera parte del diagrama se ve el envío de 5 mensajes de Secretaria a Formulario, estos mensajes forman la parte de un nuevo registro, luego de ello, se realiza la parte de la generación del código y la verificación del mismo, para que finalmente, como se ve en los últimos 2 mensajes enviados, entre Destinatario y Android para la notificación para no dejar pasar las fechas en la correspondencia física.

5. *Diagrama de colaboración:* En un diagrama de colaboración se ve evidenciada la interacción entre los distintos roles, para el diagrama a continuación, hay dos roles “Secretaria” y “Destinatario”, en donde la Secretaria se encarga de realizar el ingreso de datos a través de la plataforma de la aplicación web que está realizada en PHP y esto se realiza para la generación del código QR el cual es enviado a la impresora para que

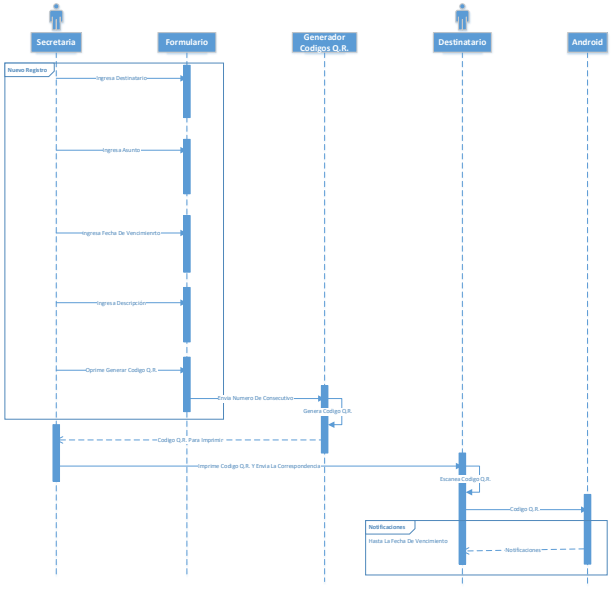


Figura 9 – Diagrama de secuencia

este sea anexado a la correspondencia que será enviada al Destinatario, para que este con ayuda de la aplicación móvil escanee el código QR que será interpretado por la misma aplicación y muestre la información para la correspondiente notificación.

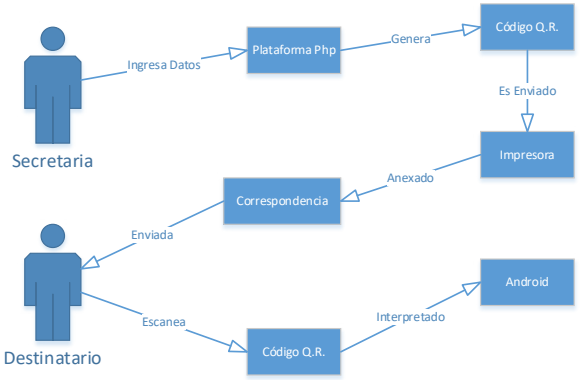


Figura 10 – Diagrama de Colaboración

6. *Diagrama de componentes:* En el siguiente diagrama de componentes, se muestra la interacción del actor con los distintos elementos que componen el sistema, a nivel general hay tres (3) sistemas: Estación de trabajo, Sistema y Android, dentro de cada uno de ellos hay componentes que se relacionan con los componentes de los otros

sistemas. Para el sistema Estación de trabajo, compuesto por Explorador web se tienen que es accedido por parte de los otros dos componentes, Sistema y Andorid, dentro de cada una de ellos existe su correspondiente IU (Interfaz de Usuario) que por otra parte están trabajando con el componente SGDB (Sistema de Gestión de Base de Datos) para adicionar, modificar y eliminar los datos.

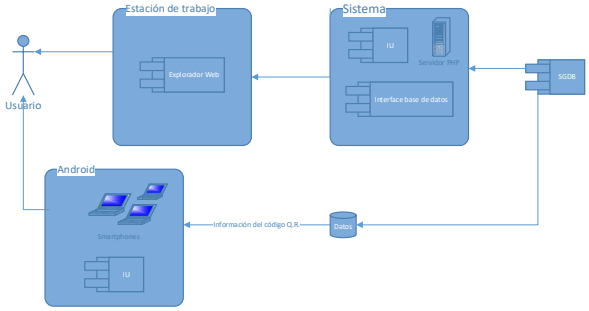


Figura 11 – Diagrama de Componentes

5. Conclusiones

A través de la metodología con su enfoque cuantitativo se mencionaron las distintas formas en las que se determinaron las necesidades del usuario para darles una prioridad, esto se hizo al plantear los requerimientos y consecuentemente los casos de uso, complementando la metodología se usó el ciclo de vida iterativo compuesto por varios ciclos de vida en cascada con lo que se obtuvieron ciertas versiones de la aplicación las cuales contenían mejoras y adelantos a medida que los ciclos iban pasando finalmente se obtuvo una aplicación con sus componentes web y móvil que satisface los requerimientos planteados.

Por otro lado, se realizó una contextualización correcta a través del marco teórico para que en la sección de desarrollo e implementación se entendiera la estructura de la aplicación, las tecnologías utilizadas, y finalmente, el modelamiento del sistema que mostró los distintos diagramas para entender la arquitectura interna de la aplicación desde distintas perspectivas incluyendo la parte de desarrollo con los diagramas de clases y componentes, y la interacción de los roles con las tareas a realizar a lo largo del tiempo con los diagramas de secuencia y colaboración.

Referencias bibliográficas

Campderrich Falgueras, B. (2013). *Ingeniería del software*. Editorial UOC.

Carnegie Mellon, U. (2008). *CMMI Destilled* (Tercera Edicion ed.). Estados Unidos de America: Addison-Wesley.

Elliott, E. (2014). *Programming JavaScript Applications: Robust Web Architecture with Node, HTML5, and Modern JS Libraries*. Sebastopol, CA : O'Reilly Media.

Erinle, B. (2014). *JMeter Cookbook*. Birmingham: Packt Publishing.

Gutiérrez, F. (2012). CODIGO QR EN BIBLIOTECAS Y ALFABETIZACION INFORMACIONAL MOVIL. *Revista Chilena de Bibliotecología*.

Harris, A. (2014). *HTML5 and CSS3 All-in-One For Dummies*. Hoboken.

Hossein, S., & Natsu, C. (1997). Characterizing a Software Process Maturity Model for Small Organizations. University of Nebraska at Omaha.

Leiva-Aguilera, J. (2012). Introducción y algunos usos de los códigos QR. *Anuario Think EPI*, 309–312.

Luque Ordóñez, J. (s.f.). *Códigos QR*. AUTORES CIENTÍFICO-TÉCNICOS Y ACADÉMICOS.

Maller, J., Ochoa, J., & Silva, C. (2004). Lightening the software production process in a CMM level 5 framework. *JISBD*.

Meneses Fernández, M., Martín Gutiérrez, J., & Álvarez Martínez, E. (2014). Uses of qr code in printed press. The audio visualization of paper. *Innovar*, 67–80.

Rochkind, M. J. (2013). *Expert PHP and MySQL: Application Design and Development*. [Berkeley, Calif.]: Apress.

Van Drongelen, M. (2015). *Android Studio Cookbook*. Birmingham, UK : Packt Publishing.

Villoldo, M., Salom, A., Pons Chaigneau, D., Rubio Montero, F., & Vallés Navarro, R. (2012). *Tecnologías móviles en bibliotecas*. Valencia: Biblioteca I Documentació Científica.

Xuelei, R., Shulin, Y., Guyang, W., & Liping, R. (2013). Research on Cross Platform Digital Publishing Technology Based on HTML5. *8th International Conference on Information Technology in Medicine and Education (ITME)*. Fuzhou.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 24/12/2017
Aceitação/Acceptance: 15/03/2018

Metodología de selección de IDE para el desarrollo de aplicaciones Android

Moreira Robles Jenny Mariela[1], Pusdá Chulde Segundo Eliceo[2]

yennymoreira86@hotmail.com, sepusda@pucesi.edu.ec.

[1] Universidad Laica Eloy Alfaro, El Carmen, Ecuador.

[2] Pontificia Universidad Católica del Ecuador, 100112, Ibarra, Ecuador.

Pages: 214–220

Resumen: En este artículo se describe el resultado del estudio sobre las herramientas IDE (Entorno de Desarrollo Integrado) que existen actualmente en el mercado tecnológico para el desarrollo de aplicaciones compatibles con el sistema operativo Android. Se realiza un análisis sobre los dispositivos móviles y las herramientas IDE en cuanto a características, componentes y estructura para el desarrollo de aplicaciones móviles en Android. El propósito de esta investigación es establecer una metodología de selección de IDE para el desarrollo de aplicaciones Android mediante un análisis y evaluación de sus características y componentes, con la finalidad que ayude en la fase de desarrollo y mejorar la productividad del programador. Se aplica la metodología de encuesta a expertos la cual se compone de dos elementos la ISO/IEC 9126 y métricas de estadística descriptiva. Se aplica la metodología a través de un formulario diseñado en Google Drive, las herramientas que se evalúan para la selección son Eclipse, NetBeans y Android Studio, los datos obtenidos son procesados y finalmente se determina cual es la mejor opción para el desarrollo de aplicaciones en Android.

Palabras-clave: Aplicaciones móviles; selección herramientas IDE; Android Studio; metodología de desarrollo; aplicación ISO 9126.

IDE selection methodology for the development of Android applications

Abstract: This article describes the result of having carried out a study on the IDE tools that currently exist in the technological market for the development of applications compatible with the Android operating system. I do analysis of the mobile devices and IDE tools in terms of their characteristics, components and structure for the development of mobile applications on Android. The purpose of this research is to establish a methodology for selecting IDE for the development of Android applications, by analyzing and evaluating its characteristics and components, to verify that it helps to improve the productivity of the programmer. The expert survey methodology is proposed, which is composed of two elements, ISO / IEC 9126 and descriptive statistics metrics. The methodology is applied through a simple form designed in Google Drive, the tools that are evaluated for the selection are Eclipse, NetBeans and Android Studio, the data obtained are

processed and finally it is determined which is the best option for the development of applications on Android.

***Keywords**:* Mobile apps; IDE tools selection; Android Studio; development methodology; ISO 9126 application.

1. Introducción

El crecimiento tecnológico ha conllevado a mejorar las prácticas y formas de programar, de igual manera busca la mejora en la implementación de nuevas aplicaciones de software, es importante hacer un análisis retrospectivo y ver cinco años atrás donde las aplicaciones informáticas no iban más allá de tener implementado una arquitectura cliente servidor y en el mejor de los casos tener la accesibilidad por medio de una aplicación web. (Garita Araya, 2013)

El desarrollo de aplicaciones web en los últimos años ha crecido de forma importante y con ello ha surgido la necesidad de tener acceso a las funcionalidades de las aplicaciones por medio de los dispositivos móviles, es importante destacar también el crecimiento y evolución de los dispositivos móviles, ya que han permitido que sea más sencillo implementar una aplicación por medio de los diferentes componentes y sistemas operativos que optimizan el funcionamiento de los dispositivos móviles. (El Tiempo, 2014).

Los sistemas operativos han brindado las facilidades necesarias para ganar espacio y que obtener más usuarios, sin duda los sistemas operativos que en la actualidad se destacan son Android, IOS y Windows Phone, cada uno con características, ventajas y desventajas, ya depende de la necesidad del usuario y el alcance de la aplicación que se desee desarrollar (Gutiérres, 2016).

Entre los sistemas operativos que más se utiliza en los dispositivos móviles es Android, así lo demuestra en la investigación realizada por (Morales Reyes, Gómez Yopasa, & Camargo Vega, 2016), en donde realiza una comparación de las propiedades de los sistemas operativos y Android tiene una mejor aceptación en el mercado tecnológico.

Las aplicaciones hibridas han presentado un crecimiento significativo frente a las aplicaciones nativas, ya que han permitido realizar una mejor interconexión y portabilidad de las aplicaciones, otro aspecto que ha destacado las aplicaciones hibridas es en el desarrollo, ya que ha permitido integrar tecnologías como HTML5, CSS y JavaScript, y para la compilación y despliegue hace uso de otros framework como Phonegap - Cordova o Ionic que permite generar aplicaciones para cualquier plataforma sin necesidad de volver a realizar para una plataforma específica y el costo de desarrollo es bajo comparado con realizar una aplicación nativa. (Otero Escobar, Martinez Castillo, & Diaz Camacho, 2016)

Para el desarrollo de aplicaciones móviles, el primer paso a realizar es analizar las herramientas disponibles, el alcance de la aplicación y la arquitectura de la aplicación móvil, es por eso que en la fase de desarrollo de software existe el inconveniente en la selección de las herramientas para el desarrollo, y por medio de la presente propuesta se desea brindar una visión para la selección del IDE de desarrollo.

2. Metodología

Surge de la necesidad de realizar una investigación en la selección de IDE (Entorno de Desarrollo Integrado) en la fase de desarrollo de software, centrándose en las herramientas para crear aplicaciones compatibles con el sistema operativo Android.

Se analizan y evalúan las características y componentes de diferentes herramientas IDE. El objetivo principal es establecer una metodología de selección de IDE para el desarrollo de aplicaciones en Android (aplicaciones nativas, programación Java) y sobre todo que sirva de apoyo al programador en la selección adecuada de la herramienta IDE.

La metodología está basada con la implementación de una encuesta a expertos por la cual se obtendrá un análisis y evaluación de la herramienta IDE en cuanto a componentes y características respaldada en dos elementos: el primero de ellos es la ISO/IEC 9126-1 que permite definir cuáles son las características a evaluar de cada una de las herramientas IDE, enfocado a la usabilidad. Evaluando la calidad en cuanto a características y componentes; el segundo elemento consiste en realizar un cálculo por medio métricas de estadística descriptiva como la desviación típica y moda que permitirá medir cuantitativamente las características de cada herramienta IDE.

La desviación típica genera como resultado un valor numérico que brinda una idea de que tan cerca o lejos se distribuyen los datos y poder distinguir en varios grupos de estos y permite obtener una visión más acorde con la realidad y poder interpretar para tomar decisiones.

Al obtener los resultados por parte de los expertos se aplican las métricas de estadística descriptiva para cada IDE. Este cálculo se lo realiza por medio de una hoja de Excel diseñada especialmente para la obtención de resultados automáticamente. Finalmente se obtiene el resultado siendo el IDE que obtenga mayor uniformidad en cuanto a la valoración de las características por medio de la desviación típica y promedio.

2.1. Decripción de la metodologia

Primer elemento: ISO/IEC 9126-1. Evaluación de la calidad del software.

En esta norma se enumeran seis características a evaluar.

1. Funcionalidad: Las características se enmarcan a las capacidades de los IDE para el desarrollo de aplicaciones Android.
2. Confiabilidad: Aquí podemos verificar que la herramienta brinde garantías para el mejor desarrollo en la programación en Java para aplicaciones Android.
3. Uso: También se verificará el uso de la herramienta que sea eficaz a la hora de desarrollar software que brinde un entorno amigable para el programador.
4. Eficiencia: Se evalúa la capacidad de la herramienta promoviendo el rendimiento de manera adecuada según lo requerido.
5. Mantenimiento: Validamos que el software sea capaz de permitir la realización de modificaciones de una forma sencilla.
6. Portabilidad: Es el que se debe tomar muy en cuenta en la capacidad y flexibilidad que el entorno permita transferir los datos a otro entorno en caso de requerirse.

Segundo elemento: Métricas estadísticas descriptiva (Promedio, desviación típica y moda).

1. Función promedio: Medida de posición central.

Dados los n números {x1, x2, ……, xn}, la media aritmética se define como:

$$x = \frac{1}{n}\sum_{i}^{n} xi = \frac{x_1 + x_2 + x_3 + \cdots x_n}{n}$$

Figura 1 — Función promedio o media aritmética

2. Desviación típica: Medida de dispersión que se asocia a la media. Mide el promedio de datos a través de una muestra de los mismos.

$$\boldsymbol{Sx = \sqrt{\frac{\sum_{i=1}^{N}(Xi - Media(X))^2}{N-1}}}$$

Figura 2 – Desviación típica (Morales Reyes, Gómez Yopasa, & Camargo Vega, 2016)
Siendo (X1, X2…, Xn) conjunto de datos.

3. Moda: El valor que más se repite en el conjunto de datos obtenidos. La frecuencia relativa es mayor.

2.2. Construcción del formulario encuesta a expertos

Para la aplicación del método propuesto se realizar el diseño de la encuesta a través de Google Drive según las características de los IDE.

Los usuarios que deseen aplicar esta metodología puede diseñar el formulario según el medio que mejor le convenga de hecho se lo puede aplicar de manera física.

2.3. Diseño

Para la aplicación de la metodología se implementan cuatro fases generales para la selección de la Herramienta IDE. Se detallan a continuación:

1. Herramientas IDE a evaluar: En esta fase se define dos o más herramientas para realizar la evaluación comparativa entre ellas.
2. Encuesta a expertos: Se selecciona un grupo de programadores o gestores expertos en el uso y conocimiento de cada una de las herramientas para que brinden su valoración con respecto a cada una de ellas.
3. Análisis y procesamiento de resultados: Luego de obtener los datos de la encuesta aplicada se procede a realizar el análisis y proceso de resultados mediante las métricas establecidas para este proyecto (estadística descriptiva). Además, se

realiza una descripción general del número de datos recolectados y número de respuestas por ítem.

4. Herramientas IDE: En esta fase se realiza la selección del IDE, en bases a las fases anteriores en las cuales ya se ha realizado un análisis y procesamiento de datos de la encuesta aplicada a los expertos con respecto a los IDE a evaluar.

2.4. Prueba y validación

Se realiza la aplicación de la encuesta a los expertos por medio de las fases generales de selección de Herramienta IDE.

Datos generales: La encuesta se aplicó a 20 expertos los cuales evaluaron el IDE del que mayor conocimiento tienen, algunos evaluaron 2 herramientas, el resto las tres herramientas y se obtuvo un total de 31 datos recolectados. El análisis de los datos son los siguientes:

Fase 1: Se eligieron tres herramientas IDE que actualmente están en auge en el desarrollo tecnológico, según la investigación plasmada en el marco teórico de esta investigación las herramientas a evaluar son: Eclipse, Android Studio y NetBeans.

Fase 2: Una vez creado la encuesta para ser aplicada a expertos, se aplica con 20 miembros de la Universidad Laica Eloy Alfaro de Manabí y otras empresas, la misma que se envió a través de correos electrónicos para la recopilación de datos.

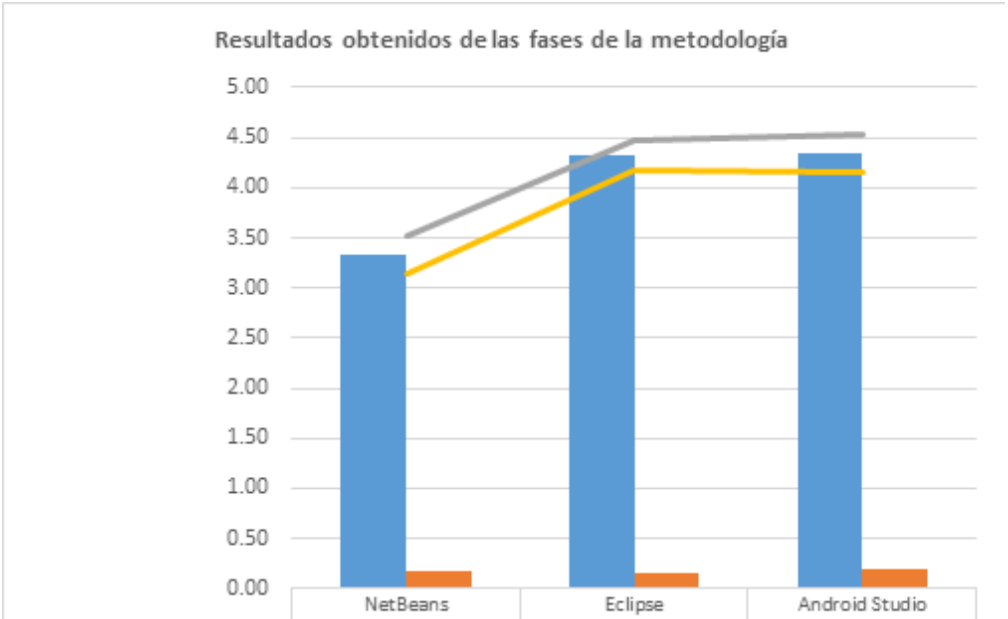
Fase 3: Análisis y procesamiento de resultados. Ya con los datos obtenidos por medio de la encuesta aplicada a los expertos, se realizó el procesamiento automático de resultados mediante la hoja de cálculo que ha sido diseñada en una hoja de Excel conjuntamente con la encuesta.

En la tabla 1 y en la figura 1 se muestra que los datos están por fuera del límite máximo, la desviación estándar por encima y por debajo del promedio es de 0.19, el mínimo es 4.15 y el máximo 4.53

IDE'S	Promedio	Desviación Estandar	Límite Máximo	Limite Mínino
NetBeans	3.34	0.18	3.52	3.15
Eclipce	4.33	0.15	4.48	4.17
Android Studio	4.34	0.19	4.53	4.15

Tabla 1 – Resultados obtenidos de los tres IDE's

Fase 4: Selección de la herramienta IDE: A pesar que Android Studio es un IDE específicamente para desarrollar aplicaciones móviles para dispositivos con sistema



	NetBeans	Eclipse	Android Studio
Promedio	3.34	4.33	4.34
Desviación Estándar	0.18	0.15	0.19
Limite Máximo	3.52	4.48	4.53
Limite Mínimo	3.15	4.17	4.15

Figura 1 – Resultados de los valores del uso de las herramientas IDE

operativo Android, en los resultados de la encuesta aplicada se determina que Eclipse sigue siendo el IDE con mayor valoración y de uso primario por los programadores.

El IDE Eclipse obtuvo mayor puntuación en cuanto a las características de manera general y como segundo IDE más utilizado es Android Studio, se resalta de este IDE que posee mayor puntuación en cuanto a la funcionalidad y eficiencia, NetBeans esta equivalente en las seis características generales que se evaluaron, por lo tanto, se ubica a Eclipse como la mejor opción en IDE para el desarrollo de aplicaciones Android.

3. Conclusiones

- La metodología está diseñada para aplicarse en la fase de desarrollo de software, y esta debe ser ejecutada por el programador de las aplicaciones móviles.
- Una de las practicas más importantes señaladas en la fase 1 de la implementación de la metodología se establece que se debe conocer para que sistema operativo se desarrollará la aplicación móvil, el lenguaje a utilizar y el tipo de aplicación. Esto bridará un enfoque de los posibles IDE a evaluar y compara para la su selección.

- El estándar ISO 9126 brinda parámetros que se utiliza como guía para la evaluación y medición de la calidad de un producto de software, las mismas se sirven de base durante el ciclo de vida del software.

Referencias

El Tiempo. (14 de noviembre de 2014). *El Tiempo*. Recuperado el 17 de enero de 2018, de http://www.eltiempo.com/archivo/documento/CMS-14879418

Garita Araya, R. A. (3 de julio de 2013). *e-Ciencias de la Información*. Recuperado el 16 de enero de 2018, de http://www.redalyc.org/articulo.oa?id=476848738003

Gutiérres, Ó. (18 de agosto de 2016). *CNET*. Recuperado el 16 de enero de 2018, de https://www.cnet.com/es/noticias/android-market-share-abril-junio-android-vs-ios-mercado-2016/

Morales Reyes, Y., Gómez Yopasa, J. D., & Camargo Vega, J. J. (mayo - agosto de 2016). *Revista Virtual Universidad Católica del Norte*. Recuperado el 17 de enero de 2018, de http://www.redalyc.org/pdf/1942/194245902018.pdf

Otero Escobar, A. D., Martinez Castillo, J., & Diaz Camacho, J. E. (15 de abril de 2016). *Revista de Transformación Educativa*. Recuperado el 17 de enero de 2018, de http://murueta.mx/attachments/article/61/RETE%20-%20tem%C3%A1tico%20Educaci%C3%B3n%20mediada%20por%20Tecnolog%C3%ADa.pdf

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 19/12/2017
Aceitação/Acceptance: 24/03/2018

Selección de configuraciones de despliegue usando Sistemas de Recomendación en Android

Jorge L. Rodas[1], José A. Galindo[2], David Benavides[2], Robert Soriano[3]

jorge.rodass@gmail.com, {jagalindo, benavides}@us.es, rsoriano@nexcol.com.ec
email_autor_uno@xyz.pt, email_autor_dos@xpto.pt, ...

[1] Facultad de Ciencias de la Ingeniería, Universidad Estatal de Milagro, Cdla. Universitaria Km 1 ½ vía Km 26, Milagro, Ecuador.

[2] Escuela Superior de Ingeniería Informática, Universidad de Sevilla, Av. De Reina Mercedes s/n, Sevilla, España.

[3] Departamento de Tecnologías de Información, Nexcol S.A., Av. Francisco de Orellana – World Trade Center, Guayaquil, Ecuador.

Pages: 221–233

Resumen: Los sistemas de alta variabilidad son sistemas de software que describen una gran cantidad de configuraciones. Gestionar la variabilidad en estos sistemas es costoso y a menudo difícil por la cantidad de configuraciones que pueden derivarse. Para un desarrollador de software seleccionar la plataforma de despliegue para un producto es una actividad compleja de resolver. Para mitigar este problema investigaciones proponen el uso de técnicas automatizadas; sin embargo, hemos detectado que la información empleada en la mayoría de estas propuestas no se actualiza constantemente. Por esta razón, proponemos el uso de información extraída de informes de usuarios que es explotada mediante un sistema de recomendación que emplea algoritmos de filtrado colaborativo. En este trabajo presentamos RESDEC, una propuesta diseñada para guiar al ingeniero de software la selección y priorización de configuraciones de despliegue en sistemas de alta variabilidad. La propuesta se valida con un dataset que contiene información de dispositivos y aplicaciones móviles que se ejecutan en Android.

Palabras-clave: sistemas de recomendación, variabilidad, Android

Selection of Deployment Configurations using Recommender Systems on Android

Abstract: Variability intensive systems are software systems that describe a large number of configurations. Managing variability in these systems is expensive and often difficult because of the number of configurations that can be derived. For a software developer selecting the deployment platform for a product is a complex activity to solve. To mitigate this problem, research proposes the use of automated techniques; however, we have detected that the information used in most of these proposals is not constantly updated. For this reason, we propose the use of information extracted from user reports that is exploited through a

recommendation system that uses collaborative filtering algorithms. In this paper we present RESDEC, a proposal designed to guide the software engineer in the selection and prioritization of deployment configurations in variability intensive systems. The proposal is validated with a dataset that contains information about mobile devices and applications that run on Android.

***Keywords**:* Recommender systems, variability, Android.

1. Introducción

Los sistemas de alta variabilidad son sistemas de software cuyo comportamiento puede ser personalizado de acuerdo a las necesidades específicas de un contexto particular (Babar, Lianping Chen, & Shull, 2010). Esta personalización se materializa a través de un conjunto bien definido de puntos de variación, cada uno de los cuales captura una posibilidad de personalización que el sistema permite.

Cuando un ingeniero de software toma una decisión para todos y cada uno de los puntos de variación, se dice que define una configuración. Para representar la variabilidad existente en un sistema de alta variabilidad se emplean modelos de características. En la industria, podemos encontrar varios ejemplos de modelos que representan la variabilidad en entornos reales, como el caso de los dispositivos móviles en Android (Galindo, Turner, Benavides, & White, 2016), Linux Kernel (She, Lotufo, Berger, Wasowski, & Czarnecki, 2010) o los sistemas de gestión de precios en la nube (García-Galán, Rana, Trinidad, & Ruiz-Cortés, 2013).

En los casos citados anteriormente, hay cientos de configuraciones diferentes que complican el proceso de aseguramiento de la calidad y su gestión. Por ejemplo, para garantizar la calidad de un sistema en producción es deseable que el despliegue o ejecución (Dearle, 2007) se realice sobre configuraciones que han sido probadas previamente. Esto, en la práctica, es muy difícil realizarlo de manera manual debido al gran número de configuraciones que se derivan de un modelo. Para mitigar este problema, aparece como alternativa el análisis automatizado de modelos de características (AAFM) (Benavides, Segura, & Ruiz-Cortés, 2010). El AAFM ayuda al ingeniero de software en el manejo de configuraciones mediante algoritmos de búsqueda o programación con restricciones. Sin embargo, a pesar del uso de recursos de computación, el manejar cientos de configuraciones hace que el proceso sea lento y genere altos costos.

En el ecosistema Android podemos encontrar 224 combinaciones de configuraciones válidas (Galindo et al., 2016). La alta demanda de dispositivos Android (Forni & Vander, 2016) ha hecho que seleccionar las plataformas sobre la cuales desplegar una aplicación sea una tarea difícil para el ingeniero de software.

Para contrarrestar este problema, investigaciones sugieren que antes de desplegar un producto, primero debe ser probado sobre un conjunto limitado de configuraciones. Dichas configuraciones deben seleccionarse (Rothermel & Harrold, 1997) y priorizarse (Srikanth, Williams, & Osborne, 2005) de acuerdo a algún criterio que maximice la tasa de beneficios para la empresa y defina aquellas configuraciones que resulten "más importantes" en el cual desplegar un producto.

En este contexto, hemos encontrado en los informes de usuarios información que puede ser explotada mediante técnicas de análisis automatizado. Por un lado, podemos confiar en soluciones basadas en CSP (Galindo et al., 2016), filtrando configuraciones no óptimas. Sin embargo, los sistemas de recomendación aparecen como una alternativa ideal para recolectar información presente en los informes de usuarios para estructurarlos en una base de conocimiento dinámica que pueda ser procesada en cualquier instante del tiempo y guie al ingeniero de software de manera personalizada en la búsqueda de configuraciones óptimas para el despliegue de sus productos.

En este artículo proponemos RESDEC, una solución basada en sistemas de recomendación para la selección de configuraciones de despliegue para un producto de software, el mismo que se encuentra estructurado de la siguiente manera: La sección 2 muestra algunos antecedentes para comprender el alcance de la propuesta. La sección 3, describe los escenarios de implementación y los algoritmos de recomendación utilizados en la propuesta. En la sección 4 presentamos el diseño, arquitectura, implementación y los datos empleados en RESDEC para su validación. Finalmente en la sección 6 se concluye el trabajo.

2. Preliminares

2.1. Análisis automatizado de Modelos de Características

Existen más de 30 operaciones de análisis usando modelos de características (Benavides et al., 2010). No obstante nuevas aplicaciones del mismo están siendo usadas en entorno de pruebas, configuración, entre otros.

La selección de configuraciones en sistemas de alta variabilidad representa un gran reto para el ingeniero encargado del aseguramiento de la calidad del software. Para sobrellevar el proceso de selección de configuraciones, investigaciones proponen el uso de pruebas de interacción combinatoria (Nie & Leung, 2011) que explora las características comunes de un producto para reducir el costo incurrido al realizar las pruebas. Una de estas propuestas proponen el uso de técnicas t-wise para obtener un conjunto de configuraciones que necesitan ser probadas dentro de un subconjunto de todas las configuraciones (Perrouin et al., 2012).

Se ha comprobado que las pruebas combinatorias producen buenos resultados en estudios empíricos, principalmente porque los puntos de interacción entre los productos de software han sido probados como fuentes clave de errores (Cohen, Dwyer, & Jiangfan Shi, 2008). Sin embargo, aun hay espacio para la mejora para reducir el costo de las pruebas mientras se maximiza su valor.

2.2. Sistemas de Recomendación

Un sistema de recomendación se define como un sistema inteligente que proporciona a los usuarios una serie de sugerencias de forma personalizada de acuerdo a los gustos o preferencias sobre algún producto o servicio. Los sistemas de recomendación nacen en la década de 1990 (Goldberg, Nichols, Oki, & Terry, 1992) y desde de esa fecha han crecido enormemente en términos de desarrollo algorítmico, así como en aplicaciones implementadas.

En el mercado existen experiencias practicas exitosas de la implementación de los métodos de recomendación en contextos de comercio electrónico, como los casos de Amazon (Linden, Smith, & York, 2003) y Netflix (Tuzhilin, Koren, Bennett, Elkan, & Lemire, 2008). En un contexto diferente, los sistemas de recomendación son utilizados además para la clasificación de imágenes médicas en el diagnóstico de enfermedades. Todo este panorama, pone de relieve la importancia de los sistemas de recomendación en el estado actual de las cosas abriendo espacio al desarrollo de herramientas en nuevos campos de aplicación. En (Jesus Bobadilla, Hernando, Ortega, & Bernal, 2011)an increasing need arises to develop some kind of evaluation framework for collaborative filtering measures and methods which is capable of not only testing the prediction and recommendation results, but also of other purposes which until now were considered secondary, such as novelty in the recommendations and the users\u2019 trust in these. This paper provides: (a y (J. Bobadilla, Ortega, Hernando, & Gutiérrez, 2013) se describen en detalle varias aplicaciones que emplean sistemas de recomendación.

La literatura (Adomavicius & Tuzhilin, 2005) divide a los sistemas de recomendación en dos grupos: sistemas basados en filtrado colaborativo y sistemas basados en filtrado por contenido. Los sistemas basados en filtrado colaborativo (Konstan et al., 1997), (Linden et al., 2003) se basan en el concepto de análisis de perfiles de usuarios, en donde las recomendaciones se generan de acuerdo a los gustos de usuarios con preferencias similares. Por otro lado, los sistemas basados en filtrado por contenido (Pazzani & Billsus, 1997) son aquellos en el cual la recomendación de un ítem o producto se genera a partir de la descripción de sus características y el perfil de intereses de los usuarios. El uso de este tipo de sistemas está enmarcado en una variedad de dominios que van desde la recomendación de sitios web, viajes, restaurantes, series de TV, artículos de venta, entre otros.

A pesar de los grandes avances tecnológicos de los sistemas de recomendación, pocas son las propuestas encaminadas a la mejora continua en el campo de la ingeniería de software, abriendo un mundo de posibilidades para introducir el concepto de sistemas de recomendación en esta área.

3. Descripción de la Propuesta

En esta sección presentamos RESDEC (REcommender system for Selecting DEployment Configurations), una propuesta basada en sistemas de recomendación

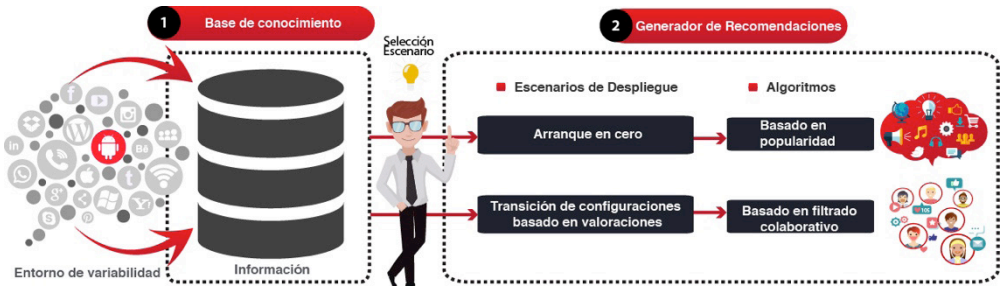


Figura 1 – Componentes de RESDEC

que fue diseñada para ayudar al ingeniero de software en la selección y priorización del entorno de despliegue para sus productos de software antes de ser enviados a producción. RESDEC fue construido sobre la base del backend de TESALIA (Galindo et al., 2016) y es actualmente compatible con el ecosistema FaMa (Benavides, Segura, Trinidad, & Ruiz-Cortés, 2007). La solución consta de dos componentes: 1) Base de Conocimiento y 2) Generador de Recomendaciones. La figura 1 ilustra los componentes que integra RESDEC.

3.1. Base de Conocimiento

La base de conocimiento representa el eje principal de nuestra propuesta y se construye a partir de los valores que recogen los informes de usuarios.

En nuestra solución hemos usado los componentes de un sistema de recomendación común: 1) usuarios, 2) ítems y 3) puntuaciones, de la siguiente manera: los usuarios están representados por los productos *p* que serán desplegados, los ítems por las configuraciones de despliegues *d* que se recomendarán y las valoraciones v por los valores que aparecen en un informe de usuario. La base de conocimiento se construye a partir de los informes de usuarios y da origen a la matriz $M1 \in M(m,n,\mathbb{R})$, de órdenes diferentes que contienen la información necesaria para llevar a cabo el proceso de recomendación.

La matriz M1 relaciona m configuraciones de despliegue $(d_1,d_2,d_3,...,d_m)$ con *n* productos $(p_1,p_2,p_3,...,p_n)$, dónde las celdas contienen números reales determinados por una función, en este caso por el valor promedio $\bar{x}$ de las valoraciones emitidas por un conjunto de usuarios que han usado los productos *p* sobre las configuraciones *d*. Estos valores podrían representar criterios de los usuarios en relación a gustos, funcionalidad, errores o desperfectos que un producto pudiera tener al ser desplegado en un ecosistema en particular. En nuestro caso, estos valores reflejan los niveles de funcionalidad que podría tener un producto p_i en una configuración de despliegue d_j a partir de un valor entre 1 y 5.

La figura 2 muestra la representación gráfica de la matriz *M1*.

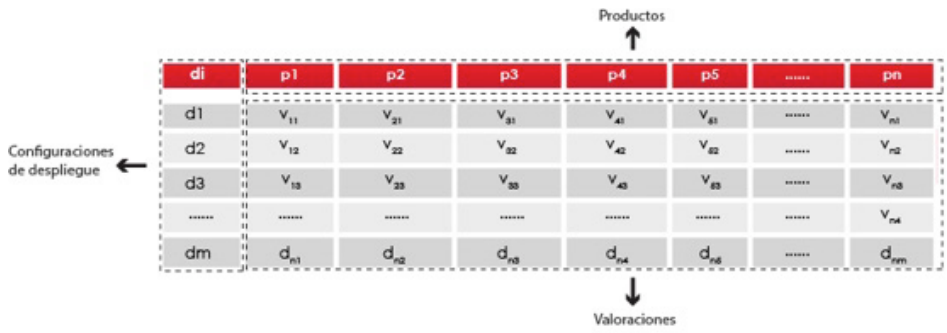


Figura 2 – Elementos de la matriz *M1*

3.2. Generador de Recomendaciones

Dependiendo de las necesidades específicas del ingeniero de software, hemos identificado dos escenarios donde se puede utilizar información dinámica generada a partir de informes de usuario para definir la estrategia de despliegue de un producto.

