2024 19th Iberian Conference on Information Systems and Technologies (CISTI) - Iberian Proceedings of CISTI 2024

Editors
Álvaro Rocha, Francisco Peñalvo, Ramiro Gonçalves,
Alicia Garcia Holgado, Fernando Moreira

INFORMATION AND TECHNOLOGY
MANAGEMENT ASSOCIATION

ISBN: 978-989-36481-1-7

WEB: http://www.cisti.eu/

Copyright 2024: Information and Technology Management Association (ITMA)



2024
19th Iberian Conference on Information Systems and Technologies (CISTI) - Iberian Proceedings of CISTI 2024

Editors
Álvaro Rocha, Francisco Peñalvo, Ramiro Gonçalves,
Alicia Garcia Holgado, Fernando Moreira

INFORMATION AND TECHNOLOGY
MANAGEMENT ASSOCIATION

INTRODUCTION

This book brings together a selection of papers, written in Portuguese and Spanish, that were presented at CISTI'2024 – the 19th Iberian Conference on Information Systems and Technologies, held from June 25 to 28, 2024, at University of Salamanca, Salamanca, Spain.

Organized jointly by University of Salamanca and the Information and Technology Management Association (ITMA), CISTI'2024 provided an international platform for researchers and industry practitioners to share and discuss recent advancements, emerging trends, experiences, and future concerns across the diverse domain of Information Systems and Technologies.

The Scientific Committee comprised 347 international experts from multiple disciplines within Information Systems and Technologies, who rigorously evaluated submissions using a double-blind peer-review process. This meticulous procedure ensured the high quality and relevance of contributions selected for presentation in the conference's key thematic areas:

A) Organizational Models and Information Systems
B) Knowledge Management and Decision Support Systems
C) Software Systems, Architectures, Applications, and Tools
D) Computer Networks, Mobility, and Pervasive Systems
E) Human-Centered Computing
F) Health Informatics
G) Information Technologies in Education
H) Architecture and Engineering of Construction

CISTI'2024 attracted more than 600 paper submissions from 39 countries worldwide, demonstrating the conference's global reach and academic significance. Accepted papers presented at the conference are published by Springer, as well as by ITMA with this book, and will be submitted for potential indexing in renowned databases such as Scopus, WoS, EI-Compendex, DBLP, and Google Scholar.

We extend our sincere gratitude to all contributors whose dedication and effort made CISTI'2024 possible, including authors, committee members, workshop organizers, and sponsors. Their valuable support has significantly contributed to the continued success and prestige of the conference.

ORGANIZATION

Coordinating Committee
Álvaro Rocha, ISEG, Universidade de Lisboa (General Chair)
Francisco Peñalvo, Universidad de Salamanca (Doctoral Symposium)
Ramiro Gonçalves, Universidade de Trás-os-Montes e Alto Douro (Workshops)
Carlos Ferrás Sexto, Universidad de Santiago de Compostela
Adolfo Lozano Tello, Universidad de Extremadura
Miguel de Castro Neto, NOVA Information Management School (NOVA IMS), Universidade Nova de Lisboa
Gonçalo Paiva Dias, Universidade de Aveiro
David Fonseca, La Salle, Universitat Ramon Llull
Mário Piattini, Universidad de Castilla-La Mancha
Isabel Pedrosa, Coimbra Business School | ISCAC, Polytechnic Institute of Coimbra
Borja Bordel, Universidad Politécnica de Madrid

Local Organizing Committee
Francisco Garcia-Peñalvo, Universidad de Salamanca (Chair)
Miguel Ángel Conde-González, Universidad de Salamanca
Alicia García-Holgado, Universidad de Salamanca
Lucía Garcías-Holgado, Universidad de Salamanca
Andrea Vazquez-Ingelmo, Universidad de Salamanca
Roberto Therón-Sánchez, Universidad de Salamanca

Keynote Speaker
Carlos J. Costa, ISEG, University of Lisbon, Portugal

Scientific Committee
Fernando Moreira, Universidade Portucalense (Chair)
Abel Méndez Porras, Instituto Tecnológico de Costa Rica
Abel Suing, Universidad Técnica Particular de Loja
Adérito Fernandes-Marcos, University of Saint Joseph in Macao
Admilson de Ribamar Lima Ribeiro, Federal University of Sergipe
Agostinho Sousa Pinto, CEOS.PP - ISCAP - P.PORTO
Alcides Alvear, Universidad Ana G Méndez, Puerto Rico
Alcinia Zita Sampaio, IST, University of Lisbon
Aleardo Manacero, Sao Paulo State University - UNESP
Aleteia von Paumgartten, Universidade de Barsília
Alexandre L'Erario, UTFPR
Alexandre Silva, Coimbra Business School | ISCAC
Alexandre Valle, FEUP
Alexandrino José Gonçalves, CIIC-ESTG-Polytechnic University of Leiria

Alicia García-Holgado, Universidad de Salamanca
Alma Gómez-Rodríguez, University of Vigo
Altino J Mentzingen Moraes, Brazilian Ministry of Management and Public Services Innovation & ADVANCE, ISEG, University of Lisbon
Álvaro López-Martín, University of Malaga
Amadeo Arguelles, Instituto Politecnico Nacional
Amélia Cristina Ferreira da Silva, ISCAP, P.PORTO
Ana Amaro, Coimbra Business School, ISCAC-IPC
Ana Azevedo, CEOS.PP, ISCAP, P.PORTO
Ana Bastos, Universidade de Trás-os-Montes e Alto Douro
Ana Carla Amaro, Universidade de Aveiro
Ana Dinis, Research Centre on Accounting and Taxation (CICF), Polytechnic Institute of Cávado and Ave
Ana Grasielle Dionísio Corrêa, Universidade Presbiteriana Mackenzie
Ana Isabel Martins, University of Aveiro
Ana Maria Correia, Retired
Ana Patrícia Oliveira, University of Aveiro
Ana Rita Calvão, Escola Superior de Tecnologia e Gestão de Águeda, Universidade de Aveiro
Ana Velhinho, Universidade de Aveiro
Anabela Marcos, Coimbra Business School/ISCAC
Anabela Mesquita, ISCAP / IPP
Anabela Moreira Bernardino, Computer Science and Communication Research Centre, Polytechnic of Leiria
Anacleto Correia, CINAV / Escola Naval
André Zúquete, DETI / IEETA / LASI, University of Aveiro
Andrea Vázquez-Ingelmo, University of Salamanca
Ângela Oliveira, Instituto Politécnico de Castelo Branco
Ania Cravero Ania, Universidad de La Frontera
Antoni Lluís Mesquida Calafat, University of the Balearic Islands, UIB
António Andrade, Universidade Católica Portuguesa
António Ferreira da Silva, ISEP - Instituto Superior de Engenharia do Porto
Antonio Garcia Loureiro, Universidad de Santiago de Compostela
António Godinho, Polytechnic Institute of Coimbra
Antonio Jiménez-Martín, Universidad Politécnica de Madrid
António Jorge Gouveia, Universidade de Trás-os-Montes e Alto Douro
António José Gonçalves Fernandes, Instituto Politécnico de Bragança
Arnulfo Alanis, Tecnologico Nacional de México/campues tijuana
Arsénio Reis, UTAD
Arturo José Méndez Penín, University of Vigo
Augusto Sousa, FEUP/INESCTEC
Baltasar García Perez-Schofield, University of Vigo
Beatriz Lopes Cancela, Coimbra Business School
Beatriz Sainz de Abajo, Universidad de Valladolid
Bráulio Alturas, Instituto Universitário de Lisboa (ISCTE-IUL)
Brenda L. Flores-Rios, Universidad Autónoma de Baja California

