UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Gestión de la Seguridad y Protección de la Información de la UTMACH mediante estándares y buenas prácticas.

DIAZ QUEZADA IVAN FABRICIO
INGENIERO EN TECNOLOGIAS DE LA INFORMACION

RAMIREZ SAMANIEGO ELIAN JOSUE
INGENIERO EN TECNOLOGIAS DE LA INFORMACION

MACHALA
2023

UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Gestión de la Seguridad y Protección de la Información de la UTMACH mediante estándares y buenas prácticas.

DIAZ QUEZADA IVAN FABRICIO
INGENIERO EN TECNOLOGIAS DE LA INFORMACION

RAMIREZ SAMANIEGO ELIAN JOSUE
INGENIERO EN TECNOLOGIAS DE LA INFORMACION

MACHALA
2023

UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

PROPUESTAS TECNOLÓGICAS

Gestión de la Seguridad y Protección de la Información de la UTMACH mediante estándares y buenas prácticas.

DIAZ QUEZADA IVAN FABRICIO
INGENIERO EN TECNOLOGIAS DE LA INFORMACION

RAMIREZ SAMANIEGO ELIAN JOSUE
INGENIERO EN TECNOLOGIAS DE LA INFORMACION

LOJA MORA NANCY MAGALY

MACHALA
2023

Ramirez

por Nancy Loja Mora

Fecha de entrega: 25-feb-2024 11:54a.m. (UTC-0500)

Identificador de la entrega: 2299863700

Nombre del archivo: E_PROYECTO_DE_INTEGRACI_N_CURRICULAR_DIAZ_-_RAMIREZ_TURNITIN.pdf (1.14M)

Total de palabras: 16737

Total de caracteres: 94936

Ramirez

INFORME DE ORIGINALIDAD

5%	5%	1%	0%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	Submitted to University of Hertfordshire Trabajo del estudiante	<1%
2	americanae.aecid.es Fuente de Internet	<1%
3	bettercarenetwork.org Fuente de Internet	<1%
4	www.facebook.com Fuente de Internet	<1%
5	www.kimaldi.com Fuente de Internet	<1%
6	www.rentokil.com Fuente de Internet	<1%
7	Maria Emilia Marcondes Barbosa, Ellen Vanuza Martins Bertelli, Cristiane De Mello Aggio, Giovana Aparecida De Souza Scolari et al. "Fatores associados à adesão de adultos/idosos ao tratamento da hipertensão arterial na atenção básica [Factors associated with adult/elderly adherence to the treatment	<1%

	of arterial hypertension in primary care] [Factores asociados con la adherencia de adultos/ancianos al tratamiento de la hipertensión arterial en atención primaria]", Revista Enfermagem UERJ, 2019 Publicación	
8	al-khalidiyah.balticecovillages.eu Fuente de Internet	<1 %
9	archbronconeumol.org Fuente de Internet	<1 %
10	blogs.manageengine.com Fuente de Internet	<1 %
11	estudiantes.medicinatv.com Fuente de Internet	<1 %
12	latam.kaspersky.com Fuente de Internet	<1 %
13	repositorio.usmp.edu.pe Fuente de Internet	<1 %
14	strands.motorcykeldating.dk Fuente de Internet	<1 %
15	www.nebrija.com Fuente de Internet	<1 %
16	"Inter-American Yearbook on Human Rights / Anuario Interamericano de Derechos Humanos, Volume 32 (2016)", Brill, 2018 Publicación	<1 %

17	Edita Fino, Judith K. Daniels, Giulia Micheli, Domenica Gazineo et al. "Moral injury in a global health emergency: a validation study of the Italian version of the Moral Injury Events Scale adjusted to the healthcare setting", European Journal of Psychotraumatology, 2023 Publicación	<1 %
18	docplayer.com.br Fuente de Internet	<1 %
19	docplayer.fr Fuente de Internet	<1 %
20	europapress.net Fuente de Internet	<1 %
21	microdata.worldbank.org Fuente de Internet	<1 %
22	repositorio.uotavalo.edu.ec Fuente de Internet	<1 %
23	ribuni.uni.edu.ni Fuente de Internet	<1 %
24	techpedia.fel.cvut.cz Fuente de Internet	<1 %
25	ticnomatic.blogspot.com Fuente de Internet	<1 %
26	www.gobernabilidad.cl	

	Fuente de Internet	<1 %
27	www.iesbiogas.it Fuente de Internet	<1 %
28	www.insi.org Fuente de Internet	<1 %
29	www.kaspersky.es Fuente de Internet	<1 %
30	www.meetup.com Fuente de Internet	<1 %
31	www.metacompliance.com Fuente de Internet	<1 %
32	www.produccioncientificaluz.org Fuente de Internet	<1 %
33	www.tabernero.com.ar Fuente de Internet	<1 %
34	Anabela Malpique, Ana Margarida Veiga-Simão. "Argumentative writing by junior high school students: discourse knowledge and writing performance / Escritura argumentativa en alumnos de secundaria: conocimiento sobre el discurso y rendimiento en la escritura", Infancia y Aprendizaje, 2015 Publicación	<1 %
35	blog.seidor.com Fuente de Internet	

		<1 %
36	espanol.cdc.gov Fuente de Internet	<1 %
37	repositorio.udl.edu.pe Fuente de Internet	<1 %
38	ulaweb.adm.ula.ve Fuente de Internet	<1 %
39	www.cimm.cl Fuente de Internet	<1 %
40	www.ddllmm.eu Fuente de Internet	<1 %
41	www.derechoshumanos.org.mx Fuente de Internet	<1 %
42	www.managementsolutions.com Fuente de Internet	<1 %
43	www.mincomercio.gov.co Fuente de Internet	<1 %
44	www.monografias.com Fuente de Internet	<1 %
45	www.neosecure.cl Fuente de Internet	<1 %
46	www.oerknowledgecloud.org Fuente de Internet	<1 %

47	www.rainforest-alliance.com Fuente de Internet	<1 %
48	www.scsalud.com Fuente de Internet	<1 %
49	www.seguridadinformatica.cl Fuente de Internet	<1 %
50	www.sfia-online.org Fuente de Internet	<1 %
51	www.trc.pe Fuente de Internet	<1 %
52	www.universocristiano.com Fuente de Internet	<1 %
53	"Inter-American Yearbook on Human Rights / Anuario Interamericano de Derechos Humanos, Volume 33 (2017)", Brill, 2018 Publicación	<1 %
54	"Inter-American Yearbook on Human Rights / Anuario Interamericano de Derechos Humanos, Volume 9 (1993)", Brill, 1996 Publicación	<1 %
55	ECOLOGIA Y TECNOLOGIA AMBIENTAL S.A.C. "MEIA para la Implementación del Proyecto Implementar Línea de Cal, Mejoras Ambientales e Integración de Instrumentos Ambientales en la Planta Condorcocha-	<1 %

IGA0006877", R.D. N° 081-2018-PRODUCE/DVMYPE-I/DIGGAM, 2020
Publicación

56	Marta Ruiz del Pino, Antonio Rosales-Castillo, José María Navarro-Marí, José Gutiérrez-Fernández. "Importancia clínica del aislamiento de Haemophilus spp. (excluyendo H. ducreyi) en muestras genitales. Revisión sistemática", Enfermedades Infecciosas y Microbiología Clínica, 2023 Publicación	<1 %
57	academy.pega.com Fuente de Internet	<1 %
58	apps.who.int Fuente de Internet	<1 %
59	barrapunto.com Fuente de Internet	<1 %
60	business.un.org Fuente de Internet	<1 %
61	doku.pub Fuente de Internet	<1 %
62	dpwprod.azureedge.net Fuente de Internet	<1 %
63	encolombia.com Fuente de Internet	<1 %

extranet.who.int

64	Fuente de Internet	<1 %
65	manizales.gov.co Fuente de Internet	<1 %
66	monster.emagister.com Fuente de Internet	<1 %
67	nemesisnoticias.wordpress.com Fuente de Internet	<1 %
68	peacekeeping.un.org Fuente de Internet	<1 %
69	public.dhe.ibm.com Fuente de Internet	<1 %
70	rebacc.crcrj.org.br Fuente de Internet	<1 %
71	revistas.usantotomas.edu.co Fuente de Internet	<1 %
72	rzweb.com.ar Fuente de Internet	<1 %
73	suarakampus.com Fuente de Internet	<1 %
74	www.3htp.com Fuente de Internet	<1 %
75	www.ad-hoc.de Fuente de Internet	<1 %