Arranque en cero.- El primer escenario se presenta cuando hay un usuario nuevo y desea conocer que configuraciones de despliegue serían las más opcionadas para poner en ejecución un producto de software. Esto ocurre por ejemplo, cuando el ingeniero de software diseña una nueva aplicación y desconoce en qué dispositivos móviles sería más óptimo instalarlo, para ello, el sistema hace la recomendación considerando los dispositivos móviles más populares en donde otras aplicaciones han sido desplegadas con éxito.

Para realizar recomendaciones en este escenario hemos empleado un algoritmo basado en popularidad (1). Cuando se usa un algoritmo basado en popularidad, el sistema toma la matriz *M1* y prioriza configuraciones basado en la mayor cantidad de interacciones que una configuración *d* ha tenido con los productos *p*. Una vez priorizada la información, recomienda las configuraciones *d* por orden de popularidad, dando exactamente el mismo ranking a cada uno de los productos *p*.

$$f(p,d) = \{r(v,d) \neq \emptyset \,|\, v \in U\} \tag{1}$$

Transición de configuraciones basadas en valoraciones.- El segundo escenario se presenta cuando el usuario ha usado previamente una configuración de despliegue para un producto y basado en esa experiencia quiere explorar otras configuraciones para obtener nuevas alternativas de recomendación. Esto ocurre, por ejemplo, cuando el ingeniero de software ha implementado una aplicación en un dispositivo móvil y desea conocer en qué otros dispositivos podría también instalarse, para ello, el sistema considera las aplicaciones más similares a la aplicación instalada y las valoraciones que han recibido dichos dispositivos.

Como alternativa de solución hemos integrado en RESDEC el algoritmo *Item – basedCollaborativeFiltering* (Melville & Sindhwani, 2011), en el cual en lugar de encontrar productos *p* similares, el algoritmo se centra en la similaridad entre configuraciones *d*. En nuestro trabajo el algoritmo toma la matriz *M1* y establece la similaridad entre las configuraciones *d* que ha usado un producto *p* y los compara con configuraciones similares. Para encontrar la similaridad entre dos configuraciones *i* y *j* utilizando el algoritmo *Item – basedCollaborativeFiltering* usamos el coeficiente de correlación de Pearson tal y como se describe en (2):

$$s_{i,j} = \frac{\sum_{u \in U}(v_{u,i} - \bar{v}_i)(v_{u,j} - \bar{v}_j)}{\sqrt{\sum_{u \in U}(v_{u,i} - \bar{v}_i)^2}\sqrt{\sum_{u \in U}(v_{u,j} - \bar{v}_j)^2}} \tag{2}$$

Donde U es el conjunto de todos los productos que han valorado tanto las configuraciones i como j, $v_{u,i}$ es la valoración del producto u en la configuración i, y $\bar{v}_i$ es la valoración promedio de las configuraciones i entre los productos.

Establecida la similaridad entre las configuraciones, en (3) usando un promedio de ponderación simple, el algoritmo predice la valoración para una configuración *i* por parte de un producto *a*.

$$f_{a,p} = \frac{\sum_{j \in K} r_{a,j} w_{i,j}}{\sum_{j \in K} |w_{i,j}} \quad (3)$$

Donde $f_{a,p}$ es la predicción para la configuración *d* por parte del producto activo *a*, $w_{i,j}$ es la similitud entre las configuraciones *i* y *j*, y *K* representa el conjunto de las *k* configuraciones valorados por el producto *a* que son más similares a *i*.

4. Aplicación Web y Resultados Preliminares

En esta sección, presentamos el experimento llevado a cabo para evaluar nuestra propuesta. La sección se divide en dos partes, la primera presenta una visión general sobre el diseño y arquitectura de la herramienta web RESDEC y la segunda describe los mecanismos empleados para evaluar la solución.

4.1. Diseño de RESDEC

RESDEC [1] (https://github.com/RESDEC) es una aplicación web diseñada en Java que usa como motor de base de datos MySql y está organizada en tres módulos para permitir la recomendación de las plataformas de despliegue.

El primer módulo *Usuario* que permite el registro de los usuarios del sistema que pueden obtener las recomendaciones de los entornos de despliegue.

El segundo módulo *Entorno de despliegue* que alimenta el sistema con la información necesaria para establecer nuevas recomendaciones, el cual varía en función del entorno en el que se utilice el sistema; y finalmente, el módulo *Recomendaciones* , que ejecuta el algoritmo de recomendación apropiado.

4.2. Arquitectura

La arquitectura RESDEC se compone de dos partes, como se muestra en la Figura 3: El servidor de aplicaciones y la interfaz de usuario.

El *servidor de aplicaciones* está conformado por el servidor GlassFish 4.1 el cual contiene un conjunto de vistas, creadas en Java Server Faces 2.1[2] , el cual usa como framework PrimeFaces[3], empleadas para el diseño de la interfaz gráfica; el controlador Faces Servlets encargado de administrar el ciclo de vida de los JSF; una capa de instrumentación en Managed Beans[4] el cual contiene todos los atributos, métodos y propiedades de las entidades del sistema y con los cuales interactúan los JSF; y finalmente el servidor de datos MySql el cual almacena la información que procesa el sistema en DBKnowledge. La

[1] RESDEC Website: http://www.resdec.com
[2] JSF website: http://www.oracle.com/technetwork/java/javaee/overview-140548. html
[3] PrimeFaces website: https://www.primefaces.org/
[4] MBeans website: http://javabeat.net/jsf-2-managed-beans/

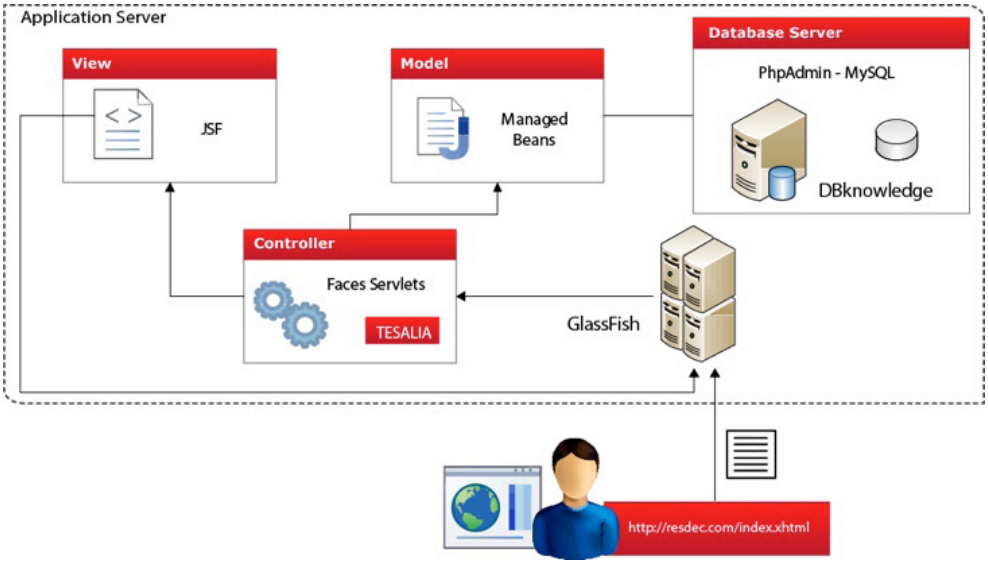


Figura 3 – Arquitectura de RESDEC

interfaz de usuario es la capa de presentación que permite la comunicación bidireccional entre el usuario y el sistema a través de un navegador web.

4.3. Dataset y Validación

Dataset de dispositivos móviles de Android: Para recolectar la información almacenada en el dataset de Android, se realizó una encuesta a 2,099 usuarios de la comunidad estudiantil y docente de la Universidad Estatal de Milagro, Ecuador[5]. La población comprende usuarios con edades entre 17 y 56 años de edad, de los cuales el 72% fueron de género femenino y el 28% del género masculino; de estos dos grupos, el 16% corresponden al área de ingeniería y tecnología, el 23% a administración, el 28% salud, el 12% educación, el 4% turismo, el 2% idiomas y el 15% a áreas de diseño gráfico, psicología y comunicación social.

Esta encuesta nos permitió conocer que aplicaciones son las más utilizadas por los usuarios, los dispositivos que poseen, el comportamiento de las aplicaciones en sus dispositivos y las valoraciones que se les asignan. El cuestionario se puede encontrar en el sitio web de RESDEC. Después de recopilar los datos para este dataset, estructuramos la información para la matriz *M1*, la cual establece la relación entre las aplicaciones, dispositivos y valoraciones.

Resultados.- Finalmente, la información fue registrada en la base de datos DBKnowledge. Las pruebas finales involucraron la generación automática de recomendaciones de entre un conjunto de datos de 832 dispositivos móviles que fueron puestas a prueba en el departamento de Tecnologías de la Información y de la Comunicación de la Universidad Estatal de Milagro para seleccionar los entornos de

[5] UNEMI website: http://www.unemi.edu.ec

despliegue en los cuales se podría implementar la versión móvil del Sistema de Gestión Académico UNEMI (SGA UNEMI)[6].

5. Trabajo Relacionado

A continuación revisamos algunos trabajos que se relacionan directamente con nuestra propuesta.

Sistemas de recomendación de características.- (Mazo, Dumitrescu, Salinesi, & Diaz, 2014) presentan una propuesta en el cual mediante el uso de una colección de heurísticas y utilizando programación con restricciones, priorizan configuraciones para acelerar el proceso de configuración de un producto y evitar errores a los cuales están expuestos.

No obstante, la propuesta se basa en el uso de heurísticas que no tienen en cuenta las preferencias de los usuarios, lo cual podría llevar al usuario a configurar productos que no satisfacería sus requerimientos.

Sistemas de recomendación de productos.- (Martinez et al., 2015) proponen el uso de un algoritmo genético interactivo para predecir configuraciones idóneas. La propuesta pone a los usuarios a evaluar un conjunto de configuraciones de un producto utilizando una escala del 1 al 5 (1=malo, 5=bueno) a partir del cual se construye un dataset que es explotado usando técnicas de minería de datos.

Si bien es cierto que la propuesta contiene todos los elementos que necesita un sistema de recomendación (usuarios, productos y valor), los algoritmos genéticos empleados no se benefician de la información de las características de las configuraciones para hacer las recomendaciones, de hecho, el usuario no valora las características sino configuraciones.

Sistemas de recomendación personalizados.- (Pereira et al., 2016) nos presentan una propuesta en la cual se usa como elemento importante del sistema de recomendación al usuario, siendo la primera propuesta en la que no se excluye en su totalidad a los usuarios.

Sin embargo, los datos que procesa el sistema no provienen de un contexto donde el usuario sea quien lo retroalimente; es decir, las configuraciones que se usan para establecer la similitud no tienen una variable que determine si esa configuración ha sido evaluada de forma positiva o negativa por el usuario que hizo uso de la misma en el pasado. Siendo las opiniones o valoraciones de los usuarios una de las bases principales para establecer las recomendaciones.

6. Conclusiones y Trabajo Futuro

En este artículo, se ha presentado un enfoque diferente para la selección de configuraciones en sistemas de alta variabilidad. El uso de sistemas de recomendación integrado con herramientas de análisis automatizado, es uno de los aportes nuevos de esta investigación en la industria de la ingeniería de software. A futuro nuestro trabajo pretende abordar los siguientes temas:

[6] UNEMI SGA website: https://sga.unemi.edu.ec

a. Explorar algoritmos basados en filtrado por contenido para establecer recomendaciones basadas no sólo en valoraciones sino en las características de las configuraciones de un producto.
b. Extender las utilidades de la herramienta RESDEC incorporando diversos algoritmos de filtrado colaborativo y filtrado por contenido.
c. Evaluar los resultados que procesa el sistema mediante el uso de técnicas y procedimientos que se usan en la evaluación de sistemas de recomendación.

Referencias

Adomavicius, G., & Tuzhilin, A. (2005). Toward the next generation of recommender systems: a survey of the state-of-the-art and possible extensions. *IEEE Transactions on Knowledge and Data Engineering*, *17*(6), 734–749. https://doi.org/10.1109/TKDE.2005.99

Babar, M. A., Lianping Chen, & Shull, F. (2010). Managing Variability in Software Product Lines. *IEEE Software*, *27*(3), 89–91, 94. https://doi.org/10.1109/MS.2010.77

Benavides, D., Segura, S., & Ruiz-Cortés, A. (2010). Automated analysis of feature models 20 years later: A literature review. *Information Systems*, *35*(6), 615–636. https://doi.org/10.1016/J.IS.2010.01.001

Benavides, D., Segura, S., Trinidad, P., & Ruiz-Cortés, A. (2007). Fama: Tooling a Framework for the Automated Analysis of Feature Models. *VaMoS*. Retrieved from https://idus.us.es/xmlui/handle/11441/26357

Bobadilla, J., Hernando, A., Ortega, F., & Bernal, J. (2011). A framework for collaborative filtering recommender systems. *Expert Systems with Applications*, *38*(12), 14609–14623. https://doi.org/10.1016/J.ESWA.2011.05.021

Bobadilla, J., Ortega, F., Hernando, A., & Gutiérrez, A. (2013). Recommender systems survey. *Knowledge-Based Systems*, *46*, 109–132. https://doi.org/10.1016/J.KNOSYS.2013.03.012

Cohen, M. B., Dwyer, M. B., & Jiangfan Shi. (2008). Constructing Interaction Test Suites for Highly-Configurable Systems in the Presence of Constraints: A Greedy Approach. *IEEE Transactions on Software Engineering*, *34*(5), 633–650. https://doi.org/10.1109/TSE.2008.50

Dearle, A. (2007). Software Deployment, Past, Present and Future. In *Future of Software Engineering (FOSE '07)* (pp. 269–284). IEEE. https://doi.org/10.1109/FOSE.2007.20

Forni, A., & Vander, R. (2016). Gartner Says Five of Top 10 Worldwide Mobile Phone Vendors Increased Sales in Second Quarter of 2016. Retrieved March 13, 2018, from https://www.gartner.com/newsroom/id/3415117

Galindo, J. A., Turner, H., Benavides, D., & White, J. (2016). Testing variability-intensive systems using automated analysis: an application to Android. *Software Quality Journal*, *24*(2), 365–405. https://doi.org/10.1007/s11219-014-9258-y

García-Galán, J., Rana, O., Trinidad, P., & Ruiz-Cortés, A. (2013). Migrating to the Cloud - A Software Product Line based Analysis. In *Proceedings of the 3rd International Conference on Cloud Computing and Services Science* (pp. 416–426). SciTePress - Science and and Technology Publications. https://doi.org/10.5220/0004357104160426

Goldberg, D., Nichols, D., Oki, B. M., & Terry, D. (1992). Using collaborative filtering to weave an information tapestry. *Communications of the ACM*, *35*(12), 61–70. https://doi.org/10.1145/138859.138867

Konstan, J. A., Miller, B. N., Maltz, D., Herlocker, J. L., Gordon, L. R., & Riedl, J. (1997). GroupLens: applying collaborative filtering to Usenet news. *Communications of the ACM*, *40*(3), 77–87. https://doi.org/10.1145/245108.245126

Linden, G., Smith, B., & York, J. (2003). Amazon. com recommendations: Item-to-item collaborative filtering. *IEEE Internet Computing*. Retrieved from http://ieeexplore.ieee.org/abstract/document/1167344/

Martinez, J., Rossi, G., Ziadi, T., Bissyandé, T. F. D. A., Klein, J., & Le Traon, Y. (2015). Estimating and Predicting Average Likability on Computer-Generated Artwork Variants. In *Proceedings of the Companion Publication of the 2015 on Genetic and Evolutionary Computation Conference - GECCO Companion '15* (pp. 1431–1432). New York, New York, USA: ACM Press. https://doi.org/10.1145/2739482.2764681

Mazo, R., Dumitrescu, C., Salinesi, C., & Diaz, D. (2014). Recommendation Heuristics for Improving Product Line Configuration Processes, 511–537. https://doi.org/10.1007/978-3-642-45135-5_19

Melville, P., & Sindhwani, V. (2011). Recommender Systems. In *Encyclopedia of Machine Learning* (pp. 829–838). Boston, MA: Springer US. https://doi.org/10.1007/978-0-387-30164-8_705

Nie, C., & Leung, H. (2011). A survey of combinatorial testing. *ACM Computing Surveys*, *43*(2), 1–29. https://doi.org/10.1145/1883612.1883618

Pazzani, M., & Billsus, D. (1997). Learning and Revising User Profiles: The Identification of Interesting Web Sites. *Machine Learning*, *27*(3), 313–331. https://doi.org/10.1023/A:1007369909943

Pereira, J. A., Matuszyk, P., Krieter, S., Spiliopoulou, M., Saake, G., Pereira, J. A., … Saake, G. (2016). A feature-based personalized recommender system for product-line configuration. *ACM SIGPLAN Notices*, *52*(3), 120–131. https://doi.org/10.1145/3093335.2993249

Perrouin, G., Oster, S., Sen, S., Klein, J., Baudry, B., & le Traon, Y. (2012). Pairwise testing for software product lines: comparison of two approaches. *Software Quality Journal*, *20*(3–4), 605–643. https://doi.org/10.1007/s11219-011-9160-9

Rothermel, G., & Harrold, M. J. (1997). A safe, efficient regression test selection technique. *ACM Transactions on Software Engineering and Methodology*, *6*(2), 173–210. https://doi.org/10.1145/248233.248262

She, S., Lotufo, R., Berger, T., Wasowski, A., & Czarnecki, K. (2010). The Variability Model of The Linux Kernel. *VaMoS*. Retrieved from https://www.researchgate.net/profile/Andrzej_Wasowski/publication/220789837_Evolution_of_the_Linux_Kernel_Variability_Model/links/54ccb7f10cf298d6565ac185.pdf

Srikanth, H., Williams, L., & Osborne, J. (2005). System test case prioritization of new and regression test cases. In *International Symposium on Empirical Software Engineering, 2005*. (pp. 62–71). IEEE. https://doi.org/10.1109/ISESE.2005.1541815

Tuzhilin, A., Koren, Y., Bennett, J., Elkan, C., & Lemire, D. (2008). Large-scale recommender systems and the netflix prize competition. *In KDD Proceedings*. Retrieved from http://www.exercicescorriges.com/i_337810.pdf

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 12/12/2017
Aceitação/Acceptance: 31/03/2018

Desarrollo de un framework metodológico para la innovación educativa en el contexto de la acción tutorial basado en metodologías ágiles y estándares de conocimiento de ingeniería de software.

Fernanda Maricela Soto-Guerrero[1], Pablo Alejandro Quezada–Sarmiento[2-3], Lorena del Cisne Condolo–Herrera[1], Diego Israel Moreno–León[1], Israel Leonardo Rey- Mendoza[1]

fmsoto@utpl.edu.ec, paquezadasa@uide.edu.ec, paquesar@alumni.uv.es ldcondolo@utpl.edu.ec, santiago.mengual@uv.es, dimoreno@utpl.edu.ec, iarey@utpl.edu.ec

[1] Universidad Tecnica Particular de Loja, Departamento de Ciencias de la Computación y Electrónica, Loja Ecuador, 1101608

[2] Universidad Internacional del Ecuador, Docente Investigador Escuela de Informática y Multimedia-Titulación de Ingeniería en Tecnologías de la Información, Consejo de Investigación; Av. Simón Bolívar y Av. Jorge Fernández, Quito, Ecuador.

[3] Universitat de Valencia, Doctorando Programa de Doctorado en Educación, Facultad de Filosofía y Ciencias de la Educación, Av. Blasco Ibáñez 30, 46010 València, España

Pages: 233–242

Resumen: La acción tutorial es un recurso de aprendizaje indispensable en un entorno de educación superior, cuyo objetivo es ofrecer a los estudiantes apoyo en el progreso académico, además de ser un componente fundamental de la acción educativa. En el caso de la Universidad Técnica de Loja a pesar de haber definido un proceso para la acción tutorial, esto ha sido deficiente debido a la falta de asistencia y poco interés de los alumnos, sin descuidar también la falta de motivación por parte de los docentes. En apoyo de la mejora del proceso tutorial, se propone un nuevo modelo que permitirá una mejor interacción tutorial entre el alumno y el profesor, apoyado por TIC, a través del uso de una aplicación móvil que promueve la tutoría, que organiza mejor el tiempo de aprendizaje de los participantes y registra las dudas de los estudiantes. La presente aplicación híbrida que presentamos y que está disponible para sistemas operativos móviles Android e iOS se implementó en base a la metodología ágil de desarrollo de Scrum y al estándar de conocimiento en el contexto de la ingeniería.

Palabras-clave: Acción tutorial; Tutorías; Tecnologías de la información y comunicación; Aplicación móvil, Scrum.

Development of a methodological framework for educational innovation in the context of the tutorial action based on agile methodologies and software engineering knowledge standards.

Abstract: The tutorial action is an indispensable learning resource in a higher education environment, which goal is to offer the students support in academic progress, as well as being a fundamental component of the educational action. In the case of the Technical University of Loja despite of having defined a process for the tutorial action, this has been deficient due to the lack of assistance and low interest of the students, without neglecting also the lack of motivation from the teachers. In support of the improvement of the tutorial process, a new model is proposed which will allow a better tutorial interaction between the student and the teacher, supported by TIC, through the use of a mobile application that promotes tutoring, that better organizes the learning time of the participants and records the students doubts. The present hybrid application that we present and that is available for Android and iOS mobile operating systems was implemented based on the agile Scrum development methodology and knowledge standard in engineering context.

Keywords: Tutorial action; Tutorials; Information and communication technologies; Mobile application; Scrum.

1. Introducción

La innovación de la calidad de la enseñanza y el aprendizaje en las Universidades se ha convertido en algo primordial y aunque es difícil realizar cambios en una institución, se debe tomar en cuenta que si no hay cambios no se puede avanzar en el conocimiento (Alarcón, Fernández, Mahillo & Álvarez,2014). Es por esto que las instituciones están obligadas a dar respuesta a las necesidades de su entorno, no solo por cubrir necesidades básicas sino también por el acelerado cambio económico, social y tecnológico, que demandan una nueva forma de ver la educación y que a la vez afecta a la institución y a sus procesos de aprendizaje (Quezada &Mengual, 2017).

Ahora bien, un punto de atención en los métodos de innovación en la educación superior, se encuentran los modelos de acción tutorial, debido a que es un elemento relacionado con el aprendizaje y la formación académica. Hay que mencionar, además que dentro de la innovación educativa la acción tutorial se ha convertido en un aspecto elemental y más aún en el entorno de la Universidad Técnica Particular de Loja (UTPL), debido a los compromisos que tiene con respecto a la formación de profesionales y a las estrategias para atender a las necesidades de los estudiantes.

La UTPL años atrás estableció un proceso de acción tutorial que desempeña como guía para la actividad tutorial, así como para el control de la misma y que se caracteriza por procurar la atención de aspectos académicos de los estudiantes universitarios, sin embargo, este primer proceso no cumple con una integración a las Tecnologías de la Información y Comunicación (TIC) y a la vez a la innovación educativa. Para desarrollar apropiadamente esta actividad la UTPL diseñó su nuevo proceso con su propia plataforma para la acción tutorial denominada Sistema de Seguimiento y Control a Clases y Tutorías (Sistema Qr) a partir de las necesidades de los docentes, sin embargo, esta plataforma solo permite el acceso a los docentes para un programa semanal de tutorías con horarios preestablecidos.

Con estos antecedentes el presente artículo plantea un análisis; que, partiendo de los procesos actuales de la acción tutorial, se realicen mejoras a fin de presentar el diseño de un modelo metodológico específico para la acción tutorial de la UTPL con el propósito de mejorar la calidad de las tutorías. Este modelo metodológico seguirá la normativa señalada por el Vicerrectorado Académico de la UTPL, pero añadirá aspectos específicos y peculiares del proceso de enseñanza y aprendizaje. Como apoyo a la innovación del proceso se propone la sistematización del modelo mediante la implementación de una herramienta móvil de uso masivo, siguiendo la metodología de desarrollo ágil Scrum y los principios de ingeniería de software y conocimiento BOK (Quezada, Garbajosa & Enciso, 2016), (Quezada, Enciso & Garbajosa, 2015), (Quezada, Garbajosa, Washizaki & Enciso, 2016).

2. Trabajos Relacionados

En la presente sección se presentan algunas propuestas relacionadas a la acción tutorial en el contexto Educativo.

Proyecto La Hora TutHora.- Según (Santos, Adrada , Montes & Castedo,2012) en la Universidad Politécnica de Madrid (UPM), para mejorar el rendimiento en la acción tutorial, por la preocupación sobre la baja utilización de las tutorías, desde el curso 2010/2011 se puso en marcha un proyecto denominado "La Hora TutHora", con el propósito de introducir nuevas metodologías docentes y la aplicación de las TIC en la enseñanza, una herramienta de ordenación académica para incrementar la acción tutorial en la Escuela Universitaria de Ingeniería Técnica Industrial de la UPM.

Proyecto VIRTICS. - En la Universidad Rovira i Virgili (URV), se realizó la implantación de un programa piloto de tutoría virtual, para profesionales de enfermería noveles, en la que se destaca su importancia para poder responder a la necesidad de apoyo y soporte emocional. Basándose en experiencias, URV parte de "La necesidad de apoyo al proceso de inserción laboral de los profesionales de enfermería" (Fortuño, Cervera, Molías, Vidal, Martínez & Riobóo, 2013).

Proyecto TutorialAction. -La Universidad Politécnica de Madrid, presenta una herramienta software orientada a potenciar y facilitar la asistencia a tutorías, como modo de mejorar el servicio ofrecido a los estudiantes del Grado en Ingeniería del Software, la misma que permite a los estudiantes realizar una reserva automatizada de tutorías presenciales con sus docentes, y a los docentes les posibilita realizar el registro de los temas tratados en cada sesión.

3. Metodologia

Según los creadores de Scrum; es un marco de trabajo para el desarrollo, un método de gestión de proyectos que se adapta a cualquier tipo de proyecto y está basada en un enfoque iterativo e incremental y de revisiones continuas. Scrum es una metodología ágil, orientada a la gestión de proyectos, en el que se puede utilizar varios procesos y técnicas, "El marco de trabajo Scrum consiste en los Equipos Scrum, roles, eventos, artefactos y reglas asociadas" (Schwab & Sutherland, 2013).

Scrum es un marco de trabajo incremental e iterativo para el desarrollo de proyectos, que se organiza en iteraciones de 1 a 4 semanas, llamados Sprints, los sprint son de un tiempo fijo, finalizan en una fecha determinada así no se haya terminado el sprint y se desarrollan uno después del otro. Al inicio de cada Sprint un equipo elige los requisitos del cliente de una lista priorizada, el equipo tiene reuniones diarias para informar el progreso del proyecto y una vez finalizado el Sprint, se presenta lo que se ha construido a los interesados del proyecto, ya que Scrum hace hincapié en productos funcionales listos para entregar (Deemer, Benefield, Larman, & Vodde, 2009)

3.1. Adaptación de Scrum al Proyecto

A continuación, se presenta la adaptación de la metodología Scrum al proyecto, facilitando el desarrollo mediante los siguientes componentes que cabe mencionar son los difundidos por el manifiesto ágil (Calderon & Valverde, 2007).

Valores:

- Valorar más a las personas y su interacción que a las herramientas y procesos.
- Valorar más el producto funcional que los artefactos absolutos y exhaustivos.
- Valorar más la cooperación con el cliente que el convenio.
- Valorar más la solución a las modificaciones que a un seguimiento riguroso de un régimen.

Prácticas:

- Planificación ágil: Planificación distribuida a lo largo del proyecto.
- Historias de Usuario: Descripción de las funcionalidades.
- Periodos semanales: Planificación en periodos de corta duración.
- Entregables pequeños: Rápidas versiones funcionales.
- Pruebas: Pruebas realizadas por diferentes usuarios.

Roles:

- Scrum Master: Conocedor de Scrum.
- Product Owner: Persona que tiene la visión del producto a desarrollar.
- Team Developer: Equipo encargado de desarrollar el producto.

Reuniones:

- Reuniones diarias: Facilitando transferencia de información.
- Reuniones de planificación: Asignación de tareas y distribución del trabajo.
- Reuniones de revisión: Entrega del resultado funcional.
- Reuniones de retrospectiva: Análisis de avance del sprint (Alliance, 2001), (Calderon & Valverde, 2007), (Awad, 2005), (Quezada, Chango, López, Pacheco & Enciso , 2017).

En la siguiente Figura 1 se presenta la adaptación de la metodología Scrum, donde se muestra los roles y elementos aplicados.

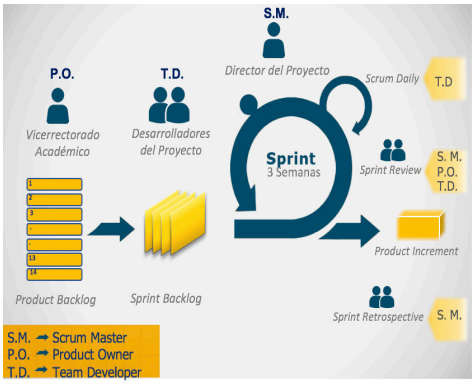


Figura 1 – Adaptación de Scrum al proyecto desarrollado

Propuesta del modelo:

Para poder realizar la solución y presentar la mejora del proceso de acción tutorial, se ha llevado a cabo un análisis del proceso que se realizaba anteriormente y del proceso actual de la UTPL, es por esto que se ha optado por desarrollar el siguiente framework metodológico, el cual nos permitirá gestionar una tutoría y definir qué recursos deben ser utilizados, con la finalidad de sistematizar la secuencia repetitiva de actividades de una tutoría, conocido como proceso de acción tutorial.

Modelo metodológico:

En la Figura 2 presentamos la propuesta de la mejora del proceso de acción tutorial, es decir el modelo metodológico. En donde se puede observar tres bases en la que interactúa el estudiante, docente y el personal administrativo en una acción tutorial.

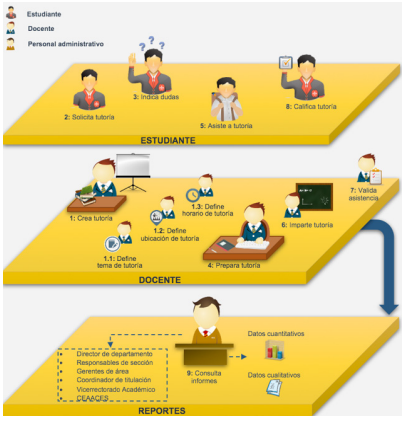


Figura 2 – Modelo Tutorial

Descripción del modelo:

Con la propuesta de este modelo metodológico pretendemos promover la consideración de nuevas alternativas para el apoyo del aprendizaje de los estudiantes mediante actividades específicas, entre las que cabe destacar un impulso decidido a la aplicación de las TIC (Quezada & Mengual, 2018). De hecho, las medidas que se proponen en el modelo metodológico se centra en el desarrollo de tareas para garantizar un servicio tutorial eficiente y a la vez una mejora de la interacción tutorial entre alumnos y docentes.

Lo fundamental del modelo es promover la organización y comunicación del estudiante con el docente, es por esto que se plantea una propuesta de cooperación y trabajo tutorial sustentada en la utilización de dispositivos móviles con la ayuda de una aplicación de fácil uso, que optimiza muchos de las actividades que son llevadas a cabo de manera manual, pero lo importante es que no sustituye la comunicación presencial cara a cara entre alumno y docente, sino que ofrece un canal adicional de comunicación, aprovechando la cultura de interacción de los estudiantes mediante sus dispositivos móviles, todo para mejorar la calidad del trabajo tutorial. Sin embargo, el docente no debe percibir una opresión sino un llamado a su motivación docente.

Este modelo metodológico, además presenta otro tipo de acción tutorial, las tutorías telemáticas, las cuales permiten realizar un seguimiento continuo del progreso de los estudiantes, por lo tanto, se convierte en un soporte informativo que un docente necesita para el análisis y acompañamiento académico.

En la Tabla 1 se presenta el detalle de la relación que existe entre cada actividad, agrupada en procesos con su respectivo responsable.

Las ventajas principales que tiene la acción tutorial y que se incluyen en el modelo son las siguientes:

- Permite una comunicación integral con todo el grupo de estudiantes con sus respectivos docentes (Quezada, Enciso & Garbajosa, 2015).
- Permite conocer anticipadamente las dudas o inquietudes puntuales de los estudiantes. Esto implica que el docente pueda brindar una tutoría eficaz.
- Organización del tiempo de tutorías evitando que otras actividades se interpongan.
- Posibilidad de programar tutorías grupales mediante la incorporación de inquietudes del mismo interés.
- Posibilidad de calificación de la tutoría impartida por el docente y que servirá para una evaluación continua.
- Historial de cumplimiento y participación que indica las acciones realizadas por los estudiantes y docentes.
- Evidencia para entes con interés en la Educación Superior.
- Reportes estadísticos como apoyo a un mayor análisis para toma de decisiones (Jumbo, Quezada, Bustamante & López 2018).

Así mismo para el correcto desarrollo de la aplicación se estableció una arquitectura de software; la misma que es presentada en la figura 3.

Proceso	Actividad	Descripción	Responsable
1 Planificación de tutoria	1. Cera tutoria 1.1. Define tema de tutoria 1.2. Define ubicación de tutoria 1.3. Define horario de tutoria	El docente al crear la tutoria, define el tema, ubicación y horario donde se impartirá la tutoria.	Docente
2 Solicitud de tutoria	2. Solicita tutoria 3. Indica dudas	El estudiante solicita una tutoria al docente e indica dudas sobre algún tema específico. ¿Cómo? El estudiante reserva un espacio temporal de 10, 20 o de 30 minutos en el horario establecido por el docente para el desarrollo de la acción tutorial, de forma que tanto el docente como el estudiante tenga disponible ese tiempo, sin tener el problema de que otras actividades se interpongan.	Estudiante
3 Desarrollo de tutoria	4. Prepara tutoria 5. Asiste a tutoria 6. Imparte tutoria 7. Valida asistencia 8. Califica tutoria	El docente prepara la tutoria respecto a las dudas indicadas, el estudiante asiste y el docente imparte la tutoria, una vez finalizada se procede a validar la asistencia del estudiante y luego a calificar la tutoria por parte del estudiante.	Docente Estudiante
4 Reportes	9. Consulta informes 10. Obtiene reportes	Los interesados (Director de departamento, Responsables de sección, Gerentes de área, Coordinador de titulación, Dirección General Académica y CEAACES) Consulta informes sobre las tutorías realizadas de cada componente académico y obtiene reportes cuantitativos y cualitativos.	Interesados
Fin del proceso			

Tabla 1 – Procesos de acción tutorial

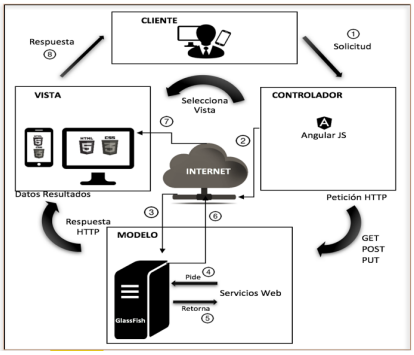


Figura 3 – Arquitectura de Software planteada.

En el mismo contexto en la figura 4 podemos visualizar la aplicación móvil desarrollada para la innovación tutorial, así como de la aplicación de los principios de ingeniería de software.

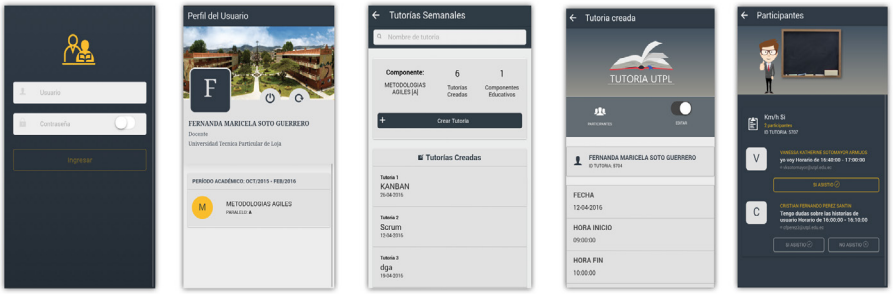


Figura 4 – Aplicación Móvil Acción Tutorial Docente.

Así mismo en la figura 5 se puede apreciar la acción tutorial por parte del estudiante.

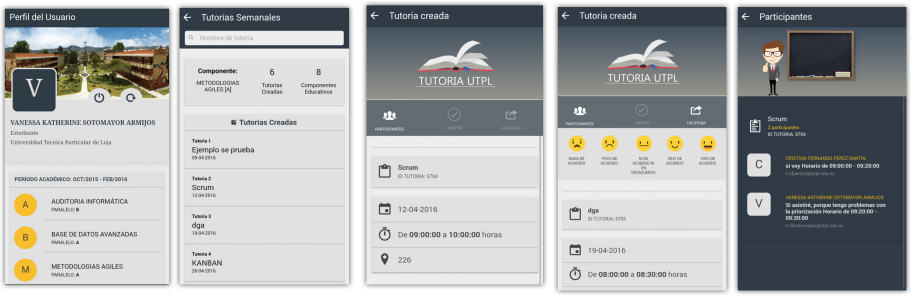


Figura 5 – Aplicación Móvil Acción Tutorial Estudiante.

Una vez finalizado el proceso tutorial, se procedió a la evaluación del nuevo modelo, mediante una encuesta final que nos permite realizar una validación del proyecto (modelo metodológico junto con la herramienta móvil)

Por otra parte, se procedió a realizar una encuesta de satisfacción a los estudiantes y docentes que pertenecen a componentes de la Titulación de Sistemas Informáticos y Computación, para conocer sus opiniones y en base de ellas poder plantear mejoras a la aplicación en nuevo versionamiento.

4. Conclusiones

El modelo de tutorías que se ha propuesto para la modalidad presencial de la UTPL se adapta a las necesidades de sus actores: docentes y estudiantes. Esto se ve reflejado en la sistematización del aplicativo móvil desarrollado para gestionar los horarios de tutoría y conocer las dudas o contenidos a tratar. Consideramos que la tendencia del uso de las TIC se incrementa día a día y esto facilita la comunicación con el docente y a la vez se convierte en un complemento para la acción tutorial presencial.