Bruno Miguel F. Gonçalves, Instituto Politécnico de Bragança
Carlos Afonso
Carlos Balsa, Instituto Politécnico de Bragança
Carlos Carreto, Polytechnic Institute of Guarda
Carlos Costa, ISEG, Universidade de Lisboa
Carlos Costa, Universidade de Aveiro
Carlos Grilo, Politécnico de Leiria
Carlos Juiz, University of Balearic Islands
Carlos Morais, Instituto Politécnico de Bragança
Carlos Rompante Cunha, UNIAG & CeDRI, Polytechnic University of Bragança
Carlos Serrão, Iscte - Instituto Universitário de Lisbo
Carlos Vaz de Carvalho, Instituto Politécnico do Porto
Cecília Carmo, Universidade de Aveiro - ISCA
Célia Ramos, ESGHT & CinTurs, Universidade do Algarve
Célio Marques, Instituto Politécnico de Tomar
Cesar Collazos, Universidad del Cauca
Ciro Martins, Universidade de Aveiro
Clara Silveira, Instituto Politécnico da Guarda
Claudia Berra Barona, Universidad Autónoma de Baja California
Caludia Lengua, CECAR
Cristina Caridade, Instituto Politécnico de Coimbra - Instituo Superior de Engenharia de Coimbra
Cristina Wanzeller, Instituto Politécnico de Viseu
Daniel Polónia, Universidade de Aveiro
Diana Cecilia Yacchirema Vargas, Escuela Politécnica Nacional
Dora Simões, University of Aveiro
Ed Bezerra, Universidade Federal da Paraíba
Eduardo Amadeu Dutra Moresi, Universidade Católica de Brasília
Eduardo Marques, Universidade da Madeira
Edwin Juvenal Cedeño Herrera, Universidad de Panamá
Elisabete Paulo Morais, Instituto Politécnico de Bragança | UNIAG
Elisabete Vieira, University of Aveiro
Esteban Castellanos, ESPE
Eugénia Bernardino, Polytechnic of Leiria
Fábio Marques, ESTGA, Universidade de Aveiro
Fátima Avilés, Universidad Indoamérica
Fernando Bobillo, University of Zaragoza
Fernando Cruz Bandeira, University Fernando Pessoa
Fernando De la Prieta, University of Salamacna
Fernando Moreira, REMIT, Universidade Portucalense
Fernando Ribeiro, Polytechnic Institute of Castelo Branco
Fernando Silva, Polytechnic University of Leiria
Fernando Suárez, Colexio Profesional de Enxeñaría en Informática de Galicia
Filipe Caetano, Polytechnic of Guarda
Filipe Caldeira, Polytechnic Institute of Viseu

Filipe Cardoso, IPS - ESGTS
Filipe Fidalgo, Instituto Politécnico de Castelo Branco
Filipe Montargil, ESCS - Escola Superior de Comunicação Social
Filipe Portela, University of Minho
Flor de María Sánchez Aguirre, Universidad César Vallejo
Francisco Antunes, University of Beira Interior and INESC Coimbra
Francisco de Arriba Pérez, University of Vigo
Francisco J. García Tartera, UCM
Francisco Javier ARCEGA, EINA - Universidad de Zaragoza
Francisco Medeiros, Federal Institute of Paraiba
Frank Affonso, UNESP
Franyelit Suarez, Universidad de las Américas
Frederico Branco, Universidade de Trás-os-Montes e Alto Douro
Gabriel Alberto García-Mireles, University of Sonora
Gabriel Gomes de Oliveira, UNICAMP
Gabriel Guerrero-Contreras, University of Cádiz
Gabriel Pestana, Polytechnic Institute of Setúbal
Gerardo González Filgueira, Universidade da Coruña
Gloria Valencia, Universidad de las Fuerzas Armadas
Graça Azevedo, University of Aveiro - ISCA-UA
Guilhermina Miranda, Universidade de Lisboa
Gustavo Callou, UFRPE
Gustavo R. Alves, Polytechnic of Porto
Hélder Gomes, Universidade de Aveiro
Hélia Guerra, University of the Azores
Henrique Gil, Polytechnic University of Castelo Branco
Hugo Cordeiro, Instituto Superior de Engenharia de Lisboa (ISEL)
Hugo Sanjurjo-González, University of Deusto
Inês Messias, Instituto Politécnico de Santarém
Isabel de la Torre,
Isabel Lopes, Instituto Politécnico de Bragança/UNIAG
Isabel Sofia Brito, ESTIG/Instituto Politécnico de Beja
Isidro Calvo, Faculty of Engineering of Vitoria-Gasteiz (UPV/EHU)sp
Isidro Navarro Delgado, UPC-ETSAB
Ismael Etxeberria-Agiriano, University of the Basque Country (UPV/EHU)
Ivaldir de Farias Junior, Universidade de Pernambuco - UPE
Ivan Armuelles Voinov, Universidad de Panamá
Javier Medina, Universidad Distrital Francisco José de Caldas
Jean Carlos Teixeira de Araujo, Universidade Federal do Agreste de Pernambuco
Jeimy Cano, Uniandes
Jesualdo Fernandes, ISEG Lisbon School of Economics & Management
Jimmy Aurelio Rosales Huamani, National University of Engineering
Joana Leite, Coimbra Business School | ISCAC - Polytechnic Institute of Coimbra
João Carlos Silva, Polytechnic Institute of Cávado and Ave

João Fabro, UTFPR-Federal University of Technology - Parana
João Gondim, Universidade de Brasília
Joao Luis de Miranda, Polytechnic University of Portalegre
João Pascoal Faria, Faculty of Engineering of the University of Porto
João Paulo Costa, Faculty of Economics of the University of Coimbra
João Paulo Ferreira, ISEC, Polytechnic of Coimbra
João Reis, GOVCOPP/Aveiro University
João Reis, Lusofona University
João Roberto de T Quadros, CEFET/RJ
João Sousa, IDMEC, Instituto Superior Tecnico, Universidade de Lisboa
João Tavares, FEUP, University of Porto
Joaquim Leite, Instituto Politécnico de Bragança
Joaquim P. Silva, Politécnico do Cávado e do Ave
Joaquim Reis, ISCTE-IUL
Joe Carrión-Jumbo, Universidad Internacional SEK
Jorge Barreiros, Polytechnic of Coimbra - ISEC
Jorge Buele, Universidad Indoamérica
Jorge Eduardo Ibarra-Esquer, Universidad Autónoma de Baja California
Jorge González Domínguez, Universidade da Coruña
Jorge Vareda Gomes, CSG/ADVANCE/ISEG
José Álvarez-García, Universidad de Extremadura
José Augusto Fabri, Universidade Tecnológica Federal do Paraná
José Borbinha, INESC-ID, IST, Universidade de Lisboa
José Braga de Vasconcelos, Universidade Lusófona
Jose Carlos Metrôlho, Polytechnic Institute of Castelo Branco
José Lousado, Estgl/IPV
José Luís Pastrana Brincones, Universidad de Málaga
Jose M. Molina, Universidad Carlos III de Madrid
Jose Machado, Universidade do Minho
José Manuel Villegas Izaguirre, Universidad Autonoma de Baja California
José Rosado, ISEC-IPC
José Salgado, Instituto Politecnico Guarda
Jose Silva, CINAMIL
Jose Torres, Universidade Fernando Pessoa
Juan Ángel Contreras Vas, Universidad de Extremadura
Juan Jesus Ojeda Castelo, Universidad de Almería
Juan M. Santos-Gago, atlanTTic - University of Vigo
Juan Pablo DAmato, CONICET
Kadna Camboim, Universidade Federal do Agreste de Pernambuco (UFAPE)
Karina Caro, Autonomous University of Baja California (UABC)
Leila Weitzel, Fluminense Federal University
Leonardo Bermon Angarita, Universidad Nacional de Colombia Sede Manizales
Leonel Santos, Polytechnic University of Leiria