76	www.agapea.com Fuente de Internet	<1 %
77	www.alfa21.com Fuente de Internet	<1 %
78	www.cienciasmarinas.com.mx Fuente de Internet	<1 %
79	www.contraloria.gob.pa Fuente de Internet	<1 %
80	www.diariodelsur.com.co Fuente de Internet	<1 %
81	www.eff.org Fuente de Internet	<1 %
82	www.eliobastias.com.ar Fuente de Internet	<1 %
83	www.eureg.org Fuente de Internet	<1 %
84	www.europarl.europa.eu Fuente de Internet	<1 %
85	www.gerencia.cl Fuente de Internet	<1 %
86	www.hyland.com Fuente de Internet	<1 %
87	www.iered.unicauca.edu.co Fuente de Internet	<1 %

88	www.incom.cl Fuente de Internet	<1 %
89	www.infoaqui.com Fuente de Internet	<1 %
90	www.mondragon.edu Fuente de Internet	<1 %
91	www.mtc.gob.pe Fuente de Internet	<1 %
92	www.redclara.net Fuente de Internet	<1 %
93	www.siama.info.ve Fuente de Internet	<1 %
94	www.sinembargo.mx Fuente de Internet	<1 %
95	www.ub.es Fuente de Internet	<1 %
96	www.unodc.org Fuente de Internet	<1 %
97	www.upf.edu Fuente de Internet	<1 %
98	Submitted to KTH - The Royal Institute of Technology Trabajo del estudiante	<1 %

Excluir citas	Activo	Excluir coincidencias	Apagado
Excluir bibliografía	Activo		

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

Los que suscriben, DIAZ QUEZADA IVAN FABRICIO y RAMIREZ SAMANIEGO ELIAN JOSUE, en calidad de autores del siguiente trabajo escrito titulado Gestión de la Seguridad y Protección de la Información de la UTMACH mediante estándares y buenas prácticas., otorgan a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tienen potestad para otorgar los derechos contenidos en esta licencia.

Los autores declaran que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

Los autores como garantes de la autoría de la obra y en relación a la misma, declaran que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asumen la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

DIAZ QUEZADA IVAN FABRICIO
0705179547

RAMIREZ SAMANIEGO ELIAN JOSUE
0750338188

UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

TRABAJO DE INTEGRACIÓN CURRICULAR

OPCIÓN

TRABAJO DE INTEGRACIÓN CURRICULAR,

PROPUESTAS TECNOLÓGICAS

TEMA

GESTIÓN DE LA SEGURIDAD Y PROTECCIÓN DE LA INFORMACIÓN DE LA UTMACH MEDIANTE ESTÁNDARES Y BUENAS PRÁCTICAS.

AUTOR(ES)

RAMIREZ SAMANIEGO ELIAN JOSUE

DIAZ QUEZADA IVÁN FABRICIO

MACHALA, 28 DE DICIEMBRE DEL 2023

PERÍODO LECTIVO

2023-D2

TRABAJO DE INTEGRACIÓN CURRICULAR

MODALIDAD DE PROPUESTAS TECNOLÓGICAS

RESUMEN

Este proyecto ha logrado su objetivo principal de desarrollar una propuesta de sistema de gestión de seguridad de la información (SGSI) específica para la Universidad Técnica de Machala (UTMACH), abordando la falta de un sistema robusto de seguridad de la información y haciendo frente a amenazas potenciales. A partir de un diagnóstico inicial, se identificaron brechas y oportunidades para mejorar la seguridad de la información, y se diseñó una propuesta de SGSI alineada con estándares y mejores prácticas. Esta propuesta incluye medidas de seguridad tanto técnicas como administrativas y promueve el desarrollo de una cultura de seguridad entre el personal administrativo. La evaluación de conformidad en el área TIC ofreció perspectivas valiosas, revelando fortalezas como la clasificación de activos, y necesidades como identificación de vulnerabilidades. Se estableció una base sólida sobre seguridad de información universitaria. Existe alto nivel de conformidad en TIC con el SGSI propuesto, especialmente en recolección de información, plan de contingencia y formación. Este enfoque integral subraya la importancia de un SGSI adaptado que no solo mejora la protección de los activos informáticos en la UTMACH, sino que también sirve como modelo para otras instituciones académicas, contribuyendo al conocimiento académico sobre la seguridad de la información en contextos universitarios. A nivel académico, este estudio representa una oportunidad para generar nuevo conocimiento sobre seguridad de la información aplicada al ámbito universitario, un área aún poco explorada, introduciendo consideraciones éticas sobre la protección de datos sensibles de la comunidad educativa.

PALABRAS CLAVE

gestión de seguridad de la información, estándares de seguridad, buenas prácticas de seguridad, protección de datos, tecnologías de la información, SGSI

SUMMARY

This project has achieved its main objective of developing a proposal for an information security management system (ISMS) specific to the Technical University of Machala (UTMACH), addressing the lack of a robust information security system and addressing potential threats. Based on an initial diagnosis, gaps and opportunities to improve information security were identified, and an ISMS proposal was designed, aligned with standards and best practices. This proposal includes both technical and administrative security measures and promotes the development of a security culture among administrative personnel. In conducting the compliance assessment of the ICT area, it has offered valuable insights, revealing compliance in certain areas such as the classification and registration of identified assets and highlighting needs for improvement in others, such as the identification of vulnerabilities. This comprehensive approach underscores the importance of an adapted ISMS that not only improves the protection of IT assets at UTMACH, but also serves as a model for other academic institutions, contributing to academic knowledge about information security in university contexts. At the academic level, this study represents an opportunity to generate new knowledge on information security applied to the university environment, an area still little explored, introducing ethical considerations on the protection of sensitive data of the educational community.

KEY WORDS

information security information security, security standards, good security practices, data protection, information security, data protection, information technologies, SGSI

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

GLOSARIO

- **Gestión de seguridad**: Proceso de identificar, evaluar y mitigar riesgos relacionados con la información.
- **Protección de datos**: Medidas y técnicas utilizadas para salvaguardar la confidencialidad, integridad y disponibilidad de la información.
- **Confidencialidad**: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Integridad**: Propiedad de exactitud y completitud de la información.
- **Disponibilidad**: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.
- **SGSI**: Sistema de Gestión de Seguridad de la Información. Conjunto de políticas, procesos y controles implementados para gestionar los riesgos de seguridad de la información y proteger los activos informáticos.
- **Riesgo**: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.
- Amenaza: Causa potencial de un incidente no deseado que puede provocar daños a un sistema o a una organización.
- **Vulnerabilidad**: Debilidad de un activo o medida de seguridad que puede ser explotada por una o más amenazas.
- Incidente de seguridad: Evento no deseado o inesperado con probabilidad significativa de comprometer las operaciones de negocio y amenazar la seguridad de la información.
- **Estándares de seguridad**: Conjunto de directrices técnicas desarrolladas por organizaciones expertas para implementar controles de seguridad efectivos. Algunos ejemplos son ISO/IEC 27001, NIST CSF, PCI DSS.
- **ISO/IEC 27001**: Estándar internacional que especifica los requisitos necesarios para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información.
- **Buenas prácticas**: Conjunto coherente de acciones que han demostrado su efectividad para ayudar a proteger la información y que se recomienda adoptar.
- **Controles de seguridad**: Medidas técnicas, físicas, organizativas o legales que permiten gestionar los riesgos, garantizando la confidencialidad, integridad y disponibilidad de los activos de información.
- **Análisis de riesgos**: Proceso sistemático para identificar riesgos, determinar su probabilidad de ocurrencia e impacto, y definir acciones para mitigarlos.
- **Recuperación ante desastres**: Planes y procedimientos que permiten la continuidad del negocio y la recuperación de sistemas críticos ante un desastre o interrupción grave.
- **Seguridad física**: Controles para proteger las instalaciones, equipos e información de amenazas físicas como robo, fuego o inundaciones.
- **Concientización en seguridad**: Capacitación para que los empleados comprendan sus responsabilidades y buenas prácticas de seguridad.
- **Cumplimiento normativo**: Proceso para asegurar que las prácticas y controles de una organización cumplen con las leyes y regulaciones aplicables.