De acuerdo a los resultados obtenidos del caso de estudio aplicado a los componentes de la Titulación de Sistemas Informáticos y Computación, consideramos que la aplicación móvil que sistematiza el framework metodológico propuesto, es de utilidad para los estudiantes y docentes por la fomentación de participar en la actividad tutorial que influye en el proceso de enseñanza, aprendizaje y en el rendimiento académico.

La utilización de la metodología ágil Scrum, brindó resultados favorables para el desarrollo de este proyecto, ya que se implicó de una forma permanente al Product Owner y evitó riesgos durante el desarrollo, permitiendo responder de mejor manera al cambio.

Finalmente, las herramientas móviles permiten una mejor interactividad entre el estudiante y el docente, pero no la suficiente como para reemplazar la interacción que tiene un estudiante en el aula, pero es importante mencionar que la interacción aumenta cuando se organiza anticipadamente una tutoría, esta coordinación y planificación inicial se torna fundamental puesto que tienen claro qué contenidos serán expuestos en la tutoría. En consecuencia, esta herramienta es elemental para conseguir varios de los objetivos de formación en la educación superior.

Referencias

Alarcón, P. P., Fernández, D., Mahillo, A., & Álvarez, M. D. (2014). Gestión Automatizada de Tutorías. REDU: Revista de Docencia Universitaria, 12(2), 351–373.

Amaro Calderón, S. D., & Valverde Rebaza, J. C. (2007). Metodologías Ágiles. Universidad Nacional de Trujillo-Escuela de Informática.

Alliance, A. (2001). “Agile manifestó”. Online at http://www.agilemanifesto.org.

Awad, M. (2005). A comparison between agile and traditional software development methodologies. University of Western Australia.

Deemer, P., Benefield, G., Larman, C., & Vodde, B. (2009). Información básica de SCRUM (THE SCRUM PRIMER), 1–20.

Fortuño, M. L., Cervera, M. G., Molías, L. M., Vidal, C. E., Martínez, J. G., & Riobóo, N. A. (2013). Tutoría virtual para profesionales de enfermería noveles. RIED: Revista Iberoamericana de Educación a Distancia, 16(1), 199–215.

Jumbo-Flores, L. A., Quezada-Sarmiento, P. A., Bustamanteordoñez, S. J., & López-Alama, E. J. (2018). Development of application for the management of shrimp production. [Desarrollo de Aplicación Web para la Gestión de Producción de Camarón] Espacios, 39(4)

Quezada-Sarmiento, Pablo Alejandro and Mengual Andrés, Santiago Implementación de una solución web y móvil para la gestión vehicular basada en Arquitectura de Aspectos y metodologías ágiles: Un enfoque educativo de la teoría a la práctica. RISTI, Dic 2017, no.25, p.98-111. ISSN 1646-9895

Quezada, P., Garbajosa, J., Enciso, L. Use of standard and model based on BOK to evaluate professional and occupational profiles (2016) Advances in Intelligent Systems and Computing, 444, pp. 287-296. DOI: 10.1007/978-3-319-31232-3_27

Quezada, P., Enciso, L., Garbajosa, J. Using tools of cloud computing for defining, planning, monitoring innovation projects and knowledge generation [Uso de herramientas de computación en la nube para definir, planificar, controlar proyectos de innovación y generación de conocimiento] (2015) XI Jornadas Iberoamericanas de Ingeniería de Software e Ingenieria del Conocimiento, JIISIC 2015, pp. 121-131.

Quezada-Sarmiento, P. A., Garbajosa, J., Washizaki, H., & Enciso, L. (2017). Knowledge description model for bodies of knowledge in software engineering context. Iberian Conference on Information Systems and Technologies, CISTI, doi:10.23919/CISTI.2017.7976058

Quezada-Sarmiento, P. A., Chango-Cañaveral, P. M., López-Criollo, J., Pacheco-Viteri, F. A., & Enciso, L. (2017). Design of a wireless network of temperature and lighting sensor for gastronomic laboratories under the principles of agile scrum methodology. [Diseño de una Red de sensores inalámbricos de temperatura e iluminación para laboratorios Gastronómicos bajo principios de la metodología ágil Scrum] Espacios, 38(46)

Quezada-Sarmiento, P. A., & Mengual-Andrés, S. (2018). Promoting innovation and skills entrepreneurship in training professionals in software engineering: A focus on academy and bodies of knowledge context. [Fomento de la innovación y competencias de emprendimiento en los profesionales en formación en Ingeniería de Software: Un enfoque de la academia y Cuerpos de Conocimiento] Espacios, 39(6)

Santos Olalla, F., Adrada Guerra, T., Albéniz Montes, J., & Castedo Cepeda, L. (2012). La Hora TutHora: Una herramienta de Ordenación Académica para incrementar la Acción Tutorial en la Escuela Universitaria de Ingeniería Técnica Industrial de la UPM. Revista Del Congrés Internacional de Docència Universitària I Innovació (CIDUI), 1(1).

Schwab, K., & Sutherland, J. (2013). La Guía Definitiva de Scrum: Las Reglas del Juego.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 07/12/2017
Aceitação/Acceptance: 10/03/2018

Diseño de un sistema de apoyo al proceso de Enseñanza-Aprendizaje

Rivero-Albarrán D.,[1] Rivas-Echeverría F.[2] Yépez-Durán P.[3] Quishpe-Morales S.[4]

milagro@ula.ve, frivas6@gmail.com, milagro@ula.ve, frivas6@gmail.com, pyepez@pucesi.edu.ec, squishpe@pucesi.edu.ec

[1] Universidad de Los Andes Mérida, Venezuela

[2] Universidad de Los Andes Mérida, Venezuela

[2] Pontificia Universidad Católica del Ecuador-Sede Ibarra

[3] Pontificia Universidad Católica del Ecuador-Sede Ibarra

[4] Pontificia Universidad Católica del Ecuador-Sede Ibarra

Pages: 243–255

Resumen: El uso y elaboración de recursos didácticos que apoyen el proceso de enseñanza aprendizaje ha crecido en los últimos años, parte de este crecimiento se debe a la evolución de las tecnologías de información y comunicación. Para la construcción de los recursos didácticos se usan diferentes herramientas y/o plataformas de desarrollo, requiriendo, en algunos casos, la integración de diversas herramientas, lo que puede ser complicado para algunos docentes. Este trabajo presenta el diseño de un sistema que apoya la elaboración de guías didácticas en ambientes WEB, ofrece a los docentes los elementos necesarios para organizar y elaborar guías didácticas interactivas, se estructura en temas, cada tema tiene asociado los contenidos, recursos, actividades y evaluaciones. La herramienta realiza un seguimiento a cada estudiante y así permite conocer el avance de ellos. Para evaluar la herramienta se elaboró una guía didáctica de una asignatura, la cual se presenta en este trabajo.

Palabras Clave - TIC para la enseñanza, sistemas tutoriales, guías didácticas, desarrollo de software.

Design of a support system for the Teaching-Learning process

Abstract: The use and development of teaching resources that support the teaching-learning process has grown in recent years, part of this growth is due to the evolution of information and communication technologies. Different tools and/or development platforms are used for the construction of the didactic resources, requiring, in some cases, the integration of different tools, which can be complicated for some teachers. This work presents the WEB-based design of a system that supports the development of didactic guides, offers teachers the necessary elements to organize and develop interactive didactic guides, it is structured into themes, each

topic has associated contents, resources, activities and evaluations. The tool keeps track of each student and thus allows to know the progress of them. To evaluate the tool, a didactic guide of a subject was elaborated, which is presented in this work.

Keywords: ICT for teaching, tutoring systems, didactic guides, software development.

1. Introducción

El mundo de hoy se caracteriza por su constante cambio, parte de estos cambios se deben al creciente desarrollo y evolución de las Tecnologías de Información y Comunicación (TIC) y a su incorporación en el quehacer diario. Las TIC se han convertido en un elemento fundamental en todos los campos del conocimiento, incluyendo el campo educativo. Esta evolución tecnológica ha permitido el desarrollo de aplicaciones y herramientas que hasta hace poco se pensaban difíciles de desarrollar, tales como los sistemas basados en lenguajes naturales, sistemas de búsqueda y análisis de información, herramientas para la gestión de objetos en diferentes medias, etc. Estos desarrollos han sido utilizados en diferentes dominios, uno de estos dominios es el de enseñanza-aprendizaje.

En la actualidad, los docentes, se apoyan de alguna manera en herramientas tecnológicas para lograr los resultados de aprendizaje esperados, de manera que el estudiante con los conocimientos adquiridos desarrolle las habilidades necesarias para que pueda aplicar este conocimiento en la solución de problemas reales. Una manera de alcanzar este objetivo es incorporar herramientas tecnológicas que apoyen las distintas estrategias o modelos de enseñanza existentes, es específico el modelo constructivista, brindando así, herramientas y medios al estudiante con el fin de que éste sea un elemento activo en su propio proceso de aprendizaje.

Por otro lado, los organismos responsables de la educación en los distintos países han puesto énfasis en alcanzar una educación de calidad, enfocándose en las competencias que los estudiantes deben alcanzar durante su ciclo de formación. Para ello, los docentes deben incorporar en el proceso de enseñanza nuevas estrategias educativas, que permitan una mayor participación del estudiante en su proceso de aprendizaje, mejorando el nivel de interacción entre los estudiantes y el profesor [1].

Las nuevas estrategias de enseñanza a distancia requieren de las TIC. que permiten desarrollar ambientes de aprendizaje interactivos, eficientes, accesibles y distribuidos. Generando espacios que incentivan a los estudiantes a participar de forma activa en su proceso de aprendizaje, y por ende a la creación de su propio conocimiento. La educación apoyada por herramientas digitales se puede clasificar en [2]:

- Formación basada en computadoras (Computer Based Training CBT): utilizada en muchas instituciones educativas y organizaciones. Está basada en lecturas de documentos digitales e incorpora mecanismos de retroalimentación pregunta-respuesta, convirtiendo al alumno en un ente más activo dentro de su propio proceso formativo;
- Formación basada en internet (Internet Based Training IBT): siguiente paso evolutivo de los sistemas de aprendizaje basados en computador, utiliza el internet como medio para hacer llegar los contenidos a sus destinatarios;

- Formación haciendo uso de la web (Web Based Training WBT): los contenidos se reciben a través de la web. El Campus Virtual de cualquier plataforma educativa forma parte de este tipo de aprendizaje.

La guía didáctica, como estrategia de enseñanza interactiva, puede ser utilizada en cualquiera de los tipos de aprendizajes anteriores. Según Yépez [3] Las guías didácticas son recursos docentes que desarrolla los valores y los procedimientos cognitivos y motrices planteados en los módulos de formación.

En la actualidad, se encuentran una variedad de plataformas y herramientas digitales para la enseñanza, por citar algunos se tiene: la elaboración de tutoriales inteligentes para la enseñanza en áreas específicas, como ALICE [4], tutoriales para la enseñanza en programación, el desarrollo de guías didácticas hipermedias para la educación como el realizado en la Universidad Nacional de Educación a Distancia en universidad de España [5]; una pizarra digital interactiva para la enseñanza de la matemática [6].

Para el desarrollo de las herramientas didácticas se utiliza diferentes herramientas tecnológicas, como son: *Exelearning* [7] que permite a docentes la creación y publicación de contenidos didácticos, plataformas para el desarrollo de Cursos Masivos Abiertos en Línea (MOOC de sus siglas en inglés) utilizado por Coursera [8] y ddx [9], herramientas para la creación de libros digitales cuadernia [10] y Moodle la plataforma de aprendizaje integrada para crear ambientes de aprendizaje personalizados [11]

El diseño del sistema que se presenta en este trabajo, tiene como objeto proveer una plataforma para la elaboración de guías didácticas como herramienta de apoyo para la enseñanza. La plataforma permite elaborar cursos de cualquier asignatura, administrando en cada curso sus objetos de aprendizajes (recursos digitales). Además, lleva registros para medir del desempeño de cada estudiante y poder tomar acciones para reforzar las debilidades encontradas. La herramienta integra los elementos necesarios para la elaboración de guías didácticas, además de poseer un foro de discusión, espacio en el cual el profesor y los estudiantes podrán interactuar permitiendo una mediana interacción (no en tiempo real). El sistema es una combinación de los conceptos básicos del sistema tutoriales y los sistemas de entornos virtuales.

El resto de trabajo está organizado de la siguiente manera: la sección II presenta la metodología utilizada para el desarrollo de este trabajo. En la sección III se presenta diseño que se obtuvo, para cumplir con los requisitos establecidos. Además, se muestra una guía didáctica para la asignatura Lógica Difusa y Aplicaciones Lógicas, construida con el prototipo desarrollado. Finalmente, en la sección IV se presentan las conclusiones y trabajo futuro.

2. Metodología

Para el desarrollo del sistema, con el objeto de comprender los conceptos y características más importantes de los modelos y estrategias de enseñanza-aprendizaje clásicas y basadas en computadoras, se realizó una revisión bibliográfica de los trabajos y enfoques utilizados hasta ese momento, de esta revisión se obtuvo un modelo de procesos asociados a este dominio, Luego se realizó un análisis de dominio para

derivar los requisitos funcionales (RF) y no funcionales (RNF) del sistema. El conjunto de requisitos RF y RNF sirvieron para que, utilizando, ara su gestión y desarrollo un método ágil y para el diseño la estrategia evolutiva para transformar el modelo de objetos de negocio en un modelo de servicios [12].

3. Conceptos del dominio de la Enseñanza

3.1. Modelos y métodos de enseñanza

Según Jean Pierre Astolfi [13] existen principalmente tres modelos de enseñanza-aprendizaje generales: la transmisión, el conductismo y el constructivismo. Este último modelo es el modelo en el que se basó este trabajo. Ve en este modelo, el estudiante tiene un papel principal y activo como participe de su aprendizaje. El constructivismo sostiene que los nuevos conocimientos se adquieren a partir de la relación con conocimientos anteriores, por tanto, es un proceso progresivo [14].

Por otro lado, un modelo de enseñanza-aprendizaje debe incluir los siguientes aspectos:

- Estrategias para alcanzar sus objetivos;
- Medios para potenciar esas estrategias;
- Una vía de interpretación para adecuar, modificar lo anterior a los contextos.

En la actualidad se encuentran diferentes metodologías para la enseñanza, Jorge [1] indica en su trabajo que las metodologías más utilizadas son: “La metodología expositiva, caracterizada por utilizar la experiencia del sujeto como fuente de aprendizaje, donde el alumnado obtiene la información de manera activa y constructiva; y la metodología interactiva donde el docente y alumnado interactúan mediante el debate o diálogo para profundizar en un tema”.

Toda metodología requiere de un método de enseñanza, que marque el camino e indique las herramientas concretas para transmitir los contenidos a los estudiantes con el objeto de lograr los objetivos de aprendizaje propuestos. En la actualidad, algunos de los métodos de enseñanza utilizan las TIC como mecanismo de refuerzo, usando un conjunto de recursos (imágenes, videos, lecturas) que facilita el debate de ideas entre los estudiantes y el docente [15].

3.2. Método de Enseñanza interactivas

Según Yépez [3], “la enseñanza interactiva guía y dirige las actividades del estudiante para ayudarle a ampliar, entender e interpretar los contenidos críticos de la clase, lección o contenidos de una asignatura interactúa permanentemente con el alumno y le provee una retroalimentación inmediata, capacitando y facilitando al estudiante alcanzar los requisitos de desempeño establecidos”

El método de enseñanza interactiva se basa en un conjunto de principios centrados en el estudiante, requiere de su participación activa en el proceso de aprendizaje, participación que se logra a través de un conjunto de preguntas y respuestas que indican el progreso del estudiante, en este aspecto el uso de las TIC es un elemento importante, ya que facilita este proceso.

El término interactivo en el contexto de los sistemas multimedia se refiere a un sistema en el que se conjugan vídeo, audio, informática, publicaciones electrónicas y un sistema de diálogo. La selección de la información a presentar, está sujeta a las respuestas o decisiones del estudiante [15]. Unos sistemas de enseñanza hipermedia permiten que el estudiante:

- Disponga de una gran variedad de formas de acceso a la información;
- Acceda a la información de la base de conocimiento que desee;
- Redefina la estructura y contenido del material a utilizar.

La calidad de los contenidos y los medios de presentación son aspectos fundamentales en el proceso de enseñanza. Según González (2004) "El éxito de un programa educativo, su calidad y efectividad, dependen principalmente de la capacidad de comunicación que posea la presentación de contenidos"

Por otro lado, el método de enseñanza interactiva mantiene una retroalimentación con el estudiante que permite suministrarle información en función del resultado de sus respuestas. Además, el seguimiento a sus respuestas permite identificar si el estudiante requiere de algún refuerzo y que tipo de refuerzo es el más adecuado. Este seguimiento requiere de herramientas tecnológicas que permitan realizar los procesos de evaluación y diagnóstico del estudiante.

3.3. Sistemas tutoriales

Las técnicas aplicadas en los Sistemas Enseñanza Aprendizaje (SEA) basados en WEB fueron adoptadas del área de los Sistemas Tutoriales Inteligentes (STI) o del área de los Sistemas Adaptativos Hipermedia (HAS de sus siglas en inglés) [16]. En la Fig. 1 se muestran los componentes de un sistema tutorial, éstos son: el módulo de secuenciación de contenidos, con los contenidos curriculares; el módulo de análisis de las soluciones generadas por los estudiantes, el módulo de soporte para la resolución de tareas de forma interactiva y finalmente, un módulo para trabajo colaborativo.

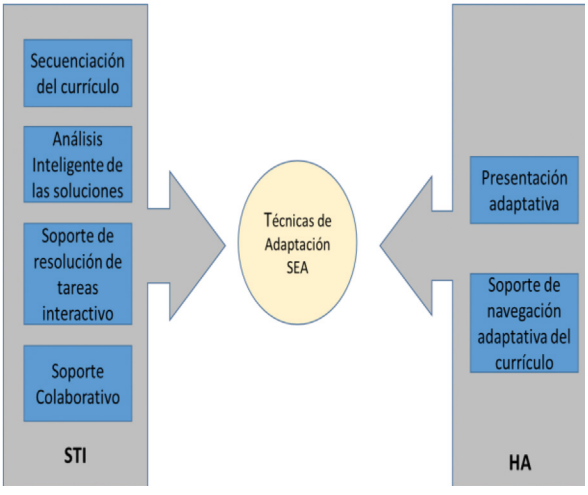


Figura 1 – Técnicas de adaptación provenientes de los STI y los HA [16].

Los sistemas tutoriales inteligentes pretenden ofrecer a cada estudiante un mayor ajuste e individualización de la secuencia de contenidos y de tareas en el proceso de aprendizaje. Estos sistemas proponen una estructura contenidos secuenciados, conocida como técnica de secuenciación de currículum, la cual persigue la planificación instruccional de los ejemplos, preguntas, problemas, entre otros.

4. Análisis del sistema

4.1. Análisis del dominio

En la primera fase se realizó un análisis del dominio educativo, con el objeto de identificar aspectos importantes como: los procesos que se llevan a cabo, los recursos que utilizan, las reglas que lo rigen, las actividades que se realizan en cada proceso y los actores involucrados. La Fig. 2 presenta los procesos asociado al dominio educativo, específicamente a lo referente a la enseñanza y el aprendizaje. La Fig. 3 y Fig. 4 muestra los diagramas de las actividades que se realizan en los procesos de planificación del curso y el dictado de clases. El análisis del dominio se apoyó, para su verificación, en el trabajo de Losavio y Esteves [17].



Figura 2 – Diagrama de procesos del dominio de enseñanza aprendizaje.

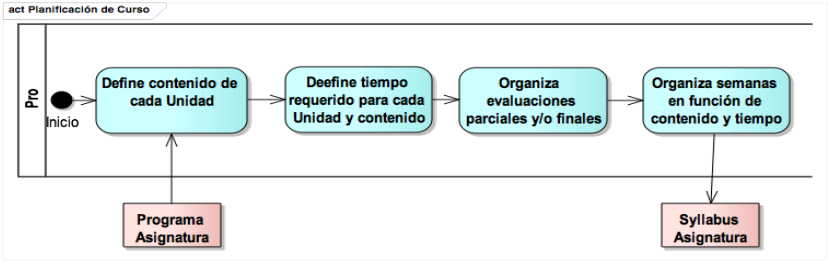


Figura 3 – Diagrama de actividades del proceso de planificación

4.2. Análisis de requisitos

En la fase de análisis requisitos se identificaron los requisitos funcionales y no funcionales del sistema (RF, RNF) Los RF se obtuvieron a partir de los diagramas de actividades realizados en la fase anterior. Además, se identificaron las responsabilidades de los actores que participan en el proceso, de enseñanza-aprendizaje, estos son: el

profesor (conocido también como tutor) que es responsable de la planificación y elaboración de los contenidos de la asignatura, dar tutoría al estudiante, impartir los contenidos del curso de acuerdo al plan y llevar el seguimiento al curso; los estudiantes, que deben seguir el contenido del curso de acuerdo a plan especificado en la guía, realizar las actividades prácticas y hacer las evaluaciones requeridas.

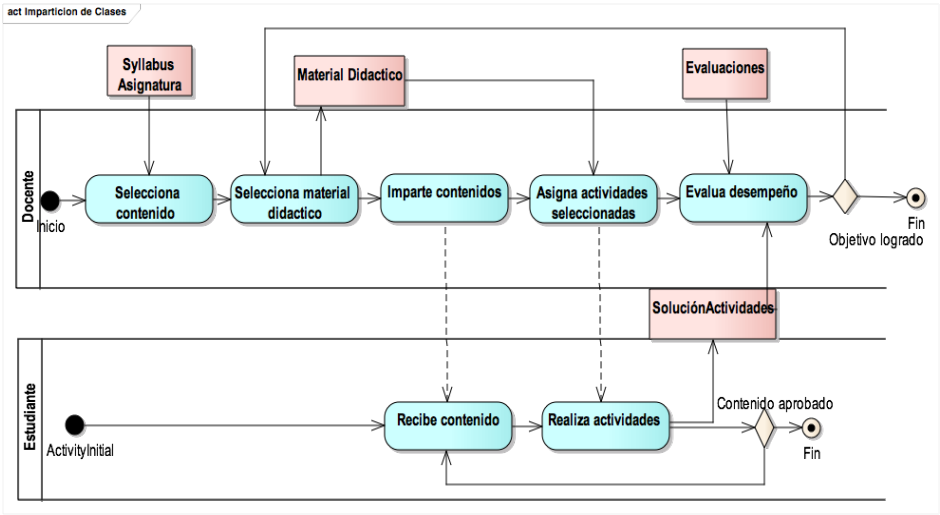


Figura 4 – Diagrama de actividades del proceso dictado de clases.

La Fig. 5 presenta el diagrama de casos de uso general del sistema que muestra las principales funciones que la herramienta debe soportar. Los casos de uso del recuadro de enseñanza le permiten al profesor gestionar los contenidos de cada asignatura, bajo el concepto y la estructura de guía didáctica. Los casos de uso en el recuadro de aprendizaje contienen las funciones o servicios requeridos por el estudiante para acceder al material del curso. Estos requisitos se agruparon, de acuerdo a su objetivo, en un modelo de componentes llamada la arquitectura de componentes inicial y a partir de este modelo, utilizando la estrategia propuesta en [12], se diseñó y refino la arquitectura a medida que se construía el sistema.

5. Diseño de la Herramienta para la Enseñanza Didáctica

Para el diseño y construcción se utilizó un método ágil de desarrollo, para ello se asignó una prioridad y un grado de dificultad, calculado en horas/hombre, a cada funcionalidad y se comenzó la planificación de cada iteración en base a estos valores. El diseño de la herramienta se fundamentó en un enfoque autónomo y de colaboración. Autónomo para que el estudiante, en base a la organización del curso y al plan del curso, pudiera acceder a los contenidos de cada tema y realizar las actividades asignadas, apoyándose en los diferentes recursos asignados al tema. De colaboración porque el estudiante podrá interactuar con el docente o con el grupo a través de foros, este espacio servirá

para aclarar dudas o compartir ideas, reforzando sus conocimientos y/o reduciendo sus debilidades, fomentando la construcción de conocimiento autónomo.

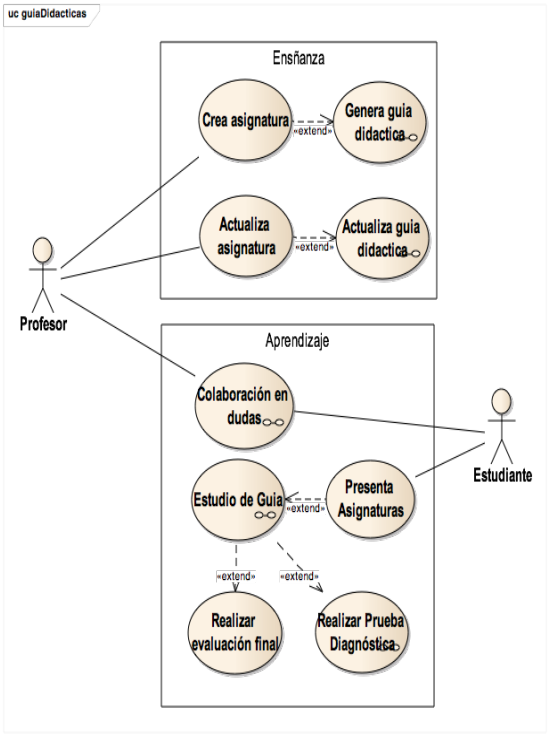


Figura 5 – Diagrama general de Casos de Uso

Cada caso de uso se refinó para identificar las funciones que se requerían de más bajo nivel requerida (granula fina), los conjuntos de funciones se agruparon, de acuerdo a su granularidad, en diferentes componentes. La Fig. 6 presenta el diagrama de caso de uso refinado del caso de uso Estudio de guía, en este refinamiento se especifica que se deben presentar contenidos de diversas medias, los cuales, en su conjunto se convertirán en un hiperespacio de objetos de aprendizajes. Este material suministrado al estudiante para el aprendizaje de un tema específico, se seleccionará en base a la complejidad del contenido y el progreso del estudiante.

Para asegurar el acceso a la plataforma en cualquier lugar, se decidió diseñar una aplicación del tipo WBT con un enfoque de una arquitectura orientada a servicios. Para identificar las funciones de granula más fina (funciones de los objetos del negocio) se modelaron las interacciones que se daban entre los objetos del sistema y los actores. La figura 7 muestra el diagrama de componentes final, en este modelo métodos de granula más fina corresponden a las entidades del negocio y las más gruesas a componentes de servicios.

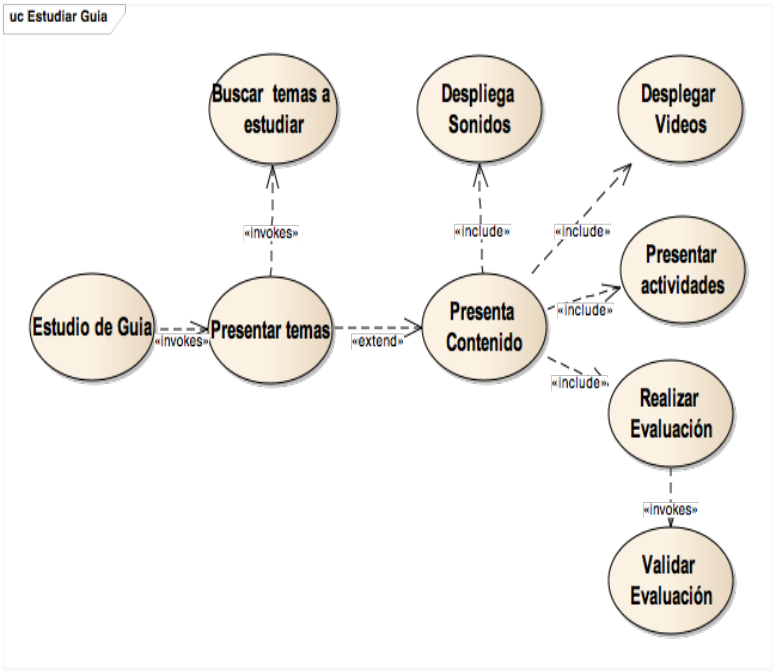


Figura 6 – Diagrama refinado del caso de uso Estudio de guía

El diseño contempló dos técnicas de secuenciación de contenidos propios delos sistemas tutoriales, que son:

- Técnica de alto nivel o secuenciación del conocimiento, que permite seleccionar los próximos contenidos o temas que el estudiante, de acuerdo a su evolución, puede acceder;
- Secuenciación a bajo nivel o secuenciación de tareas para determinar el conjunto de tareas o actividades a realizar del tema que se está estudiando, estas pueden ser problemas, ejemplo, evaluaciones, entre otras.

Las capas arquitectónicas se diseñaron de forma independiente. La Fig. 7 presenta el diseño de los componentes que manejan directamente los objetos llamados servicios para la gestión de objetos del negocio. La Fig. 8 presenta el diseño los componentes de granula más gruesa llamados los servicios del negocio, en ambas figuras sólo se muestran los servicios más importantes para la construcción de la herramienta. Además, existen dos componentes internos, uno responsable de la gestión de los componentes del curso, componente para la gestión de los objetos de aprendizajes que provee las funciones de creación y recuperación de los objetos de aprendizajes requeridos por el componente de enseñanza y otro componente responsable de la gestión de contenidos de cada curso, vinculado al componente de enseñanza.

6. Resultados

Para probar la herramienta, desde el punto de vista de funcionalidad, se desarrolló una guía interactiva para la asignatura de Lógica Difusa y Aplicaciones Lógicas que es una de las asignaturas del plan de estudios de la carrera de Ingeniería de sistemas de la Pontificia Universidad Católica del Ecuador sede en Ibarra. Se presentan los resultados, desde el punto de vista de interfaz, que se obtienen cuando se elaboró el curso con el sistema. La herramienta carece, para la construcción de la guía de una interfaz amigable, ya que el objetivo del curso era validar la integración de los conceptos de guías interactivas y sistemas tutoriales. A continuación, se muestran tres de las vistas finales que se obtuvieron al utilizar la aplicación.

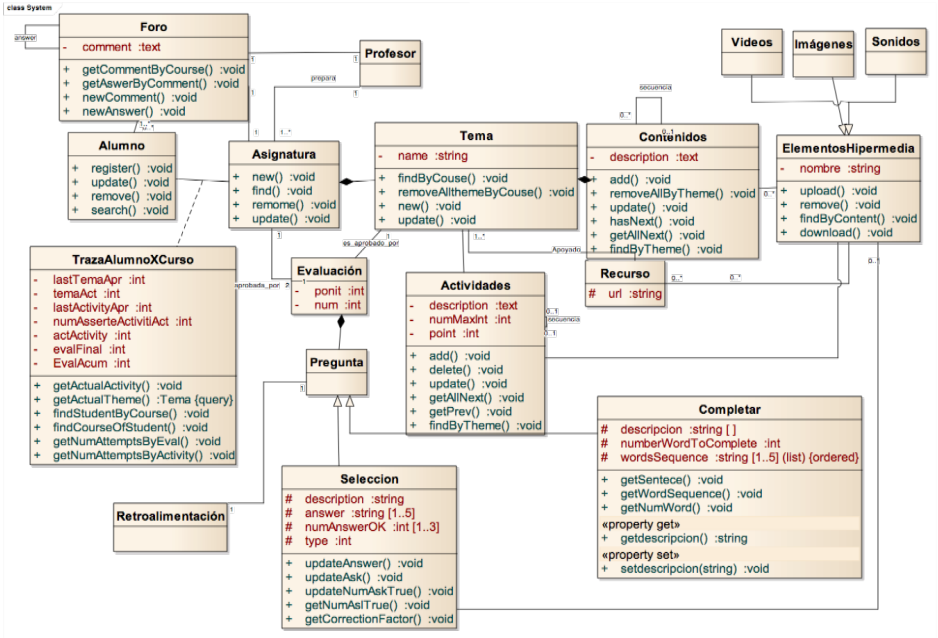


Figura 7 – Diagrama de componentes de servicios para los objetos del negocio.

Se definió una estructura general de pantalla de presentación para cualquier guía, su estructura se muestra en la Fig. 9, se observa en la parte superior el nombre de curso, al lado izquierdo sus contenidos, es decir los temas, resaltando en base al seguimiento realizado a cada estudiante, el tema que tiene disponible. Además, de los temas se presenta la lista de contenidos, actividades y evaluaciones definidos para el tema, Al seleccionar de lista de contenidos la actividades, evaluaciones o recursos del tema, en el área principal, lado derecho, se presenta el contenido seleccionado del tema.

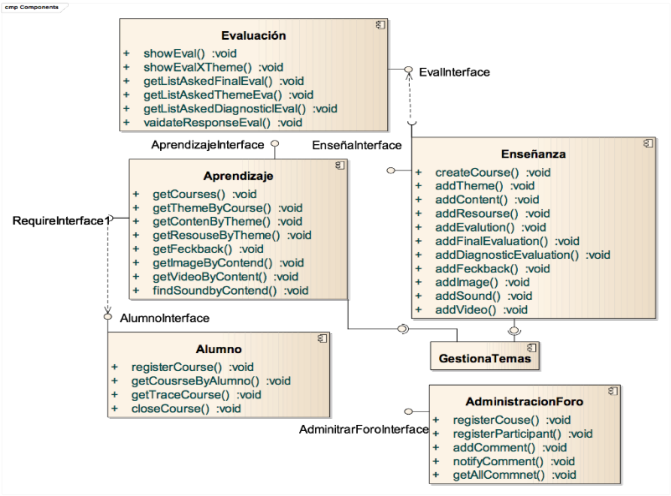


Figura 8 – Diagrama de componentes de servicios para los servicios del negocio

Como se mencionó anteriormente, el sistema posee una serie de evaluaciones por tema que permitirán decidir si el estudiante ha aprobado el tema. De ser así, se habilitan los próximos temas del curso. Al finalizar el curso, luego que el sistema verifique que se realizaron las evaluaciones de todos los temas, se habilita, en el menú de la izquierda, la evaluación final. Las figuras 10 muestran cómo se presenta la evaluación final de la guía. Para finalizar, el sistema permite manejar un foro de discusiones por curso, en el que cualquier estudiante puede hacer un comentario, es un espacio abierto donde estudiantes y docentes plantean sus dudas o inquietudes, la figura 11 presenta la pantalla del foro de una asignatura.

7. Conclusiones

Con base en los resultados hasta ahora obtenidos se puede decir que la herramienta pudo integrar los conceptos de guías interactivas, gestión de contenido multimedia a través de os objetos de aprendizaje. Además, Incorporó a la evaluación de cada estudiante, una retroalimentación y un seguimiento a su desempeño, característica de los STI, el seguimiento de su desempeño facilitó la selección de los contenidos a presentar a cada estudiante, dando inicio a una enseñanza más personalizada. La guía sirve como herramienta de refuerzo de los temas de un curso y como herramienta de apoyo, puede ser utilizada tanto dentro como fuera de las aulas.

El uso de una herramienta computacional facilita a los docentes la elaboración de material de apoyo de sus cursos y la evaluación y seguimiento de los estudiantes.

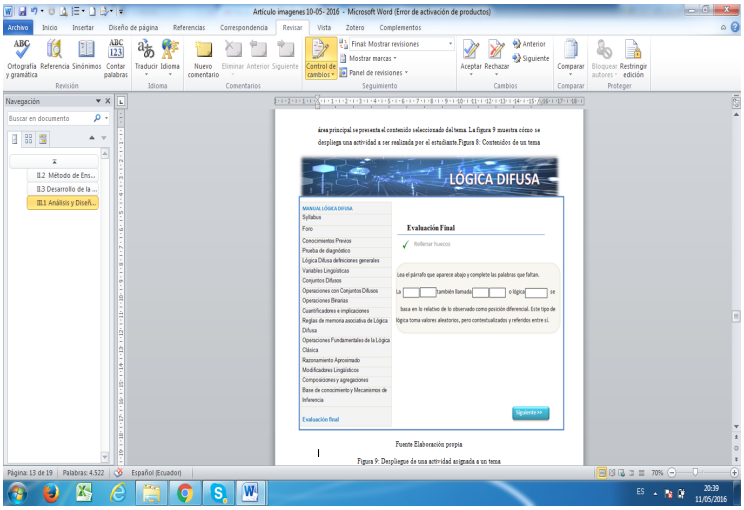


Figura 9 – Imagen de la pantalla general del sistema una vez elaborada una aplicación

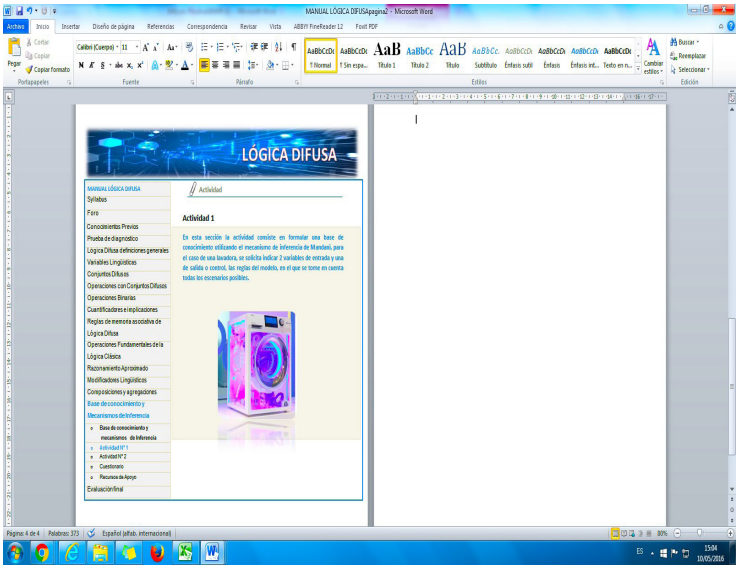


Figura 10 – Diagrama de componentes de servicios para los objetos del negocio

Agradecimientos

El presente trabajo ha sido realizado en el marco del proyecto “Plataforma Inteligente en ambientes Educativos: Caso Dirección de Estudiante PUCESI” de Centro de Investigación de la Pontificia Universidad Católica de Ecuador Sede Ibarra (PUCESI).