Leonilde Reis, Politécnico de Setúbal
Lilia Muñoz, Universidad Tecnológica de Panamá
Liliana Enciso, Universidad Técnica Particular de Loja
Lucila Ishitani, Pontifícia Universidade Católica de Minas Gerais
Lucila Romero, Universidad Nacional del Litoral
Luis Bernardo, FCT, Universidade Nova de Lisboa
Luís Bruno, Politécnico de Beja
Luis Camarinha-Matos, NOVA University Lisbon
Luís Filipe Barbosa, Universidade de Trás-os-Montes e Alto Douro
Luis Frazao, CIIC - Politécnico de Leiria
Luís Mendes Gomes, Universidade dos Açores
Luísa Miranda, Instituto Politécnico de Bragança
Luz María Hernández Cruz, Universidad Autónoma de Campeche
Luz Sussy Bayona Ore, Universidad Nacional Mayor de San Marcos
Mahdieh Zakizadeh, MOP & IAU
Maicon Herverton Barros, Universidade de Pernambuco
Malheiro Benedita, Instituto Superior de Engenharia do Porto, Politécnico do Porto & INESC TEC
Manuel Cebrián de la Serna, Universidad de Málaga
Manuel Fernández-Veiga, University of Vigo
Manuel Sousa Pereira, IPVC
Manuela Aparicio, NOVA Information Management School (NOVA IMS), Universidade Nova de Lisboa
Marcelo de Paiva Guimarães, Federal University of São Paulo (UNIFESP)
Marcelo Lopez, Universidad de Caldas
Marcelo Marciszack, Universidad Tecnológica Nacional - Facultad Regional Córdoba
Marcelo Mendonça Teixeira, Universidade de Pernambuco
Marcelo Zambrano, Instituto Universitario Rumiñahui
Marcio Victorino, University of Brasilia
Marco Javier Suarez Baron, UPTC
Marco Painho, Nova Information Management School
Maria Beatriz Piedade, Instituto Politécnico de Leiria
Maria Bernardo, Universidade Aberta e INESCTEC
Maria Cecília Santos Rosa,
María Clara Gomez, Universidad Nacional de Colombia
Maria Cristina Marcelino Bento, UNIFATEA
María de la Cruz del Río-Rama, Universidad de Vigo
María Dolores De Acuña Garrido, University of Seville
Maria Elisabete Neves, Coimbra Business School | ISCAC
Maria Isabel Ribeiro, Instituto Politécnico de Bragança - CIMO/SuSTEC
María J Lado, University of Vigo
Maria João Ferreira, Universidade Portucalense
Maria João Gomes, University of Minho
Maria José Angélico Gonçalves,
Maria Sousa, ISCTE - Instituto Universitário de LIsboa

María Teresa García-Álvarez, University of A Coruna
María Visitación Hurtado Torres, University of Granada
Mariana Carvalho, Polytechnic Institute of Porto, School of Technology and Management
Mario Chacón-Rivas, Instituto Tecnológico de Costa Rica
Marisol B. Correia, ESGHT-Universidade do Algarve & CiTUR
Maristela Holanda, Universidade de Brasilia
Maria Teresinha Barbosa Geller
Marta Lopez Fernandez, Universidad Complutense de Madrid
Martin Llamas Nistal, atlanTTic-Universidade de Vigo
Mazyar Zand, MOP & Sharif University of Technology
Mercedes Ruiz, University of Cádiz
Miguel A. Brito, University of Minho
Miguel Á. Conde, Universidad de León
Miguel Casquilho, University of Lisbon
Miguel Negrao, IPLeiria
Miguel Ramón González Castro, Centro Tecnológico Aimen
Mirna Muñoz, Centro de Investigación en Matemátcias A.C.
Mónica da Costa, Escola Superior de Tecnologia, Instituto Politécnico de Castelo Branco
Natalia Gomes, Polytechnic University of Guarda
Nídia Salomé Morais, Instituto Politécnico de Viseu - Escola Superior de Educação
Nilton Canto, Faculdade Impacta de Tecnologia
Norma Velasquez, Universidad Católica Sedes Sapientiae
Nuno Costa, IPLeiria
Nuno Escudeiro, Instituto Politécnico do Porto
Nuno Geada, ISCTE Lisbon
Nuno Magalhães Ribeiro, Universidade Fernando Pessoa
Nuno Martins, School of Design, Polytechnic of Cávado and Ave
Nuno Melão, Instituto Politécnico de Viseu
Nuno Rodrigues, CIIC, ESTG, Politécnico de Leiria
Olger Gutierrez Aguilar, Universidad Nacional de San Agustín
Orlando Belo, University of Minho
Óscar Mealha, Universidade de Aveiro
Patrícia Dias, Universidade do Estado de Minas Gerais - UEMG
Patrícia Leite, Instituto Politécnico Cavado e Ave - Escola Superior de Tecnologia
Patricia Takako Endo, Universidade de Pernambuco
Patricio Domingues, Polytechnic of Leiria
Paula Escudeiro, ISEP/GILT (Games Interaction & Learning Technologies)
Paula Peres, Polytechnic of Porto / ISCAP
Paula Prata, Universidade da Beira Interior
Paulo Martins, Universidade de Trás-os-Montes e Alto Douro & INESC TEC
Paulo Pinto, Universidade Nova de Lisboa
Paulo Rurato, Universidade Fernando Pessoa
Pedro Araújo, Universidade da Beira Interior

Pedro Cabral, Nanjing University of Information Science & Technology
Pedro Castro, Instituto Politécnico de Viana do Castelo
Pedro J. Clemente, Universidad de Extremadura
Pedro Manuel do Espírito Santo, Polytechnic University of Leiria, Portugal
Pedro Martins, Coimbra Business School, Polytechnic Institute of Coimbra
Pedro Martins, Polytechnic of Viseu
Pedro Ribeiro, University of Minho
Pedro Sanz Angulo, University of Valladolid
Pedro Sobral, Universidade Fernando Pessoa
Pedro Sousa, University of Minho
Radhakrishna Bhat, Manipal Adademy of Higher Education
Ramadile Moletsane, Vaal Universuty of Technology
Ramón Alcarria, Universidad Politécnica de Madrid
Renata Spolon Lobato, Universidade Estadual Paulista “Júlio de Mesquita Filho”
Renato Mauricio Toasa Guachi, Universidad Tecnológica Israel
René Garzozi-Pincay, Universidad Estatal Península de Santa Elena
Ricardo Linden, CEPEL
Ricardo Simoes, Polytechnic Institute of Cavado and Ave
Rita M. T. Ascenso,
Rita Oliveira, University of Aveiro
Roberta Spolon, UNESP
Roberto Henriques, NOVA IMS
Roberto Marichal, Universidad de La Laguna
Rocío González-Sánchez, Rey Juan Carlos University
Rodrigo Rocha, UFAPE
Rogéria Cristiane Gratão de Souza, São Paulo State University - UNESP
Rogerio Eduardo Garcia, São Paulo State University - UNESP
Rosa Reis, ISEP
Rui Araújo, University of Coimbra
Rui Cruz, INESC-ID
Rui Humberto Pereira, ISCAP/CEOS.IPP
Rui Jose, University of Minho
Rui Pedro Marques, University of Aveiro
Rui Pitarma, Polythecnic Institute of Guarda
Rui Quaresma, Universidade de Évora
Rui Rodrigues, ESMAD - Escola Superior de Media Artes e Design
Rui Silva Moreira, UFP
Rute Abreu, Instituto Politécnico da Guarda
Samuel Silva, IEETA / DETI - University of Aveiro
Sandro Carvalho, Instituto Politécnico do Cávado e Ave - IPCA
Santiago Raul Gonzales Sánchez, Universidad César Vallejo
Sara Balderas-Díaz, University of Cádiz
Sara Dias-Trindade, University of Porto