INTRODUCCIÓN

La administración competente de la protección de los datos se ha vuelto un elemento clave para cualquier compañía en el mundo digital de hoy en día. La información sensible puede enfrentar diversas amenazas tanto internas como externas, que podrían poner en grave riesgo factores de carácter reservado, la precisión y el acceso a la información. Las instituciones educativas como universidades no están exentas de estos desafíos. Por el contrario, los centros de educación superior frecuentemente manejan grandes volúmenes de información delicada, incluyendo datos personales de estudiantes, información de investigaciones, registros académicos, entre otros. Proteger adecuadamente estos activos informáticos es un imperativo.

Según la definición anterior, la Universidad Técnica de Machala (UTMACH) no tiene un sistema robusto de gestión de seguridad de la información. Esta situación la expone a importantes riesgos y amenazas, como posibles accesos no autorizados, interrupciones de servicios, y pérdidas o daños a los datos institucionales. Claramente, esto podría tener graves consecuencias para la universidad, no solo desde la perspectiva de la protección de la información, sino también para su reputación y responsabilidades legales.

En este proyecto de investigación aborda la problemática ya mencionada mediante una propuesta de sistema de gestión de seguridad de la información (SGSI), adaptado a las necesidades y contexto de la UTMACH. La intención es robustecer la protección de los bienes informáticos de la institución, poniendo en marcha un Sistema para Administrar la Seguridad de los Datos basado en estándares, buenos procedimientos y un análisis exhaustivo de los riesgos existentes.

El método para elaborar la propuesta del SGSI conllevará una fase de diagnóstico del estado actual de la protección, posterior a eso un análisis de deficiencias fundamentado en estándares como la ISO 27001. Culminando con la sugerencia adecuada de los controles de seguridad de los datos pertinentes y la revisión efectiva del Sistema de Gestión resultante.

Los descubrimientos de esta investigación suministrarán un modelo que se podría ampliar a otras instituciones de enseñanza superior para robustecer sus tácticas de administración de la seguridad de los datos. Asimismo, este estudio representará una contribución al conocimiento en este campo, particularmente en el contexto de las universidades.

i. Declaración y formulación del problema

La UTMACH en la actualidad no cuenta con un sistema completo para la administración de la seguridad de los datos. Esta circunstancia hace vulnerable a la universidad ante diversas debilidades y peligros, poniendo en riesgo la confidencialidad, integridad y acceso a la información institucional.

La ausencia de un mecanismo sólido de protección de datos ocasiona que la UTMACH sea susceptible a incidentes como accesos no autorizados, interrupciones de servicio, pérdida o corrupción de datos. Además, dificulta la capacidad de la universidad para implementar estrategias efectivas que le permitan prevenir y responder ante posibles brechas de seguridad.

Esta problemática no solo tiene implicaciones para la protección de los activos informáticos, sino que también puede dañar su reputación y generar consecuencias legales si ocurriera un incidente de seguridad significativo.

Por consiguiente, es imperioso hacer frente a esta coyuntura mediante la elaboración y ejecución de un sistema sólido e integral de gestión de la seguridad de los datos, basado en estándares internacionales y buenos procedimientos.

La UTMACH dispone de un área de Tecnologías de la Información y la Comunicación (TICs) que administra la infraestructura tecnológica vinculada a los sistemas y recursos de información. Sin embargo, este departamento se enfrenta a una escasez de documentación y procedimientos estandarizados para la administración y mantenimiento de la seguridad de dicha infraestructura y los recursos de información. Asimismo, se identifica la carencia de un sistema de gestión de la seguridad de los datos, planes de contingencia y continuidad del negocio ante incidentes o desastres que puedan afectar la confidencialidad, integridad y accesibilidad de los recursos de información. En la Figura 1, se muestran los posibles problemas causados por la falta de una gestión de seguridad.

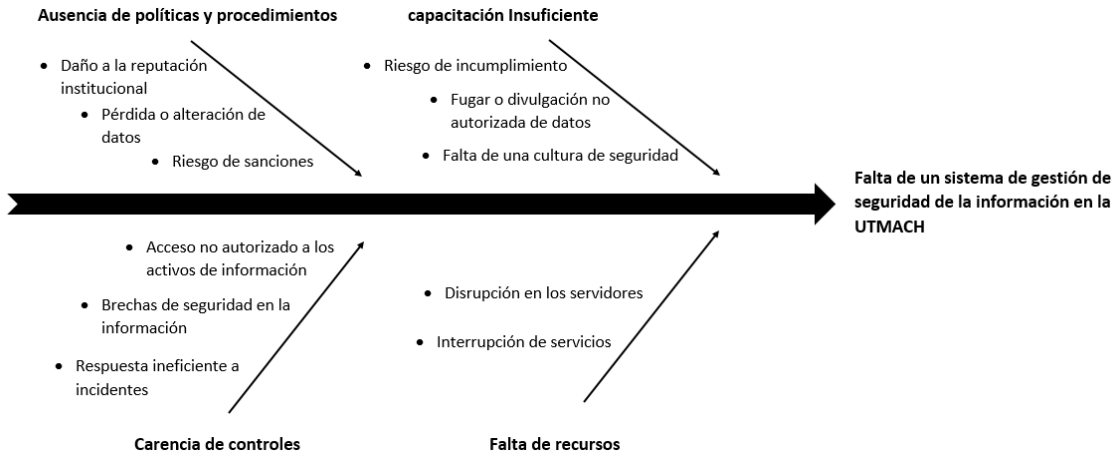


Figura 1 Árbol de causas, problema y efectos

Formulación del problema

Problema principal:

- La falta de un sistema de gestión de seguridad pone a la UTMACH en riesgo, expuesta a vulnerabilidades y amenazas que podrían comprometer la confidencialidad, integridad y disponibilidad de la información institucional. Además, esta situación podría conducir a consecuencias perjudiciales como el acceso no autorizado, la pérdida de datos, la interrupción de servicios, el daño a su reputación y posibles repercusiones legales.

Problemas específicos:

- ¿Cuáles son los estándares y marcos de trabajo más adecuados para gestionar la seguridad de la información en una institución educativa como la Universidad Técnica de Machala?

- ¿Cuáles son las principales vulnerabilidades y peligros más relevantes en materia de seguridad de la información a los que se expone la Universidad Técnica de Machala?
- ¿Cómo se pueden identificar y evaluar de manera sistemática los riesgos de seguridad de la información en la universidad?
- ¿Cuáles son las mejores prácticas para los controles de protección de datos efectivos en la UTMACH (Universidad Técnica de Machala)?
- ¿Qué medidas de concienciación y capacitación en seguridad de la información son necesarias para el personal y los usuarios de la universidad?
- ¿Cómo se puede establecer un marco de respuesta y recuperación ante incidentes de seguridad de la información en la Universidad Técnica de Machala?
- ¿Cuáles son los recursos y la infraestructura necesarios para mantener un sistema de gestión de seguridad de la información robusto y eficiente en la universidad?
- ¿Cuál es el impacto financiero y la viabilidad de un sistema de estándares y buenas prácticas en la gestión de la seguridad de la información en la Universidad Técnica de Machala?

ii. Objeto de estudio y Campo de acción

Objeto de estudio

- Sugerir gestión de protección de datos en UTMACH.
- Evaluar políticas y riesgos en seguridad de información de UTMACH.
- Investigar y adaptar estándares ISO 27000 a UTMACH.
- Proponer sistema de protección de activos TIC en UTMACH.