Referencias

Astolfi, J. P. Tres modelos de enseñanza. Aprender en la escuela. 1997. 127–135.

Boneu, J. M. Plataformas abiertas de e-learning para el soporte de contenidos educativos abiertos. RUSC. Universities and Knowledge Society Journal, 4(1). 2007.

Carnegie Mellon University. (1999). Alice. Obtenido de http://www.alice.org/index.php

Coursera. Obtenido de https://es.coursera.ocrg/ 2016.

Edx. edx. Obtenido de https://www.edx.org/. 2012

eXeLearning. Obtenido de http://exelearning.net/ 2012.

González, C. S. Sistemas Inteligentes en la Educación: Una revisión de las líneas de investigación actuales. 2004. Recuperado el 03 de 2015, de Revista ELectrónica de Investigación y Evaluación Educativa, v. 10, n. 1: .http://www.uv.es/RELIEVE/v10n1/RELIEVEv10n1_1.htm

Jorge, Carmen Hernández. Metodologías de enseñanza y aprendizaje en altas capacidades. Universidad de la Laguna, 1997.

Junta de Comunidades de Castilla-La Mancha. Cuadernia. Recuperado el 2015, de http://cuadernia.educa.jccm.es/. 2012.

March, A. F. Metodologías activas para la formación de competencias. 2006. Recuperado el 2015, de http://red-u.net/redu/documentos/vol8_n1_completo.pdf

Moodle. Obtenido de https://moodle.org/ 2016.

NODA, María Aurelia. Pizarra digital interactiva en aulas de matemáticas.

Números. Revista de Didáctica de las Matemáticas, 2009, vol. 72, p. 121–127.

Rivero-Albarrán, D., Barrios-Albornoz, J., & Rivas-Echeverria, F.

Rojas, M. 1999. Recuperado el marzo de 21015, de http://www.scielo.cl/scielo.php?pid=S0716-98681999000100012 &script=sci_arttex.

Transforming the Business Object Model in a Web Services Model:

Evolutionary Strategy. En X. Zhuang, Recent Advances in Information.

Barcelona: WSEA. 2016. pp. 183-191.

UNED. (s.f.). Universidad Nacional de Educación a Distancia. Obtenido de http://www2.uned.es/catedraunesco-ead/editorial/p7-2-2009.pdf

Yépez D., P. M. Metodología interactiva para la enseñanza - aprendizaje de la asignatura lógica difusa y aplicaciones lógicas para la Escuela de Ingeniería de la PUCESI. Ibarra: Pontificia Universidad Católica de Ecuador sede Ibarra. 2015

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 05/12/2017
Aceitação/Acceptance: 25/03/2018

Estudio de innovación tecnológica aplicada en procesos formativos con sistemas de gestión de aprendizaje (LMS) en la educación universitaria del Ecuador

Darwin Marcelo Pillo Guanoluisa[1], Leandro Alexander Bermúdez Herrera[2]

dmpillo@pucesi.edu.ec, leandro.bermudez@gmail.com

[1] Escuela de Ingeniería, Pontificia Universidad Católica del Ecuador Sede Ibarra, Av. Jorge Guzmán Rueda y Av. Aurelio, Ibarra, Ecuador.

[2] Facultad de Postgrado, Universidad de las Américas UDLA, José Queri – 170137, Quito, Ecuador.

Pages: 256–270

Resumen: La investigación revisa la incidencia y evolución de las TIC en la educación universitaria, con observación en los espacios educativo y tecnológico aplicados a los sistemas de gestión de aprendizaje (LMS) en las mejores universidades del mundo; así como también un análisis especifico en el Ecuador. El estudio avanza reconociendo sobre los LMS las innovaciones aprovechadas en los ámbitos educativo, tecnológico e institucional, en base a la metodología de innovación TRIZ (Teoría de la solución de problemas de inventiva) como una metodología propia del área de Ingeniería; La investigación propone un modelo para incorporar innovación tecnológica en los LMS de las universidades, establecido en tres fases: valoración del LMS, análisis y propuesta de innovación, aplicación y validación del LMS. El modelo propone actividades y procedimientos para la gestión integral de los procesos relacionados con la enseñanza presencial, online y aprendizaje semipresencial que mejoran el rendimiento de los métodos educativos tradicionales.

Palabras-clave: Sistema de gestión de aprendizaje (LMS); Innovación Tecnológica; Educación Universitaria; Metodología TRIZ.

Study of technological innovation applied in training processes with learning management systems (LMS) in the university education of Ecuador

Abstract: The research reviews the incidence and evolution of ICT in university education, with observation in the educational and technological items applied to learning management systems (LMS) in the best universities in the world; as well as a specific analysis in Ecuador. The study progresses recognizing the LMS innovations used in the educational, technological and institutional, based on the innovation methodology TRIZ (Theory of the solution of problems of inventiveness) as a methodology of the area of Engineering; The research proposes a model to incorporate technological innovation in the LMS of the universities, established

in three phases: assessment of the LMS, analysis and proposal of innovation, application and validation of the LMS. The model proposes activities and procedures for the integral management of the processes related to face-to-face, online and blended learning that improve the performance of traditional educational methods.

***Keywords**:* Learning management system (LMS); Technological innovation; University education; TRIZ Methodology.

1. Introducción

Considerando que, en el contexto mundial los medios de comunicación tradicionales como prensa, radio y televisión han sufrido vertiginosas transformaciones en la última década y fruto de aquellos cambios, la sociedad ecuatoriana incluye las nuevas Tecnologías de la Información y Comunicación (TIC) en la educación.

Según el estudio de Global Information Technology Report (GITR) en el año 2014, "Ecuador ocupa el lugar 82, en su nivel de respuesta para aprovechar las TIC" (MINTEL, 2014) y acorde al Informe sobre Medición de la Sociedad de la Información 2015 de la Unión Internacional de Telecomunicaciones (UIT), "ubica al Ecuador en el puesto 90 de un total de 167 países, con indicadores de acceso, aptitudes y utilización de las TIC" (Unión Internacional de Telecomunicaciones, 2015).

En la Figura 1 se muestra, una comparativa considerando el indicador indice de Preparación en Materia de Redes (NRI por sus siglas en inglés: Networked Readiness Index) obtenido de la base de datos del GITR (Global Information Technology Report) año 2014, el cual hace referencia a la medida de preparación de un país para beneficiarse de los desarrollos de las TIC.

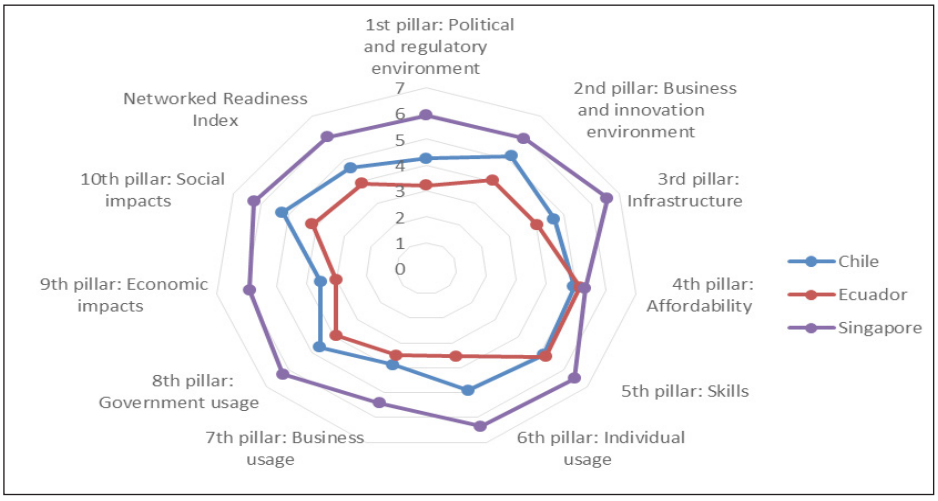


Figura 1 – Comparativa Indicadores NRI, entre Ecuador el referente mundial Singapur y el regional Chile (Indicadores NRI, 2014)

El indicador muestra que el Ecuador tiene sus puntuaciones más bajas en el entorno político y regulatorio, de igual manera una baja capacidad para aprovechar las Tecnologías de Información y Comunicación (TIC). Con el surgimiento de la era de las Tecnologías de la Información (TI) se modificaron las formas de transferencia del conocimiento en las Instituciones de Educación Superior (IES) que a nivel mundial fueron incorporando tecnología que permita apoyar sus procesos de enseñanza-aprendizaje, adoptando sistemas de gestión de aprendizaje (LMS).

En los últimos años, "las universidades han tendido a centralizar sus sistemas de e-learning adoptando LMS que combinan características de tipo tecnológico con herramientas específicas que dan soporte al aprendizaje" (Weller, 2009), y que mediante su adopción y el cumplimiento de estándares, se transforman en unidades de innovación que han permitido fomentar la educación superior con modalidades presencial, con soporte de aula virtual, semipresencial, virtual y a distancia.

Considerando el criterio emitido durante el seminario virtual (webinar) realizado el 21 de mayo 2015 "Las TIC en la educación superior" organizado por la SENESCYT, en donde se identifica que "las universidades e institutos debe generar políticas de innovación educativa, brindando la infraestructura adecuada para poder aplicar esta renovación en las aulas" (Gonzales, 2015).

Se plantea realizar un estudio respecto del uso y aplicación de las innovaciones tecnologías instauradas en los LMS, para generar un compendio o repositorio adecuado de buenas prácticas y herramientas para las Universidades del Ecuador. Se sugieren componentes que permitan la inserción de innovación tecnológica en los LMS y se plantea utilizar una metodología basada en el conocimiento denominada TRIZ como el "proceso sistemático, permite a cualquier técnico desarrollar significativamente sus habilidades de pensamiento crítico y fomentar sus capacidades tanto inventiva como creativa para la resolución de problemas" (Ernst & Young, 2013).

Finalmente, se propone un modelo que permita incorporar innovación tecnológica en los LMS de las Universidades, aplicable tanto en modalidades presencial, semipresencial, en línea o a distancia. Siendo este un proceso que conlleva grandes desafíos sobre todo a los sectores inmersos en la confluencia de estos dos universos esenciales de la sociedad, la tecnología aplicable a través de los LMS y la educación universitaria del Ecuador.

2. Materiales y métodos

2.1. Evolución de los LMS en la educación universitaria

En La Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), hace referencia a que las TIC pueden contribuir con: "acceso universal a la educación, la igualdad en la instrucción, el ejercicio de la enseñanza y el aprendizaje de calidad y el desarrollo profesional de los docentes, así como a la gestión, dirección y administración más eficientes del sistema educativo" (UNESCO, 2016); Por tanto es fundamental la incidencia en uso de las TIC desde la educación universitaria hacia los demás niveles de formación.

La integración de las telecomunicaciones con dispositivos personales como computadores, teléfonos inteligentes, tabletas entre otros, potencian el uso de las TI en razón de que con estas transformaciones tecnológicas redujo las distancias y permitieron los avances del proceso enseñanza/aprendizaje no presencial.

En un breve resumen evolutivo de las TIC y la educación podemos citar lo siguiente: "De la educación por medio impreso y unidireccional se pasó a la enseñanza por correspondencia y de esta a la audiovisual. De la enseñanza audiovisual se evolucionó hacia la formación apoyada en la informática, para finalizar con la era de la telemática en la que nos encontramos inmersos" (García, 2011). En la Tabla 1 se indica los LMS de acuerdo con un criterio de acceso:

Tipo	Descripción	Ejemplos
Comercial o propietario	Se debe pagar por el uso a una empresa que desarrollo o distribuye. Ofrece diversas funcionalidades y costos.	Blackboard, eCollege, Fronter, SidWeb, e-ducativa
"Open Source" código abierto	Son de libre acceso, permite al usuario ser autónomo del uso de la manipulación del software	ATutor, Dokeos, Claroline, dotLRN, Moodle y Sakai

Tabla 1 – Tipos de LMS

En cuanto a las características mínimas con las que debería contar todo LMS de acuerdo con (Clarenc, 2013) son: Interactividad, flexibilidad, escalabilidad, estandarización, usabilidad, funcionalidad, ubicuidad, accesibilidad y la persuabilidad (capacidad que tiene de una plataforma de convencer, fidelizar a un usuario). Conforme al ranking mundial de universidades en la Web, elaborado por el Consejo Superior de Investigaciones Científicas de España en Julio de 2011, se puede identificar las tendencias en cuanto al tipo de LMS usados en la educación universitaria conforme detalla la tabla 2, 3, 4 (Pontificia Universidad Javeriana, sf).

Ranking	Universidad	LMS
1	MIT	Dot Learn, Stellar (Sakai)
2	Harvard University	Blackboard
3	Stanford University	Moodle,Sakai, Blackbo.
4	Cornell University	Moodle, Blackboard
5	University of California Berkeley	Sakai (bspace)
6	University of Michigan	Sakai (CTools)
7	University of Wisconsin Madison	Moodle, Desire2Learn
8	University of Washington	Moodle, Blackboard
9	University of Minnesota	Moodle
10	University of Pennsylvania	Blackboard, Sakai

Tabla 2 – Ranking de USA y uso de LMS

Ranking	Universidad	LMS
1	University of Cambridge	Camtools (Sakai)
2	University of Oxford	WebLearn (Sakai)
3	University of SSouthampton	Blackboard
4	University College London	Moodle
5	Swiss Federal Institute of Technology	Moodle
6	University of Oslo	Fronter
7	University of Edinburgh	Moodle, Blackboard
8	Utrecht University	Blackboard
9	University of Helsinski	Moodle
10	Universität Wien	Moodle, Fronter

Tabla 3 – Ranking de Europa y uso de LMS

Ranking	Universidad	LMS
1	Universidade de São Paulo	Moodle
2	Universidad Nacional Autónoma de México	Moodle
3	Universidade Federal do Rio Grande do Sul	NAVi, Moodle
4	Universidade Estadual de Campinas	Moodle, Sakai
5	Universidade Federal do Rio de Janeiro	Moodle
6	Universidade Federal de Santa Catarina	Moodle, Blackboard
7	Universidad de Chile	Moodle
8	Universidade Estadual Paulista Júlio de Mesquita Filho	Moodle
9	Universidade Federal de Minas Gerais	Moodle
10	Universidad de Buenos Aires	Moodle

Tabla 4 – Ranking de Latinoamérica y uso de LMS

De la información recolectada se puede identificar las tendencias en cuanto al tipo de LMS usados en la educación universitaria, por ejemplo, que Moodle y Sakai son utilizados en 5 universidades de USA, de igual manera en Europa la plataforma más usada en las 10 universidades con mejor ranking es Moodle, le sigue Blackboard y en tercer lugar Sakai y Fronter. Finalmente, en las 10 mejores universidades de Latinoamérica el sistema de gestión del aprendizaje más utilizado es Moodle, que al parecer tiene una gran aceptación por la academia en nuestro contexto.

Dentro del estudio también se ha considerado como referencia de rankings generalistas mundiales al sitio on line Webometrics por estar considerado entre los siete más destacados de acuerdo con el estudio realizado por (Lorenzo & Cruz, 2015).

De Webometrics se ha tomado a las dos mejores universidades por región para investigar respecto al uso de los LMS en dichas instituciones.

2.2. Análisis situacional de la educación universitaria en el Ecuador

Dentro de la Constitución de la República del Ecuador del año 2008, se generaron importantes cambios en la estructura de las organizaciones que ejercían la regulación, administración y control de la educación superior en el país. Mediante la publicación del Suplemento del Registro oficial No.298, del 12 de octubre de 2010 la Ley Orgánica de Educación Superior, en su artículo 15 menciona a los organismos públicos que rigen el sistema de educación superior, el Consejo de Educación Superior (CES) y el Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior (CEAACES). Así también en el artículo 182 cita:

> La Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT), es el órgano que tiene por objeto ejercer la rectoría de la política pública de educación superior y coordinar acciones entre la Función Ejecutiva y las instituciones del Sistema de Educación Superior (Consejo de Educación Superior, 2010).

Estas tres instituciones CES, CEAACES y SENESCYT generan información sobre la educación superior, la direccionan a través del Sistema Nacional de Información de la Educación Superior del Ecuador (SNIESE), que es un "sistema conectado e integrado que gestiona la información pública de educación superior para la rendición de cuentas y la toma de decisiones de la política pública" (Sistema Nacional de Información de Educación Superior del Ecuador, sf).

En el Ecuador, el *Reglamento para carreras y programas académicos en modalidades en línea, a distancia y semipresencial o de convergencia de medios* emitido por el CES establece una relación con la utilización de los LMS en la educación universitaria.

> Artículo 71.- Plataforma tecnológica. - Todas las Instituciones de Educación Superior (IES) que oferten carreras y programas en línea y a distancia deberán tener una plataforma tecnológica, mediante la cual el estudiante pueda acceder a las aulas virtuales de las asignaturas, cursos o equivalentes y a otras actividades de interacción entre pares, con sus profesores autores, profesores tutores, técnicos docentes y personal administrativo. Estas plataformas deberán apoyar a la organización del aprendizaje, debiendo facilitar espacios para el desarrollo de las actividades de docencia, de prácticas de aplicación y experimentación y de aprendizaje autónomo, como se establece en el Reglamento de Régimen Académico. *Todas las IES que oferten carreras y programas en línea deberán tener aplicaciones informáticas que permitan el acceso a los Campus Virtuales, éstos contendrán aulas virtuales de aprendizaje de tipo LMS (Learning Management System)*, exclusivamente para fines académicos (Consejo de Educación Superior, 2015).

De igual manera, en marzo del año 2016 el CES emitió el *Instructivo de los parámetros específicos de infraestructura tecnológica para carreras y programas en modalidades de estudio en línea, a distancia y semi presenciales*; Que en su artículo 5, sobre recursos digitales indica:

> Artículo 5.- Las IES para ofertar carreras o programas en modalidades de estudio en línea y a distancia, deberán contar con los siguientes parámetros referidos a los recursos digitales:
>
> a. Sistema de gestión del aprendizaje virtual, que permita administrar, distribuir y controlar las actividades del proceso formativo no presenciales de tipo LMS (Learning Management System).
> b. Sistema de gestión de contenidos de tipo CMS (Content Management System), que faculte el intercambio de información entre los usuarios de la plataforma informática y los servicios que contengan los portales electrónicos.
> c. Políticas respecto del tiempo de funcionamiento de las aulas o del campus virtual, que determinen disponibilidad de 24 horas diarias y acceso desde todo tipo de dispositivos electrónicos.
> d. Uso de elementos tecnológicos y comunicativos avanzados dentro del proceso de aprendizaje (herramientas sociales, blogs, wikis, contenidos multimedia, video chats, foros, entornos 3D, videojuegos, etc.)[…] (Consejo de Educación Superior, 2016).

Revisadas las dos normativas, se puede evidenciar las fundamentales implicaciones que tienen los LMS en las modalidades de educación superior semipresencial, en línea o virtual y a distancia, y de igual manera como soporte en las carreras presenciales. Dentro de la investigación se analizó a todas las universidades en categoría A y algunas representativas de la categoría B, para identificar el tipo de LMS que utilizan, las cuales se muestran en la Tabla 5.

Universidad	**LMS**
Escuela Politécnica Nacional	MOODLE
Universidad San Francisco De Quito	DESIRE2LEARN, D2L
Escuela Superior Politécnica del Litoral	CANVAS
Universidad Espíritu Santo (UEES)	BLACKBOARD
Facultad Latinoamericana de Ciencias Sociales Sede Ecuador (FLACSO)	BLACKBOARD
Universidad Andina Simón Bolívar	MOODLE
Universidad de Fuerzas Armadas ESPE	MOODLE
Universidad de Cuenca	MOODLE
Escuela Politécnica del Chimborazo	MOODLE
Pontificia Universidad Católica del Ecuador	MOODLE
Universidad de las Américas (UDLA)	MOODLE

Tabla 5 – Resumen de los LMS utilizados en universidades del Ecuador

2.3. Innovaciones de los LMS en la educación universitaria

Según la comunidad del III Congreso Internacional sobre Aprendizaje, Innovación y Competitividad (CINAIC), que en la parte de su definición de innovación educativa

establece que: "para que se considere innovación educativa el proceso debe responder a unas necesidades, debe ser eficaz y eficiente, además de sostenible en el tiempo y con resultados transferibles más allá del contexto particular" (Fidalgo, & García, 2015). Indicando también que de las diferentes dimensiones del contexto del aprendizaje se profundiza en cuatro características que son: actividad, tecnología, métodos y técnicas y resultados. En la Figura 2 se muestra un mapa de las tendencias en Innovación Educativa y se complementa con la Tabla 6 que describe un resumen de las innovaciones orientadas a los LMS.

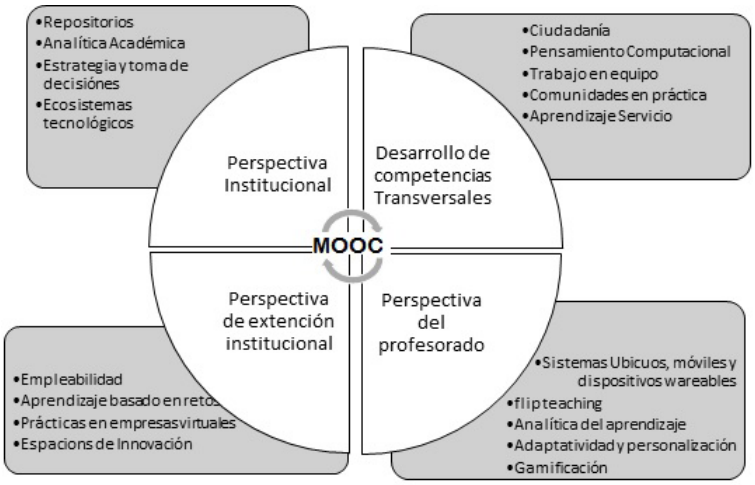


Figura 2 – Mapa de tendencias en Innovación (García, 2015).

Ámbito	Tema	Descripción
Tecnológico	OCW	Iniciativa de compartir los contenidos abriendo la posibilidad de uso, que abarca múltiples instituciones universitarias.
	MOOC	Cursos Masivos Abiertos en línea, catalogados como una innovación disruptiva implementados en importantes universidades del mundo.
	PCE-GA	Evolución de cursos personalizados basados en algoritmos genéticos – Desarrollado por Zhejiang University
	mPLE	Los Entornos Personales de Aprendizaje Móvil, que van acoplados en una nueva arquitectura que consta del LMS y mPLE.
	Gamificación (Serious Game)	Aplicaciones basadas en juegos que apoyan el proceso de enseñanza- aprendizaje
	WhatsApp	Utilización de la aplicación en un LMS
	Video	Inclusión de videos en los LMS

Ámbito	Tema	Descripción
Pedagógico	Modelos	ADIEE. - Serie de pasos relacionados con un proceso educativo ordenado. AZZURE. - Énfasis en identificar características y necesidades reales de los estudiantes
	Metodologías	PACIE. - Enfocando principalmente el esquema pedagógico de la educación real. OOHDM. - Combina el estilo incremental, iterativo y basado en prototipos. Aula Invertida, como la utilizada por la Universidad de Stellenbosch WISE.- Personalización de curso en la Universidad de Oxford
	Web Social	Gestión del aprendizaje en educación superior y la web social
Institucional	Integración de sistemas Weblearn de Oxford	Arquitectura Orientada a Servicios recomendado por el JISC, aplicado en Oxford University
	Arquitectura de un ecosistema de e-learning MIT	Modular Service Framework, es la base del nuevo LMS modular del MIT

Tabla 6 – Innovaciones orientadas a los LMS

Como un ejemplo de caso de éxito de innovación tecnológica institucional, es la realizada por el Profesor Bernd J. Krämer, en la que plantea que los LMS pueden ser gestionados

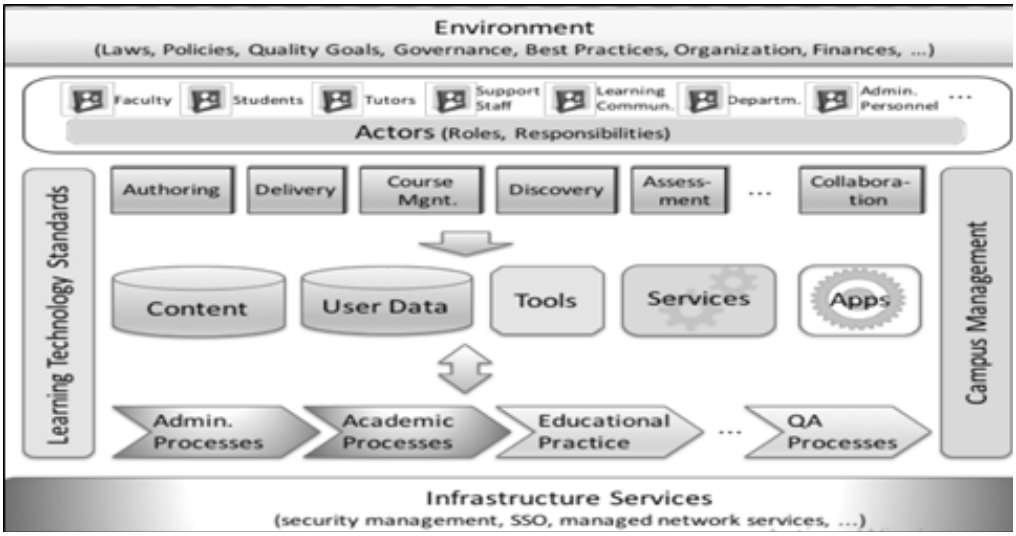


Figura 3 – Concepto y método de AE en un ecosistema e-learning (Krämer, 2015)

mediante la aplicación del concepto y método de Arquitectura Empresarial (AE); Llegando a la conclusión de que "La arquitectura abre el camino a la colaboración entre instituciones en la educación y permite un entorno de soporte de aprendizaje extensible y personalizado." Y propone la arquitectura de un ecosistema de e-learning como se indica en la Figura 3.

3. Resultados

En el análisis de las once instituciones universitarias del Ecuador de acuerdo al presente estudio, se verificó que han seleccionado implementar LMS como Moodle, Blackboard, Canvas y Desire2learn. Los cuales en algunas IES han sido incorporados en la última década y en otras recientemente desde el año 2016. En la Figura 4 se muestra el Modelo de Innovación Tecnológica en los LMS de las universidades del Ecuador

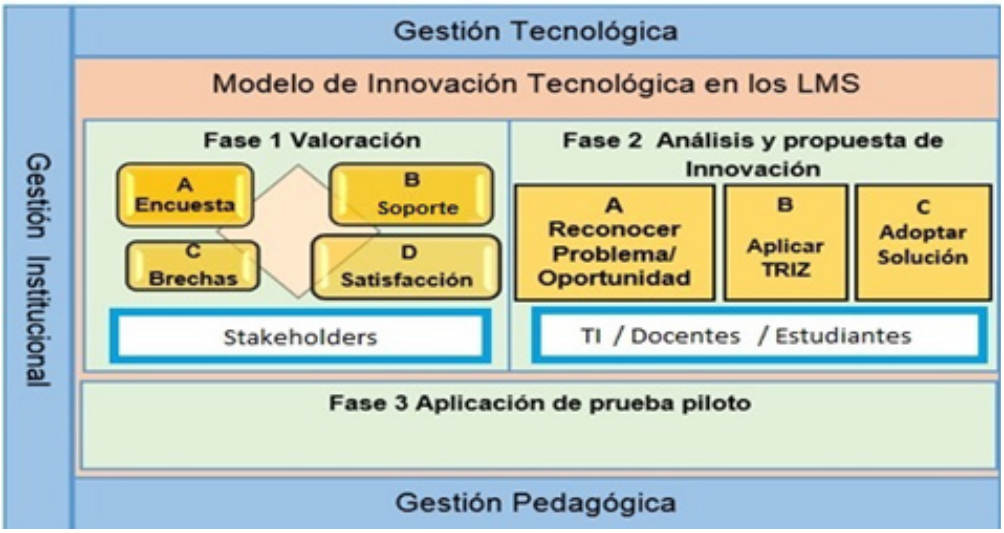


Figura 4 – Modelo de Innovación Tecnológica en los LMS de las universidades del Ecuador

3.1. Fase 1: Valoración del LMS

Descripción. - Para el inicio de la aplicación del modelo propuesto se requiere realizar un análisis de la situación actual (AS-IS) de la IES, para poder proyectar un alcance de innovación tecnológico en el LMS de la institución.

Considerando que las universidades y escuelas politécnicas del país de acuerdo a la normativa vigente, amparada en la Ley de Educación Superior, pueden ofertar sus carreras bajo las modalidades: presencial, semipresencial, a distancia, virtual, en línea y otros; Es importante que la IES establezcan a qué tipo de modalidad se va a aplicar el presente modelo propuesto.

Por lo tanto, para esta valoración se aplicarán las siguientes herramientas:

- Análisis de la situación actual (AS-IS) de la IES
- Encuesta Inicial sobre el LMS.
- Rúbrica de soporte LMS.
- Análisis de brechas del LMS.
- Nivel de satisfacción de los stakeholders (Parte interesada).

Objetivos:

- Identificar el nivel de la estructura de soporte del LMS implementado en la IES.
- Reconocer el estado del LMS mediante un análisis de brechas (GAP).
- Determinar el nivel de satisfacción de los stakeholders de la Institución Universitaria respecto al LMS.

Procedimiento:

Para la adopción del modelo es necesario que exista la aprobación y apoyo de las autoridades dentro de la IES en implementar el LMS, ya sea para solucionar algún problema existente o para ejecutar oportunidades de mejora. Dentro de este contexto para él o los gestores que lideren la implementación del modelo se recomienda las siguientes actividades en esta fase inicial.

- Se presentará la propuesta de aplicación del modelo de innovación tecnológica para LMS como un proyecto ante las máximas autoridades de la IES, destacando sobre todo los objetivos de mejoramiento académico que se persiguen, las justificaciones y los alcances de la propuesta, acompañadas de un cronograma detallado de ejecución de las tres fases.
- Las autoridades emitirán una resolución con la correspondiente aprobación, correcciones o negación de la propuesta presentada.
- El en caso de ser aprobada la propuesta, el líder de la propuesta deberá dirigir una petición al departamento o unidad de Tecnologías o su similar que conste como responsable del LMS, para que conforme un equipo destinado a la implementación del modelo.
- Él o los gestores que lideran la propuesta, junto con el equipo conformado desde el departamento de tecnologías, aplicaran las herramientas de valoración propuestas para el LMS.
- Entregar los resultados y sustentos a las autoridades de la IES.
- Un comité designado por la máxima autoridad de la IES deberá validar los resultados y emitir un informe.

3.2. Fase 2: Análisis y propuesta de innovación.

Descripción. - Una vez que la IES haya realizado su valoración en la fase previa, los gestores de la propuesta de modelo y el equipo conformado deben identificar la oportunidad de mejora o problema de LMS y aplicar la metodología para resolver problema de inventiva o innovación denominado TRIZ, que es una base fundamental en la obtención de soluciones.

Objetivos:

- Establecer cuáles son los problemas u oportunidades de mejora con los que más se identifica la IES respecto al LMS.
- Aplicar la metodología TRIZ mediante la matriz de contradicciones para el LMS.
- Proponer soluciones a los problemas/oportunidades del LMS.

Procedimiento:

- Se conforma un equipo multidisciplinario de personas de la institución que tengan relación con el uso del LMS, (Decano, Administrador, Diseñador Instruccional, Diseñador Gráfico, Tutor, Estudiantes)
- Se determina un posible problema u oportunidad de innovación (uno por participante) que sea aplicable al LMS.
- Se aplica la matriz de Vester para determinar causas y consecuencias de la situación problema/oportunidad.
- Se obtiene el cuadro para establecer el problema crítico resultante.
- Se utiliza la metodología TRIZ, que consta de:
  - Problema particular o específico.
  - Problema genérico.
  - Solución general.
  - Solución específica.
- Se presenta el sustento y solución de los problemas seleccionados ante las autoridades.
- Se solicita autorización de aprobación para implementar las soluciones obtenidas en la fase 3 del presente modelo.

En la Figura 5, se muestra las etapas y resultados de la aplicación de matriz de contradicciones TRIZ

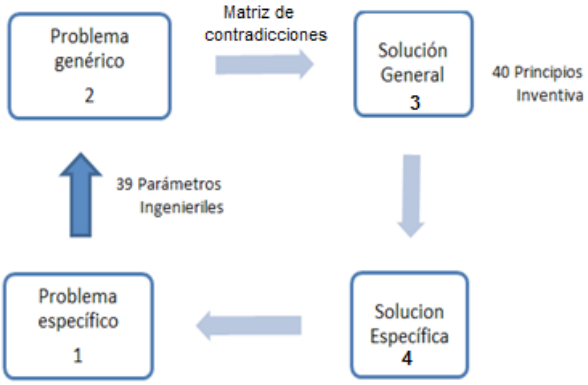


Figura 5 – Etapas y Resultados de la Aplicación de la Metodología TRIZ

1. **Problema específico.** - Identificación del problema/oportunidad del LMS y replanteamiento en términos de T RIZ, estableciendo la relación entre el problema y los parámetros ingenieriles involucrados (mejora / deteriora)

2. **Problema genérico. -** Aplicar la matriz de contradicciones TRIZ.
3. **Solución General**. - Con la identificación de los principios de inventiva determinados en la matriz de contradicciones, se busca una solución general al problema.
4. **Solución específica**. - Se propone posibles soluciones particulares al problema propuesto.

3.3. Fase 3: Aplicación de prueba piloto

Descripción. - Se realiza una etapa de prueba y evaluación del funcionamiento de las soluciones propuestas por los responsables del LMS.

Objetivo:

- Desarrollar una prueba piloto en la IES, que incluya un proceso de evaluación con un grupo determinado de usuarios del LMS.

Procedimiento:

- Se designará un responsable directo preferentemente con un nivel jerárquico decanato o coordinación y un equipo que respalde el seguimiento de la implementación de la prueba piloto del modelo.
- El departamento de TI, realizara la selección de las carreras, alumnos, docentes, cantidad y tipo de cursos en los que se aplicaran las soluciones propuestas a partir del modelo.
- Luego de haberse identificado a cada participante y habiendo culminado las fases previas, se procede a implementar las innovaciones tecnológicas que hayas sido escogidas y se realizará el seguimiento durante al menos un ciclo de estudio (1 semestre)
- Implementar un proceso de evaluación del LMS implementado.
- Los resultados de la prueba piloto serán remitidos a los responsables del LMS, quienes analizaran los mismos y entregaran recomendaciones.
- Los gestores del modelo, revisaran el cumplimiento de las fases y una vez recibido el informe de TI y las recomendaciones de los responsables del LMS, se elabora un informe para las autoridades y solicitaran la aplicación del modelo en toda la IES.

Las autoridades del IES recibirán el informe final y resolverán la aprobación y recomendaciones para la aplicación del modelo LMS en toda la IES.

4. Conclusiones

De la investigación realizada se puede concluir que la búsqueda de adaptación de los LMS en la educación universitaria es una constante que ha tenido su evolución y además se puede distinguir una brecha de utilización y aprovechamiento entre aquellas instituciones de mejor ranking que tienen alrededor de 3 décadas de exploración y las universidades de nuestro país que tienen menos de una década.

Existen innovaciones interesantes que se destacan de acuerdo con los ámbitos: Tecnológico (OCW, MOOC, PCE-GA, mPLE, Gamificación, Serious Game, WhatsApp,

Video). Pedagógico con modelos como (ADIEE y AZZURE) así como metodologías (PACIE y OOHDM) y la Web Social. En cuanto al ámbito institucional se identifican innovaciones como la Integración de sistemas Weblearn de Oxford y Arquitectura de un ecosistema de e-learning MIT.

Dentro del marco regulatorio de las instituciones administradoras de la educación superior del país (CES, CEAACES, SENESCYT), los recientes reglamento e instructivo vinculados a la utilización de los LMS en la educación superior, están orientados a las carreras con modalidades en línea, a distancia y semipresencial o de convergencia de medios.

Entre las universidades ecuatorianas en categoría A y B clasificada por el CEAACES, la mayoría utilizan el LMS open source denominado Moodle y que varias de las instituciones actualmente ofertan los cursos MOOC al público.

Se concluye que fue posible la aplicación de la metodología TRIZ, en la generación del modelo para incorporar innovación tecnológica en los LMS de las universidades.

Se concluye que el modelo propuesto en esta investigación para incorporar innovación tecnológica en los LMS de las universidades, provee un componente útil que es adaptable a las condiciones y características de cualquier universidad o institución de educación superior y que podrá aplicarse independientemente de la experiencia que se tenga con los LMS.

Referencias

Clarenc, C. (2013). *Analizamos 19 plataformas de e-Learning Investigación colaborativa sobre LMS*. [En línea]. Disponible en: http://www.cooperacionib.org/191191138-Analizamos-19-plataformas-de-eLearning-primera-investigacion-academica-colaborativa-mundial.pdf.

Consejo de Educación Superior – CES. (2010). *Ley Orgánica de Educación Superior*. [En línea]. Disponible en: http://www.yachay.gob.ec/wp- content/uploads/downloads/2013/12/LEY-ORGANICA-DE-EDUCACION-SUPERIOR-ANEXO-a_1_2.pdf

Consejo de Educación Superior – CES. (2015). *Reglamento para carreras y programas académicos en modalidades en línea, a distancia y semipresencial o de convergencia de medios*. [En línea]. Disponible en: http://www2.ucsg.edu.ec/distancia/dmdocuments/reglamento_para_carreras.pdf.

Consejo de Educación Superior – CES. (2016). *Instructivo de los parámetros específicos de infraestructura tecnológica para carreras y programas en modalidades de estudio en línea, a distancia y semi presenciales*. [En línea]. Disponible en: http://www.ces.gob.ec/index.php?option=com_phocadownload&view=category&id=12&Itemid=303&limitstart=20.

Ernst & Young. (2013). *Metodología TRIZ para la creatividad e innovación*. Asociación Madrileña de calidad asistencial. Disponible en: https://www.academia.edu/31187429/Asociaci%C3%B3n_Madrile%C3%B1a_de_Calidad_Asistencial_Metodolog%C3%ADa_TRIZ_para_la_creatividad_e_innovaci%C3%B3n.

Fidalgo & García. (2015). *Mirando hacia el futuro: Ecosistemas tecnológicos de aprendizaje*. III Congreso Internacional sobre Aprendizaje, Innovación y Competitividad (CINAIC 2015). (págs. 554-558). Madrid. España.