Sara Paiva, Instituto Politécnico de Viana do Castelo
Sergio Araya Guzmán, Universidad del Bío-Bío
Sérgio Correia, Portalegre Polytechnic University
Sergio F. Lopes, University of Minho
Sergio Nunes, ISEG, Universidade de Lisboa
Shashi Kant Gupta, Eudoxia Research University
Silvia García Méndez, University of Vigo
Sónia Nogueira, Polytechnic University of Bragança
Sónia Rolland Sobral, Universidade Portucalense
Supriya Lamba Sahdev, ISBR Business School
Tânia Rocha, Universidade de Trás-os-Montes e Alto Douro
Telmo Silva, University of Aveiro
Thiago Dias, CEFET-MG
Tiago Trancoso, IPVC
Valderi Leithardt, ISEL - Instituto Superior de Engenharia de Lisboa
Valeria Farinazzo Martins, Universidade Presbiteriana Mackenzie
Valério Rosset, Instituto Tecnológico da Aeronáutica - ITA
Veronica Segarra-Faggioni, Universidad Internacional SEK
Verónica Vasconcelos, Coimbra Institute of Engineering, Polytechnic University of Coimbra
Vicente Morales, Universidad Tecnica de Ambato
Víctor Mondelo, Universidade de Vigo
Virginia Araujo, Atlantica University
Vitor Gonçalves, Instituto Politécnico de Bragança
Vitor Mendonça, Instituto Politécnico de Bragança
Vitor Santos, Universidade Nova de Lisboa - NOVA IMS
Wagner Tanaka Botelho, Universidade Federal do ABC
Willian Zamora, ULEAM
Zenaide Silva, Universidade Federal do Sul e Sudeste do Pará (UNIFESSPA)

Plan de seguridad informática y autenticación de red inalámbrica en sector educación

Information security plan and wireless network authentication in the educational sector

Omar Enrique Ajila Pinzón [1],
U.E.F. Santa Juana de Arco La Salle, Cariamanga, Ecuador [1]
jace.omar.ajila@lasalle-cariamanga.edu.ec

Mikel Ugando Peñate [2], Ángel Ramón Sabando García [2]
Departamento de Ciencias Administrativas y Contables [2],
Pontificia Universidad Católica del Ecuador, Sede Santo Domingo de los Tsáchilas, Ecuador
mugandop@pucesd.edu.ec, arsabando@pucesd.edu.ec

Reinaldo Armas Herrera [3], Elvia Rosalía Inga Llanez[3], Ángel Alexander Higuerey Gómez [3],
Departamento de Ciencias Empresariales[3].
Universidad Técnica Particular de Loja
Loja, Ecuador.
ahreinaldo@utpl.edu.ec, eringa1@utpl.edu.ec, aahiguerey@utpl.edu.ec,

Resumen — **Debido a la popularidad de las redes de área local inalámbrica (WLAN) y el crecimiento de ataques a su vulnerabilidad, el tema de seguridad es una línea de investigación relevante en el contexto actual. Esta investigación tiene por objetivo diseñar un plan de seguridad que permita la autenticación en redes inalámbricas basado en la norma IEEE 802.1X. La metodología sigue un enfoque mixto, con diseño no experimental, la medición numérica determina los niveles de seguridad informática. Los resultados parciales, permiten diagnosticar la infraestructura de red local, evaluando los posibles riesgos y vulnerabilidades. Se ha implementado el Marco de Ciberseguridad 1.1 de NIST en las cinco áreas estratégicas: identificar, proteger, detectar, responder y recuperar. El plan de seguridad permitió definir los riesgos de ciberseguridad, protegiendo las redes y datos de los usuarios recomendando la implementación de un un sistema de autenticación RADIUS para garantizar el control de acceso y autenticación de la red inalámbrica local.**

Palabras Clave – Autenticación, red local inalámbrica, IEEE 802.1x, Ciberseguridad, FreeRadius.

Abstract — **Due to the popularity of wireless local area networks (WLAN) and the growth of attacks on their vulnerability, the security issue is a relevant line of research in the current context. This research aims to design a security plan that allows authentication in wireless networks based on the IEEE 802.1X standard. The methodology follows a mixed approach, with a non-experimental design, numerical measurement determines the levels of computer security. The partial results allow the local network infrastructure to be diagnosed, evaluating possible risks and vulnerabilities. The NIST Cybersecurity Framework 1.1 has been implemented in the five strategic areas: identify, protect, detect, respond and recover. The security plan allowed defining cybersecurity risks, protecting networks and user data, recommending the implementation of a FreeRADIUS authentication system to guarantee access control and authentication of the local wireless network.**

Keywords – Authentication, wireless local network, IEEE 802.1x, Cybersecurity, FreeRADIUS.

I. Introducción

La tendencia en constante aumento de los ataques cibernéticos hace que sea vital para cualquier organización proteger y asegurar su red e infraestructura informática. Con el progreso continuo al que se enfrenta Internet, las instituciones deben mantenerse al día creando e implementando planes de seguridad informática que incluyan diversas políticas que contengan productos de software, equipos de red y sistemas avanzados para proteger de forma articulada sus activos tecnológicos contra diversos ataques, [1].

Este es el caso de la U.E.F. Santa Juana de Arco La Salle Cariamanga, institución que posee un conjunto de activos tecnológicos para el procesamiento y almacenamiento de los datos. Y que entre todos sus servicios digitales como la telefonía IP, circuito cerrado de tv, los diferentes sistemas informáticos utilizados para la gestión académica, la red local y principal la red inalámbrica muestra algunos indicios de vulnerabilidad en el método de autenticación de los usuarios que acceden al servicio de wifi. Por tanto, es importante disponer de un Plan de Seguridad Informática que disminuya los riesgos y detecte posibles amenazas de seguridad para garantizar el uso adecuado de los recursos de hardware y sistemas informáticos de la institución.

La presente investigación tiene por objetivo proponer el diseño de un plan de seguridad informático aplicando el Marco de Ciberseguridad 1.1 de NIST que permita la autenticación de la red inalámbrica local basado en la norma IEEE 802.1X.

El resto del artículo tiene la estructura siguiente: en la sección dos está la revisión de literatura científica especializada en bases de datos indexadas como ACM, IEEE, Web of Science y Scopus. Se analizan y describan estudios similares en cuanto a

Identify applicable sponsor/s here. If no sponsors, delete this text box. (sponsors)

2024 19th Iberian Conference on Information Systems and Technologies (CISTI) – Iberian Proceedings of CISTI 2024
25th – 28th June 2024, University of Salamanca, Salamanca, Spain
ISBN: 978-989-36481-1-7

procesos de autenticación utilizando el estándar IEEE 802.1X. En la sección tres se detalla el marco metodológico, mientras que en la sección cuatro están los resultados y discusión de estos, describiendo los datos obtenidos en cumplimiento de los objetivos. Finalmente, se encuentran las conclusiones del artículo.