Campo de acción

- El Mejorar la seguridad de la información en el área TIC de la UTMACH mediante el análisis, evaluación de riesgos y propuesta de soluciones prácticas basadas en estándares y buenas prácticas.

iii. Objetivos

Objetivo General

- Elaborar una propuesta para la gestión de la seguridad y protección de la información en la UTMACH mediante estándares y buenas prácticas que sirva de guía para la mitigación de incidentes informáticos.

Objetivos específicos

- Desarrollar el marco teórico de la investigación a través de la revisión de antecedentes históricos, teóricos y contextuales sobre la gestión de seguridad de la información en el ámbito de la UTMACH, que permita establecer los requerimientos para la propuesta del sistema de gestión.
- Identificar vulnerabilidades y desarrollar políticas, procedimientos y controles de seguridad de la información para la UTMACH según estándares y necesidades específicas.

- Realizar actividades de sensibilización y establecer un marco de respuesta ante riesgos en protección de datos para fomentar una cultura de seguridad sólida en la UTMACH.
- Evaluar el esquema de seguridad basado en estándares y buenas prácticas.

iv. Hipótesis y variables o Preguntas de investigación

- ¿Cuáles son las vulnerabilidades y riesgos específicos relacionados con la seguridad de la información que enfrenta la UTMACH?
- ¿Cómo se pueden identificar y evaluar de manera sistemática dichas vulnerabilidades y riesgos en la universidad?
- ¿Qué normativas, métodos y medidas de protección de datos deben desarrollarse e implementarse fortalecer la protección de los activos informáticos en el área de TIC de la UTMACH?
- ¿Qué protocolos y procedimientos deben establecerse para una reacción y restauración efectivas frente a situaciones de brechas de protección de datos en la institución académica?

v. Justificación

La propuesta de reglamentaciones sustentadas en estándares y buenos procedimientos en la administración de la seguridad de la información en la UTMACH es un estudio que tiene una relevancia fundamental en varios aspectos.

A nivel teórico, este estudio ofrece una oportunidad única para cubrir una brecha significativa en el conocimiento existente en torno a una gestión de seguridad de basada en normativas y prácticas óptimas de seguridad de datos en el contexto universitario. No existe literatura académica suficiente que analice la relación entre la administración de la seguridad de la información y las normas en este ámbito. La realización de este estudio proporcionaría un valioso aporte a esta área, fomentando el desarrollo y la expansión del cuerpo de conocimientos de la seguridad en los activos informáticos en instituciones educativas. Además, podría potencialmente llevar a la generación de nuevas hipótesis e ideas que podrían ser exploradas en futuros estudios.

La necesidad de proteger los datos confidenciales de los estudiantes y del personal de la UTMACH, junto con el requerimiento de resguardar la reputación de la institución y acatar las normas, brinda un estímulo convincente para este estudio. Además, existe una motivación interna para contribuir al progreso científico en este ámbito, y para mejorar la forma en que las instituciones de educación superior gestionan y protegen la información.

La finalidad primordial de este estudio es plantear un sistema integral para la administración de la seguridad de la información en la UTMACH, fundamentado en normas y buenos procedimientos. Para conseguirlo, se empleará una metodología que conllevará la revisión minuciosa de dicho estándar, la adaptación de las mejores prácticas al contexto particular de la UTMACH, y la evaluación del sistema de seguridad resultante.

Las ventajas de este estudio serán multifacéticas. En primer lugar, la UTMACH se beneficiará directamente de la propuesta de un sistema de seguridad de la información sólido y fundamentado en estándares. Esto no solo resguardará los datos confidenciales de la universidad, sino que también coadyuvará a robustecer su reputación y acatar las normativas.

Además, la comunidad universitaria en su conjunto -incluyendo estudiantes, personal y todos los interesados en la protección de datos también se beneficiará. Las ventajas para estos grupos abarcan desde la protección de sus datos personales hasta una mayor confianza en la universidad.

La realización de esta investigación es altamente factible. Esto se debe a la disponibilidad de estándares y marcos de trabajo reconocidos internacionalmente, que proporcionan un camino claro y estructurado para la instauración de sistemas de protección de datos. Además, se espera contar con la cooperación de la UTMACH, que proporcionará el entorno necesario para la evaluación del sistema de seguridad propuesto.

Este estudio también tiene una utilidad metodológica significativa. A través de su desarrollo, podremos contribuir a la creación de nuevos métodos, así como posibles técnicas de investigación que pueden ser relevantes en este campo. Esta investigación no solo ayudará a desarrollar y probar una metodología basada en estándares y buenas prácticas en instituciones educativas, sino que también podría sugerir cómo estudiar más adecuadamente la seguridad de la información en este tipo de entornos.

vi. Organización del documento

La documentación de este proyecto se categoriza en tres capítulos, que abordan las actividades realizadas durante el proceso de titulación.

- **Capítulo 1**: Sección que abarca la fundamentación teórica del proyecto, se presentan definiciones, hechos cronológicos, metodología de revisión de literatura y hechos contextuales.
- **Capítulo 2**: Capítulo compuesto por etapas relacionadas al desarrollo y ejecución del prototipo, se describe la metodología de desarrollo, elaboración y ejecución del prototipo.
- **Capítulo 3**: Apartado compuesto de pruebas del prototipo, se compone de un plan de evaluación y análisis de los resultados conseguidos.

1. CAPÍTULO I. MARCO TEÓRICO

1.1. Antecedentes de la Investigación

Para elaborar los antecedentes del presente trabajo sobre seguridad de la información en la UTMACH, se realizó una Revisión Sistemática de Literatura con el objetivo de identificar, examinar e interpretar las pruebas científicas previas sobre la administración de la seguridad de la información, la aplicación de estándares y procedimientos adecuados empleados en instituciones de educación superior. Mediante este proceso se examinaron estudios relacionados que aportaron insumos valiosos para enmarcar la investigación actual, contextualizando adecuadamente los antecedentes del problema con base en el conocimiento y experiencias de trabajos previos, según la metodología de Revisión Sistemática.

a) Preguntas de investigación

La Tabla 1, muestra las preguntas de investigación formuladas, las cuales permiten determinar la orientación y el desarrollo del proyecto. Estas preguntas ayudan a analizar y establecer claramente la problemática a solucionar mediante la investigación.

Tabla 1 Preguntas de investigación

Preguntas de investigación	Descripción y motivación
¿Cuáles son las vulnerabilidades y riesgos específicos de seguridad de la información que enfrenta la Universidad Técnica de Machala?	Descripción: Esta pregunta busca identificar y entender las vulnerabilidades y riesgos específicos de seguridad de los datos que enfrenta la UTMACH. Motivación: Al identificar las vulnerabilidades y riesgos específicos, se pueden desarrollar estrategias y medidas de seguridad más efectivas y personalizadas. Esta pregunta es esencial para entender la situación presente de la protección de datos en la universidad y para determinar qué áreas necesitan ser mejoradas.
¿Cómo se pueden identificar y evaluar de manera sistemática dichas vulnerabilidades y riesgos en la universidad?	Descripción: Esta pregunta busca explorar métodos y técnicas para identificar y evaluar de manera sistemática las vulnerabilidades y riesgos de los datos en la universidad. Motivación: Una determinación y evaluación sistemática de las vulnerabilidades y riesgos puede ayudar a la universidad a priorizar sus esfuerzos y recursos en las áreas que más lo necesitan. Esta pregunta es relevante para desarrollar un enfoque más estructurado y eficiente para la gestión de la seguridad de la información.