García, F. (2015). *Mapa de tendencias en Innovación Educativa*. Mapa de tendencias en Innovación Educativa (págs. 6-7). Madrid: Universidad de Salamanca.

García, L. (2011). *La educación a distancia*. Disponible en: http://www.terras.edu.ar/aula/cursos/3/biblio/GARCIA_ARETIO_Lorenzo-CAP_2_(fragmento)-Perspectiva_historica.pdf

Gonzales, E. (2015). *Las TIC en la Educación Superior*. Disponible en: http://prometeo.educacionsuperior.gob.ec/las-tic-en-la-educacion-superior/.

Indicadores NRI. (2014). *Comparativo Indicador NRI (Finlandia, Chile, Ecuador Año 2014)*. [En línea]. Disponible en: https://observatoriotic.mintel.gob.ec/indicadores-2/.

Krämer, B. (2015). Time to Redesign Learning Spaces. United States of America. [En línea]. Disponible en: https://www.researchgate.net/publication/282666337_Time_to_Redesign_Learning_Spaces

Lorenzo & Cruz. (2015). *Calidad y evaluación de la educación superior y una perspectiva transnacional a través de los ranking*. [En Línea]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/5168194.pdf

MINTEL. (2014). *Ecuador sigue escalando posiciones en índice de reducción de brecha digital y uso de las TIC*. [En línea]. Disponible en: http://www.telecomunicaciones.gob.ec/ecuador-sigue-escalando-posiciones-en-indice-de-reduccion-de-brecha-digital-y-uso-de-las-tic/

Pontificia Universidad Javeriana. (sf). *Proyecto evaluación LMS*. Cali, Colombia, [En línea]. Disponible en: http://portales.puj.edu.co/javevirtual/proyecto_evaluacion/documentos/Proyecto_Evaluacion_LMS.pdf.

UNESCO. (2016). *Las TIC en la educación*. Disponible en: Obtenido de https://es.unesco.org/themes/tic-educacion.

Unión Internacional de Telecomunicaciones – UIT. (2015). *Informe sobre Medición de la Sociedad de la Información*". Ginebra. Suiza. [En línea]. Disponible en: https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ICTOI-2015-SUM-PDF-S.pdf.

Weller, M. (2009). *The centralization dilemma in educational IT*. The Open University, Reino Unido.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 11/12/2017
Aceitação/Acceptance: 28/03/2018

Gestión emergente de espacios colaborativos de aprendizaje

Luis Barba-Guamán[1], Priscila Valdiviezo-Diaz[1], José Aguilar[2]

lrbarba@utpl.edu.ec, pmvaldiviezo@utpl.edu.ec, aguilar@ula.ve

[1] Universidad Técnica Particular de Loja, 1101608, Loja, Ecuador.

[2] Universidad de los Ándes, Mérida, Venezuela.

Pages: 271–281

Resumen: Este modelo propone la auto-gestión de espacios de aprendizaje colaborativo, basados en el paradigma de sistemas emergente. Dada la dinámica presente en los espacios de aprendizaje mediados por las Tecnologías de Información y Comunicación (TICs), la aparición de procesos de aprendizaje colaborativo ha emergido como una forma de aprendizaje cada vez más utilizada. En ese sentido, se requieren de nuevos mecanismos que permitan la auto-configuración de comunidades de aprendizaje, en base a las características de los aprendices y del dominio de conocimiento. En este trabajo, proponemos un sistema de auto-gestión de espacios colaborativos de aprendizaje, usando enfoques de la programación emergente, y en particular, el modelo de "agregación". Basado en esa estrategia, el sistema es capaz de auto-organizar las comunidades de aprendizaje, haciéndolas hacer aparecer/desaparecer, o actualizándolas, en función de las características de los aprendices. Los resultados preliminares a pequeña escala son motivadores, ya que permite la auto-gestión de dichas comunidades.

Palabras-clave: Sistemas inteligentes, educación, sistemas emergentes, espacios colaborativos, comunidades de aprendizaje.

Emergent management of collaborative learning spaces

Abstract: This model proposes the self-management of collaborative learning spaces based on the emerging systems paradigm. Given the dynamics present in learning spaces mediated by Information and Communication Technologies (ICT), the emergence of collaborative learning processes has emerged as a form of learning increasingly used. In this way, new mechanisms are required that allow the self-configuration of learning communities based on the characteristics of the learners and knowledge domain. In this work, we propose a system of self-management of collaborative learning spaces, using emerging programming approaches, and particulary, the "aggregation" model. Based on this strategy, the system is capable of self-organize learning communities, making them appear / disappear, or updating them, depending on the features learners. Preliminary results on a small scale are motivating, since it allows the self-management of these communities.

Keywords*:* Intelligent systems, education, emerging systems, collaborative spaces, learning communities.

1. Introducción

El interés del uso de los espacios colaborativos de aprendizaje, tiene que ver con su posibilidad para la creación espontánea de comunidades de aprendizaje, de tipo abiertas, no predeterminadas, que emergen o desaparecen según los procesos de aprendizaje. Los espacios colaborativos de aprendizaje posibilitan nuevos paradigmas emergentes de aprendizaje, que rompen con las limitaciones de las teorías clásicas de aprendizaje (como el constructivismo, el conductismo y el cognitivismo), para explotar la no linealidad y la incertidumbre de los entornos de aprendizaje mediados por la Internet. Un ejemplo de esos paradigmas de aprendizaje es el conectivismo (Mosquera & Aguilar, 2015; Siemens, 2005), el cual se basa en conectar fuentes de conocimiento y actores del proceso de enseñanza-aprendizaje, para conformar comunidades especializadas de aprendizaje, como estrategias de aprendizaje.

Ahora bien, un aspecto fundamental para esos entornos de aprendizaje tiene que ver con la creación de Redes de Conocimiento, o lo que nosotros hemos denominados en este trabajo como, espacios colaborativos de aprendizaje. En ese sentido, estos nuevos paradigmas emergentes de aprendizaje requieren de mecanismos, plataformas, entre otras, que permitan la creación y gestión de espacios de gestión colaborativa. En específico, se requieren de herramientas que permitan formar, analizar y evaluar estos espacios, que emerjan como consecuencia del proceso de aprendizaje.

Nuestra propuesta se enfoca en proveer una herramienta para la autogestión de espacios colaborativos de aprendizaje, que puede ser usada tanto en espacios para el aprendizaje formal como en los espacios de aprendizaje informal, como los promovidos desde el eco-conectivismo (Mosquera & Aguilar, 2015). En particular, es una propuesta de autogestión de espacios colaborativos de aprendizaje usando la teoría de sistemas emergentes. De esta manera, los modelos emergentes permiten la aparición y desaparición de los espacios colaborativos de aprendizaje, basado en las características de los individuos (estudiantes) y de los mismos espacios en un momento dado.

2. Espacios colaborativos de aprendizaje y Sistemas emergentes

De acuerdo con (Andr, Roa, Andr, Morales, 2016; Snowdon, Churchill, & Munro, 2001), los espacios colaborativos de aprendizaje se definen como puntos de encuentro entre la academia, las tecnologías, y los profesores y estudiantes, que no están necesariamente físicamente contiguos (Rodríguez, et al., 2012) Su propósito es complementar los procesos educativos que se dan dentro del aula, al estimular el uso de espacios alternos, informales, físicos o virtuales, no necesariamente enmarcados en el contexto académico, para llevar a cabo el acto educativo (Dongfeng, et al., 2015).

Algunos trabajos se han enfocado al desarrollo de ambientes de aprendizaje colaborativos, presentando arquitectura para dichos ambientes, tomando en cuenta tecnologías emergentes (Corrie, et al., 2003) y juegos serios (Donfeng, Barba-Guamán, Valdiviezo-Díaz, Riofrio, 2017), entre otros. En (Vilanova, 2016) se presenta un modelo pedagógico emergente para el trabajo colaborativo y desarrollo de proyectos basados en casos reales en el ámbito universitario.

Ahora bien, un elemento esencial es la capacidad de autogestión de los espacios colaborativos, tal que ellos puedan emerger, fusionarse, actualizarse o desaparecer, en función de las dinámicas de aprendizaje y características de los individuos (estudiantes). Al respecto, no existen muchos trabajos en la literatura. En ese sentido, en este trabajo se propone un enfoque de autogestión de los espacios colaborativos basados en los sistemas emergentes

En ese sentido, la "emergencia" ha sido definida en (Aguilar, 2014) como "un comportamiento de un sistema, que emerge desde las interacciones entre sus componentes, difíciles o imposibles de predecir". La emergencia permite explicar algunos fenómenos habitualmente inexplicables, pero también, es posible coadyuvar a la aparición de dinámicas emergentes. Es esta la arista de interés en este trabajo, en particular, para posibilitar la emergencia de espacios colaborativos de aprendizaje que posibiliten procesos modernos de aprendizaje. En general, en los sistemas emergentes se pueden constatar la macro-inteligencia y la adaptabilidad, productos de un conocimiento local, basado en 5 principios básicos (para más detalles, ver (Aguilar, 2014)): i) Entre más miembros es mejor; ii) La ignorancia es útil; iii) Se deben provocar encuentros casuales; iv) Se deben buscar patrones en los signos; v) Es importante prestar atención a sus vecinos.

A partir de esos principios, es posible la aparición de sistemas emergentes en diferentes contextos. Por ejemplo, en la literatura se han analizado sistemas emergentes en la ecología (por ejemplo, para describir el ecosistema de los lagos (Fernandez, Aguilar, Gershenson, Piña, 2017), en Internet (por ejemplo, para describir las dinámicas alrededor de Wikipedia (Perozo, Aguilar, Terán & Molina, 2013)), en las ciudades (por ejemplo, para describir sus comportamientos del trafico (Zubillaga,2014), en la biología (para describir el comportamiento del cerebro), entre otros.

En la literatura se han propuesto varios modelos emergentes, especialmente, basados en los comportamientos de los insectos. Es así como se han propuestos modelos de asignación de tareas, de agregación, entre otros, inspirados en las hormigas, abejas, entre otros insectos. Así, las sociedades de insectos han sido muy utilizadas como fuentes de inspiración, para proponer modelos de comportamiento emergente. En particular, en este trabajo estamos interesados en un modelo de Agregación.

La agregación es uno de los fenómenos sociales más básicos (muchas actividades de los insectos sociales están vinculadas a la misma), y juega un papel esencial en la organización del comportamiento social en las sociedades de insectos. La agregación actúa como reguladora de las actividades colectivas. Los patrones de agregación son muy diversos. Un ejemplo clásico es la tendencia de las hormigas, abejas, etc. de agregar los huevos y larvas en montones separados. El modelo de agregación que nos interesa en este trabajo, consiste en que los elementos deben ser recogidos si sus vecinos son diferentes, y dejados en un lugar donde varios de los elementos de ese tipo estén presentes. Así, la probabilidad de que en un movimiento al azar de un trabajador sin carga encuentre un objeto para recoger en un punto, viene dado por:

$$P_r = \left(\frac{K_1}{K_1 + f}\right)^2 \quad (1)$$

Donde, f es la fracción percibida de elementos iguales en la vecindad del trabajador, k1 es un umbral (constante). Cuando $f << k_1$, P_r es cercano a 1, es decir, la probabilidad de recoger un elemento es alta cuando no hay muchos elementos similares en la zona. Por otro lado, la probabilidad de depositar un objeto, de un trabajador con carga, es:

$$P_d = \left(\frac{f}{K_2 + f}\right)^2 \quad (2)$$

Donde, k2 es otro umbral (constante). Para $f >> k_2$, P_d es cercano a 1 (es decir, la probabilidad de depositar un elemento es alta cuando hay muchos elementos similares en la zona). Este modelo puede ser fácilmente extensible cuando se tienen diferentes tipos de objetivos en el ambiente.

3. Diseño del modelo emergente

El sistema de autogestión de espacios colaborativos de aprendizaje permite la creación de comunidades de aprendizaje, las cuales van emergiendo conforme a los perfiles y necesidades de los participantes. Además, permite el auto-ajuste de espacios colaborativos de aprendizaje, tal que los mismos se puedan redefinir autónomamente,

Este modelo considera variables del contexto educativo, las cuales permiten establecer las comunidades o espacios colaborativos del sistema emergente. El sistema se adapta a las necesidades que surjan en la comunidad, a fin de lograr una colaboración eficaz. La tabla 1 presenta las variables usadas en el modelo, pero puede ser extendido para considerar otras varias del proceso educativo que impacten los espacios colaborativos de aprendizaje. Cada una de ellas puede ser caracterizada desde entornos reales. Por ejemplo, el nivel de interactividad puede ser definido según el uso de foros, chats, etc. por parte de los estudiantes. De esta manera, se puede caracterizar el comportamiento de cualquier estudiante/individuo (e_1, e_2 y e_3.), tal que el valor 0 o 1 representan el no cumplimiento o cumplimiento de ese comportamiento en un individuo dado. Igual son caracterizadas el resto de las variables.

Categoría
Nivel de interacción
Uso de herramienta
Rendimiento académico

Tabla 1 – Variables de la comunidad de aprendizaje.

El modelo matemático se basa en el modelo de “agregación” de una sociedad de insectos, presentado en la sección 2. El modelo matemático utiliza las ecuaciones 1 y 2 definidas en la sección 3. Ahora bien, en este caso f es sustituido por d, y las variables del modelo tienen el siguiente significado: *Pr* es la probabilidad de recolección; *Pd* es la probabilidad de depósito; k_1 y k_2 son umbrales (constante), y d es la distancia que hay entre las características del individuo y la comunidad de aprendizaje.

En ese sentido, nuestro modelo requiere determinar el patrón de cada comunidad Ca, para lo cual usa las características de los individuos que la conforman (e_1, …, e_n). Este patrón es un vector, que se obtiene según la Tabla 2:

Ca	Cra
$X_{11}...X_{1n}$	max{ $X_{11}...X_{1n}$ }
$X_{21}...X_{2n}$	max{ $X_{21}...X_{2n}$ }
...	...
$X_{k1}...X_{kn}$	max{ $X_{k1}...X_{kn}$}

Tabla 2 – Patrón de la comunidad de aprendizaje C_a.

Donde: Cr_a: Patrón de la comunidad de aprendizaje *a*; *n*: número total de individuos que pertenecen a la comunicad de aprendizaje; *k*: número de características de la comunidad; X_{ij}= {1 si se cumple ese comportamiento *i* en ese individuo *j*; 0 de lo contrario, ver Tabla 1}

Con ese patrón, ahora podemos comparar cualquier individuo con una comunidad de aprendizaje. Para ello, se utiliza la ecuación 3:

$$S_{i,Ca} = \sum_{j=1,k} comparar\,(X_{ji}, Cra_j) \tag{3}$$

Donde: $S_{j,Ca}$: Es la distancia del individuo *i* a la comunidad *Ca*; *comparar (entrada1, entrada2)*: método que compara la entrada1 y entrada2, tal que si entrada1 = entrada2 el valor de salida es 0, caso contrario el valor de salida es 1.

Ahora se calcula el inverso de la distancia que existe entre el patrón de características de cada individuo y el patrón de cada comunidad:

$$d = \frac{1}{S_{i,Ca}} \tag{4}$$

En las ecuaciones (1) y (2) se usa el valor de (4), para determinar si un individuo debe dejarse o retirarse de una comunidad, y en este último caso, a cuál comunidad debe moverse, de la siguiente manera:

1. Si *Pr(i, Ca)* es mayor a un U_1, el individuo i tiene que retirarse de la comunidad Ca. En caso contrario, deje dejarse en dicha comunidad.
2. *Si Pd(i, Ca)* es mayor a un U_2, el individuo i se debe mover a la comunidad Ca, de otra manera se debe continuar identificando la comunidad de aprendizaje a la que debe pertenecer ese individuo (puede ser una existente, o creársele una nueva compuesta por él).

Donde U_1 y U_2 son los valores límites de las probabilidades, para determinar si se debe mover o asignar un individuo en una comunidad.

A continuación, el primer macro-algoritmo, el cual determina qué debe hacer el sistema: si crear una nueva comunidad (sino existen) o actualizar las existentes, lo que eventualmente puede conllevar a fusionarlas.

```
#Macro-algoritmo 1. Creacion de comunidades
Inicio creacion_comunidades
Si Comunidades==0
     Crear Comunidades
Sino
          Si ya existen comunidades de aprendizaje
            Reajustar comunidades
Fusionar comunidades
Fin creacion_comunidades
```

Ahora, pasamos a describir a cada macro-algoritmo invocado por el de creación de comunidades.

El macro-algoritmo *crear comunidades* es utilizado en el caso en el que no existe comunidades creadas, es decir, donde $C=0$, que es cuando llega un nuevo individuo y no existe ninguna comunidad creada. El primer paso sería crear un espacio colaborativo formada por el mismo individuo. En caso de que llegue otro individuo y exista alguna comunidad, se deberá realizar la comparación entre el individuo y el patrón de las comunidades existentes (ver ecuación 3), para verificar si el individuo cumple las condiciones para ser depositado en alguna de esas comunidades. Caso contrario, se debe crear una nueva comunidad, y así sucesivamente, para los nuevos individuos que vayan apareciendo en el sistema.

```
#Macro-algoritmo 2. Crear comunidades
Repetir por cada individuo nuevo
Si C == 0
    Formar nueva comunidad          # Crear C1
    Patrón C1= valor de las características
Sino
  Si la comunidad tiene un solo individuo
      Patrón Cra= Obtener patrón
  Sino
        Calcular el patrón de cada comunidad Cra
# Calcular la d entre el patrón de características del
# individuo nuevo y el patrón de la comunidad
Calcular Pd usando la ecuación 2
Si Pd > U2 entonces
  Calcular Cj = max(Pd(ei,Ca+1))
  Depositar ei,Cj
```

```
Sino
  Formar nueva comunidad                    #Crear Cn+1
Fin repetir
```

Ahora bien, el sistema de autogestión de comunidades puede conseguir un entorno de aprendizaje donde ya existan los espacios colaborativos de aprendizaje. En ese caso, el interés no es determinar donde asignar un nuevo individuo, sino reajustar las comunidades creadas en períodos anteriores, con individuos agrupados no necesariamente con similares características. Para solucionar esta problemática, se plantea el macro-algoritmo 3. En este escenario, lo que se hace es un reajuste de las comunidades, este reajuste consiste en ir verificando si los individuos que conforman una comunidad comparten similares características. Caso contrario, deben ser retirados de las comunidades en las que se encuentran, y depositados en las que cumplan con el requerimiento de similaridad (ver ecuación 2). Así, para esos individuos a migrar, el sistema primero verificará si el individuo puede ser depositado en una comunidad existente, caso contrario se deberá crear una nueva comunidad.

```
#Macro-algoritmo 3. Reajuste de comunidades
Repetir para todos los individuos
Calcular el patrón de cada comunidad Cra
Repetir para cada individuo en cada comunidad
  Calcular la distancia
      Si Pr >U1 entonces
      Mover individuo de esa comunidad
Fin repetir
Calcular la d entre el individuo a mover con el patrón de las
otras comunidades
Calcular Pd usando Ec. 2

Si Pd > U2 entonces
   Calcular Cj = max(Pd(ei, Ca+1))
     Depositar ei,Cj
Sino
     Formar nueva comunidad
Fin repetir
```

Una vez que se tienen las comunidades creadas, se debe entrar a una fase para verificar si existen comunidades iguales. Para ello, se debe pasar por un proceso de análisis de las posibles fusiones de comunidades, usando el macro algoritmo 4. El macro algoritmo 4 lo que hace es verificar los centroides entre comunidades, si estos son iguales, entonces las comunidades se deben fusionar, y nuevamente hacer el proceso de retirar los individuos que no se ajusten a esa comunidad, y hacer el reajuste de esta.

```
#Macro-algoritmo 4:    Fusión de comunidades
Pr = Buscar_patron_de_comunidades(M_comunidades)
```

```
Repetir la comparación de patrones de Pt
Comparar_patrones(Pr)
    Si Comparar_Patrones > Umbral
  Separar individuos de la comunidad
Fin_Repetir
  Enviar a reajustar
```

4. Validación de comunidades

Para validar la calidad de las comunidades creadas, se utilizan las métricas de cohesión y separación, para diferentes valores de los parámetros del modelo. En particular, se consideró como parámetro clave en este proceso al U_2, por ser el umbral que tiene que ver con el depósito de individuos en las comunidades. La idea es conocer si el modelo presenta buen desempeño en la construcción de las comunidades.

Cohesión: Esta métrica consiste en que el individuo de cada comunidad debe estar lo más cercano posible a los otros individuos de la misma comunidad. Esta métrica se calcula considerando la distancia promedio entre los elementos de la comunidad y su centroide. Para obtener esta métrica, se usa la ecuación siguiente:

$$Co = \frac{1}{n}\sum_{i=1}^{n} |C_i - x_i| \tag{5}$$

Donde:
n: número de individuos en la comunidad
C_i: Centroide de la comunidad (patrón de la comunidad)
$C_i - x_i$ hace una comparación de todas las características de cada individuo con respecto a las características del centroide.

Separación: El objetivo de esta métrica es que las comunidades deben estar ampliamente separadas entre ellas. El enfoque utilizado para obtener esta métrica es la distancia entre los patrones de la comunidad (centroides). Para el cálculo se utiliza la ecuación siguiente:

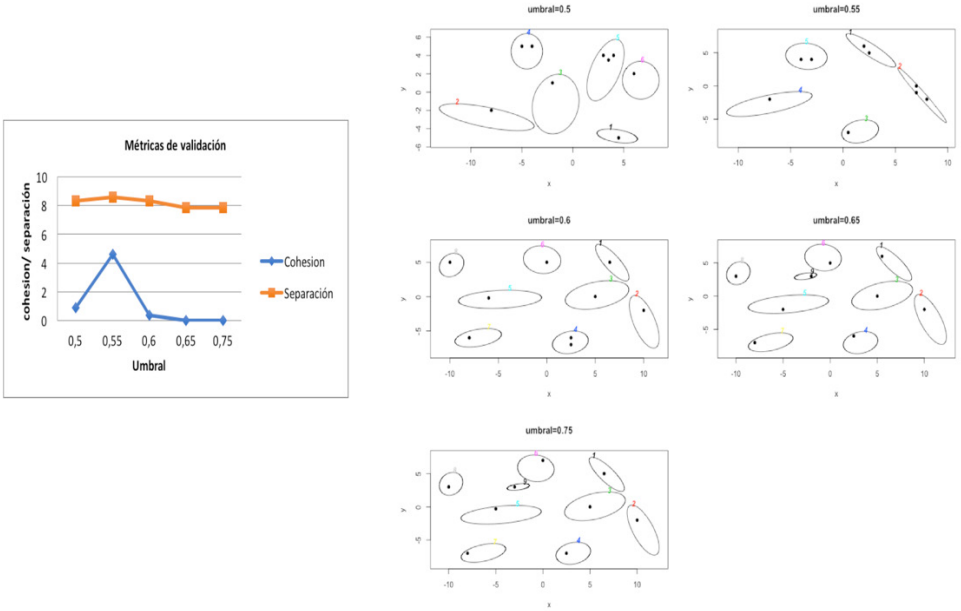
$$Sep = | C_i - C_j | \tag{6}$$

$C_i - C_j$ hace una comparación de todas las características de los centroides que se están comparando.

U2	Cohesión	Separación
0,5	0,69	8,33
0,55	**0,99**	**8,6**
0,6	0,84	8,33
0,65	0,90	7,83
0,75	0,90	7,83

Tabla 3 – Resultado de las métricas de cohesión y separación.

Basados en los resultados de la tabla 3 y en la figura 1.b, se observan que hay umbrales que separan más las comunidades, pero crean grupos muy débiles (compuesto por pocos individuos). Así mismo, hay umbrales que crean grupos muy compactos, pero con separación muy débil entre ellos. En ese sentido, es fundamental conseguir un equilibrio entre ambas métricas, con un valor de umbral que permita alcanzarlo. En particular, en la figura 1 se pueden observar las comunidades finales que emergieron para diferentes valores de U_2. El umbral que mejor desempeño presenta es 0.55, con el cual se obtienen 5 comunidades finales. Con este umbral se obtuvo una mejor agrupación entre individuos, y una mejor separación entre comunidades (logra un mejor equilibro entre esos dos criterios de calidad).



a) Métrica de cohesión y separación b) Comunidades resultantes con diferentes valores U_2

Figura 1 – Resultados de la experimentación

5. Conclusión

En el presente trabajo, hemos propuesto un sistema de autogestión de espacios colaborativos de aprendizaje basado en sistemas emergentes, los cuales permiten que emerjan, se fusionen, se actualicen o desaparezcan los mismos, en función de las dinámicas de aprendizaje y características de los individuos (estudiantes). Este enfoque es fundamental para los nuevos enfoques pedagógicos, como el eco-conectivismo, en orden a permitir la adaptación a las dinámicas de aprendizaje mediadas por la Internet.

Por otro lado, las métricas de cohesión y separación buscan crear comunidades conformadas por el mayor número de individuos bien diferenciadas, penalizando las

comunidades con individuos solitarios. Así, es necesario busca un buen equilibrio entre ambas métricas, para cumplir con el objetivo de autogestión emergente. Nuestro modelo logra alcanzar ese equilibrio a través de U_2, el cual determina cuando agregar un individuo en una comunidad.

Próximos trabajos deben considerar varios aspectos: explorar otros modelos de agregación de la teoría de los sistemas emergentes (Aguilar, 2014), considerar otras variables del contexto educativo para caracterizar las comunidades (como por ejemplo, los estilos de aprendizaje), analizar cómo obtener un valor de U_2 optimo usando las propiedades presentes en la dinámica del proceso de aprendizaje bajo estudio, y finalmente, convertir este tipo de sistemas en servicios de analítica de aprendizaje (Aguilar et al.,2017) para aulas inteligentes (Aguilar, Valdiviezo, Cordero, & Sánchez, 2015).

Referencias

Aguilar, J. (2014). Introducción a los Sistemas Emergentes. *Talleres Gráficos,* Universidad de Los Andes.

Aguilar, J., Valdiviezo, P., Cordero, J., & Sánchez, M. (2015). Conceptual Design of a Smart Classroom Based on Multiagent Systems. *Int'l Conf. Artificial Intelligence - IICAI*, 471–477.

Aguilar, J., Sánchez, M., Cordero, J., Valdiviezo-Díaz, P., Barba-Guamán, L. Chamba-Eras, L. (2017). Learning analytics tasks as services in smart classrooms, *Universal Access in the Information Society*.

Andr, N., Roa, M., Andr, O., Morales, S. (2016). Espacios colaborativos para la enseñanza de las ciencias administrativas y contables: un reto a las tensiones históricas de la universidad latinoamericana, 1, 58–72.

Corrie, B., Wong, H., Zimmerman, T., Street, W. H., Marsh, S., Patrick, A. S., Emond, B. (2003). Towards Quality of Experience in Advanced Collaborative Environments 2. *Barriers to the Use of Collaborative*, 1–8.

Dongfeng, L., Valdiviezo-Díaz, P., Riofrio, G., Yi-Meng, S., Barba, L. (2015). Integration of Virtual Labs into Science E-learning. *Procedia Computer Science, 75*, 95–102.

Donfeng, L., Barba-Guamán, L., Valdiviezo-Díaz, P., Riofrio, G. (2017). Intelligent tutoring Module for a 3D game-based science e-learning platform. *Inteligencia Artificial, 20(60)*, 1–19.

Fernandez N., Aguilar, J. Gershenson C., Piña C. (2017). Complexity of Lakes in a Latitudinal Gradient, *Ecological Complexity. 31*, 1–20.

Mosquera, D., & Aguilar, J. (2015). Middleware Reflexivo para la gestión de Aprendizajes Conectivistas en Ecologías de Conocimientos (eco-conectivismo). *Latin-american Journal of Computing - LAJC,* 25–32.

Perozo N, Aguilar, J., Terán O., Molina H. (2013). A Verification Method for MASOES, Coautores: *IEEE Transactions on Systems, Man, and Cybernetics: Part B, IEEE Society, 43(1)*, 64–76.

Siemens, G. (2005). Connectivism: A learning theory for the digital age. *International Journal of Instructional Technology & Distance Learning*.

Snowdon, D., Churchill, E. F., & Munro, A. (2001). Collaborative virtual environments: Digital spaces and places for CSCW: An introduction. *En Collaborative Virtual Environments,* 3–17.

Rodríguez, D., García-Martínez, R., Merlino, H., Charczuc, N., Lacabanne, Caracciolo, B., Iglesias, F. (2012). Espacios virtuales para trabajo colaborativo. *3901(1826)*, 1116–1120.

Vilanova, G. E. (2016). Modelo pedagógico emergente en la formación mediada por tecnología de ingenieros en el ámbito universitario, *(Cisci)*, 239–244.

Zubillaga D., Cruz G., Aguilar L., Zapotecatl L., Fernandez N., Rosenblueth D., Aguilar, J. Gershenson C. (2014). Measuring the Complexity of Self-organizing Traffic Lights. *Entropy, MDPI AG, 16, (5)*, 2384–2407.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 03/12/2017
Aceitação/Acceptance: 11/03/2018

Metodología contra Vulnerabilidades en Ambientes de Aprendizaje Virtuales

Diego Fernando Baroja Llanos[1], Luis David Narváez Erazo[2]

dfbaroja1@pucesi.edu.ec, ldnarvaez@pucesi.edu.ec

[1] Pontificia Universidad Católica del Ecuador Sede Ibarra, Alpachaca, 100150, Ibarra, Ecuador.

[2] Pontificia Universidad Católica del Ecuador Sede Ibarra, Ada. Eugenio Espejo, 100150, Ibarra, Ecuador.

Pages: 282–291

Resumen: Los ambientes de aprendizaje virtuales en todas las instituciones educativas a nivel mundial han evolucionado de forma incomparable, tanto información a nivel académico como investigativa, han generado millones de datos y que estos son compartidos por medio del conocimiento, las instituciones educativas solo miran el funcionamiento, la disponibilidad de los recursos didácticos, pero no se ha pensado que detrás de un servidor orientado al manejo de entornos virtuales pueden estar varios usuarios con un fin nada ético para sabotear la información, accediendo de forma inusual para realizar cambios de notas, denegación de servicios, y lo más preocupante acceder al resto de información de todas las áreas en lo particular áreas financieras y operativas, todo esto marca la posibilidad que los ambientes virtuales de aprendizaje no cuenten con metodologías apropiadas entorno a la seguridad informática, lo que implica tener un alto riesgo de ser las posibles víctimas de un ataque informático.

Palabras-clave: Palabras Clave – Test de penetración, Campus Virtual, Seguridad en Internet, Aprendizaje en línea.

Methodology against Vulnerabilities in Virtual Learning Environments

Abstract: he virtual learning environments in all educational institutions worldwide have evolved incomparably, both information at the academic and research level, have generated millions of data and that these are shared through knowledge, educational institutions only look at the operation, the availability of didactic resources, but it has not been thought that behind a server oriented to the management of virtual environments can be several users with an unethical purpose to sabotage the information, accessing in an unusual way to make changes of notes, denial of services , and most worrying to access the rest of the information of all the areas in the particular financial and operational areas, all this marks the possibility that virtual learning environments do not have appropriate methodologies around computer security, which implies having a high risk of being the possible victims of an attack computer.

Keywords*:* Keywords - Penetration test, Virtual Campus, Internet Security, Online Learning.

1. Introducción

El vertiginoso crecimiento de las comunicaciones ha desatado una problemática muy puntal sobre el mundo de las seguridades de la información, es importante que todas las empresas e instituciones financieras, bancarias, educativas, plataformas de gobiernos electrónicos, los cuales administran información en la web, más aún si ésta información es de valiosa importancia para quienes están detrás de un computador planificando la forma de cómo acceder a ella en forma no autorizada, con el fin de apropiarse de ella o quizás adulterarla para buscar beneficio de algo encontrado como claves de acceso, o en el peor de los escenarios destruirla, boicotearla, estos pueden ser unos cuantos ejemplos de lo que podría pasar con la información si no se toman las medidas necesarias para controlar todas las posibles vulnerabilidades que pueden llegar a suscitarse. (Cano Ramírez, 2014).

La evolución de la educación a nivel mundial se ha dado gracias a la masificación del internet, la educación en línea es la nueva forma de llegar a muchas partes de mundo entero, compartir grandes cantidades de recursos educativos, que sin duda forman al estudiante con las destrezas necesarias para estar a la vanguardia de los últimos conocimientos en todas las áreas de formación. (Narváez, 2017)

El desarrollo de la metodología contra vulnerabilidades en ambientes virtuales de aprendizaje ha tomado en cuenta las recomendaciones y parámetros del proyecto de evaluación de vulnerabilidades OWASP (Open Web Application Security Project) (Meucc & Muller, 2014), la propuesta contiene las siguientes etapas:

- Fase de planificación.
- Fase de actuación.
- Fase de generación de informes

En la figura 1 se presentan las fases de la metodología desarrollada para la mitigación de vulnerabilidades.

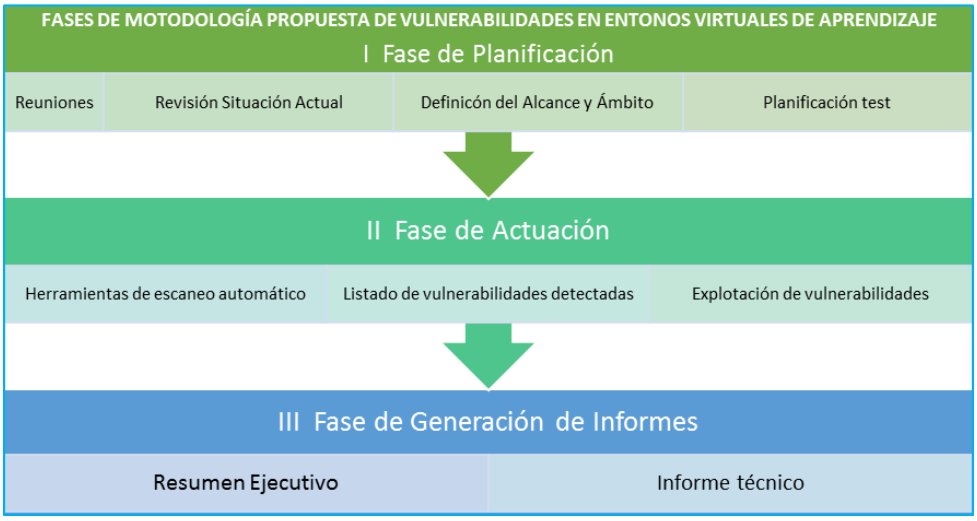


Figura 1 – Fases de las metodologías propuestas de vulnerabilidades en entor nos virtuales de Aprendizaje (Baroja, 2017)

2. Fundamentación Técnica Auditoria De Aplicaciones Web

2.1. Vulnerabilidades

Las vulnerabilidades se las conocen como una debilidad que pueden poner en riesgo la seguridad de un sistema informático, se las puede clasificar en los siguientes aspectos de acuerdo a recursos TIC. (Peña Torres, 2016).

1. *Diseño:*

- Deficiencia y debilidad en la implementación de protocolos de red.
- Deficiencia o inexistencia de políticas de seguridad.

2. *Implementación*

- Deficiencias y errores de programación.
- Mala configuración por dejar puertas traseras abiertas dentro de un sistema informático.

3. *Uso*

- Deficiente configuración de sistemas informáticos.
- Poco conocimiento de los usuarios por políticas de autenticación.
- Falta de incentivo de administradores a los usuarios a manejar adecuadamente los sistemas de información.
- Proliferación de herramientas que generan ataques informáticos.
- Poco incentivo de los gobiernos por implementación de políticas de seguridad.

2.2. Explotación de vulnerabilidades web

En la actualidad un servidor de aplicaciones web que carezca de protección y sin la aplicación de una auditoria de código sería el blanco perfecto para sufrir ataques con todas las facilidades que la tecnología desarrolla cada día, por lo que es viable la implementación de técnicas para la revisión de filtros y cuando estos no cuentan con el respectivo funcionamiento, el atacante puede aprovechar de estos descuidos de parte de los desarrolladores y ser víctimas de dichos ataques. (Tilborg & Jajodia, 2011).

Las vulnerabilidades web más comunes que se deben considerar al momento de aplicar el plan de seguridad de datos para un servidor de aplicaciones web son:

2.2.1. *Cross Site Scripting*

Se la conoce también de forma abreviada como XSS (Cui & Yang, 2017) en la cual están clasificadas una serie de riesgos en todas sus modalidades y variantes en donde pueden ocasionar daños principalmente de usuarios y afectar a la reputación del dominio o institución que puede ser afectada por lo que puede derivar en problemas relacionados con:

- Generación de ataques de navegación dirigida.
- Posibles ataques de phishing.
- Distribución de malware.

- Apropiación indebida de credenciales.
- Ejecución de pequeños scripts conocidos como “JavaScript”
- Ser víctimas de clickjacking, secuestro del clic, técnica maliciosa para apoderarse de la información del usuario en la web. (Kim & Kim, 2014)
- Ser blanco de defacement sin o con alteraciones de la página web real, es decir cambia el contenido real de la página web, este tipo de vulnerabilidades puede resultar muy peligroso ya que por el desconocimiento del usuario, al tomar el control remoto del navegador en donde puede haber varios vectores de ataque con la ejecución de un control JavaScript, uno de ellos conocido como Main in the middle Browser, MITB puede controlar el navegador y ejecutar exploits por realizar un posible acceso de privilegio del sistema, aquí factores como la ingeniería social y el desconocimiento de los usuarios sobre la información web pueden resultar afectados sin darse cuenta del riesgo que se exponen. (Davanzo, Medvet, & Bartoli, 2008)

2.2.2. Cross Site Scripting Reflejado.

Para aplicar esta vulnerabilidad, el fallo se basa en la manipulación de un determinado parámetro que puede ser vulnerable con el propósito de que se sobreponga un enlace modificado y que permita embeber código HTML o su vez scripts, la utilización de proxy inverso genera llegar a este tipo de vulnerabilidades. Por lo general el punto de inicio es al hacer un clic a una URL que se haya sido manipulada, se llenan los datos en el formulario afectado o adulterado, enviándose el script infectado al servidor web sin ser filtrado y por la misma el servidor web nuevamente regresa al cliente este código malicioso que no se almacena en el servidor web. (Simos, Kleine, Ghandehari, Garn, & Lei).