II. Revisión de la literatura

A. Seguridad de red y autenticacion WLAN

La seguridad de la red implica proteger todos los recursos de una red frente a las amenazas [2], debe considerar no solo las computadoras en la red, sino también otros dispositivos, medios de transmisión y los datos que se transmiten a través de la red, [3]. Todas las comunicaciones inalámbricas actuales, incluidas las móviles, satelitales, celulares y Wi-Fi, utilizan el protocolo ALOHAnet para establecer un enlace inicial, [4].

La seguridad informática es un conjunto de estrategias, procesos y tecnologías que protegen los sistemas informáticos del acceso no autorizado, robo, daño e interrupción de los servicios que brindan, [5]. Las amenazas tradicionales a las que se enfrentan los datos y la infraestructura de una red incluyen hackers, programas maliciosos y virus, los cuales intentan acceder a la red para modificarla o dañarla, [6].

La autenticación de WLAN, en todas sus variantes, es lo que debe ocurrir antes de que un individuo o dispositivo pueda acceder a los recursos de la red. La autenticación es la verificación de la identidad y las credenciales de los usuarios, [7]. Los usuarios deben identificarse y presentar credenciales, tales como nombres de usuario y contraseñas o certificados digitales. Después de autenticarse con éxito (a través de cualquier método), se puede realizar el cifrado, pero se debe hacer una distinción importante; la autenticación debe considerarse mutuamente excluyente del cifrado.

La autenticación, autorización y contabilidad (AAA) es un concepto común de seguridad informática que define la protección de los recursos de la red. De acuerdo con [8], la autenticación consta de dos actos, primero el acto de proporcionar la prueba de autenticidad de la información que se entrega o almacena, y segundo, el acto de verificar la prueba de autenticidad de la información que se recibe o recupera. La autorización es el acto de determinar si se puede otorgar un privilegio particular al presentador de una credencial particular, [9]. Sin embargo, la contabilización consiste en rastrear el uso de los recursos de la red por parte de los usuarios y dispositivos

B. Autenticación 802.1X/EAP

Estudios recientes, [10], [11], muestran que la autenticación con el estándar IEEE 802.1x, es el estándar principal de WLAN por poseer más ventajas que otros tipos autenticación. 802.1x proporciona control de acceso basado en puertos. Cuando se usa junto con EAP, puede ser un medio para autenticar dispositivos que intentan conectarse a un puerto LAN específico. Aunque EAP fue diseñado para el mundo cableado, se usa en Wi-Fi como una forma de comunicar información de autenticación y claves de cifrado entre un cliente o suplicante y un servidor de control de acceso como RADIUS, [12].

[1] destaca las bondades de los sistemas de autenticación y los certificados digitales para proteger la información confidencial en línea, además de la prioridad del uso para cualquier organización. 802.1X es una extensión del protocolo IEEE 802 y, como tal, opera en la capa 2 del modelo de interfaz de sistema abierto (OSI). [13] demuestra la optimización en la seguridad de red inalámbrica IEEE 802.1X mediante la implementación del protocolo PEAP.

El uso de contraseñas para acceder a la red inalámbrica generalmente no es lo más práctico para evitar que se vulnere la seguridad y accedan a los recursos de forma no autorizada. Por tal motivo, el estudio realizado por [14] describe que un proceso de autenticación robusto es aquél donde un usuario provee sus credenciales de autenticación a un servidor, y luego el servidor las verifica.

En la propuesta realizada por [15] se puede observar algunos métodos de autenticación, el más destacable es el protocolo ligero de acceso a directorios (LDAP). Además [16], proponen RADIUS como un estándar industrial de facto utilizado por varias empresas de productos de red, siendo un estándar IETF. La propuesta de [17] da soluciones óptimas de un módulo de protección, el cual, consta de nuevas funciones añadidas al programa AAA existente, implementado en el servidor RADIUS.

C. Credenciales del solicitante y protocolo EAP

El solicitante utilizará un protocolo EAP para presentar las credenciales al servidor de autenticación para probar la identidad. Según el tipo de protocolo EAP que se utilice, las credenciales de identidad del solicitante pueden ser: nombres de usuario y contraseñas, certificados digitales, credenciales de acceso protegido (PAC), dispositivos de token de seguridad dinámicos, tarjetas inteligentes, USB y autenticación de máquina. La aplicación más común de EAP es WPA-Enterprise en redes Wifi [18].

Los métodos de autenticación EAP más seguros incorporan el concepto de autenticación mutua. La mayoría de los protocolos EAP utilizan un certificado del lado del servidor para las credenciales del servidor de autenticación (AS), [11]. También se puede usar un certificado del lado del servidor para brindar protección a las credenciales de nombre de usuario y contraseña en un proceso conocido como autenticación de túnel. [19] concluye que probablemente la mayor ventaja de los métodos de autenticación EAP-LEAP es la baja sobrecarga asociada con este método EAP en particular.

De acuerdo con figura 1, se debe crear e instalar un certificado de servidor en el servidor de autenticación. Además, el certificado público raíz de la entidad emisora de certificados (CA) que se utilizó para crear el certificado del servidor debe instalarse en los solicitantes. La distribución e instalación del certificado CA raíz a múltiples solicitantes de WLAN suele ser el mayor desafío al implementar la seguridad 802.1X/EAP, [20] y [21].

Dado que EAP es un marco que tiene en cuenta la extensibilidad, utiliza uno de los muchos métodos disponibles para autenticar a un usuario, [22]. EAP se ha redefinido en IETF RFC

2024 19th Iberian Conference on Information Systems and Technologies (CISTI) – Iberian Proceedings of CISTI 2024
25th – 28th June 2024, University of Salamanca, Salamanca, Spain
ISBN: 978-989-36481-1-7

3748 para su uso con el control de acceso basado en puertos 802.1X. La autenticación mutua requiere no solo que el servidor de autenticación valide las credenciales del cliente, sino también que el solicitante autentique la validez del servidor de autenticación, [23].



Figure 1. Certificado raíz CA y certificado zervidor

III. Metodología y unidad de análisis

A. Metodología

La investigación sigue la metodología propuesta por el Instituto Nacional de Estándares y Tecnología a través del Marco de Ciberseguridad 1.1, [24] el cual servirá como guía para la elaboración del Diseño del Plan de Seguridad que permita la autenticación de las redes inalámbricas basado en la norma IEEE 802.1X para la U.E.F. Santa Juana de Arco La Salle Cariamanga. Es una metodología con un enfoque para reducir el riesgo vinculado a las amenazas cibernéticas que puedan comprometer la seguridad de la información, y está compuesto por tres partes: el Núcleo del Marco, los Niveles de Implementación y los Perfiles del Marco.

El Núcleo del Marco consta de cinco funciones simultáneas y continuas: Identificar, Proteger, Detectar, Responder y Recuperar. Cuando se consideran juntas, estas funciones proporcionan una visión estratégica de alto nivel del ciclo de vida del proceso de gestión de riesgos de seguridad cibernética de una organización, [25]. El Núcleo del Marco identifica Categorías y Subcategorías claves y subyacentes (que son resultados discretos) para cada Función, y las compara con ejemplos de Referencias Informativas como estándares, directrices y prácticas existentes en cada Subcategoría.