¿Qué normativas, métodos y medidas de protección de datos deben desarrollarse e implementarse fortalecer la protección de la información en la universidad?	Descripción: Esta pregunta busca determinar qué normativas, métodos y medidas de protección de datos deben ser desarrollados e implementados en la universidad para mejorar la protección de los activos informáticos. Motivación: normativas, métodos y medidas de seguridad son fundamentales para fortalecer la protección de la información. Esta pregunta es relevante para desarrollar un marco efectivo y completo para la institución.
¿Cuál es la mejor manera de concienciar y capacitar al personal y usuarios de la universidad en seguridad de la información?	Descripción: Esta pregunta busca identificar las mejores prácticas y métodos para concienciar y capacitar al personal y usuarios de la universidad en la protección informática. Motivación: La concienciación y formación en seguridad de datos son esenciales para fortalecer que todos los miembros de la universidad comprendan su papel en la protección de la información. Esta pregunta es relevante para desarrollar un programa de concienciación y capacitación efectivo y atractivo.
¿Qué protocolos y procedimientos deben establecerse para una actuación y restauración eficientes frente a situaciones relacionadas con brechas de seguridad de datos en el ámbito en la universidad?	Descripción: Esta pregunta busca determinar qué protocolos y procedimientos deben ser establecidos en la universidad para una gestión y recuperación efectivas tras eventos de seguridad de la información. Motivación: Tener protocolos y procedimientos de respuesta y recuperación eficientes es crucial para minimizar el impacto de situaciones relacionadas con la protección de datos. Esta pregunta es relevante para mejorar que la universidad esté preparada para responder y recuperarse de manera eficiente ante cualquier incidente de seguridad de la información.

b) Palabras claves y Cadena(s) de búsqueda

Para la revisión sistemática de literatura se definieron palabras clave y cadenas de búsqueda considerando términos sobre gestión de seguridad de la información, uso de estándares y buenas prácticas aplicados en la UTMACH, permitiendo descubrir trabajos académicos relevantes sobre análisis de riesgos, requisitos de seguridad, normas ISO 27001, confidencialidad, integridad y disponibilidad de la información. Esta cadena de

búsqueda enfocada fue esencial para seleccionar y revisar estudios previos con aportes aplicables al problema de gestionar la seguridad de la información en la UTMACH.

Cadena de búsqueda en español:

("Requisitos de seguridad" O "ingeniería de seguridad" O "ingeniero de seguridad" O "equipo de seguridad" O "análisis de seguridad" O "especificación de seguridad") Y ("Gestión de seguridad de información" O "Seguridad de datos" O "Seguridad informática" O "Protección de la información") Y ("Estándares de seguridad" O "Normas de seguridad" O "Regulaciones de seguridad") Y ("Buenas prácticas" OR "Mejores prácticas globales") Y ("Universidad Técnica de Machala" O "UTMACH") Y ("Confidencialidad" O "Integridad" O "Disponibilidad") Y ("Ciberseguridad" O "Seguridad de redes" O "Seguridad de sistemas") Y ("Riesgos de seguridad" O "Amenazas de seguridad" O "Vulnerabilidades de seguridad")

Cadena de búsqueda en inglés:

("Security requirements" OR "security engineering" OR "security engineer" OR "security team" OR "security analysis" OR "security specification") AND ("Information security management" OR "Data security" OR "IT security" OR "Information protection") AND ("Security standards" OR "Security norms" OR "Security regulations") AND ("Best practices" OR "Global best practices") AND ("Universidad Técnica de Machala" OR "UTMACH") AND ("Confidentiality" OR "Integrity" OR "Availability") AND ("Cybersecurity" OR "Network security" OR "Systems security") AND ("Security risks" OR "Security threats" OR "Security vulnerabilities")

c) Criterios de inclusión y exclusión

En la Tabla 2 se establecen los criterios de inclusión y exclusión de trabajos relacionados al tema de investigación, estos criterios serán aplicados en la Revisión Sistemática de literatura.

Tabla 2 Criterios de inclusión y exclusión

#	CRITERIOS DE INCLUSIÓN
1	Estudios que se centren en la protección de los datos de información en instituciones de educación superior.
2	Investigaciones que utilicen o discutan estándares y buenas prácticas como ISO/IEC 27000, COBIT v5, ITIL v4, ISO/IEC 20000 y PMBOK v6, en el contexto de la gestión de protección de la información.
3	Trabajos que presenten desafíos y oportunidades en la administración de la seguridad informática en las entidades de educación avanzada.
4	Estudios que discutan cómo la gestión de la seguridad de la información puede contribuir a la misión y los objetivos estratégicos de las instituciones de educación superior.
5	Investigaciones publicadas en los últimos 10 años para garantizar la relevancia y actualidad de la información.
#	**Criterios de Exclusión**

1	Estudios que no se centren en la gestión de la seguridad de la información o que se centren en otros aspectos de las tecnologías de la información.
2	Investigaciones que no utilicen o discutan estándares y buenas prácticas en el contexto de la gestión de salvaguardar de la información.
3	Trabajos que no presenten desafíos y oportunidades específicos en la gestión de la protección de los datos en las áreas tecnológicas de una institución universitaria.
4	Estudios que no discutan cómo la protección de la información puede contribuir a la misión y los objetivos estratégicos de las instituciones de educación superior.
5	Investigaciones publicadas hace más de 10 años, ya que la información puede no ser relevante o estar actualizada.

d) Proceso y resultados de la búsqueda

El proceso de recolección de información involucró la identificación de bases de datos pertinentes que albergan publicaciones fidedignas relacionadas con el tema de investigación. En la Figura 2, se expone de manera detallada el procedimiento de selección y los artículos identificados. Posteriormente, se llevaron a cabo consultas utilizando las cadenas de búsqueda previamente definidas, y se implementaron múltiples filtros de exclusión de manera secuencial para descartar aquellos trabajos que no satisfacían los criterios preestablecidos.

En una exploración más profunda, este proceso comenzó con una fase de identificación, donde se seleccionaron bases de datos que son reconocidas por su relevancia y confiabilidad en el ámbito del tema de investigación. La Figura 2 proporciona una descripción exhaustiva de cómo se efectuó la selección y los artículos que fueron identificados como resultado de este proceso.

Una vez identificadas las bases de datos, se procedió a la fase de consulta, en la cual se utilizaron cadenas de búsqueda específicas, diseñadas para refinar y focalizar la búsqueda de información relevante. Esta etapa es crucial, ya que permite una exploración eficaz y dirigida dentro del vasto mar de información disponible.

La fase final del proceso involucró la aplicación de una serie de filtros de exclusión, ejecutados de manera sucesiva para eliminar los trabajos que no cumplían con los criterios establecidos para esta investigación. Estos filtros ayudan a asegurar que la información recolectada sea de alta relevancia y calidad, descartando aquellos trabajos que podrían desviar o diluir el enfoque de la investigación.

Este método meticuloso asegura una recolección de datos precisa y relevante, que es fundamental para el éxito y la validez de cualquier proyecto de investigación.