2.2.3. Cross Site Scripting Persistente

Este tipo de ataques se caracteriza por invadir código HTML por medio de inserción de etiquetas <script> y <frame> en sitios que pueden ubicarse y que permita realizarlo. Adicionalmente este tipo de ataques los archivos maliciosos se almacenan en el servidor web y estos son destinados a liberarse en cada petición que hace una página web desde el navegador. (Software and Systems, vol. 9976, F. Wotawa, M. Nica, y N. Kushik, Eds, 2016)

Para este tipo de ataques son blancos propicios las páginas web dinámicas y que permiten guardar datos del usuario y estos son transferidos sin métodos de control o alguna codificación. De igual manera los blogs y los foros son los blancos perfectos ya que no se restringen o se aplican métodos de control, aquí los atacantes agregan el código Script dañado para el usuario, sin percatarse, hace clic y empieza el proceso de esta vulnerabilidad.

2.3. OWASP ZAP (Zed Attack Proxy)

Open Web Application Security Project OWASP es catalogado como un proyecto abierto mencionado también sin ánimo de lucro con el fin de mejorar la seguridad de los servicios y aplicaciones web con la posibilidad de que el trabajo en internet sea más seguro.

Dentro de este proyecto existe la herramienta ZAP denominada Zen Attack Proxy, conocida como una herramienta potente para el análisis de vulnerabilidades web de

organizaciones y una de las más utilizadas al momento de realizar una auditoria informática en la web. (Gupta & Gupta, Ene. 2017)

2.3.1. Características

- Es una herramienta plenamente gratuita y es de código abierto.
- Herramienta que trabaja en multiplataforma.
- Fácil instalación a nivel de Windows y Linux, la cual depende de java 1.7 o versiones superiores de la misma.
- Asignación de sistemas de prioridades al momento de su configuración técnica.
- Divulgación de manuales técnicos de ayuda y múltiples grupos establecidos en una gran comunidad para su mejor utilización.

2.3.2. Usabilidad

Dentro de la usabilidad de esta herramienta se podrán realizar diferentes tipos de test a las aplicaciones web y dentro de este aspecto una gran cantidad de análisis específicos y funciones.

- Localiza recursos del servidor.
- Comprobar las peticiones y respuestas entre el cliente y servidor.
- Programación de análisis automáticos y pasivos.
- Programación de múltiples ataques a la vez.
- Utiliza certificados SSL dinámicos.
- Posibilidad de realizar análisis de sistemas de autenticación.
- Mantiene soporte para utilizar tarjetas inteligentes y certificados personales.
- Actualización automática del software de la herramienta ZAP.
- Disponibilidad de plugins existentes en la web para potencializar la herramienta.

3. Fases De La Metodología

El diseño de la metodología para ambientes virtuales de aprendizaje considera como base los lineamiento de la Guía de pruebas OWASP versión 4 (Acetozi, 2017), la misma que tiene vigencia desde el año 2014 la cual se basa en 11 fases y más de 100 pruebas sobre seguridad, y también basado en el top 10 de las vulnerabilidades detectadas por OWASP en el año 2013. (Meucc & Muller, 2014).

Es importante resaltar que el desarrollo de la metodología abarca un modelo genérico que sería utilizado para la evaluación de los sistemas Web, adicionando alcances genéricos que no solamente se deben considerar para la administración completa de un campus virtual, sino que se debe asumir con todas las implicaciones y considerar que puede ser un blanco perfecto si se descuidan detalles importantes como la administración de credenciales, políticas para la administración de usuarios y cierre de sesiones.

La propuesta en mantener una metodología genérica, dinámica, que abarque la mayoría de fortalezas que OWASP plantea al momento de realizar pruebas de rigurosidad para evaluar todos los aspectos comprometidos con la seguridad.

3.1. Fase de Planificación

La fase de planificación implica el desarrollo del alcance, definiendo estrictamente en que campo apunta la metodología planificada, y además se deben considerar los acuerdos previos que se deben suscribir en términos de magnitud y responsabilidades, entre los autores de la investigación y autoridades de la organización auditada, todo esto en reuniones previas y como resultado final de esta fase es dejar sentada la planificación el test de pruebas a realizarse (Ascencio Mendoza & Moreno Patiño, 2011)[15]. Acá se describe una lista de las actividades a realizarse en esta fase.

- Propuestas sobre reuniones iniciales.
- Situación actual y definición del alcance de la auditoría y ámbito de la misma.
- Ámbito para la aplicación de las pruebas.
- Planificación del proceso de auditoría.
- Parte final y propósito de la fase de planificación.

3.2. Fase de actuación.

Esta fase está determinada para el diseño y planificación de pruebas técnicas en lo referente para el análisis de vulnerabilidades del campus virtual con la respectiva explotación de los resultados encontrados. En esta parte se deben considerar los resultados encontrados utilizando herramientas de escaneo automático, obteniéndose como resultado el listado de vulnerabilidades, además de que dichos resultados deben ser corroborados con la parte de explotación, con el afán de eliminar falsos positivos y generar resultados veraces.

En esta fase se realizan las siguientes actividades:

- Test de caja negra
- Test de caja blanca.
- Test de caja gris.

Mediante la siguiente figura se establece el alcance que tiene la clasificación de los test. (Ver figura 2)

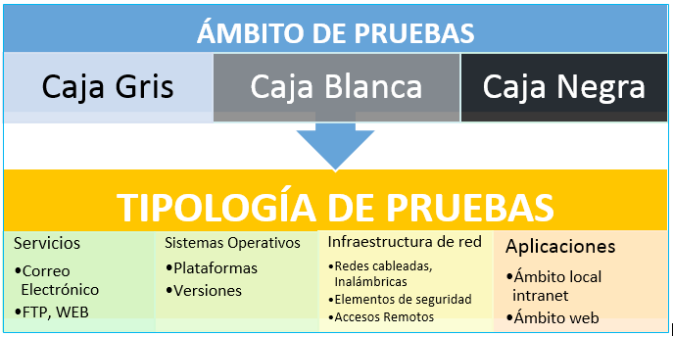


Figura 2 – Ámbito de pruebas (Baroja, 2017)

3.2.1. Recopilación de información

Dentro de esta sección es importante, destacar que para la recolección de información la metodología cumple con los siguientes pasos.



Figura 3 – Hitos en la recolección de información (Baroja, 2017)

La recolección de la información se clasifica en dos instancias decisivas, la primera parte *Footprinting* (Información publicada) y la segunda parte *Fingerprinting* (Información técnica). Dentro del Footprinting se lo conoce también como *External Footprinting*, técnica de recolección de la información de forma ordenada, esta se clasifica en dos instancias más particulares, la primera denominada *Active Footprinting* donde se busca información directamente en la infraestructura de la Institución; y la segunda parte denominada *Passive Footprinting* donde la búsqueda la información se la realiza con las herramientas de la web, técnicas avanzadas de búsquedas de datos son las más utilizadas en este contexto.

Para la búsqueda de la información netamente técnica que permita conocer la información más exacta, conocer que sistemas están activos, puertos habilitados, servicios que están funcionando, aplicaciones instaladas, todas estas actividades se las puede realizar con los aplicativos: Nmap, netCat, hping y Traceroute. Como resultado del Fingerprinting se puede llegar a obtener información de los hosts activos, direcciones IP de elementos de red, rangos y subredes, así como la detección de mecanismos criptográficos en redes inalámbricas (Gurary, Zhu, Bettati, & Guan, 2016).

3.2.2. Análisis de vulnerabilidades

Para esta fase es importante contar con la información previa en la sección de recolección de información, así mismo contar con la infraestructura de elementos de la red. Para la

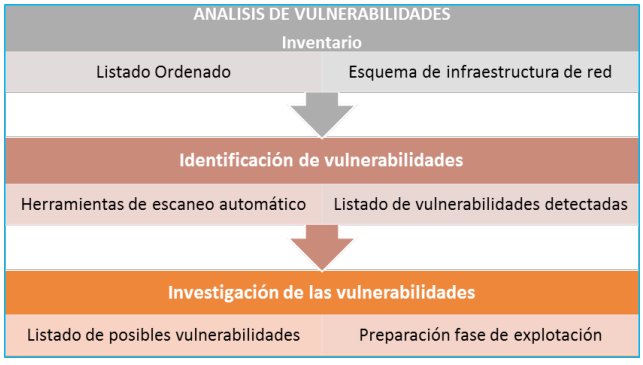


Figura 4 – Etapas de un análisis de vulnerabilidades (Baroja, 2017)

identificación de vulnerabilidades se utilizan herramientas de escaneo activo y como resultado se obtiene una lista de vulnerabilidades, que con el paso final de las pruebas de intrusión se llegarán a descartar falsos positivos. (Ver figura 4)

3.2.3. Explotación de vulnerabilidades

Concebido como el procedimiento más importante dentro del proceso de auditoría, aquí se realizan las pruebas de intrusión para descartar falsos positivos, y de esta manera conocer realmente cuáles son las vulnerabilidades que existen mediante la aplicación de pruebas de intrusión, en la figura 5 se ilustran los pasos a seguir.

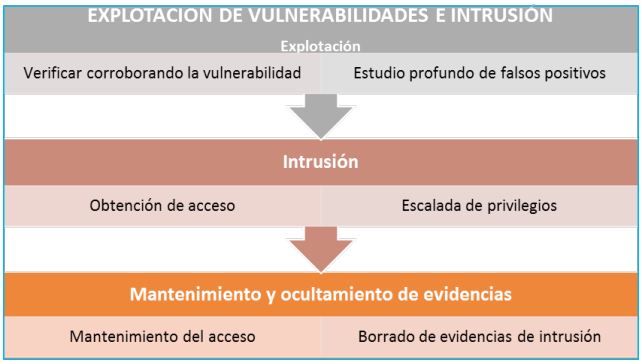


Figura 5 – Etapas de la explotación de vulnerabilidades e intrusión (Baroja, 2017)

El objetivo primordial en esta fase es, generar las explotaciones encontradas en procesos anteriores, realizar las intrusiones por medio de conmutadores, router, puntos de acceso, aplicativos web, servidores FTP, telnet o través de servidores de acceso o autenticación.

3.2.4. Fase de Generación de informes.

Es la fase final de proceso de la auditoría y por esa misma razón hay que darle la importancia necesaria ya que será la carta de presentación del equipo auditor como evidencia de todo el proceso de auditoría que se haya realizado, en los cuales constará el resumen del proceso llevado a cabo en la auditoría. Los puntos más importantes son el Resumen Ejecutivo y el Informe de Resultados:

Para la presentación del resumen ejecutivo el equipo auditor debe preparar esta información en forma detallada pero lo más importante es que debe estar redactado con la adecuación de que los dueños de organizaciones o instituciones no dominen el lenguaje técnico, además debe estar diseñado con gráficos sobre estadísticas del nivel de riesgo que mantiene la organización.

La última sección del informe incluye información técnica detallada sobre las vulnerabilidades encontradas y las acciones necesarias para eliminar y resolverlas. Esta sección tiene como objetivo presentar de forma técnica para que los encargados de los departamentos de TI puedan evaluar la situación y empezar a resolverlas, cada registro

debe estar lo más conciso posible para que se puedan emprender acciones correctivas lo más pronto posible.

4. Conclusiones

La propuesta de planteamiento de las tres fases desarrolladas durante la investigación, permitirán al equipo auditor, contar con un conjunto de procesos sistematizados para realizar una auditoría técnica y de esta manera determinar las vulnerabilidades que adolece un campus virtual de aprendizaje.

La aplicación de la técnica de *Footprinting* permite encontrar resultados sumamente importantes como: la sección del contador de visitas, donde se registran accesos desde otras latitudes, en este caso se registran accesos desde países principalmente africanos, lo que hace imaginar que las Universidades en algún momento pueden ser víctimas de ataque desde países lejanos geográficamente o detectar cualquier otra anomalía que se esté pensando realizar, por lo que las alertas se deben encender entorno a la seguridad de la información en los accesos a los entornos virtuales de aprendizaje.

La generación de la fase final de la propuesta planteada con respecto al Resumen Ejecutivo y al Informe técnico, debe expresar los resultados de forma ágil para que los administradores o propietarios puedan entender el riesgo eminente cuando se han encontrado vulnerabilidades y no se toman acciones con respecto al campo de la seguridad informática.

Referencias

Acetozi, J. (2017). Types of Automated Tests. *Pro Java Clustering and Scalability, Berkeley, CA: Apress*, 119–120.

Ascencio Mendoza, M., & Moreno Patiño, P. J. (2011). *Desarrollo de una Propuesta Metodológica para determinar la seguridad en una aplicación Web*. Obtenido de http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/2511/0058A811.pdf;jsessionid=BCBCD28D1FB843F56E1F34C5CB5DFB10?sequence=1

Baroja, D. (2017). *Metodología contra vulnerabilidades en Ambientes de Aprendizajes Virtuales (Moodle)*. Ibarra: Universidad Internacional de La Rioja.

Cano Ramírez, J. (08 de 2014). *Certified Offensive and Defensive Security Professional - Entrenamiento E-learning* -. Obtenido de https://juliocanoramirez.files.wordpress.com/2014/08/analisis-de-vulnerabilidades.pdf

Cui, B., & Yang, W. (2017). *Advances on Broad-Band Wireless Computing, Communication and Applications, vol. 2, L. Barolli, F. Xhafa, y K. Yim, Eds. Cham*. Springer International Publishing,pp. 353–361.

Davanzo, G., Medvet, E., & Bartoli, A. (2008). Comparative Study of Anomaly Detection Techniques in Web Site Defacement Detection. *Proceedings of The Ifip Tc 11 23rd International Information Security Conference, vol. 278, S. Jajodia, P. Samarati, y S. Cimato, Eds. Boston*, 711–716.

Gupta, S., & Gupta, B. B. (Ene. 2017). Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art»,. *International Journal of System Assurance Engineering and Management, vol. 8, n.o S1*, 512–530.

Gurary, J., Zhu, Y., Bettati, R., & Guan, Y. (2016). Operating System Fingerprinting. *Digital Fingerprinting, C. Wang, R. M. Gerdes, Y. Guan, y S. K. Kasera, Eds. New York, NY: Springer New York*, 115–139.

Kim, D., & Kim, H. (2014). We Are Still Vulnerable to Clickjacking Attacks: About 99 % of Korean Websites Are Dangerous. *Information Security Applications, vol. 8267, Y. Kim, H. Lee, y A. Perrig, Eds. Cham*, 163–173.

Meucc, M., & Muller, A. (2014). *OWASP Testing Guide Release*. Obtenido de Testing Guide Release v4: https://www.owasp.org/images/1/19/OTGv4.pdf

Narváez, D. (2017). *Metodología de test de penetración para redes inalámbricas en campus universitarios*. Ibarra: Universidad Internacional de La Rioja.

Peña Torres, I. (6 de 06 de 2016). *Auditoría Técnica de Seguridad de aplicaciones Web*. Obtenido de http://openaccess.uoc.edu/webapps/02/bitstream/10609/53506/9/ipenatTFM0616memoria.pdf

Simos, D. E., Kleine, k., Ghandehari, L. S., Garn, B., & Lei, Y. (s.f.). A Combinatorial Approach to Analyzing Cross-Site Scripting (XSS) Vulnerabilities in Web Application Security Testing. *Testing*.

Software and Systems, vol. 9976, F. Wotawa, M. Nica, y N. Kushik, Eds. (2016). *Springer International Publishing*, 70–85.

Tilborg, H. C., & Jajodia, S. (2011). *Encyclopedia of Cryptography and Security*. Boston: Springer US.

Vela, F., & Andrade, R. (5 de 03 de 2017). *Traducción de la Guia de OWASP Versión 4 al español*. Obtenido de OWASP Testing Guide 4.0 en Español: https://www.dragonjar.org/owasp-testing-guide-4-0-en-espanol.xhtml

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 22/12/2017
Aceitação/Acceptance: 06/03/2018

Propuesta de innovación educativa utilizando TIC´s y el Diseño Universal para el Aprendizaje implementada a la asignatura de Psicología General de la Universidad de las Fuerzas Armadas "ESPE"

Daysi Karina Flores Chuquimarca[1], Ramiro Delgado Rodriguez[2], Aida Noemí Bedón Bedón[3]

[1]daysi.kary@hotmail.com, [2]rndelgado@espe.edu.ec, [3]anbedon@espe.edu.ec.

[1, 2, 3] Universidad de las Fuerzas Armadas ESPE, Av. General Rumiñahui s/n, 171103, Sangolquí, Ecuador.

Pages: 292–303

Resumen: El artículo describe una propuesta de innovación educativa usando las Tecnologías de la Información y Comunicación (TIC`s) y el Diseño Universal para el Aprendizaje que fue implementada en la asignatura de Psicología General en la Universidad de las Fuerzas Armadas "ESPE". La propuesta tuvo como objetivo dinamizar los entornos de aprendizaje y mejorar la competencia digital y la autonomía del aprendizaje. Los resultados obtenidos muestran un incremento significativo en las competencias analizadas que reflejan el interés de los estudiantes por nuevos escenarios educativos.

Palabras-clave: Educación superior; innovación educativa; tecnologías de las información y la comunicación; diseño universal del aprendizaje.

Proposal of educational innovation using TIC´s and Universal Design for Learning implemented to General Psychology subject at University of the Armed Forces "ESPE"

Abstract: The article describes a proposal of educational innovation using the Information and Communication Technologies (TIC`s) and the Universal Design for Learning that was implemented in the General Psychology subject at the University of the Armed Forces "ESPE". The aim of the proposal was to boost learning environments and improve digital competence and autonomy of learning. The results showed a significant increase in the competences level that reflect the interest of the students for new educational scenarios.

Keywords*:* Higher education; educational innovation; information and communication technologies; universal design for learning.

1. Introducción

El Plan Nacional de Desarrollo 2017-2021 del Ecuador, da importancia a la innovación manifestada en el progreso de una sociedad del conocimiento que contribuya a la matriz

productiva y la consolidación de la educación universal, considerando al uso de las Tecnologías. Priorizando la generación de igualdad de oportunidades para recrear la interculturalidad, valorando la diversidad de nuestro país multiétnico y pluricultural. Con la simple intención de profundizar el goce de los derechos (SENPLADES, 2017).

Tomando en consideración que las TIC se han constituido en un apoyo de la educación debido a las diversas posibilidades que ofrece para abrir nuevos espacios de aprendizaje en los diferentes niveles de formación (Orjuela, 2010) y muy especialmente en el contexto universitario, su integración aporta matices a la gestión docente y a la formación de los nuevos formadores. Por tanto, es importante repensar los procesos de aprendizaje, para enfrentar los desafíos y requerimientos de la sociedad actual.

A la luz de ello, las instituciones de educación superior "IES" del Ecuador y en particular la Universidad de las Fuerzas Armadas ESPE, enfrenta el reto de desarrollar procesos de calidad que promuevan entornos de aprendizaje innovadores como lo plantea el Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior "CEACCES"; con la finalidad de dinamizar los procesos metodológicos de aprendizaje, proyectando a los estudiantes hacia la consecución de competencias básicas, para aprender a aprender en la sociedad digital. En este sentido, se pretende contribuir a la mejora de las prácticas educativas mediante el desarrollo de una propuesta innovadora con el uso de las TIC.

El presente estudio se desarrolló en la Carrera de Educación Infantil, y responde la siguiente pregunta de investigación ¿La introducción de escenarios de innovación educativa con TIC dinamizan el proceso de formación y contribuyen a mejorar las competencias de los estudiantes: autonomía del aprendizaje y competencia digital? La propuesta se orienta al uso de las TIC y el Diseño Universal para el Aprendizaje "DUA", que permitan desarrollar estrategias sustentadas en TIC, con el propósito de fortalecer los procesos de aprendizaje.

2. Marco Teórico

2.1. Innovación educativa en la educación Superior.

El uso de las TIC constituye una mediación imprescindible en la sociedad digital que permite diversificar y ampliar nuevos escenarios virtuales de aprendizaje. Sin embargo, la importancia de valorar sus posibilidades didácticas en relación a los objetivos y fines educativos, se convierte en el mayor desafío de los profesores según Sánchez (2001). Así como la integración curricular de las TIC que garantice la formación de los estudiantes en los diferentes niveles de educación.

Debido a la complejidad que va adquiriendo la educación, por la cantidad de información que tiene a su disposición el estudiante, surge la necesidad de establecer estrategias para filtrar la información y enseñarle a identificar lo relevante y útil para su aprendizaje. Delors (1996) señala *"...que ya no basta con que cada individuo acumule al comienzo de su vida una reserva de conocimientos a la que podrá recurrir después sin límites."* y propone cuatro pilares del conocimiento: aprender a conocer, aprender a hacer, aprender a vivir juntos y aprender a ser. De los que se derivan una serie de directrices importantes

para que el individuo pueda conocer y regular sus propios procesos de aprendizaje, considerando la aceptación de errores como una oportunidad de crecimiento (Guido Williamson, 2013).

2.2. Innovaciones educativas en el contexto ecuatoriano.

La Educación Superior ecuatoriana, durante los últimos 8 años tuvo una serie de transformaciones que han dado paso a leyes y reglamentos que postulan principalmente a la formación de excelencia de los futuros profesionales y la calidad del proceso educativo. En la Ley Orgánica de Educación Superior "LOES", se consideran ciertos principios que garantizan el derecho a la educación superior de calidad que propenda a la excelencia y al acceso universal. En su art. 350 señala que el sistema de Educación Superior tiene como finalidad la formación académica y profesional con visión científica, humanista y tecnológica; la innovación, promoción, desarrollo y difusión de los saberes y las culturas; la construcción de soluciones para los problemas del país, en relación con los objetivos nacionales de desarrollo (Asamblea Nacional del Ecuador, 2010).

La riqueza del conocimiento está contenida en la propia sociedad, en donde existen diferentes saberes. La universidad ecuatoriana debe dialogar con la pluralidad para retroalimentar y generar a la vez más conocimiento sistemático, articulando la universidad con la acción cooperativa del intelecto colectivo (sector industrial, Estado, gobiernos locales, cooperativas, actores populares, organismos no gubernamentales, parques tecnológicos, etc.) (Ramírez Gallegos, 2013).

Las IES del Ecuador enfrentan la necesidad de mejorar sus procesos formativos constantemente, en busca de la excelencia y la calidad educativa sustentada en la ciencia y la tecnología. En este proceso de transformación las actividades rutinarias imposibilitan la consecución de resultados eficientes y eficaces, por ello se habla de procesos de innovación, que buscan una reestructuración parcial o total de los procesos formativos.

Garcés Suárez & Alcívar Fajardo afirman que en los últimos años la presencia de las TIC en los procesos formativos universitarios del Ecuador han ocasionado un cambio en la manera de concebir las prácticas educativas (Garcés Suárez, Garcés Suárez, & Alcívar Fajardo, 2016). En torno a estas exigencias, requerimientos y necesidades académicas las Universidades Ecuatorianas han iniciado el rediseño de los procesos formativos que contribuyan no solo a mejorar sus experiencias educativas sino a cumplir con los indicadores de evaluación con fines de acreditación, establecidos por las entidades de control como el CEAACES.

2.3. Diseño Universal para el Aprendizaje.

El DUA es un enfoque didáctico creado principalmente para fomentar el cambio en el conocimiento y las habilidades de los estudiantes en la diversidad, siendo indispensable considerar los elementos críticos de las diferencias individuales abordados en cualquier ambiente de aprendizaje y aprovechando la flexibilidad de la tecnología para articular practicas eficaces (Alba Pastor, Zubillaga del Río, & Sánchez Serrano, 2015). Un diseño que plantea un plan de estudio flexible, accesible y diverso garantizando la equidad educativa, buscando facilitar las condiciones y experiencias de aprendizaje que colocan

al estudiante como el eje central de la formación diferenciada. El DUA a través de sus directrices guía la integración de las tecnologías con miras a la innovación.

En la tabla 1 se muestra un ejemplo de diseño de contenidos de acuerdo a los principios sobre los cuales se fundamenta el DUA.

DISEÑO UNIVERSAL PARA EL APRENDIZAJE TIC		
Fase 1 ¿Por qué? Motivación	**Fase 2 ¿Qué?** Presentación de Materiales	**Fase 3 ¿Cómo?** Evaluación
Video Motivador Caso práctico Experiencia	Archivos de lectura (PDF, Word, entre otros) Presentación Power Point Videos Mapas	Examen tradicional Cuestionario plataforma con preguntas de: Selección múltiple, V o F, Emparejar, ensayo, entre otros. Presentación de proyectos.

Tabla 1 – Fases del diseño de contenidos

Rose & Gravel (2010) plantean que el DUA requiere que los medios de aprendizaje sean accesibles y respondan a los objetivos pedagógicos, con métodos y materiales acordes a las necesidades educativas y una evaluación que visibilice la competencia o conocimiento adquirido, potenciando el uso de los medios y resultados a través de la accesibilidad.

3. Metodología

La presente investigación se enmarca en un estudio de caso; considerando que las investigaciones en los contextos educativos no pueden ser generalizados. La tarea fundamental fue entender la naturaleza distintiva del caso en particular, donde aparecieron una diversidad de experiencias, conclusiones, anécdotas que permitieron comprender lo que sucede en el contexto educativo, con la finalidad de mejorar los procesos de aprendizaje (Bolívar Botía, 2002).

La investigación social utiliza un conjunto de instrumentos y técnicas que surgen de la naturaleza de la problemática. El presente estudio utilizó las siguientes técnicas e instrumentos: el cuestionario, la entrevista y el focus group (Dias, 2009). El enfoque fue mixto, datos cuantitativos analizados con estadística descriptiva usando el programa SPSS y datos cualitativos analizados con la tabla de tendencias de significado, que permitió identificar categorías, subcategorías y unidades de registro de los datos recogidos a través del focus group y entrevistas.

Los sujetos de estudio fueron 170 estudiantes de la asignatura de Psicología General en la Universidad de las Fuerzas Armadas “ESPE”. Para su selección se tomaron como referencia los siguientes criterios:

- La asignatura de Psicología General es un eje esencial en la formación de los profesionales de la Universidad.

- Los estudiantes están iniciando su carrera universitaria, por tanto, se encuentran con expectativas respecto a su proceso de aprendizaje.
- La profesora que dirige la asignatura se encuentra motivada con el uso de las TIC para mejorar su práctica educativa.

Para la sistematización de la propuesta de innovación educativa se aplicó la metodología de diseño instruccional: Análisis, Diseño, Desarrollo, Implementación y Evaluación denominado ADDIE. Este modelo permite maximizar la comprensión, el uso y la aplicación de la información con estructuras sistemáticas, metodológicas y pedagógicas a través de sus cinco fases (Candia García, 2016).

A continuación, se describe los resultados obtenidos en cada una de las fases del modelo ADDIE.

4. Resultados

4.1. Análisis

La primera fase permitió establecer una línea base, para la posterior toma de decisiones, centradas en las necesidades reales que presentaron los estudiantes en relación a la competencia digital que les permita comunicarse en el contexto social, acceder a la información, elaborar y transferir conocimientos (Martínez, Padilla, & Meneses, 2014).

Los resultados revelaron que el 60% son de sexo femenino y el 40% de sexo masculino. El grupo se encuentra en un rango de edad entre los 19-21 años. Referente que según Gisbert & Esteve (2011) es positivo, pues, los jóvenes tienen mayor facilidad para incorporarse al uso de las tecnologías, ya que se enfrentan a una cantidad de información instantánea colocada en la web y una diversidad de artefactos tecnológicos. Sin embargo, Abamu (2017) señala que no se puede obviar su trayectoria educativa, basada en modelos educativos convencionales y ello trae consigo actitudes negativas en el uso de las tecnologías cuando se trata de procesos más formales.

4.2. Diseño

A partir de la fase anterior se proyectó la adecuación del programa de Psicología General a una innovación educativa, en acuerdo con la profesora titular de la asignatura, y, se estableció un proceso para el diseño de la propuesta (Figura 1). En la primera etapa se establecieron las competencias a potencializar especialmente la autonomía del aprendizaje y la competencia digital.

La segunda etapa consistió en un análisis del sílabo de la asignatura identificando aspectos significativos como los objetivos, las unidades de contenido, resultados de aprendizaje, sistemas de tareas, proyecciones metodológicas y organizativas que fueron analizadas para escoger los recursos y herramientas digitales a implementarse en el proceso. La principal finalidad de la asignatura es aportar nuevos enfoques en la formación de los estudiantes (Moñivas, 1994). Siendo un eje esencial para la formación profesional de las educadoras infantiles.



Figura 1 – Proceso para el diseño de la propuesta de innovación educativa.

La tercera etapa introdujo las aportaciones y directrices del DUA para potencializar el uso de las TIC. Se identificaron los diferentes estilos de aprendizaje de los estudiantes, aspecto que dio la pauta de las múltiples formas de presentar los contenidos.

La última etapa hace referencia al diseño de la propuesta de innovación educativa cuyo eje principal es el estudiante, y que plantea dinamizar el proceso metodológico de la asignatura de Psicología General, integrando una plataforma de gestión del aprendizaje "MOODLE" y diferentes recursos y herramientas tecnológicas como Timeline, Popplet, Zoom, Kahoot, Pixtón y Google Drive.

4.3. Desarrollo

En este apartado se describe la aplicación de la propuesta con los elementos descritos anteriormente. En la tabla 2 se visualiza los recursos y herramientas digitales utilizados en la intervención, que fueron divididos en tres parciales del periodo académico, seleccionados de acuerdo a los contenidos de la asignatura y los resultados de aprendizaje los mismos que se conectaron con las proyecciones metodológicas implementadas en la innovación educativa.

4.4. Implementación.

La propuesta inició el 10 de Octubre del 2016 y terminó el 9 de Febrero del 2017, con clases presenciales, 4 horas a la semana, divididos en dos días lunes y viernes.

Se utilizó un laboratorio equipado con computadoras de escritorio y con acceso a internet, una por cada estudiante además de un proyector.

PARCIAL	HERRAMIENTAS Y RECURSOS DIGITALES
Primero	Moodle como herramienta de Gestión del Aprendizaje FORO TAREAS CUESTIONARIO Y algunos recursos como: ARCHIVOS, ETIQUETA, URL El BLOG Timeline Popplet Google Drive
Segundo	Moodle como herramienta de Gestión del Aprendizaje. FORO TAREAS CUESTIONARIO Y algunos recursos como: ARCHIVOS, ETIQUETA, URL Implementando las WIKIS de forma colaborativa como un diario de aprendizaje Zoom Pixtón
Tercer	Moodle como herramienta de Gestión del Aprendizaje. Glosario de términos Popplet Kahoot

Tabla 2 – Herramientas y recursos digitales



Figura 2 – Estudiantes en el laboratorio

Los estudiantes tenían actividades que realizar en casa de acuerdo al sistema de tareas y eran enviadas a la plataforma virtual “Moodle” que buscaban el fortalecimiento de las competencias de autonomía del aprendizaje y competencia digital.

5. Evaluación y discusión de los resultados

En el estudio se realizó un pre- test y post- test relacionado con la competencia digital de los estudiantes, tomando como referencia el cuestionario de competencias digitales 2.0 de estudiantes universitarios "COBADI 2013" (Marca registrada: 2970648). Se mantuvieron las siguientes categorías: consumo de la tecnología, competencia en conocimiento y uso de las TIC, búsqueda y tratamiento de la información y competencias colaborativas. Obteniendo los siguientes resultados:

Indicador	Inicial	Final	% de incremento
Usar redes sociales.	2,06	2,59	25%
Buscar información que te interese a nivel personal.	2,41	2,76	14,5%

Tabla 3 – Consumo de la tecnología.

Como se observa en la tabla 3 los estudiantes incrementaron el consumo de la tecnología, en relación a los siguientes indicadores:

El uso de redes sociales tuvo un porcentaje de incremento del 25%. La búsqueda de información que le interesa a nivel personal un 14,5%.

Indicador	Inicial	Final	% de incremento
Utiliza plataformas educativas como Moodle, educativa u otra.	2,82	4,59	62,76%
Usa actividades de diálogo, debate y reflexión en foros.	4,18	3,00	39,33%

Tabla 4 – Competencia en conocimiento y uso de la TIC.

En la categoría de competencias en conocimiento y uso de las TIC (Tabla 4), se observa que los estudiantes tienen mayor dominio en el uso de la plataforma Moodle con un incremento de 62%. Potenciando además el uso del diálogo, debate y reflexión en foros en un 39,33%.

Indicador	Inicial	Final	%de incremento
Evaluó y seleccionó fuentes de información y herramientas digitales para realizar tareas específicas.	3,24	3,82	17,90%
Organizó, analizó y sintetizó la información mediante mapas conceptuales utilizando algunas herramientas de software.	2,41	3,88	60,99%
Utilizó diferentes bases de datos que me ayudan en la búsqueda de información (Scopus, Equal, Taylor & Francis)	2,59	3,41	31,66%

Tabla 5 – Búsqueda y tratamiento de la información.

La competencia en búsqueda y tratamiento de la información fue necesaria para gestionar la información en diferentes actividades, por tanto se observa en la tabla 5 un porcentaje significativo de incremento en los siguientes indicadores:

Evaluar y seleccionar fuentes de información y herramientas digitales para realizar tareas específicas un 17,90%. La forma de organizar, analizar y sintetizar la información mediantes mapas conceptuales utilizando algunas herramientas de software en un 60,99%. El uso de diferentes bases de datos que ayudan en la búsqueda de información el 31,66%.

Indicador	Inicial	Final	% de incremento
Valora el aporte de cada miembro del equipo.	4,29	4,53	5,5%
Manifiestas tus opiniones con libertad y de forma constructiva.	3,82	4,12	7,8%
Contribuyes en la resolución de problemas grupales	4,12	4,41	7%
Escuchas, reflexionas y evalúas el trabajo de tus compañeros.	4,12	4,53	9,99%

Tabla 6 – Competencias colaborativas

Varias competencias vienen inherentes al uso de las tecnologías en el ámbito académico y las competencias colaborativas se afianzan en gran medida. En la tabla 6 se destaca el desarrollo progresivo en actitudes que permiten un mayor desenvolvimiento en los escenarios virtuales de aprendizaje basados en el trabajo colaborativo y se resalta los siguientes indicadores. Valorar el aporte de cada miembro del equipo con un porcentaje de incrementó de 5,5%. Además manifiestan sus opiniones con libertad y de forma constructiva con un 7,8%.

Los estudiantes al final de la investigación escuchan, reflexionan y evalúan el trabajo de sus compañeros en un 9,99%.

En relación al focus group aplicado a los estudiantes se obtuvieron los siguientes resultados:

Abordando los diferentes grados de precisión o complejidad con que los estudiantes alcanzaron los objetivos de la asignatura. Al respecto mencionaron: *"…me pareció primero un poco difícil de manejar porque era la primera plataforma virtual que había utilizado era MIESPE, después que ya nos explicaste, pude entrar o ver algunas partes que no entendía como se navegaba dentro de INNOVA.."*. A partir de este testimonio se evidencia que en momentos iniciales los estudiantes tuvieron dificultad en el manejo de la plataforma virtual Moodle INNOVA- ESPE. Sin embargo, con el pasar del tiempo se percibió que a mayor uso mayor destreza e interés por aprender más.

Se percibe que los estudiantes realizaban sus trabajos con mayor practicidad y rapidez, además, el uso de las tecnologías propicio nuevos escenarios de aprendizaje marcados por la innovación e interactividad de acuerdo a las afirmaciones: *"… es un trabajo más práctico, más rápido, y donde tienes opciones respecto a las pruebas", "nos dabas*

opciones divertidas no solo mecánicas que me meto acá y hago tal cosa…", "Esta experiencia me pareció interesante e innovadora", "Me pareció una plataforma muy divertida", "Es más interactiva". Situación que impulso hacia nuevas formas de trabajo, usando no solo los paquetes básicos de Office sino también los propuestos en esta innovación, generando estrategias de aprendizaje, menos complejas. Los estudiantes optimizan el tiempo y aprenden con menos esfuerzo.

La experiencia ánimo a los estudiantes a cambiar su visión en el uso de las tecnologías, esto se atribuyó a los trabajos con mayor practicidad, facilidad y rapidez que lograron realizar con los recursos tecnológicos. Dando paso a nuevas estrategias de aprendizaje aplicables a los diferentes ámbitos académicos y sociales, que contribuyen a resolver las nuevas necesidades formativas generados por las TIC (Tejada Fernández & Navío Gámez, 2005).

La autonomía del aprendizaje es otra de las competencias que se fortaleció. Se evidencio la adquisición de habilidades para dirigir, controlar, regular y evaluar su propio proceso formativo con el uso de estrategias de aprendizaje generadas en el ambiente virtual de Moodle. Al respecto los estudiantes mencionaron que: *"…cuanto lo revisas te sale hay tareas que requieren atención, entonces te hace acuerdo de que tienes que hacer las tareas", "ya te dicen que tiempo tienes para poder entregar las tareas", "te pone las fechas para que este pendiente ", "Sabíamos que ingresando a cualquier parte podríamos ayudarnos con la materia", "Fomento el autoaprendizaje, con los videos, donde se auto educa…".*

A fin de evaluar el impacto de la propuesta en el rendimiento académico de los estudiantes, el indicador a ser analizado es el promedio general obtenido en la materia en los dos periodos anteriores al experimento y relacionarlo con el periodo de aplicación de la propuesta. Los datos se presentan en la tabla 7.

Promedio final de la materia psicología general			
Periodo	Octubre 2015 Febrero 2016	Abril 2016 Agosto 2016	Octubre 2016 Febrero 2017
Nota	15,20	15,40	16,80
Incremento	10,52 %	9,09 %	

Tabla 7 – Promedio del curso en los dos periodos anteriores.

Como se observa el promedio general del curso en el periodo octubre 2016-febrero 2017, en la materia de estudio, se incrementa en un 10,52 % respecto al obtenido hace dos periodos y en un 9,09% respecto al periodo anterior, lo que muestra que la propuesta implementada permitió mejorar significativamente el aprendizaje en los estudiantes.

6. Conclusiones

- La innovación implementada generó cambios en el proceso de aprendizaje, debido al uso de las tecnologías de la información y la comunicación. Estos

cambios dependen, en gran medida, de los agentes que intervienen en la acción educativa.