Los niveles de implementación del marco proporcionan un contexto sobre cómo una organización considera el riesgo de seguridad cibernética y los procesos establecidos para gestionar dicho riesgo, [26]. La figura 2, describe los niveles en que las prácticas de gestión de riesgos de seguridad cibernética de una organización exhiben las características definidas en el Marco. Los Niveles se caracterizan en un rango, desde Parcial (Nivel 1) hasta Adaptable (Nivel 4). Estos niveles reflejan una progresión desde respuestas informales y reactivas a enfoques que son ágiles e informados sobre los riesgos. Durante el proceso de selección de Niveles, una organización debe considerar sus prácticas actuales de administración de riesgos, el entorno de amenazas, requisitos legales y reglamentarios, objetivos empresariales o de misión y las limitaciones organizacionales.



Figure 2. Niveles del marco de Ciberseguridad 1.1 de NIST

Unidad de análisis

La unidad de análisis está constituida por el conjunto de activos tecnológicos para el procesamiento y almacenamiento de los datos de la institución educativa. En la figura 3, se esquematiza los sistemas, telefonía IP, circuito cerrado de tv, la red local y los diferentes servicios web utilizados para la gestión interna y la seguridad de la información.

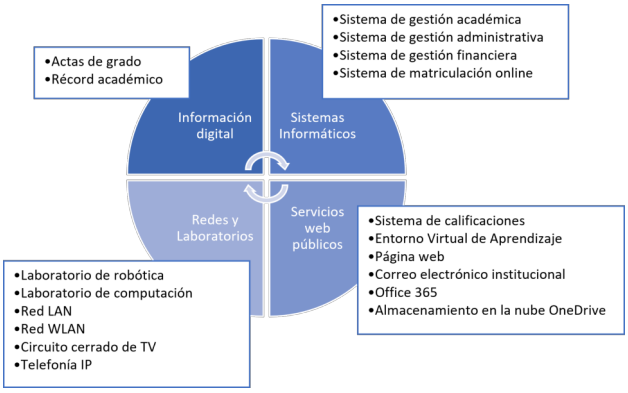


Figure 3. Diagrama de clasificación de activos tecnológicos de la institución

IV. Resultados

Como punto de partida es necesario conocer en que perfil se encuentra la institución educativa. Para esto se elabora una matriz que permite determinar el perfil actual y el perfil objetivo en base a los requerimientos de NIST. Por lo tanto, la primera tarea corresponde al diagnóstico, después se establece en un periodo de tiempo a qué nivel se aspira llegar a través del objetivo deseado de acuerdo con los niveles de riesgo. Para establecer la prioridad se realiza a través del cálculo de una brecha, la puntuación que reciba determina si el objetivo ha sido alcanzado o se encuentra en un nivel bajo, medio o alto. A continuación, se presentan los resultados derivados de la evaluación de las 5 funciones con todas sus categorías y subcategorías del Marco de Ciberseguridad 1.1 de NIST

Los resultados plasmados en la tabla I destaca lo siguiente: dentro de la función IDENTIFICAR (ID), la categoría Gestión de activos (ID.AM) es la que presenta un mayor nivel de logro en el estado actual con valor de 62,5% y por consiguiente una brecha menor de 29,17% la cual se contrasta en la figura 4 acercándose este punto al nivel objetivo deseado del 91%. Sin

2024 19th Iberian Conference on Information Systems and Technologies (CISTI) – Iberian Proceedings of CISTI 2024
25th – 28th June 2024, University of Salamanca, Salamanca, Spain
ISBN: 978-989-36481-1-7

embargo, la categoría Gobernanza (ID.GV) es la que presenta un menor nivel de logro en estado actual con valor de 25% y se observa una brecha bastante amplia de 68,75% con respeto al objetivo deseado, lo cual se evidencia en figura 4. Seguidamente las categorías Evaluación de riesgos (ID.RA), Estrategia de gestión de riesgos (ID.RM) y Cadena de Suministro (ID.SC) presentan este mismo comportamiento con brechas distantes del 58%, 50% y 30% respetivamente respecto al objetivo deseado.

TABLE I. PUNTUACIONES DEL MARCO DE CIBERSEGURIDAD NIST FUNCION IDENTIFICAR

Categoría	Logro %	Objetivo %	Brecha %
ID.AM	62,50	91,67	29,17
ID.BE	25,00	70,00	45,00
ID.GV	25,00	93,75	68,75
ID.RA	29,17	87,50	58,33
ID.RM	25,00	75,00	50,00
ID.SC	35,00	65,00	30,00
Total ID	33,61	80,49	46,88

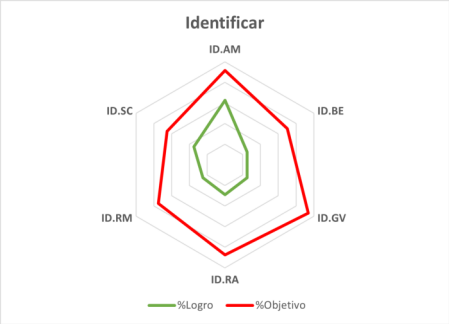


Figure 4. Función Identificar

La tabla II presenta los resultados resúmenes de la función PROTEGER (PR) y se puede destacar que la categoría Mantenimiento (PR.MA) muestra resultados muy satisfactorios donde el nivel de logro de estado actual es de 75% igual al objetivo deseado y no existe brecha o diferencias, existen puntos coincidentes dé % de logro y % objetivo según muestra la figura 5. Seguidamente las categorías Gestión de identidad, autenticación y control de acceso (PR.AC) y Concienciación y capacitación (PR.AT) ofrecen mayores niveles de logro respeto al estado actual con valor de 46,43% y 55% respectivamente y brechas o diferencias medianamente estables de 28% y 35%. Sin embargo, la categoría Procesos y procedimientos de protección de la información (PR.IP), ofrece el menor nivel de logro en estado actual con 33,3% con respecto al objetivo deseado del 81,25% y se observa la mayor distancia o brecha en la figura 3 con valor de 47,92%.

TABLE II. PUNTUACIONES DEL MARCO DE CIBERSEGURIDAD NIST FUNCION PROTEGER

Categoría	Logro %	Objetivo %	Brecha %
PR.AC	46,43	75,00	28,57
PR.AT	55,00	90,00	35,00
PR.DS	37,50	81,25	43,75
PR.IP	33,33	81,25	47,92
PR.MA	75,00	75,00	0,00
PR.PT	35,00	75,00	40,00
Total PR	47,04	79,58	32,54

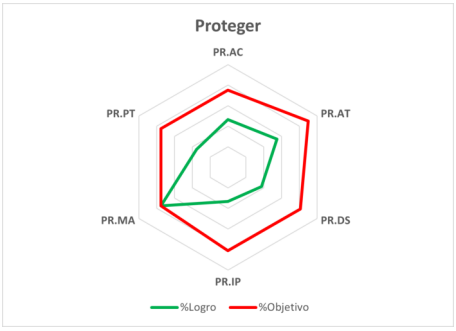


Figure 5. Función Proteger

La tabla III muestra los resultado de la función DETECTAR (DE) que consta de tres categorías en forma triangular según se observa en figura 6, es válido destacar dos cosas, en primer lugar, la categoría Anomalías y Eventos (DE.AE) es la que ofrece un mayor logro de acuerdo al estado actual con valor de 40% y una brecha moderada del 25% respeto al objetivo deseado, esta brecha es coincidente con la categoría Procesos de Detección (DE.DP) que de igual forma ofrece el 25% de logro. Sin embargo, la categoría Monitoreo Continuo de la Seguridad (DE.CM) presenta un menor nivel de logro en estado actual del 28,13% respecto al objetivo deseado y una brecha aún mayor, la cual puede ser considerada muy alta y se corrobora con la distancia del 50% existente en los puntos de intersección.