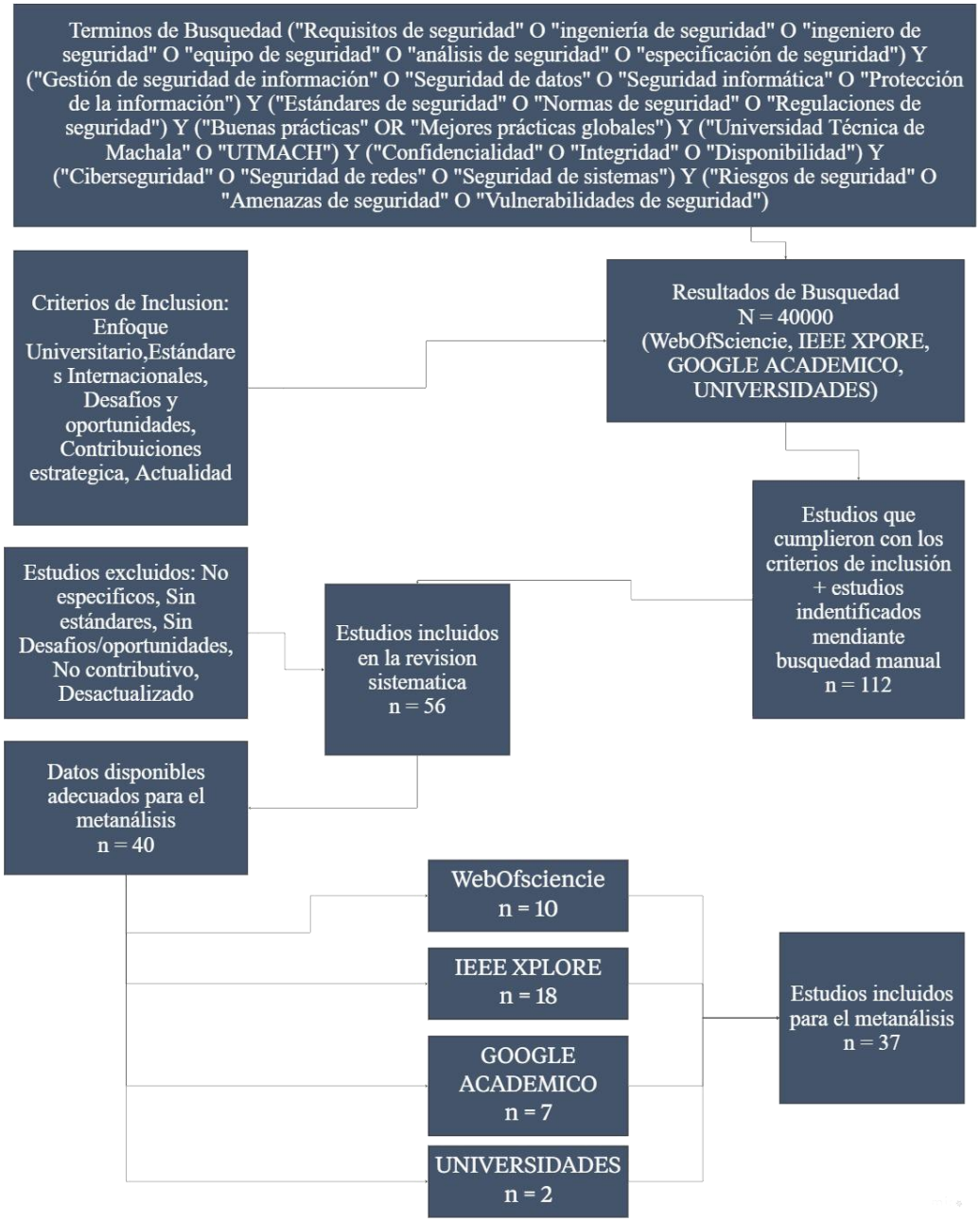


Figura 2 Diagrama del proceso de selección de papers

Resultado de Búsqueda

En la Tabla 3 se muestra la cantidad de artículos por año que se han utilizado en la investigación y en la Figura 3 se representa de forma gráfica.

Tabla 3 Datos de investigación por año

NUMERO DE INVESTIGACIONES	AÑO DE PUBLICACIÓN
1	2004
2	2010
1	2012
1	2013
1	2014

1	2015
6	2017
2	2018
12	2019
2	2020
6	2021
2	2023

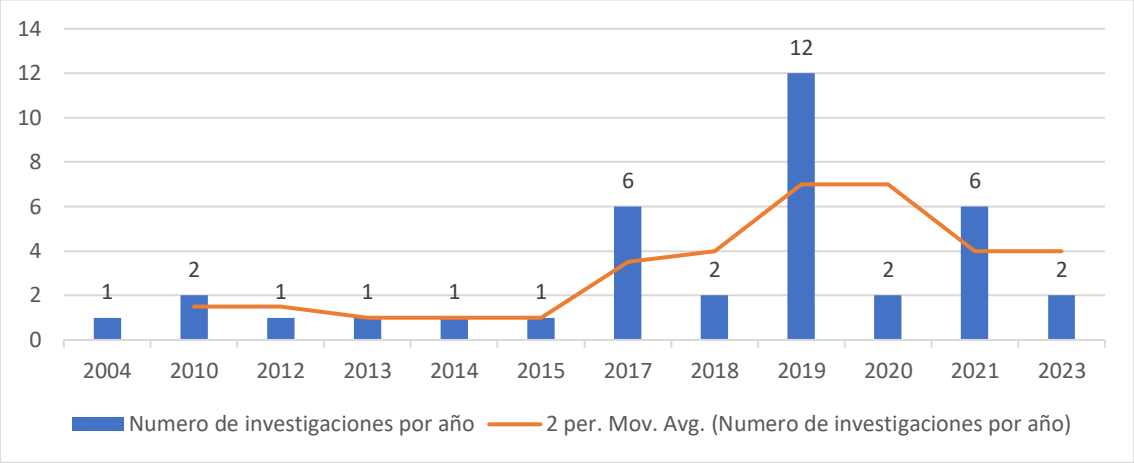


Figura 3 Cantidad de trabajos publicados por año del 2012 al 2013

1.2. Antecedentes históricos

La administración de la seguridad y resguardo de los datos es un proceso permanente que procura salvaguardar los recursos de información de una entidad, garantizando su confidencialidad, integridad y accesibilidad. En el caso de las universidades, el SGSI es indispensable para asegurar la continuidad de las operaciones, la protección de los datos de los alumnos y el acatamiento de las normativas.

La administración de la seguridad de la información en el sector bancario ha tenido una evolución significativa, ajustándose paulatinamente a las cambiantes dinámicas tecnológicas y a la proliferación de las amenazas cibernéticas. Según Bauer, et al., los bancos han ampliado su enfoque desde la protección física hacia una visión más holística que incluye la seguridad de datos, redes e información global [1]. Este cambio enfatiza la importancia de contrarrestar los riesgos derivados de las acciones humanas y las interacciones tecnológicas, subrayando la necesidad de políticas de seguridad de la información efectivas para reducir incidentes y fomentar una cultura de seguridad entre los usuarios.

Siguiendo esta línea evolutiva en el 2017, da Veiga y Martins [2] resaltan la creciente importancia de la cultura de seguridad de la información en las organizaciones actuales. Esta cultura, según ellos, debe ser moldeada e influenciada para guiar el comportamiento de todos los involucrados, desde empleados hasta terceros, con el objetivo de minimizar los riesgos asociados a los activos informativos.

Si bien no se sabe dónde podría ocurrir un incidente, puede suceder a la vuelta de la esquina por lo cual muchas organizaciones, séase de diferentes ámbitos tienen un riesgo imperante desde cualquier ámbito al que se dediquen dando una cierta sensación de

incertidumbre al no tener una documentación necesaria cuando ocurra algún incidente tales, así como la salud. Según un estudio de He y Johnson [3], las organizaciones de salud en China a menudo carecen de mecanismos estructurados para aprender de los incidentes de seguridad y aplicar ese aprendizaje para mejorar sus prácticas de seguridad. Esta falta de aprendizaje estructurado puede resultar en la repetición de errores y en la exposición a riesgos de seguridad similares en el futuro. Es esencial que las organizaciones no solo respondan a los incidentes de seguridad, sino que también aprendan de ellos y adapten sus prácticas y políticas en consecuencia.