- El estudiante sin duda, siempre será el protagónico principal en el proceso de aprendizaje. En el presente estudio se evidencia que la innovación educativa, incrementó las competencias en conocimiento y uso de las TIC y la búsqueda y tratamiento de la información llegando a valores de 62,76% y 60,99%.
- A la luz de los comentarios obtenidos en el focus group se concluyó que el grupo de estudiantes al aprender con una metodología diferente, más dinámica alcanzan mejores resultados de aprendizaje.
- El rendimiento académico de los estudiantes mejoró en 9,09% respecto al periodo anterior y 10,52% en relación a dos periodos anteriores, considerando para el análisis el promedio general obtenido en la materia

Referencias

Abamu, J. (2017). What If Students Are the Biggest Barrier to Innovation? EdSurge News. Retrieved January 10, 2018.

Alba Pastor, C., Zubillaga del Río, A., & Sánchez Serrano, J. M. (2015). Tecnologías y Diseño Universal para el Aprendizaje (DUA): experiencias en el contexto universitario e implicaciones en la formación del profesorado. *RELATEC. Revista Latinoamericana de Tecnología Educativa*, *14*(1), 89–100. http://doi.org/10.17398/1695.

Asamblea Nacional del Ecuador. Ley Orgánica de Educación Superior. (2010). Ecuador.

Bolívar Botía, A. (2002). El estudio de caso como informe biográfico-narrativo. *Arbor*, *171*(675), 559–578. http://doi.org/10.3989/arbor.2002.i675.1046

Candia García, F. (2016). Diseño de un modelo curricular E-learning, utilizando una metodología activa participativa. *Revista Iberoamericana Para La Investigación Y El Desarrollo Educativo*, *7*(13), 9.

Delors, J. (1996). Los cuatro pilares de la educación. *Informe a La UNESCO de La Comisión Internacional Sobre La Educación Para El Siglo XXI*, 1–9.

Dias, M. O. (2009). *O Vocabulário do Desenho de Investigação*. Retrieved from http://www.fnac.pt/O-Vocabulario-do-Desenho-de-Investigacao-Maria-Olivia-Dias/a646136#

Garcés Suárez, E., Garcés Suárez, E., & Alcívar Fajardo, O. (2016). Las tecnologías de la Información en el cambio de la Educación Superior en el siglo XXI: reflexiones para la práctica. *Revista Científica Multidisciplinar de La Universidad de Cienfuegos*, *8*, 171–177.

Gisbert, M., & Esteve, F. (2011). Digital Leaners : la competencia digital de los estudiantes universitarios. *La Cuestión Universitaria*, 48–59.

Guido Williamson, L. (2013). Aprender a Aprender. *Journal of Chemical Information and Modeling*, *53*(9), 110–112. http://doi.org/10.1017/CBO9781107415324.004

Martínez, A. J., Padilla, A. H. M., & Meneses, E. L. (2014). Las competencias digitales en contextos universitarios. *I Seminario Iberoamericano De Innovación Docente De La Universidad Pablo De Olavide*, 3–8.

Moñivas, A. (1994). Epistemología y representaciones sociales: concepto y teoría. *Revista de Psicología General Y Aplicada*.

Orjuela, D. L. (2010). Acercamiento a la integración curricular de las TIC. *Praxis & Saber*, *1*(2), 111–136.

Ramírez Gallegos, R. (2013). Tercera ola de tranformación de la educación superior en Ecuador. *Senescyt*, *1*(1), 51.

Rose, D., & Gravel, J. (2010). Technology and Learning Meeting Special Students Needs. *Internatinal Enciclopedia of Education*, 19–124.

Sánchez, J. H. (2001). Integración Curricular de las TICs : Conceptos e Ideas. *Departamento de Ciencias de La Computación, Univ. de Chile.*, 1–6. 4

SENPLADES. (2017). Plan nacional de desarrollo 2017-2021 "Toda una Vida." *Senplades*, 1–148.

Tejada Fernández, J., & Navío Gámez, A. (2005). El desarrollo y la gestión de competencias profesionales: una mirada desde la formación. *Revista Iberoamericana de Educación*, *37*(2), 4.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 05/12/2017
Aceitação/Acceptance: 25/03/2018

Sociedad de la tecnología la información y el conocimiento: tecnologías en la formación de ingenieros

Claudio C. González.[1], Yuri V. Nieto A.[2], Carlos E. Montenegro M[3], José F. López Q.[4]

Claudio.gonzalez@unad.edu.co, Yuri_nieto@cun.edu.co, cemontenegrom@udistrital.edu.co, fernando.lopez@unad.edu.co

[1] Facultad de Ingeniería, UNAD, Bogotá, Colombia

[2] Facultad de Ingeniería, CUN, Bogotá, Colombia

[3] Facultad de Ingeniería, Universidad Distrital FJC, Bogotá, Colombia

[4] Facultad de Ingeniería, UNAD, Bogotá, Colombia

Pages: 304–317

Resumen: El presente artículo busca socializar las comprensiones suscitadas de la investigación realizada a los procesos de apropiación y uso de las tecnologías de la información y las comunicaciones en el ámbito educativo de la Ingeniería en una Universidad de educación presencial, de carácter privado en Latinoamérica. Este estudio se desarrolla en un contexto de complejidad denominado sociedad de la información y el conocimiento, en el que se entretejen campos conexos denominados dimensiones, tales como: educación, comunicación, tecnologías de información y subjetividad. El artículo presenta resultados de los imaginarios de sociedad de información que los actores[1] (estudiantes y docentes de una facultad de ingeniería) tienen de la apropiación, reconocimiento y valoración de las tecnologías de información y comunicaciones, en su acontecimiento educativo. Los resultados analizados corresponden a las relaciones entre sociedad de la información, el conocimiento y educación.

Palabras Clave: Sociedad de la información; entornos tecnológicos; tecnologías de información y comunicación Tic's; educación; apropiación de las Tic's.

Society of information technology and knowledge: technologies in the training of engineers

Abstract: This article seeks to socialize raised understandings of research processes of appropriation and use of information technologies and communications in the field of education of engineering in a University of face-to-face education and privacy in Latin America. This study takes place in a context of complexity called the society of information and knowledge, which are interwoven related fields

[1] Se reconoce el fundamental aporte de estudiantes y profesores de la facultad de ingeniería, como sujetos actores en el proyecto de investigación.

called dimensions, such as: education, communication, information technology and subjectivity. The article presents results of the imaginaries of information society actors (students and teachers of a school of engineering) with the appropriation, recognition and assessment of information and communications technologies, in its educational event. The analyzed results correspond to the relations between the information society, knowledge and education.

***Keywords**:* information society; technological environments; technologies of information and communication ICT; education; appropriation of ICTs.

1. Introducción

La formación en ingeniería ha venido experimentando un importante descenso en su demanda; frente a lo cual se plantean razones, argumentos y propuestas varias. Dentro de las causas más referenciadas está el rechazo de muchos estudiantes, desde la educación media, por el estudio de las ciencias naturales y exactas y sus aplicaciones. Ya en las universidades, algunos estudios (González & Bravo, 2009); (Valencia, 2010) y reflexiones (Ulloa, 2010) han demostrado que el mayor índice de pérdida y repetición de cursos se presenta en aquellos que tienen como núcleo, componentes de ciencia básica, especialmente matemáticas y física. Tal situación, tiene implicaciones para los sectores productivos y la sociedad al disminuir las capacidades para atender necesidades de desarrollo o atención de retos de humanidad como el cambio climático (UNESCO, 2010) se observa en el caso de Siemens, que en el 2001 presentó un 64% de la junta directiva como ingenieros y solo el 25% en el 2010 (ACOFI, 2013).

Partiendo de un principio general, que ubica a la ingeniería como una profesión que estudia y comprende los avances de la ciencia para desarrollar innovaciones tecnológicas que generen mejoramiento en la calidad de vida, la universidad enfrenta un acontecimiento crucial en la formación de ingenieros y en el desarrollo de la ingeniería. Las estrategias implementadas para tratar de subsanar las dificultades son variadas, en especial aquellas que plantean la solución en el campo de la didáctica, en concreto el uso de mediaciones tecnológicas; bajo el supuesto, que esta generación de estudiantes se siente muy cómoda con las actividades realizadas a través de dispositivos digitales y la capacidad de conexión y tráfico de datos mediante tecnologías 3G-4G e inalámbrica (Vasquez-Cano, 2015). Tratase entonces no sólo de un problema de educación, sino también de un problema de postura como sujetos pensantes en la dimensión de su aporte a la sociedad que queremos, construida desde singularidades en tensión de una única sociedad global que se basa en la información y cuyo mayor activo es el conocimiento.

Esta investigación se concibe en una construcción de campo/cuenca transdisciplinar en el que confluyen campos de conocimiento como las tecnologías de información y comunicación, la educación, la comunicación y la sociología, en un contexto de sociedad globalizada, conocida como sociedad de la información y el conocimiento, buscando no sólo cuestionar y proponer, por y en contexto, sino también evidenciar lugares y posibilidades en dos escenarios cruciales para la concepción de sociedad que nos convoca: ingeniería y educación.

Finalmente, la pregunta orientadora a través de la investigación desarrollada fue: ¿Cuáles son las relaciones y sentidos que se perciben en estudiantes y docentes de

una Facultad de Ingeniería, frente a las mediaciones tecnológicas que forman parte de su acontecimiento educativo?, cuestionamiento que lleva a otros más específicos como: ¿Qué es considerado aprendible en la lógica unidireccional del binomio enseñanza-aprendizaje? o ¿Hasta dónde la inclusión de las Tecnologías de Información y Comunicación (Tic's) en los procesos de formación garantizan el aprendizaje de lo enseñable?, o ¿El método garantiza el aprendizaje de lo enseñable? y otras más que surgieron, dinamizaron y vigorizaron el proceso de investigación.

Los resultados de esta investigación, brindan elementos que permiten comprender características del uso de las tecnologías que conforman mediaciones en la comunidad, las relaciones generadas y sentidos posibles para y en el acontecimiento educativo, desde comprensiones epistémicas complejas concebidas en el encuentro de la educación y tecnología como campos de conocimiento enmarcados en un acontecimiento mayor denominado sociedad de la información y el conocimiento.

En el primer apartado se puede visualizar el contexto e impactos en educación, tecnología e ingeniería en el marco de una sociedad de la información y el conocimiento; partiendo de esto en el segundo apartado se hace referencia al proceso metodológico que se llevara a cabo en el marco de la investigación, con el fin de comprobar la efectividad de la misma. El análisis de los resultados obtenidos se muestra en el tercer apartado, así como los estudios similares realizados con anterioridad a la presente investigación, finalmente, en el último apartado, se encuentran las conclusiones y recomendaciones para futuros trabajos que se vayan a realizar en la temática abordaba en la presente investigación.

2. Contexto e impactos en educación, tecnología e ingeniería en el marco de una sociedad de la información y el conocimiento

La sociedad del conocimiento, está dada por la continua innovación en materia científica y tecnológica a la cual se han tenido que enfrentar y adaptar los seres humanos, esto debido a que la tecnología se ha convertido en un factor relevante en la cotidianidad de la sociedad ya que vivimos en un momento histórico donde el volumen de información aumenta exponencialmente cada día (Alfonso, 2009).

Los cambios que han venido experimentando la sociedad, en camino de consolidar los rasgos que la caractericen (información y el conocimiento), son inexorablemente extendidos a todos los ámbitos y procesos sociales, dentro de los cuales se encuentra la educación. Son muchas las manifestaciones, pero tal vez una de las más importantes es la utilización de las redes de computadores para acceder a información que, mediando políticas y procesos organizacionales y personales, se convierten en conocimiento. En consecuencia, la presente investigación se centró más en comprender y caracterizar sentidos e intereses que orientan las acciones de los sujetos y las organizaciones involucradas en el acontecimiento educativo, independientemente del nivel de formalismo que ellos tengan.

Aunque la educación con mediaciones tecnológicas no es asunto únicamente de los actuales tiempos, pues siempre han estado allí diversas tecnologías, hoy no sólo se puede asociar con dispositivos, plataformas, bases de datos, documentos, buscadores, entre otros, a los cuales les hacemos benchmarking e implementaciones para ampliar cobertura y "educar".

3. Procedimiento metodológico

Por tratarse de una investigación, se toman elementos de dos enfoques metodológicos complementarios; el cuantitativo y el cualitativo.

Aplicando el enfoque cuantitativo se estableció, en la primera fase, una descripción o caracterización de las mediaciones tecnológicas a las cuales tienen acceso estudiantes y docentes, al igual que los usos (en términos de frecuencia y tiempo de dedicación) que les dan. La tabla 1 establece las categorías, sub-categorías y variables definidas.

Categoría	Sub-categoría	Variables*
Sujeto	Estudiante	Género, edad, programa de ingeniería, semestre
	Docente	Género, Edad, Profesión
Hardware	Máquinas	Diferentes medios físicos reconocidos como equipos, discos, memorias, entre otros.
	Medios de Conexión	Medios de acceso a la Red
Software	Sistemas Operativos	Sistema operativo usado más comúnmente
	Paquetes de Utilitarios	Paquetes de software utilizados más comúnmente
	Software especializado	Paquetes de software especializados
	Origen del software	Disponibilidad de software licenciado
Usos	Frecuencia/ Uso-Servicio / Lugar	Frecuencia y lugar preferido para uso de dispositivos y acceso a contenidos
	Tiempo / Uso-Servicio / Lugar	Tiempo destinado a uso de dispositivos y consumo de contenidos

Tabla 1 – Categorías, sub-categorías y variables

Complementariamente y a través del enfoque cualitativo se realizó en la segunda fase, una comprensión de manifestaciones y apreciaciones de subjetividad alrededor de las tecnologías y sus usos, además de relaciones entre los sujetos educandos y educadores. La metódica contempló la socialización de resultados cuantitativos para dinamizar los diálogos.

3.1. Diseño y validación de instrumentos

El instrumento de recolección información se diseñó con base en las categorías, sub-categorías y variables establecidas, configurando una estructura deductiva. La validación se realizó con pruebas piloto en grupos de muestra (docentes y estudiantes), con el fin de medir: claridad de las preguntas, comprensión de los términos, niveles de empatía con el instrumento y tiempo de respuesta. Para ello se utilizó un instrumento adicional en el cual se indagaba sobre los elementos a medir; la información recabada permitió hacer los ajustes definitivos, para finalmente someter el instrumento a concepto de un investigador experto y proceder a digitalizar y ubicar la encuesta en la plataforma electrónica seleccionada (e-encuesta).

3.2. Definición de población y muestras

El estudio se realizó con las comunidades de estudiantes y docentes de una facultad de Ingeniería tradicional, con un muestreo aleatorio por participación. Para la comunidad de estudiantes se vincularon noventa y siete (97) personas en la fase 1, cifra que corresponde aproximadamente al 11% de la población estudiantil perteneciente a seis programas de pregrado en ingeniería; en la fase 2 participaron doce estudiantes. De la comunidad de docentes participaron treinta y cuatro personas, cifra equivalente al 35% de los docentes de la facultad; en la fase 2 se vincularon ocho docentes. En la siguiente tabla se aprecia la ficha técnica del estudio realizado:

Ítem	**Descripción**
Universo en estudio	880 estudiantes de la Facultad de Ingeniería. 97 docentes de la Facultad de Ingeniería
Tamaño de muestra	131 participantes en estudio cuantitativo 20 participantes en estudio cualitativo
Distribución de la muestra	97 estudiantes y 34 docentes en estudio cuantitativo 12 estudiantes y 8 docentes en el estudio cualitativo
Cobertura Geográfica	Santiago de Cali, Facultad de Ingeniería con metodología presencial.
Tipo de muestreo	Aleatorio
Recolección de la información	Encuesta entregada y diligenciada a través de plataforma electrónica Sesiones de diálogo

Tabla 2 – Ficha Técnica

3.3. Técnicas de recolección de información

Para la fase 1 se diseñaron encuestas, organizadas por las categorías, sub-categorías y variables citadas. La aplicación del instrumento se hizo a través de una aplicación de plataforma web (e-encuesta), con enlaces enviados a los correos electrónicos de los miembros de las comunidades citadas (con base en listas de correos institucionales), estableciendo una fecha de expiración de la encuesta. Posteriormente, se exportaron los registros a un archivo de Excel, en donde se les dio una estructura de datos que pudiera ser igualmente exportada a un software de análisis estadístico, en este caso el *Statistical Package for the Social Sciences* SSSP, versión 16.

Para la fase 2 la información cualitativa se obtuvo a partir de dos procesos, que, aun siendo independientes, se complementan para permitir visualizar percepciones de los sujetos. Se obtuvieron manifestaciones de los sujetos involucrados, relacionadas con significantes, usos, relaciones y percepciones de la incursión de las TIC´s en sus vidas. Paralelamente, se articularon estrategias de observación y reflexión sobre procesos formativos, presentes y pasados, en los cuales tienen y han tenido injerencia las TIC´s.Toda esta información, fue sistemáticamente transcrita e incorporada a documentos de trabajo.

3.4. Técnicas de análisis de datos

Una vez cargados en el software SSSP, los datos cuantitativos, son procesados y graficados respecto a cada una de las variables, para posteriormente interpretarlos en términos de valores porcentuales. Y finalmente establecer las relaciones con indicadores de contexto. Por otra parte, los datos cualitativos permitieron ir hilando comprensiones con mayor sentido de los datos cuantitativos, especialmente lo relacionado con el uso y las frecuencias de uso, frente a los significantes y relaciones de los sujetos, en su interacción con las mediaciones tecnológicas vinculadas a sus procesos formativos.

4. Análisis de resultados

El artículo presenta los resultados a nivel de categoría en la dimensión educación y tecnología. No obstante lo anterior existe un marco estadístico para categorías, sub-categorías y variables en cada una de las dimensiones.

4.1. Categoría: Sujeto

La gran mayoría de los sujetos estudiantes nacieron cuando dos de los elementos tecnológicos digitales que caracterizan a la sociedad de la información y el conocimiento ya habían alcanzado un importante lugar: los computadores personales (Década de los 80's) y la internet (1969) (Rubio Moraga, 1982). Sin embargo, gran parte de sus actividades, muchas de sus decisiones y la percepción del mundo que les rodea están influenciadas por las tecnologías de información y comunicación, así, puede considerarse que la gran mayoría de estudiantes participantes en el estudio son nativos digitales y todos los docentes participantes en el mismo son migrantes digitales.

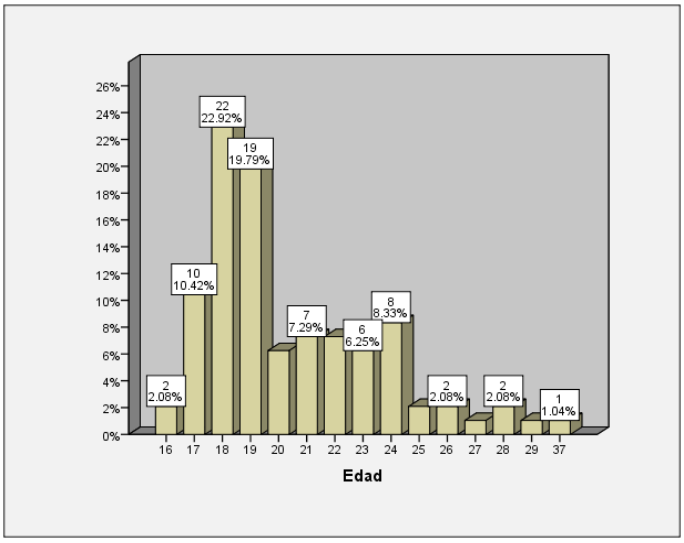


Figura 1 – Participación porcentual por edad de estudiantes.

En la gráfica No. 1 se observa que la edad de mínima de los estudiantes que participaron es de 16 años y la máxima es de 37. La edad promedio es de 20 años. Igualmente se observa que la mayoría de ellos, esto es el 53.1%, está entre los 17 y los 19 años.

4.2. Categoría: Hardware

A manera de ubicación en el contexto socio-económico, se considera importante para la relación de algunas cifras, plantear que los estudiantes de la universidad, especialmente los de la facultad de ingeniería, se ubican mayoritariamente en los estratos sociales 3 y 4 (clase media), aunque se encuentran casos en estratos 2 y 5.

Se destaca la alta penetración de la telefonía celular, siendo interesante la diferencia de casi 20 puntos porcentuales entre estudiantes y docentes que usan dispositivos de comunicación móvil. Las cifras de conectividad en ambos casos superan el 95% que en comparación con los índices nacionales e internacionales, posicionan a estas comunidades en un nivel mucho más alto, superando ampliamente los indicadores planteados por estudios recientes.

4.3. Categoría: Software

Considerando que la formación en ingeniería requiere desarrollar capacidades y destrezas para análisis, diseño e innovación en productos. Tan sólo, el 34% usa herramientas que les permite diseñar gráficas y/o programar computadores y sólo el 23.7% utiliza herramientas de simulación.

El 41% de los estudiantes usa tutoriales. De ellos, la fuente primaria es *Google*, 19.2%; le sigue *Oracle* (plataforma para bases de datos, lo cual ubica su uso en estudiantes de ingenierías relacionadas directamente con sistemas de información) con 15.4%; luego están los videos educativos en *Youtube*, 11.5%; posteriormente otros relacionados con programación de computadores con 14%. Esto ubica a los estudiantes de ingeniería de sistemas e ingeniería multimedia como los más cercanos al uso de TIC´s como soporte a su aprendizaje independiente.

Las bases de datos digitales son usadas por tan sólo el 51.5% de los estudiantes; manifiestan utilizarlo en su proceso de formación, aún más diciente es que de aquellos que manifiestan usar las bases de datos, el 24.2% relaciona a *Wikipedia*, el 18.2% relaciona a *Google* y el 9.1% a 'Encarta', herramientas estas que están lejos de ser bases de datos especializadas.

El 64.9% de los estudiantes utiliza plataformas electrónicas de educación. Se destaca el *Moodle* (plataforma institucionalizada y administrada por el centro de educación virtual) con un 58%, *CourseCompass* con el 16% y *Mymathlab* con el 8%.

4.4. Categoría: Usos

Los sitios de internet relacionados con educación (bibliotecas virtuales, plataformas educativas, entre otros) son visitados diariamente, desde los hogares, por tan sólo el 21.6% de los estudiantes, en adición, el 22.6% ingresan cinco o cuatro veces por semana.

Los sitios de internet relacionados con redes sociales o comunidades virtuales son visitados diariamente, desde la residencia, por el 51.6% de los estudiantes y tan solo por el 17.7% de los docentes.

El uso de software utilitario (procesador de texto, hoja electrónica, entre otros), es practicado diariamente desde los hogares por el 30.9% de los estudiantes, el 10.3% lo usa entre 4 y 5 veces por semana, el 15.5% entre 1 y 2 veces por semana.

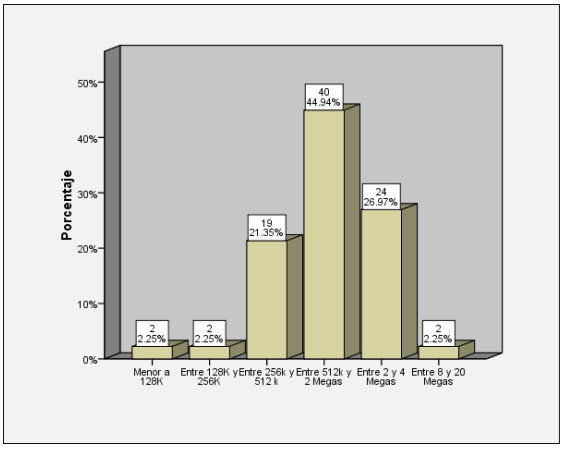


Figura 1 – Velocidad de acceso a internet dese residencia de los estudiantes.

En la gráfica No. 2 se observa que el 44.9% de los estudiantes creen que la velocidad de acceso a Internet, desde su residencia, está entre 512 Kbaudios (Kb) y 2 Megabaudios (Mb); el 26.9% cree que está entre 2 y 4 Mb; el 21.3% cree que está entre 2256 y 512 Kb; el 2.2% cree que está entre 128 y 256 Kb; el 2.2% cree que está entre 128 y 256 Kb y el 2.2% cree que está entre 8 y 20 Mb.

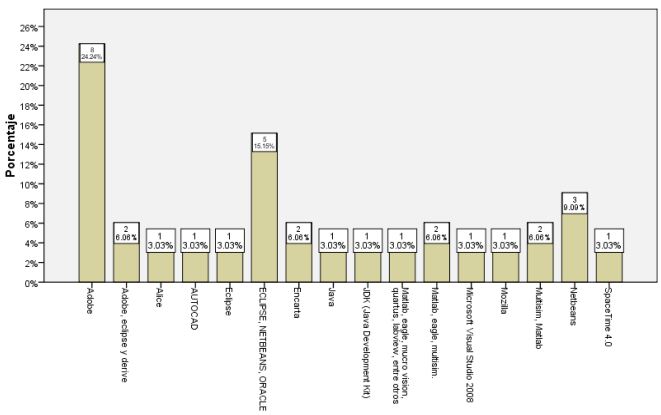


Figure 2 – Software especial usado por los estudiantes en sus computadores.

De acuerdo con la figura No. 3, sólo treinta y tres (33) estudiantes, equivalente al 34.0% del total, utiliza software especial en sus computadores. De ellos el 24.2% usa Adobe; el 15.1% usa Eclipse, Netbeans y Derive; el 9.0% usa Netbeans. Los restantes usan diversas herramientas orientadas a programación de computadores, buscadores de internet y simulación.

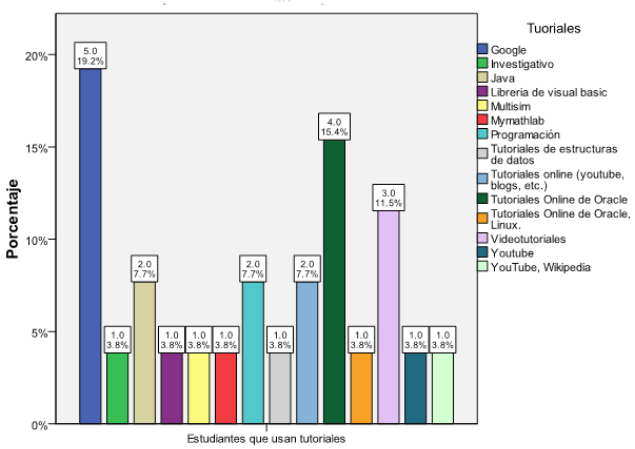


Figure 3 – Tutoriales usados por los estudiantes para sus estudios o investigaciones.

Según la figura No. 4, de los estudiantes que utilizan tutoriales, cinco manifiestan que es Google, con 19.2%, la fuente para encontrar tutoriales, sin establecer preferencia por alguno en especial. Le siguen los tutoriales on line de Oracle (bases de datos), con el 15.4%; Video tutoriales con el 11.5% y luego otros orientados a la programación de computadores: Java con 7.7%, Programación con 7.7%; también tutoriales on line con el 7.7%. Posteriormente, están investigativo con 3.8%, librería visual basic con 3.8%, Multisim con 3.8%, Mymathlab con 3.8%, estructuras de datos con 3.8%, online oracle-linex con 3.8%, youtube con 3.8% y youtube-wikipedia con 3.8%,

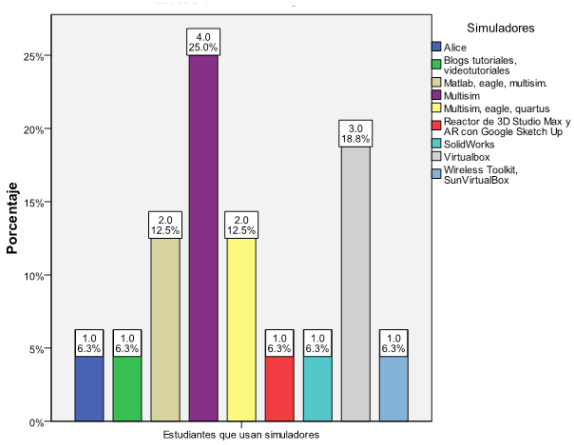


Figure 4 – Simuladores que usan los estudiantes para sus estudios o investigaciones.

Según la figura No. 5, de los estudiantes que utilizan simuladores, cuatro manifiestan predilección por Multisim, con el 25.0%, seguido de Virtualbox con el 18.8%, Matlab con el 12.5%, Multisim-eagle-quartus con el 12.5%, Alice con el 6.3%, Blogs tutoriales con el 6.3%, Reactor 3D con el 6.3%, Solidworks con el 6.3% y Wireless toolkit con el 6.3%

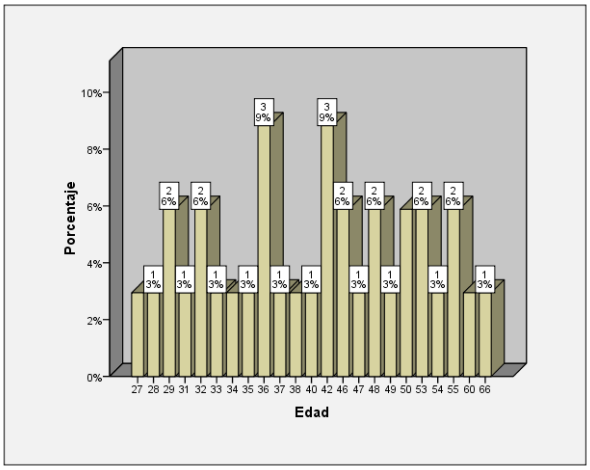


Figure 5 Participación porcentual por edad de docente.

En la figura No.6 se aprecia que la edad mínima de los docentes que participaron es de 27 años y la máxima es de 66. La edad promedio es de 42 años.

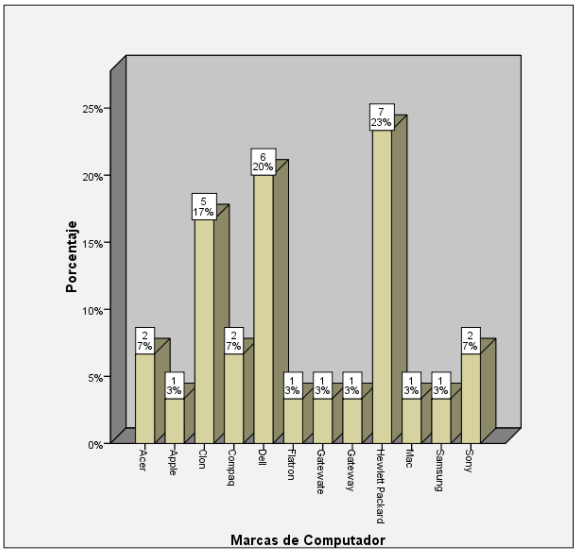


Figure 6 – Marcas de computador más usadas.

Según la gráfica No.7, la mayoría de los docentes optan por computadores de las marcas que tienen mayor penetración del mercado (Hewlett Packard, Dell), las cuales suman el 43.0% de la muestra. Igualmente existe un considerable número de docentes, 20.0%, que poseen los denominados computadores Clon[2]. En ambos grupos se puede apreciar una importante conjunción de elementos que permiten afirmar que tecnológicamente no forman parte de la brecha digital entre sociedades desarrolladas y subdesarrolladas. Claro está que debemos considerar la debilidad estructural en la velocidad de los canales de banda ancha implementados en nuestro país, si los comparamos con los de países con mayor capacidad tecnológica.

El acceso a información y el interés por el conocimiento no está dentro de las prioridades de la mayoría de participantes (docentes-estudiantes). Considerando el tiempo dedicado a los procesos de estudio-investigación-formación, en relación con el tiempo dedicado a otras actividades, se percibe, para los grupos en estudio, que las TIC´s no configuran un escenario diferenciador para el desarrollo de la autonomía de sujetos en trance de superación de modelos mediáticos impuestos con fines de consumo, y no se reflejan rasgos de autodeterminación significativa en los procesos de formación.

El poco acceso y uso de información restringida, que se encuentra disponible en plataformas institucionales, al igual que el escaso uso de herramientas que faciliten el desarrollo de habilidades requeridas en ingeniería, puede generar una brecha auto inducida frente a comunidades que tengan condiciones tecnológicas similares, con un factor de aprovechamiento más alto, contextualizándolas y potenciando ideas para desarrollos locales producto del conocimiento adquirido.

Nombre de la Investigación	País estudio o Investigación	Institución	Objetivo
La Institución Educativa en la actualidad: Un análisis del papel de las tecnologías en los procesos de subjetivación. (Vanegas Arrambide, 2002)	Barcelona, España	Universidad Autónoma de Barcelona	Determinar la influencia de las tecnologías (todo tipo de tecnologías) en la generación de subjetividades en los educandos. (Vanegas Arrambide, 2002)
Caracterización de conocimiento y uso de las herramientas especializadas de internet entre la comunidad académica, científica, profesional y cultural de la Universidad de Antioquia (Uribe Tirado, 2004).	Medellín, Antioquia	Universidad de Antioquia	Crear un modelo de datos para determinar cuáles son las herramientas de la internet más utilizadas por la comunidad académica (Uribe Tirado, 2004).
Herramientas tecnológicas para mejorar la docencia universitaria. Una reflexión desde la experiencia y la investigación (García-Valcárcel, 2007).	Salamanca, España	Universidad de Salamanca (España)	Conocer el uso que los profesores hacen de estas herramientas y las competencias específicas que los docentes deberían adquirir para una utilización efectiva de las mismas (García-Valcárcel, 2007).

Tabla 3 – Estudios Similares

[2] En el mercado de los computadores se denomina Clon a las máquinas que son armadas con partes genéricas, de diferentes fabricantes.

En general, como rasgo diferenciador, esta investigación pretende comprender las características de las tecnologías usadas por una comunidad educativa, las relaciones generadas y sentidos posibles para y en el acontecimiento educativo, desde comprensiones epistémicas complejas concebidas en el encuentro de cuatro campos de conocimiento (educación, subjetividad, comunicación y tecnologías) enmarcados en un acontecimiento mayor denominado sociedad de la información y el conocimiento.

5. Conclusiones y trabajo futuro

Las conclusiones de este trabajo se describen a continuación:

- En ambos grupos se puede apreciar una importante conjunción de elementos que permiten afirmar que tecnológicamente no forman parte de la brecha digital entre sociedades desarrolladas y aquellas en desarrollo, que ha ido generando la sociedad de la información y el conocimiento. Claro está que debemos considerar la debilidad estructural en la velocidad de los canales de banda ancha implementados en nuestro país, si los comparamos con los de países con mayor capacidad tecnológica.
- El acceso a información y el interés por el conocimiento de hechos culturales e históricos no está dentro de las prioridades de la mayoría de participantes, tanto docentes como estudiantes, lo cual establece una constante de sociedad. Podría plantearse aquí un importante eslabón para llamar la atención de los educadores de la generación pre-digital y de los educandos de la generación digital, sobre cómo desde la educación se pueden y deben generar movimientos significativos, no sólo individual sino colectivamente, que apunten a corregir falencias de la sociedad y de las relaciones de esta con el planeta, tanto en ópticas de pensamiento como en marcos de acción e interacción.
- Al existir un bajo uso de herramientas de productividad y considerando que hoy la producción de textos se realiza en este tipo de plataformas, aunado a las manifestaciones de los participantes, se puede percibir una gran debilidad en los procesos de escritura de textos producto de la lectura y/o reflexión con bases y referentes válidos.
- Considerando el tiempo dedicado a los procesos de estudio-investigación-formación, en relación con el tiempo dedicado a otras actividades, se percibe, para los grupos en estudio, que las TIC´s no configuran escenario diferenciador para el desarrollo de la autonomía de sujetos en trance de superación de modelos mediáticos impuestos con fines de consumo, esto es, no se reflejan rasgos de autodeterminación significativa en los procesos de formación.
- Con base en los contenidos y usos que privilegian los estudiantes y docentes del estudio, se puede apreciar que en la mayoría de ellos no existe identificación de rasgos distintivos entre información y conocimiento circulantes en las redes de información, por tanto el disponer de capacidades de acceso no representa ventaja alguna en el desarrollo de capacidades creativas e innovadoras, como tampoco de subjetividades para trascender el determinismo del mero consumo de información.
- El poco acceso y uso de información restringida, que se encuentra disponible en plataformas institucionales, al igual que el escaso uso de herramientas que

faciliten el desarrollo de habilidades requeridas en ingeniería, puede generar una brecha auto inducida frente a comunidades que tengan condiciones tecnológicas similares pero que sepan aprovecharlas, contextualizándolas y potenciando ideas para desarrollos locales que produzcan conocimiento.

- Mientras que los educadores le damos sentido a las tecnologías en términos de sus posibilidades como mediación del proceso educativo, los estudiantes les dan sentido en términos de relación con el mundo que les rodea, tanto cercano como lejano. Esto plantea entonces distorsiones y rupturas en los procesos comunicativos entre comunidades de sentido. Mientras el sentido para unos, en términos de objetivo principal de las mediaciones, es solucionar problemas de didácticas específicas y mejorar las competencias, para otros es tener acceso a la in-formación, estar interconectado y contar con los dispositivos más recientes y con mejores funcionalidades.
- En estas comunidades no se hacen visibles rasgos de trascendencia de los usos de las mediaciones tecnológicas, más allá del consumo de dispositivos y contenidos impuestos por agentes de mercados. En este aspecto se genera un interrogante: ¿cómo revertir estas tendencias con-sumistas en comunidades que están llamadas a utilizar la información y el conocimiento con criterios de reflexión, creación y autodeterminación?

Para futuras investigaciones se recomienda tomar en consideración los siguientes aspectos:

Establecer un proceso periódico de replicación del estudio para establecer variaciones y tendencias, en relación con los movimientos de los escenarios tecnológico y educativo.

Para facilitar el proceso de análisis se recomienda implementar una herramienta tecnológica que permita el registro y recuperación de datos, estableciendo filtros y funcionalidades para contrastar información entre diferentes versiones del estudio.

Con el fin de obtener información cualitativa se sugiere implementar espacios en plataformas electrónicas, como foros o blogs, que permitan obtener mayor cantidad de información en periodos de tiempo más amplios. Ello implica vincular estudiantes que estructuren la información de acuerdo con las categorías abordadas.

A partir de los resultados arrojados por el estudio se pueden plantear proyectos de intervención para potenciar aspectos benéficos de la inclusión de las tecnologías en el proceso educativo, como también para el desarrollo de subjetividades lúcidas frente al papel de las tecnologías en la sociedad de la información y el conocimiento.