TABLE III. SUPUESTOS PUNTUACIONES DEL MARCO DE CIBERSEGURIDAD NIST FUNCION DETECTAR

Categoría	Logro %	Objetivo %	Brecha %
DE.AE	40,00	65,00	25,00
DE.CM	28,13	78,13	50,00
DE.DP	25,00	50,00	25,00
Total DE	31,04	64,38	33,33

2024 19th Iberian Conference on Information Systems and Technologies (CISTI) – Iberian Proceedings of CISTI 2024
25th – 28th June 2024, University of Salamanca, Salamanca, Spain
ISBN: 978-989-36481-1-7

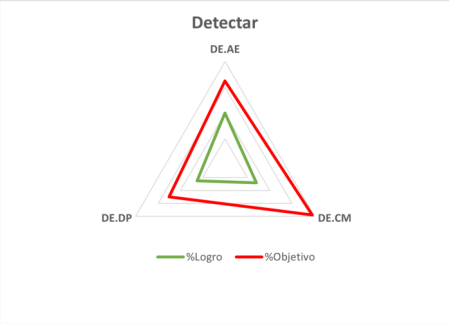


Figure 6. Función Detectar

La tabla IV muestra las cinco categorías de la función RESPONDER (RS) y es la que presenta niveles más estables respeto a las brechas y diferencias respecto al objetivo deseado. Aquí es válido destacar dos momentos importantes, en primer lugar, las categorías Análisis (RS.AN) y Mitigación (RS.MI) ofrecen un mayor nivel de % de logro en estado actual con valores de 40% y 41,67% respecto al objetivo deseado y es significativo las brechas tan pequeñas que se observan en la figura 7, con valor de 15% y 8,33% que casi coinciden en el extremo inferior de la base. Otro momento importante son los comportamientos estables de brechas respeto al valor objetivo deseado que se evidencian en las restantes categorías.

TABLE IV. Puntuaciones del Marco de Ciberseguridad NIST Funcion Responder

Categoría	Logro %	Objetivo %	Brecha %
RS.RP	25,00	50,00	25,00
RS.CO	30,00	50,00	20,00
RS.AN	40,00	55,00	15,00
RS.MI	41,67	50,00	8,33
RS.IM	25,00	50,00	25,00
Total RS	32,33	51,00	18,67

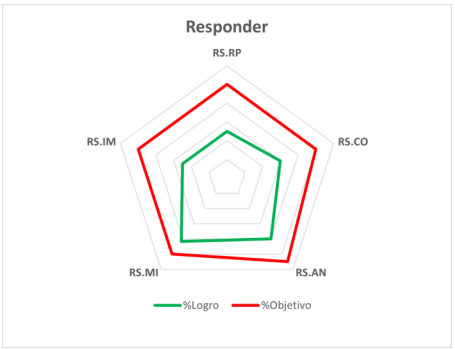


Figure 7. Función Responder

Por último, en la tabla V tenemos los resultados de la función RECUPERAR (RC), donde se destacan dos cuestiones, en primer lugar, la categoría Comunicaciones (RC.CO) ofrece el mejor nivel de logro en estado actual con valor de 41,67% respeto al objetivo deseado y una brecha muy pequeña de 8,33% casi coincidente con el punto de intersección de la base en la figura 8. En segundo lugar, las categorías Planificación de la recuperación (RC.RP) y Mejoras (RC.IM) presentan un menor % de logro con valor de 25% y 37,5% respectivamente al objetivo deseado, destacando una amplia brecha del 50% y distancia respeto a los puntos de intersección para la categoría Planificación de la recuperación (RC.RP), la cual se considera que ofrece los peores valores y se corroboran en la figura 8.

TABLE V. Puntuaciones del Marco de Ciberseguridad NIST FUNCIÓN RESPONDER

Categoría	Logro %	Objetivo %	Brecha %
RC.RP	25,00	75,00	50,00
RC.IM	37,50	75,00	37,50
RC.CO	41,67	50,00	8,33
Total RC	34,72	66,67	31,94

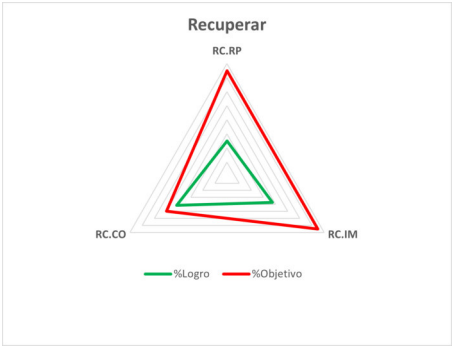


Figure 8. Función Recuperar

El Marco de Ciberseguridad 1.1 de NIST se ha desarrollado para infraestructura crítica como la banca y las industrias energéticas, pero se ha demostrado su utilidad en pequeñas empresas, gobiernos locales y el sector educativo. Este marco de ciberseguridad es el que mejor se adapta a las necesidades de la institución educativa objeto de estudio. Además, está respaldado por el Instituto Nacional de Estándares y Tecnología que es una agencia de Estados Unidos no reguladora que promueve la innovación mediante avances en metrología, normas y tecnología, y toda su documentación está abierta al público [27]; a diferencia de otros sistemas de gestión de la seguridad de la información como ISO 27001 que requiere una inversión significativa de recursos y esfuerzos, [28].

V. Conclusiones

En este artículo para dar cumplimiento al objetivo de la investigación, se determina que el diseño de autenticación más adecuado o conveniente dado las condiciones de la institución educativa sea a través de la autenticación de cliente basada en certificados EAP-TLS, pues ofrece autenticación mutua y basada en certificados del cliente y de la red. Además, la migración del sistema de autenticación 802.1X basado en contraseñas, a la

2024 19th Iberian Conference on Information Systems and Technologies (CISTI) – Iberian Proceedings of CISTI 2024
25th – 28th June 2024, University of Salamanca, Salamanca, Spain
ISBN: 978-989-36481-1-7

autenticación basada en certificados es sencilla, lo que proporciona flexibilidad en el futuro de existir esta necesidad.

Al implementar el Marco de Ciberseguridad 1.1 de NIST en las cinco áreas estratégicas: identificación, protección, detección, respuesta y recuperación; se pudo diagnosticar la situación actual de la infraestructura de red inalámbrica local. Primero se realizó un inventario de los activos tecnológicos tanto de hardware como de software. Y se procedió a analizar el nivel de riesgos al que están expuestos, concluyendo que la infraestructura de la red inalámbrica local es la que mayor puntuación recibe de acuerdo con los criterios de evaluación de riesgos.

El levantamiento del inventario de activos tecnológicos detectó que los niveles de ciberseguridad adoptados por la institución educativa son muy bajos, pues existen access point descontinuados sin actualizaciones de firmware, además utilizan métodos de seguridad Wi-Fi muy antiguos como WPA, los canales de las redes inalámbricas se superponen con las redes vecinas, los cuales deben ser inmediatamente corregidos.