En el contexto de la creciente interconexión y la evolución de las políticas de seguridad en organizaciones y sectores como la salud, surgen nuevos desafíos en el ámbito laboral: el BYOD. Esta tendencia, que faculta a los trabajadores a emplear sus propios aparatos en el ámbito laboral, brinda beneficios en cuanto a flexibilidad y costos. Sin embargo, el artículo [4] destaca que, a pesar de estos beneficios, las organizaciones a menudo pasan por alto los riesgos asociados con la privacidad y la confidencialidad. La falta de estructuras adecuadas para aprender de los incidentes de seguridad y adaptar las políticas y prácticas puede exponer a las organizaciones a vulnerabilidades significativas. En este sentido, es esencial que las organizaciones no solo implementen políticas de BYOD, sino que también establezcan marcos robustos para garantizar la preservación de la confidencialidad y la integridad de la información.

Además de los desafíos y oportunidades presentados por la interconexión y la evolución de las políticas de seguridad en organizaciones y sectores específicos, es esencial reconocer la centralidad de la investigación de seguridad y privacidad en el ámbito de los sistemas de información. Lowry et al. [5] argumentan que, en lugar de centrarse únicamente en el "artefacto de TI", es crucial considerar el "artefacto de IS" en su totalidad, que abarca no solo la tecnología sino también los procesos, políticas y prácticas relacionadas. Esta perspectiva holística es esencial para abordar de manera efectiva los desafíos de seguridad y privacidad en el mundo digital actual, especialmente con la aparición de plataformas en línea, IoT y big data.

Es esencial reconocer la centralidad de la investigación de seguridad y privacidad en el ámbito de los sistemas de información. ERCEG [6] destaca en 2019 que, a medida que las organizaciones invierten en sistemas de seguridad de la información, el comportamiento de los empleados se vuelve cada vez más crucial. El estudio revela que el comportamiento general de los trabajadores en una empresa de producción croata es más responsable en términos de seguridad de la información. Este hallazgo subraya la importancia de educar y capacitar a los empleados sobre prácticas seguras y la necesidad de fomentar una cultura organizacional que priorice la seguridad de la información.

Por otra parte, tomando un enfoque más académico en la Universidad de Tomsk de Sistemas de Control y Radioelectrónica (TUSUR), se ha llevado a cabo una investigación exhaustiva sobre la seguridad de la información, destacando la importancia de un enfoque integral para evaluar la seguridad de los sistemas de información. Shelupanov et al. [7] Subrayan que, además de los métodos tradicionales de seguridad, es esencial considerar enfoques modernos como la biometría dinámica, la esteganografía y la protección de datos en sistemas del Internet de las Cosas (IoT). Estos avances reflejan la evolución constante del campo de la seguridad de la información y la necesidad de adaptarse a las amenazas emergentes en el panorama digital.

Siguiendo este mismo contexto en la búsqueda de soluciones innovadoras para garantizar la seguridad de la información, la biometría ha emergido como una herramienta esencial durante estos años. Lalović et al.[8] Presentan en 2019 un enfoque revolucionario basado en la biometría de huellas dactilares, que no solo se centra en la autenticación y verificación de individuos adultos, sino que también aborda la crucial tarea de garantizar la identidad de los recién nacidos en las salas de maternidad. Este sistema, que combina técnicas avanzadas de biometría con algoritmos de cifrado de vanguardia, subraya la importancia de adaptar y evolucionar las soluciones de seguridad para abordar desafíos específicos y únicos en diversos contextos.

Tomando en cuenta los avances tecnológicos y metodológicos en la seguridad de la información, es crucial considerar el bienestar psicológico de los empleados encargados de implementar y mantener estas medidas de seguridad. Pham et al. [9] destacan el fenómeno del agotamiento relacionado con la seguridad de la información, que puede surgir al cumplir con las demandas de seguridad organizacional. Este agotamiento no solo puede afectar la eficacia con la que los empleados implementan medidas de seguridad, sino que también puede influir en su disposición general hacia la seguridad de la información. Por lo tanto, es esencial que las organizaciones no solo proporcionen las herramientas y recursos necesarios para garantizar la seguridad, sino que también consideren el bienestar de sus empleados, ofreciendo apoyo y capacitación adecuados para manejar el estrés y el agotamiento relacionados con la seguridad.

Retomando en el ámbito académico, la naturaleza y el desarrollo de las políticas de seguridad de la información han sido objeto de un escrutinio considerable. Paananen et al. [10] destacan la falta de consenso en la literatura sobre lo que constituye una política de seguridad de la información y cómo debería desarrollarse. A pesar de la amplia investigación en este campo, las organizaciones todavía enfrentan desafíos al tratar de definir y desarrollar políticas que sean tanto efectivas como adaptadas a sus necesidades específicas. Este hallazgo subraya la importancia de un enfoque más personalizado y contextualizado en el desarrollo de políticas de seguridad, que vaya más allá de las soluciones genéricas y considere las circunstancias y requisitos únicos de cada organización.

1.3. Antecedentes Teóricos

En la Figura 4 se muestran los temas de relevancia a tratar en el desarrollo teórico del proyecto.

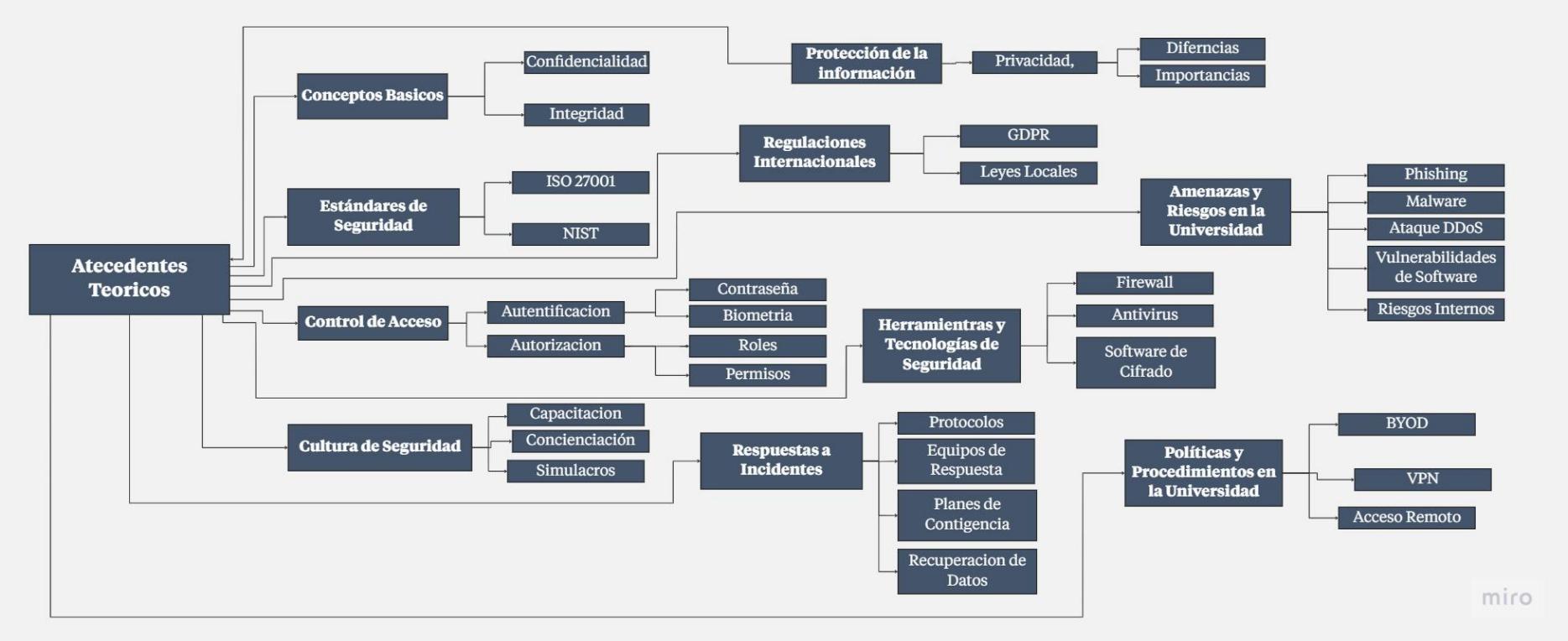


Figura 4. Mapa de antecedes Teóricos

1.3.1 Seguridad de la información

La protección de los datos alude a la práctica de salvaguardar la información de accesos no permitidos, modificaciones, destrucción o difusión. Es crucial para asegurar la confidencialidad, integridad y acceso a los datos en un mundo conectado digitalmente.