Referencias bibliográficas

ACOFI. (2013). *Una Mirada a la formación en ingenieria en el contexto internacional*. Recuperado el 2016, de http://www.acofi.edu.co/wp-content/uploads/2013/08/DOC_PE_Mirada_formacion_en_ingenieria.pdf

Alfonso, R. (2009). La sociedad del conocimiento y los nuevos retos educativos. *EticaNet, 8*. Obtenido de http://www.ugr.es/~sevimeco/revistaeticanet/numero8/Articulos/Formato/articulo9.pdf

García-Valcárcel, A. (2007). Herramientas tecnológicas para mejorar la docencia universitaria. una reflexión desde la experiencia y la investigación. *RIED. Revista Iboeroamericana de Educación a Distancia, 10*.

González, D., & Bravo, M. (2009). Retraimiento poblacional en educación superior. Ingreso, moralidad, académica y deserción. *U. San Buenventura*.

Rubio Moraga, Á. (1982). Historia de internet: aproximación al futuro de labor investigativa. *Aportacions de la comunicació a la comprensió i construcció de la història del segle XX*.

Ulloa, G. (2010). ¿Qué pasa con la ingeniería en Colombia? *Revista Ingeniería y sociedad, 2*.

UNESCO. (2010). Engineering: Issues, Challenges and Opportunities for Development. *UNESCO Publishing*.

Uribe Tirado, A. (2004). *Acceso, conocimiento y uso de las herramientas especializadas de internet entre la comunidad académica, científica, profesional y cultural de la Universidad de Antioquia*. Obtenido de http://docencia.udea.edu.co/investigacioninternet/contenido/analisis.pdf

Valencia, D. (2010). Crisis y futuro de la ingeniería. *Revista Ingeniería y sociedad, 1*.

Vanegas Arrambide, G. (2002). *La Institución Educativa en la actualidad. Un análisis del papel de las tecnologías en los procesos de Subjetivación*. Obtenido de https://ddd.uab.cat/record/37365

Vasquez-Cano, E. (2015). El reto de la formación docente para el desarrollo de una metodología ubicua en la educación superior. . *Perspectiva Educacional. Formación de Profesores., 54*, 149–162.

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 08/12/2017
Aceitação/Acceptance: 11/03/2018

TICs en Colombia: revisión a partir de la Curva de Gartner

Yuri V. Nieto A.[1], Carlos E. Montenegro M[2], José F. López Q.[3], Yesid Díaz G.[4]

Yuri_nieto@cun.edu.co, cemontenegrom@udistrital.edu.co, jose_lopezqui@cun.edu.co, Yesid_diaz@cun.edu.co

[1] Facultad de Ingeniería, CUN, Bogotá, Colombia

[2] Facultad de Ingeniería, Universidad Distrital FJC, Bogotá, Colombia

[3] Facultad de Ingeniería, UNAD, Bogotá, Colombia

[4] Facultad de Ingeniería, UNAD, Bogotá, Colombia

Pages: 318–329

Resumen: Este artículo describe una forma de medir el desarrollo y evolución de las tecnologías implementadas y administradas por el Ministerio de las Tecnologías de la Información y Comunicación en Colombia, mediante el uso de herramientas de carácter cuantitativo, donde se representa en gr***á***ficas de uso analítico, el proceso en años que ha tenido una tecnología y que tan rentable fue para dicha administración, al igual, que las diferentes comparativas que se pueden realizar con diferentes países desarrolladores de tecnología, consumidores de tecnología y/o países emergentes. Este análisis a nivel local se hace a partir de diferentes reportes de implementación de tecnología arrojados por los diferentes entes de reportes gubernamentales.

Palabras claves: Hype Curve de Gartner, Ciclo de sobre expectación, Tecnologías de la información y comunicación, Internet de las cosas, apropiación de las TIC, Toma de decisiones, Gartner.

ICTs in Colombia: review from the Gartner Curve

Abstract:- This article describes one way of measuring the development and evolution of the technologies implemented and administered by the Ministry of the information technologies and communication in Colombia, through the use of quantitative tools, where is represented in graphics for analytical use, the process in years that has had a technology and so profitable was for the Administration, as well, that the various comparisons that can be made with different developers, technology, consumer countries technology or emerging countries. This analysis at the local level is made from different reports of implementation of technology thrown by the different bodies of governmental reports.

Keywords: Hype Curve de Gartner, Ciclo de sobre expectación, Tecnologías de la información y comunicación, Internet de las cosas, apropiación de las TIC, Toma de decisiones, Gartner.

1. Introducción

La tecnología además de su evolución y desarrollo ha dado formas de medir su crecimiento en forma cuantitativa, para observar de forma científica y analítica el desarrollo y evolución que ha tenido cada tecnología, y de esta misma forma, medir si dicho avance tecnológico se quedó en procesos de desarrollo e implementación, o si finalmente logró establecerse y llegar a ser una tendencia y una necesidad para la evolución de un proceso. La primera parte o sección del articulo inicia con la conceptualización de aspectos contenidos en la Hype Curve de Gartner (Linden & Fenn, 2003), como las fases del ciclo, los diferentes criterios que se deben tener en cuenta para medir el desarrollo de una tecnología y las definiciones de cada una de sus fases.

En cuanto a la evaluación del método y su aplicación a la medición de TIC (Tecnologías de la información y comunicación) (Leal, 2008), este trabajo profundiza en el flujo o ciclo que llevan las tecnologías en los diferentes ámbitos gubernamentales, comerciales y/o industriales en los cuales son usadas, seguido, de una descripción detallada acerca de las TIC, su apropiación (Montes y Ochoa, 2006), la historia y descripción de sus conceptos y los lineamientos para ser usadas y ejecutadas de manera correcta de acuerdo al caso de uso que se le asigne.

El Segundo apartado, da una breve reseña de la evolución de las TIC y su funcionamiento en temas de apropiación de acuerdo al PETIC (Plan Estratégico de Tecnología) en Colombia (Santos, 1990), bajo la administración del MINTIC (Ministerio de las Tecnologías de la Información y Comunicación). Se explicará cómo funciona el proceso de investigación, licitación, implementación y apropiación de una nueva tecnología bajo la administración del MINTIC, en su periodo de evolución, y donde según reportes nacionales del gobierno han ocurrido los cambios más importantes de este siglo en tecnología y PETIC. Estos cambios que han ocurrido a partir de los últimos 10 años donde se ha evidenciado transformaciones en temas de apropiación de TIC en el país, priorizando sus ciudades, sus pueblos, empresas locales e inversoras extranjeras.

La última sección muestra cual fue la metodología de la investigación, y como se aplicó la Hype Curve para identificar las diferentes etapas de una TIC en Colombia desde su llegada hasta su decadencia o éxito y apropiación en el país. Así mismo, se identifican cuales tecnologías fueron adoptadas y cuáles no. Estos ejemplos y comparaciones implementadas en el modelo de la Hype curve de Gartner, sirven para encontrar las fortalezas y debilidades en las fases de investigación, desarrollo y producción de nuevas TIC. Comparar niveles de conocimiento y de forma analítica pasar al punto de toma de decisiones.

2. Qué es la curva de gartner

2.1. Hipercurva de Gartner

El Hype Curve (Traducido al español por ciclo de sobre expectación), caracteriza la progresión típica de una tecnología emergente donde se representa su paso por diferentes fases o etapas llamados ciclos en la curva de Gartner. En dicha curva, se observa la importancia que se le dan a las tecnologías emergentes y el papel que representan en un mercado o dominio de la tecnología.

Esta curva se dio a conocer en la casa de análisis e investigación Gartner, ubicada en Stanford, Estados Unidos. La cual proporciona opiniones, consejos y diferentes datos de ingeniería de negocios sobre las Tecnologías de la Información. La curva, ha sido una herramienta útil en la toma de decisiones de la compañías o gobiernos, para evaluar como una inversión puede afectar positivamente o negativamente a la economía o productividad de acuerdo a la necesidad que posean de una nueva tecnología que aporta al desarrollo de una labor específica, al igual que sirve, para medir o hacer comparativas acerca de cómo se encuentra el avance en tecnología de ciertos sectores, dando un reporte de cómo se encuentra cada innovación tecnológica y en qué fase se encuentra respecto al año anterior. Es decir, que en el primer trimestre del 2016 se entregó la curva de Gartner del 2015 donde se evidenciaron claramente los avances, retrocesos o la pérdida total respecto al año respectivo.

2.2. Fases de la Hipercurva de Gartner

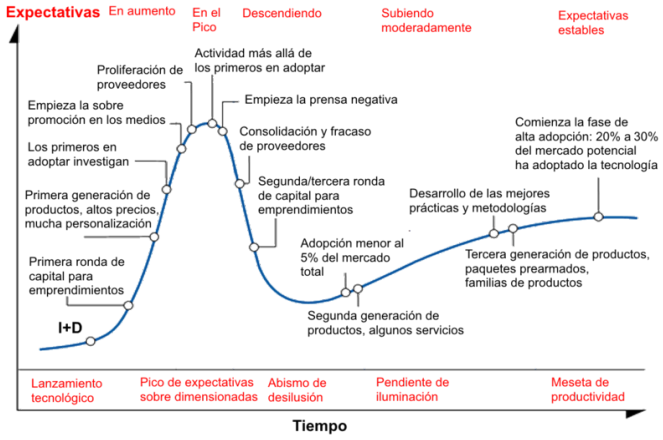


Figura 1 – Procesos de la tecnología en cada etapa. (Fuente: Gartner, Inc).

El hypecicle se mide en cinco fases (Gartner, 2011), las cuales se pueden observar en la figura 1. Estas cinco fases, representan los procesos de cambio y evolución de una tecnología donde los gobiernos, empresas, accionistas observan y tienen en cuenta si deben invertir o no en una tecnología. De acuerdo a su criterio, se realiza la interpretación y análisis sobre si se invierte o se compra, por ejemplo, por el boom de publicidad que tiene en el pico de las expectativas a una tecnología o si esta debe ser ignorada, simplemente porque no está cumpliendo con los principios básicos de expectación y hasta ahora está se encuentra en su fase de desarrollo. Las fases se describen a continuación:

1. *Lanzamiento*: Es la subida al pico de expectativas, donde artículos y medios de comunicación explican la tecnología, como funciona y discuten su impacto potencial en empresas y la sociedad. Es en esta etapa donde la tecnología comienza a surgir por medio de generaciones 1, 2, 3, 4, etc. Para que lleguen a estar posicionados en esta etapa deben ser productos muy especializados o

extremadamente difíciles de usar en el momento, dado que aún se encuentran en fase de desarrollo e investigación de usabilidad, utilidad y adaptación al usuario.

2. *Pico de Expectativas Sobre-dimensionadas*: La publicidad juega un factor importante en esta fase del ciclo, ya que si la tecnología aún no genera expectativa por si sola o por lo que hace, esta y el enfoque en los casos de éxito si pueden ser el detonante para lanzar a la fama incrementar la expectativa de dicho producto. Con el pico de expectativas, aumenta el número de proveedores que ofrecen la tecnología. Estos proveedores son principalmente las empresas y pequeños vendedores, que intentan utilizar al producto para su beneficio de marketing.
3. *Abismo de Desilusión*: La tecnología deja de ser un objetivo urgente para las empresas y los medios de comunicación. Por las quejas y contras, bajan las expectativas que se tenían del producto, y este comportamiento tiene una gran diferencia del lanzamiento y su subida al pico de expectativa. Está fase lanza al producto rápidamente a la desacreditación y al abismo de la desilusión, como es el caso de algunos productos o tecnologías que aún estaban en procesos de pruebas y pasaron muy rápido al pico de expectativas donde terminan siendo un total fracaso ya que no se les dio el espacio suficiente para su desarrollo. O en otros casos, algunas tecnologías tuvieron fallas en sus campañas de publicidad, de tal modo, que no fueron conocidos lo suficiente para llegar a mantenerse vigentes.
4. *Rampa de Consolidación*: De acuerdo a los nuevos avances en dicha tecnología, se comienza a justificar su necesidad y se realizan amplios análisis sobre cómo la innovación y desarrollo de esta tecnología puede beneficiar a las empresas, su funcionamiento y forma de apoyar los procesos corporativos se hace más fácil de entender y adaptar, dado que ya existe la suficiente documentación al respecto. Esta ya no es una fase del desarrollo como tal del producto. Es la fase de desarrollo y adaptación a una necesidad específica de cada cliente, quien experimenta y se documenta a partir de los casos exitosos y experiencias de diferentes sectores del mundo corporativo. Esta tecnología se vuelve cada vez más diversa y más comprensible en su aplicabilidad, los riesgos al ser usada disminuyen y por el contrario los beneficios aumentan.
5. *Meseta de Productividad*: La meseta representa el principio de adopción convencional de una tecnología, cuando los beneficios reales de la tecnología están demostrados y aceptados. Dichas tecnologías son apropiadas y son mucho más útiles de lo que se creía, en el desarrollo de soluciones a una necesidad específica. Al ser esta tecnología una tecnología más madura, las empresas reducen costos en investigación y ahora aumentan costos en innovación de esta y a la cultura de apropiación. A medida que esta tecnología madura y se convierte en una tecnología de alto perfil, un "ecosistema" evoluciona a menudo alrededor de él.

2.3. Las Tecnologías de la Información y la Comunicación

Las Tecnologías de la Información y la Comunicación o TIC (Levy, 1995) corresponden y se refieren a todas las tecnologías que de una u otra forma interfieren y median en los procesos informacionales y comunicativos entre seres humanos, y pueden ser entendidas

como un conjunto de recursos tecnológicos integrados entre sí, que proporcionan, por medio de facilidades de hardware, de software, y de telecomunicaciones, la semi-automatización y comunicación de procesos relativos a negocios, a investigación científica, a enseñanza, a aprendizaje, a cuestiones de la vida diaria, etc.

La importancia del uso de TIC es que se su apropiación o implementación, aumenta la productividad y por lo tanto, se pueden completar un mayor número de tareas en el mismo tiempo a un costo reducido mediante el uso de equipos que nos ayudan a lidiar con grandes cantidades de información y procesarla rápidamente. Siendo así capaz de transmitir y recibir información de forma casi inmediata, según el tipo de TIC que se use, también se pueden hacer transferencias de mensajes, datos o información desde cualquier parte del mundo en cuestión de minutos. Y bien puede decirse que el principal responsable del crecimiento y potenciación de las TIC en los diversos campos, ha sido el desarrollo y la popularización de Internet.

2.4. Apropiación TIC en los ciudadanos

Hace referencia a los conocimientos prácticos y al uso indispensables de las herramientas TIC implementadas por los ciudadanos ante los desarrollos y recursos informáticos que hacen presencia en el siglo XXI, contribuyendo así, al cierre de la brecha digital desde el acceso a Internet u otros recursos TIC (Echeverría, 2008).

La apropiación de tecnologías de la información y las comunicaciones, se entiende como el proceso por el cual un actor satisface oportuna y convenientemente las necesidades que le presenta su contexto, mediante el uso de tecnología. Para que el proceso de apropiación sea exitoso en el eslabón más importante, la sociedad, deben darse las condiciones que lo favorezcan en todos los anteriores. Es decir, las acciones de apropiación serán más eficientes en la medida que un contexto de apropiación organizacional y gubernamental también la promuevan.

Por ejemplo, cuando un ciudadano accede de manera fácil y rápida desde su casa a aplicativos que le permiten evitar largos trámites presenciales para expedir documentos, efectuar pagos o presentar solicitudes ante el gobierno, requiere que éste haya adoptado favorablemente tecnologías de información, las cuales se hacen relevantes para el usuario en el momento en que percibe que sus necesidades se satisfacen oportunamente con tecnología y, en consecuencia, siente la exigencia de apropiarlas.

El trabajo de apropiación por parte del gobierno y de organizaciones públicas y privadas tiene sentido en la medida que su fin último sea la sociedad. Por ejemplo hoy, las tabletas en los colegios son una realidad, a medida que esas tabletas se complementen con aplicativos que promuevan su uso en lo relacionado con la productividad, el bienestar, la calidad de vida y otros objetivos sociales, la apropiación será exitosa.

3. Estrategias TIC en Colombia

Los ministerios o departamentos de TIC, que existen en el gobierno de cada país, tienen como misión brindar en su administración las mejores prácticas o técnicas de apropiación e implementación de las mismas. Con esto se busca, brindar los mejores resultados en innovación, desarrollo, investigación y eficaz producción en temas de tecnología o

comunicaciones. A la vez, se pretende lograr constantes mejoras en innovación para mantenerse en la vanguardia en tecnología según su plan estratégico de tecnología e inversión por parte de gobierno lo permitan.

3.1. MINTIC y su estrategia

En Colombia, el Ministerio de las Tecnologías de la Información y las Comunicaciones (MINTIC) fue fundado el 30 de Junio de 2009; amparados por la ley 134 (C. Constitucional, 2009), el Ministerio de Comunicaciones pasó a convertirse en el nuevo MINTIC transformando con su creación la tecnología en la historia del país, el cual en los últimos 5 años ha logrado conectar más ciudadanos.

Uno de los resultados por mostrar, ha sido el de multiplicar las conexiones de internet en los hogares, en las empresas y en las entidades gubernamentales, pasando de tener de 2'000.000 de conexiones a 8.800.000 millones aproximadamente en el año 2014 y con los últimos planes a duplicar dicha cifra para el año 2017. Todo esto ha sido gracias a varios proyectos que maneja el MINTIC en temas de apropiación de TIC, para apoyar e infundir el desarrollo del sector de tecnología en el país.

Este Ministerio, como cabeza del sector tecnológico en Colombia y líder de la política en materia de tecnologías de la información y las comunicaciones desarrolló el Plan Estratégico Sectorial e Institucional con el nombre de "Plan Vive Digital", el cual, es producto de un proceso participativo donde intervinieron las entidades que hacen parte del sector administrativo, empresas representadas en diferentes gremios, la academia representada por varias universidades y la ciudadanía interesada. La parte cuantitativa de las empresas, gremios, academia y ciudadanos es difícil de indicar debido a que se tendría que relacionar con tiempos particulares del proceso de Direccionamiento Estratégico, y vigencias de Gobierno.

El sector de Tecnologías de la Información y las Comunicaciones está compuesto por industrias manufactureras, comerciales y de servicios cuyos productos recogen, procesan, crean, transmiten o muestran datos e información electrónicamente (C. Constitucional, 2009).

Para las industrias manufactureras, los productos deben estar diseñados para cumplir la función de tratamiento de la información y la comunicación, incluidas la transmisión y la presentación, y deben utilizar el procesamiento electrónico para detectar, medir y/o registrar fenómenos físicos o para controlar un proceso físico.

Para las industrias de servicios, los productos de esta industria, deben estar diseñados para permitir la función de tratamiento de la información y la comunicación por medios electrónicos, sin afectar negativamente el medio ambiente (Macau, 2004).

Sin embargo, las formas como las empresas pueden hacer propuestas al MINTIC, están enmarcadas dentro de la participación en el ejercicio de planeación, mencionado en el punto anterior y en la participación en su ejecución, de acuerdo a las propuestas que realicen a través de los mecanismos de selección objetiva. En este último, no necesariamente tienen que ser empresas del Sector TIC, sino aquellas que cumplan con los requisitos de cada proceso en particular.

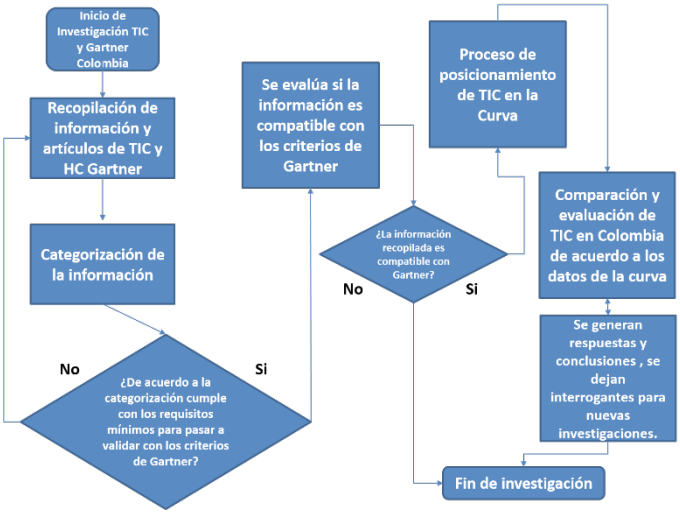


Figura 2 – Flujo de trabajo de investigación. Fuente: Gartner, Inc.

3.2. Categorización en proyectos de inversión de MINTIC

La categorización de los proyectos de inversión en el MINTIC se realiza según el Decreto 841 (2009) y estos pueden ser de cinco (5) clases:

1. Proyectos que generan beneficios directos o indirectos bajo la forma de bienes o servicios
2. Proyectos que cumplen una función de recuperación de la capacidad generadora de beneficios directos como: actividades de alfabetización, capacitación, nutrición, erradicación de enfermedades, vacunación, de atención a la mujer, a la niñez o a la tercera edad
3. Proyectos que no generan beneficios directos ni indirectos, pero permiten identificar futuros proyectos. Estos son los estudios básicos o de investigación
4. Proyectos que cumplen una función crediticia, que tienen como finalidad financiar proyectos de las categorías anteriores, en el transcurso del año de ejecución. Para éstos se aprueban montos globales y corresponderá al organismo o entidad ejecutora definir los proyectos que se habrán de financiar así.

Excepcionalmente, se podrán registrar como proyectos de inversión las partidas destinadas al pago de garantías otorgadas por la Nación, en relación con créditos concedidos a terceros, que se hayan hecho efectivas, siempre y cuando dichos créditos se hayan perfeccionado con anterioridad a diciembre 31 de 1991.

4. Desarrollo de la investigación mediante la curva de Gartner

4.1. Metodología propuesta

Gartner, ha realizado anualmente, alrededor de 5 estudios sobre TIC en diferentes entornos y referentes continentales (Chandler et Al, 2011). Desde países con un alto valor de inversión, como otros, donde las TIC hasta ahora son términos emergentes (LeHong y Fenn, 2013), es a partir de esos análisis, gráficas o reportes de donde se compara el estado de las TIC en Colombia. Con estas comparaciones, se podrían responder preguntas, como, qué tan cerca está este país de una potencia en tecnología como es la India, o que tan rezagados se encuentra comparado a países emergentes, como por ejemplo, algunos países del continente Africano.

La investigación se hizo en varias fases de acuerdo a la figura 2, donde se representa el flujo de trabajo y que se segmentó de la siguiente forma:

1. *Inicio de la investigación y Recopilación de información:* Se toma de diferentes fuentes la información, tanto las técnicas o criterios de Gartner como los reportes del MINTIC, anuales, trimestrales, semestrales, etc. Al igual que otros informes de la OCyT, SIUST y artículos relacionados con TIC, Apropiación de TIC y la curva de Gartner.
2. *Categorización de la información:* Se adopta la información y se categoriza de acuerdo a su tipo, sea una TIC con base en E-commerce, Seguridad, CRM, Trabajo 3.0, Redes, Cloud Computing, Hardware, etc.
3. *Primer filtro, y requisitos para la siguiente fase*: Se evalúa si dicha información recopilada cuenta con fechas, reportes de avances en tecnología, boom de prensa (Artículos en revistas de tecnología o pautas publicitarias).
4. *Las TIC cumplen con los criterios de Gartner*: Se toman las TIC que han cumplido con los requisitos y de las cuales se tiene información, esto no significa que las demás no sean tenidas en cuenta, solo significa que la tecnología aún no es lo suficientemente madura o conocida en el sector específico en el cual se desea medir, en este caso, Colombia y MINTIC.
5. *Segundo filtro y requisitos para la siguiente fase*: En este caso, las tecnologías ya maduras pasan a ser consideradas como tecnologías de punta o que tienen cierto nivel de importancia o reconocimiento en el MINTIC o en la apropiación de TIC en Colombia, sea en empresas privadas o públicas al igual que para la sociedad en general.
6. *Se posiciona las TIC en la curva de acuerdo a criterios*: Teniendo en cuenta los criterios de TIC se ubican de acuerdo a sus características como tiempo en mercado, niveles de inversión, proyección, cantidad de empresas que brindan soporte sobre dicha tecnología y conocimiento y apropiación de la misma.
7. *Se hacen las comparaciones respectivas de las TIC en la curva*: Se validan las posiciones que arrojaron las TIC en la curva y se comparan unas con otras, al igual que se puede hacer comparaciones u observaciones de las TIC respecto a otros países y al reporte anual de las tecnologías emergentes que arroja Gartner.
8. *Respuestas y conclusiones*: De acuerdo a las respuestas que arrojo la curva y las comparaciones que se realizaron se puede concluir o llegar a determinar que tecnologías aún no están 100% desarrolladas y son tierra fértil para invertir o

investigar, al igual, que se puede detectar si el no avance de alguna tecnología afecta positiva o negativamente a las demás, al igual se pueden realizar nuevas investigaciones.

9. Fin de investigación.

5. Resultado

Teniendo en cuenta estos recursos gráficos y reportes de gestión de TIC, se realizó el análisis completo del funcionamiento del estudio de Gartner, las técnicas para identificar el progreso de las tecnologías al igual que los criterios de posicionamiento de cada tecnología en cada una de sus fases, también los iconos de identificación de tiempos que se le pueden asignar a cada una de estas tecnologías.

En el caso de Colombia, se evaluó de acuerdo a los diferentes reportes del MINTIC, sus ajustes al PETIC, reportes semanales, mensuales y trimestrales de avances de inversión en tecnología, al igual que los diferentes reportes del Observatorio Colombiano de Ciencia y Tecnología (OCyT, 2014) de acuerdo a sus indicadores de ciencia y tecnología Colombia 2015 (ICT) y se ajustaron las diferentes tecnologías implementadas en Colombia en el gráfico de la Hype Curve de Gartner.

En el estudio a nivel global, se logró observar que implementaciones como el IOT (Internet de las cosas) en la India (Evans, 2011), se encuentra en el pico de las expectativas, mientras que aquí en Colombia hasta ahora está en la fase de lanzamiento. No porque aún no haya sido parte de la innovación, sino más bien porque el concepto y lo que implica aún no es claro en la población y más grave aún, en algunas empresas de tecnología sigue siendo abrumador el concepto que se ha adoptado al respecto.

Un caso de tecnología donde Colombia tiene tecnología en el pico de expectativas y se puede decir que ya está pasando al abismo de la desilusión para fortalecerse en la rampa de la consolidación y meseta de la productividad es el Cloud Computing y la estructura de data centers (Gartner, 2013), como se ve reflejado en los últimos reportes del año de "otros países emergentes" en Gartner.

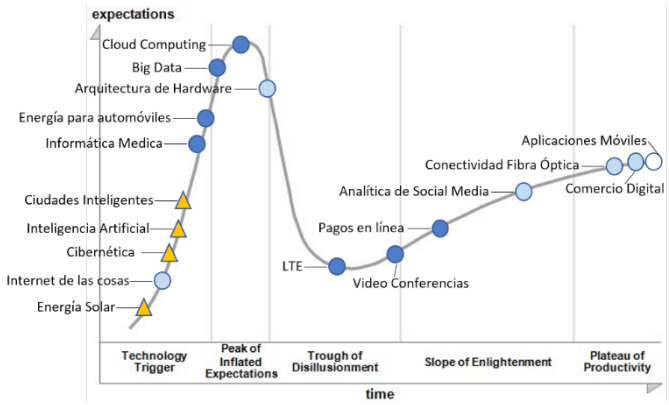


Figura 3 – Hype Curve de Gartner, TIC en Colombia. Fuente: Estudio propio.

Para la estimación de las fechas de tiempo o proyecciones, de qué tanto tardará una tecnología en implementarse, se tuvieron en cuenta los diferentes reportes y registros de impacto de publicidad a nivel tecnológico y corporativo donde se hacía alusión a dichas nuevas tecnologías, como es el caso de la entrada del Big Data en Colombia, donde sus primeras apariciones en publirreportajes de tecnología datan del 2013 (EMC, 2013), mientras que en otros países, hay registros de muchos años atrás.

Se puede ver, como las inversiones e investigaciones en tecnología han sido estratégicamente implementadas y están en procesos de apropiación. De acuerdo a las descripciones anteriores, es claro como cada tecnología que se está desarrollando en Colombia es clave para que cada una de ellas se apoye y/o articule sobre las otras. Colombia es un país emergente con alto progreso y desarrollo en tecnologías de telecomunicaciones, donde las TIC han sido su prioridad y mucho más la conectividad de un país. Colombia ha adoptado como prioridad, la conectividad a todas las zonas del país, con el fin de que la investigación y el desarrollo vayan tomando el primer lugar. Y así, ir aumentando en los porcentajes de inversión en los diferentes proyectos de investigación del gobierno nacional, los cuales, se verán reflejados a mediano plazo en los reportes del OCyT.

En comparación a otros países y la evolución de sus tecnologías, en 2015, Colombia se encontró en una posición intermedia, siendo coherentes y teniéndose en cuenta como uno de los referentes de Latinoamérica en tecnología y como un país emergente con proyección de desarrollo para nuevos inversores en tecnología, los cuales a este año siguen adelantando acuerdos y negociaciones bajo el amparo de la cancillería y la supervisión del MINTIC.

De acuerdo al desarrollo en algunas tecnologías, como el cloud computing, Colombia se encuentra en niveles parecidos a la India de acuerdo a sus niveles de soporte y asistencia en sitio. Pero la India, lleva la delantera en infraestructura tanto de Data Center como de conectividad, es decir, que aunque hay buen servicio de Cloud y Data Center, aún hace falta mejor desempeño y soporte en velocidad de transferencia y conectividad.

Es ahí donde se puede destacar la gestión de administración de recursos ya que varias tecnologías aún no han logrado llegar al pico de expectativas por causa de las fallas en conectividad que se presentan en Colombia, fallas que el MINTIC ha prometido corregir en su mayoría para este año 2018.

De modo, que la única forma de llegar a comparar a Colombia frente a otros países con excelente competitividad de tecnología, es cuando se presente una conectividad de más del 90%, aunque se viene con un crecimiento adecuado, de momento solo puede ser comparada con países emergentes como lo son los países del áfrica y algunos del Consejo de Cooperación para los Estados Árabes del Golfo, países que también están trabajando fuertemente en apropiación de TIC y como medio de dicha apropiación la implementación de conectividad, es decir, países con el conocimiento necesario en TIC desarrollado, pero aún, escasos de herramientas.

6. Conclusiones

El caso del Big Data en Colombia a diferencia de otros países con mayor inversión en desarrollo de tecnologías (ITU, 2014), donde dicha tecnología tiene lugar en proceso de

abismo de la desilusión para pasar aproximadamente de 5 a 10 años a la meseta de la productividad. En Colombia, aún falta un tiempo de 2 a 5 años para que llegue al pico de las expectativas.

Ahora, teniendo en cuenta estos datos y reportes de la Hype Curve de diferentes países y continentes, se puede empezar a tener en cuenta los reportes de desarrollo del MINTIC, artículos de revistas especializadas en desarrollo de TIC en Colombia y otros reportes de algunas casas independientes de investigación y desarrollo, se podría realizar un reporte similar a la Hype Curve de Gartner respecto al desarrollo de Colombia en los últimos años.

Se puede apreciar el desarrollo de las nuevas tecnologías en Colombia teniendo en cuenta que el presupuesto para desarrollo e investigación es en promedio el 1% del presupuesto anual del país. Donde tecnologías útiles y bio-sustentables como la energía solar, hasta ahora, están en el proceso de lanzamiento, dado que son muy pocas las empresas y organizaciones que se atreven a invertir en estos tipos de tecnologías.

Además, son tan nuevas en el país, que pueden presentar altos costos en investigación y mantenimiento de acuerdo a la descripción de la fase en la que se encuentra. Pero también, se puede apreciar que Colombia en tecnologías digitales ha presentado un gran avance, como lo son las estrategias de analítica y socialmedia, web marketing, aplicaciones móviles que están a poco tiempo (En promedio de 0 a 2 años) de llegar a estar en la meseta de la productividad con unos avances enormes en temas de desarrollo e investigación de desarrollo de software.

Una de las tecnologías que se encuentra en el abismo de la desilusión es la tecnología 4G o LTE ya que según reportes de la Asomovil, aún existen las creencias en los ciudadanos acerca de enfermedades y otros riesgos respecto a la instalación de antenas para la comunicación móvil.

De acuerdo al proyecto presidencial que finaliza en este año 2018, se quiere cerrar con un aproximado de más de 20 millones de ciudadanos conectados, pero debido a los diferentes problemas en la instalación de antenas, ha sido difícil lograr esa meta. Teniendo en cuenta esos problemas de instalación la conectividad 4G LTE se ve afectada ya que no existe gran diferencia entre un HDSPA 3.5G a un 3.75G que simulan ser un 4G LTE real.

Se puede destacar el desarrollo del cloud computing en Colombia donde se han generado diferentes empresas de soporte orientadas a los múltiples sectores de la industria que pueden requerir de dicha tecnología. Por ejemplo, en el sector salud, las clínicas están implementando tecnologías para la administración de medicina, como la informática médica. O como son las industrias agrarias donde hacen uso de la nube para llevar documentación administrativa desde la ciudad hasta las zonas rurales. Esta información y acceso a la información es posible gracias al uso de las conectividades por fibra óptica, tecnología que se encuentra a punto de pasar a la meseta de la productividad.

Referencias

C. Constitucional (2009). Ley 1341 d*e las TIC*.

Chandler, N; B. Hostmann, B; Rayner, N. y Herschel, G. (2011). "Gartner' s Business Analytics Framework," *Gartner*, no. September, pp. 1–12.

OCyT. (2014). Indicadores de ciencia y tecnología. ISSN: 2323–072x.

Echeverría, J. (2008). Apropiación social de las tecnologías de la información y la comunicación. *Rev. Iberoam. Cienc. Tecnol. y Soc.*, vol. 4, no. 10, pp. 171–182.

EMC. (2013). Resultados de Encuesta EMC Big Data.

Evans; D. (2011). Internet de las cosas Internet de las cosas Cómo la próxima evolución de Internet lo cambia todo. *Cisco Internet Bussiness Solut. Gr. - IBSG*, pp. 4–11.

Gartner Inc. (2011). Gartner Hype Cycle. *Reproduction*, vol. 9, pp. 240–252.

Gartner, Inc. (2013). Predicts 2014: Cloud Computing Affects All Aspects of IT.

ITU (International Telecommunication Union). (2014). Measuring the information society report.

Leal, E. T. (2008). Las tecnologías de la información y comunicaciones (TIC) y la brecha digital: su impacto en la sociedad de México. *Rev. Univ. y Soc. del Conoc.*, vol. 4, no. 2007, pp. 1–8.

LeHong, H. y Fenn, J. (2013). "Hype Cycle for Emerging Technologies, 2013," *Gartner*, pp. 1–99.

Lévy, P. (1995). *Tecnologias da Inteligência*.

Linden, A y Fenn, J. (2003). Understanding Gartner's hype cycles, *Strateg. Anal. Rep. No R-20-1971. Gart. Res.*, no. May, p. 12.

Macau, R. (2004). "TIC : ¿PARA QUÉ? (Funciones de las tecnologías de la información y la comunicación en las organizaciones)," *Rev. Univ. y Soc. del Conoc.*, vol. vol 1 num1, no. ISSN 1234–5678, pp. 1–12, 2004.

Montes, J. y Ochoa, S. (2006) Apropiación de las tecnologías de la información y comunicación en cursos universitarios. *Acta Colomb. Psicol.*, vol. 9, no. 2, pp. 87–100, 2006.

Santos, J. M. (1990). *PETIC*.

Critérios Editoriais

A RISTI (Revista Ibérica de Sistemas e Tecnologias de Informação) é um periódico científico, propriedade da AISTI (Associação Ibérica de Sistemas e Tecnologias de Informação), que foca a investigação e a aplicação prática inovadora no domínio dos sistemas e tecnologias de informação.

O Conselho Editorial da RISTI incentiva potenciais autores a submeterem artigos originais e inovadores para avaliação pelo Conselho Científico.

A submissão de artigos para publicação na RISTI deve realizar-se de acordo com as chamadas de artigos e as instruções e normas disponibilizadas no sítio Web da revista (http://www.risti.xyz).

Todos os artigos submetidos são avaliados por um conjunto de membros do Conselho Científico, não inferior a três elementos.

Em cada número da revista são publicados entre cinco a oito dos melhores artigos submetidos.

Criterios Editoriales

La RISTI (Revista Ibérica de Sistemas y Tecnologías de la Información) es un periódico científico, propiedad de la AISTI (Asociación Ibérica de Sistemas y Tecnologías de la Información), centrado en la investigación y en la aplicación práctica innovadora en el dominio de los sistemas y tecnologías de la información.

El Consejo Editorial de la RISTI incentiva autores potenciales a enviar sus artículos originales e innovadores para evaluación por el Consejo Científico.

Lo envío de artículos para publicación en la RISTI debe hacerse de conformidad con las llamadas de los artículos y las instrucciones y normas establecidas en el sitio Web de la revista (http://www.risti.xyz).

Todos los trabajos enviados son evaluados por un número de miembros del Consejo Científico de no menos de tres elementos.

En cada número de la revista se publican cinco a ocho de los mejores artículos enviados.

Os associados da AISTI recebem a RISTI gratuitamente, por correio postal. Torne-se associado da AISTI. Preencha o formulário abaixo e envie-o para o e-mail aistic@gmail.com

Los asociados de la AISTI reciben la RISTI por correo, sin costo alguno. Hazte miembro de la AISTI. Rellena el siguiente formulario y remítelo al e-mail aistic@gmail.com



Formulário de Associado / Formulario de Asociado

Nome/Nombre: _____

Instituição/Institución: _____

Departamento: _____

Morada/Dirección: _____

Código Postal: _____ Localidade/Localidad: _____

País: _____

Telefone/Teléfono: _____

E-mail: _____ Web: _____

Tipo de Associado e valor da anuidade:

☐ Individual - 35€

☐ Instituição de Ensino ou I&D/Institución de Educación o I&D - 250€

☐ Outro (Empresa, etc.) - 500€

NIF/CIF: _____

Data/Fecha: __/__/_____ Assinatura/Firma: _____

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies
©AISTI 2016 http://www.aisti.eu