Se procede a establecer las políticas de seguridad necesarias en el Plan de Seguridad Informática a ser implementado en la institución, y particularmente se recomienda incorporar un sistema de autenticación FreeRADIUS para garantizar el control de acceso y autenticación de la red inalámbrica local.

Como futuras líneas de investigación, se recomienda estudiar el comportamiento de los usuarios en la web, a través de un seguimiento, recopilación y evaluación de datos y actividades de los usuarios que utilizan sistemas de información en las redes de comunicación, teniendo en cuenta que no es suficiente invertir en ciberseguridad y soluciones de privacidad. La seguridad basada en el comportamiento debe ser una solución proactiva de la ciberseguridad.

Agradecimientos

Se agradecen acciones del Grupo de Investigación "Planning, Innovation and Financial Modeling Applied" aprobado por la Comisión de Investigación e Innovación y Comisión de Vinculación de la Pontificia Universidad Católica del Ecuador, Sede Santo Domingo con código GI-SANTODOMINGO-11-2019, ratificado el 10 de febrero de 2023, insertado dentro del PI-03-CP-PUCESD-2023 aprobado 10 de noviembre de 2023.

Referencias Bibliográficas

[1] V. Marmolejo Corona, G. A. Serrano Manzano, F. A. Bautista Aguilar, and Y. F. Santiago Gonzalez. "Seguridad en Sistemas de Autenticación: Análisis de Vulnerabilidades y Estrategias de Mitigación". *xikua, 11*(22), pp. 39-43, 2023.

[2] S. Serna Ramírez, Álvaro Montoya Londoño, Y. A. Quintero Barco, C. F. Henao Villa, and F. D. J. Castro Ramírez. "Desarrollo de un sistema de seguridad informática a partir de una auditoría sobre una red empresarial". *ICTI*, 9(2), pp. 135–151, 2022.

[3] A. Mendoza de los Santos, J. A. Ríos Reyes, and R. Y. Vásquez Chiclayo. "Principales riesgos de seguridad en computación móvil en la nube: una revisión de la literatura". *Rev. Científica FAREM-Estelí*, *12*(45), pp. 206–220, abr. 2023.

[4] C. Hennick. *How ALOHAnet Helped Hawaii Make Waves in Networking and IT Innovation*. State Tech Magazine, 2016.

[5] K. Daimi. *Computer and Network Security Essentials* (Primera ed). Springer International Publishing, 2018.

[6] E. Cole, R. Krutz, J. Conley, B. Reisman, M. Ruebush, and D. Gollmann. *Network Security Fundamentals Eric Cole* (Primera ed). Wiley, 2008.

[7] Y. Belfaik, A. Lmouhandiz, Y. Sadqi, and S. Safi. Single Sign-On Revocation Access. In: Y. Maleh, M. Alazab, N. Gherabi, L. Tawalbeh, A.A. Abd El-Latif. (eds) Advances in Information, Communication and Cybersecurity. ICI2C 2021. Lecture Notes in Networks and Systems, 357, pp.535-544. Springer, 2022.

[8] M. Nakhjiri, and M. Nakhjiri. *AAA and Network Security for Mobile Access: Radius, Diameter, EAP, PKI and IP Mobility* (Primera). Wiley, 2005.

[9] E. Brown. *802.1X Port-Based Authentication* (Primera ed). Auerbach Publications, 2007.

[10] T. Fathima, and S.M. Vennila. Emphasizing a Productive and Protective Access Control to Improve Authentication Using 802.1X with Software-Defined Networks. In A. Ramu, C. Chee Onn, & M. G. Sumithra (Eds.), *International Conference on Computing, Communication, Electrical and Biomedical Systems*, pp. 181–197. Springer International Publishing, 2022.

[11] X.E. Mullo-Pilamunga, A.J. Romero-Fernández, G.E. Fernández-Villacres, and R.A. Díaz-Vásquez. "Firewall para la seguridad de la red los laboratorios. Universidad Estatal de Bolívar, Ecuador", *I.P*, 5(9), pp. 111–123, 2023.

[12] M. Gregg. *The Network Security Test Lab* (Primera ed). Wiley, 2015.

[13] T. Hidayat, and I. Riadi. "Optimation Wireless Security IEEE 802.1X using the Extensible Authentication Protocol-Protected Extensible Authentication Protocol (EAP-PEAP)". *International Journal of Computer Applications*, *174*, pp. 25–30, 2021.

[14] B. Dey, S.S. Vishnu, and O.S. Swarnkar. An Efficient Dynamic Key Based EAP Authentication Framework for Future IEEE 802.1x Wireless LANs. *Proceedings of the 2nd International Conference on Digital Signal Processing*, pp. 125–131, 2018.

[15] E.M. Gould. "Authentication Methods and Recent Developments". *Serials Review*, *44*(3), pp. 247–250, 2018

[16] A. Allahdadi, and R. Morla. "Anomaly Detection and Modeling in 802.11 Wireless Networks". *Journal of Network and Systems Management*, *27*(1), pp. 3-38, 2019.

[17] G.-C. Cristescu, and V. Croitoru. Volumetric Distributed Denial-of-Service and Session Replay Attacks-Resistant AAA-RADIUS Solution Based on EAP and LDAP. *2020 14th International Symposium on Electronics and Telecommunications, ISETC-Conference Proceedings, 2020.*

[18] S. Boire, T. Akgün, P. Ginzboorg, P. Laitinen, S. Tamrakar, and T. Aura. Credential Provisioning and Device Configuration with EAP. *MobiWac 2021 - Proceedings of the 19th ACM International Symposium on Mobility Management and Wireless Access*, pp. 87 – 96, 2021.

[19] C. Romero. "*Evaluación del desempeño de los sistemas de autenticación del estándar de seguridad IEEE 802.1X para la integración de un portal cautivo bajo el protocolo de RADIUS",* Universidad de las Fuerzas Armadas ESPE, 2022.

[20] D.D. Coleman, D.A. Westcott, and B. Harkins. CWSP®: Certified Wireless Security Professional Study Guide CWSP-205. *CWSP®: Certified Wireless Security Professional Study Guide CWSP-205*, 2016a

[21] D.D Coleman, D. Westcott, and B.E. Harkins. *802.1X/EAP Authentication*, 2016b.

[22] D. Walt. *FreeRADIUS Beginner's Guide* (Primera). Packt Publishing Ltd, 2011.

[23] P.A. Noreña Cardona and S. Calderón Restrepo. "Técnica de protección para credenciales de autenticación en redes sociales y correo electrónico ante ataques phishing". *Publ. investig.*, 12(2), pp. 23–34, 2018.

[24] Instituto Nacional de Estándares y Tecnología. "Marco para la mejora de la seguridad cibernética en infraestructuras críticas", 55, 2018.

[25] J.M. Amy-Mahn. "Primeros pasos de NIST Marco de ciberseguridad". *Primeros Pasos de NIST*, *1*, 2021.

[26] E. Villar García, A. Venegas Villarreal, A. Soto Alarcón, and CA. Mendoza de los Santos. "Implementación de medidas de Control de Acceso en Software web para la Gestión Empresarial", *Biotech & Engineering*, 3(1), 2023.

[27] Instituto Nacional de Estándares y Tecnología. "The NIST Cybersecurity Framework (CSF) 2.0", pp. 1-32, 2024.

[28] G. Culot, G. Nassimbeni, M. Podrecca, and M. Sartor, M. "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda". *The TQM Journal*, *33* (7), pp. 76-105, 2021.

ISBN: 978-989-36481-1-7