Conceptos Básicos

Los elementos básicos de la protección de la información son la confidencialidad, integridad y accesibilidad. Estos conceptos garantizan que la información esté resguardada de miradas no deseadas, permanezca intacta y esté accesible cuando se necesite.

- **Confidencialidad**
  La confidencialidad es un pilar fundamental en una amplia variedad de contextos, desde el ámbito médico y legal hasta el empresarial y tecnológico. Este principio se enfoca en la salvaguarda de información delicada, garantizando que únicamente las personas autorizadas tengan acceso a ella. En un mundo cada vez más digitalizado, donde los datos fluyen velozmente a través de múltiples plataformas, la relevancia de mantener la confidencialidad se ha vuelto más crítica que nunca. No solo es una cuestión de ética y responsabilidad, sino que también puede tener implicaciones legales y financieras significativas. La violación de la confidencialidad puede resultar en pérdida de confianza, perjuicio a la reputación y, en casos extremos, sanciones legales.
  Siguiendo esta misma línea, la confidencialidad en las redes inalámbricas adquiere una relevancia especial. Según Wei Jiang et al. [11], las redes inalámbricas críticas para misiones enfrentan diversas amenazas de seguridad, como la intercepción y alteración de datos. Para mitigar estos riesgos, se implementó una serie de servicios de seguridad. Entre ellos, los servicios de confidencialidad utilizan diferentes algoritmos de cifrado, cada uno con su propio tiempo de procesamiento, para asegurar la integridad de los datos transmitidos.
  En el ámbito tecnologico blockchain, la confidencialidad también es crucial. De acuerdo con un estudio reciente [12], la combinación de blockchain con Entornos de Ejecución de Confianza (TEE) puede mejorar significativamente tanto el rendimiento como la confidencialidad de las transacciones en la cadena de bloques.
- **Integridad**
  La integridad en la tecnología de la información (TI) es un pilar fundamental para salvaguardar la confiabilidad, seguridad y eficiencia de los sistemas y sus datos. Este concepto abarca una amplia gama de prácticas y políticas que buscan asegurar que la información se mantenga precisa, completa y accesible solo para aquellos con autorización adecuada. En un mundo tan cambiante y digitalizado, donde la información es un activo invaluable para individuos y organizaciones, la integridad en TI se convierte en una preocupación crítica.
  En este sentido, es fundamental garantizar la integridad de los datos almacenados en entornos de nube.
  De acuerdo con un estudio reciente, se ha desarrollado un esquema que utiliza la estructura de árbol rojo-negro para mejorar significativamente la eficiencia en el almacenamiento de datos en la nube, al mismo tiempo que simplifica las operaciones de actualización de los mismos [13]. Este enfoque innovador no solo

asegura que los datos permanezcan íntegros, sino que también optimiza los costos asociados con el almacenamiento y la computación. Por lo tanto, la implementación de soluciones robustas para mantener la integridad es más crítica que nunca en la era digital actual.

Conforme a esta línea de pensamiento, es fundamental señalar que la auditoría de la integridad de los datos en ambientes de nube ha sido un asunto muy estudiado en investigaciones recientes. Según un estudio llevado a cabo por Yan y Gui [14], se ha introducido un protocolo de auditoría pública que no solo verifica la integridad de los datos almacenados en la nube, sino que también protege la privacidad de la identidad de los usuarios involucrados. Este enfoque innovador permite que un Tercero Autorizado (TPA) realice auditorías sin comprometer la privacidad del usuario, lo cual es un avance significativo en la mejora de la seguridad y la eficiencia en la gestión de la integridad de los datos en la nube. Por lo tanto, este nuevo método se suma a las estrategias ya existentes que buscan optimizar el almacenamiento y reducir los costos, ofreciendo una solución más completa y robusta para la era digital actual.

1.3.2 Protección de la Información

La protección de la información se centra en salvaguardar los datos, especialmente aquellos sensibles o personales, de posibles amenazas y garantizar la privacidad de los usuarios.

Privacidad. Seguridad

Aunque a menudo se usan indistintamente, privacidad y seguridad tienen matices distintos. Mientras que la seguridad se centra en la protección contra amenazas, la privacidad se refiere a cómo se recopilan, almacenan y comparten los datos personales.

- **Diferencia**
  La diferencia principal es que la privacidad se enfoca en el derecho del individuo a controlar su información, y la seguridad se centra en las medidas técnicas para proteger esa información. Ambos son indispensables para asegurar la confidencialidad y la integridad de los datos en el universo digital.
- **Importancia**
  La importancia radica en que la privacidad permite a las personas controlar su información personal, mientras que la seguridad asegura que esta información esté protegida contra accesos no autorizados.

1.3.3 Estándares de Seguridad

Los estándares proporcionan un marco y directrices para las organizaciones, ayudándolas a implementar prácticas de seguridad efectivas y coherentes.

ISO 27001

Estándar internacional que especifica las pautas a seguir para establecer, implementar, mantener y mejorar un sistema relacionados con la administración de seguridad de la información (SGSI).

Según un análisis publicado en IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT [15], la ISO 27001 no solo proporciona un marco robusto para la administración de la seguridad de la información, sino que también establece directrices

para la evaluación y mitigación de riesgos relacionados con la ciberseguridad. Al adoptar este estándar, las organizaciones pueden fortalecer su postura de seguridad y demostrar un compromiso serio con la protección de datos y activos de información.

NIST

El Instituto Nacional de Estándares y Tecnología proporciona directrices detalladas sobre prácticas de seguridad, ayudando a las organizaciones a proteger sus sistemas y datos.

En el estudio realizado por Moreira [16], se analizó cómo los controles de ciberseguridad del marco de infraestructura crítica de NIST podrían colaborar con un gran banco brasileño que maneja millones de dólares por hora, especialmente en el sector tecnológico que se encarga del área internacional. Esta investigación utilizó la Metodología Multicriterio de Apoyo a la Decisión Constructivista (MCDA-C) para evaluar la eficacia de estos controles, demostrando que ciertos controles, como el "FPV 2 - Monitoreo Continuo de Seguridad", son esenciales para mejorar la ciberseguridad del banco.

1.3.4 Regulaciones Internacionales

Con la creciente globalización de la información, las regulaciones internacionales juegan un papel crucial en la definición de cómo se deben manejar y proteger los datos personales.

GDPR

El Reglamento General de Protección de Datos es una regulación de la UE que protege los datos personales de los ciudadanos europeos, estableciendo directrices estrictas sobre cómo se deben recopilar, almacenar y procesar estos datos.

Según J. Oh [17], esta regulación no solo tiene un impacto significativo en Europa, sino que también afecta a las empresas y servicios en línea de todo el mundo que interactúan con ciudadanos europeos. Además, su objetivo principal es garantizar los derechos de privacidad de los individuos y asegurar que las organizaciones sean transparentes y responsables en sus prácticas de manejo de datos. Sin embargo, a pesar de su implementación, muchos sitios web y servicios aún luchan por cumplir plenamente con sus disposiciones, lo que ha llevado a la necesidad de herramientas y estudios que evalúen el nivel de cumplimiento de estas entidades.

Leyes Locales

Además de las regulaciones internacionales, las leyes locales también juegan un papel crucial en la protección de datos, y varían según el país o la región.

En el contexto ecuatoriano, se ha identificado una preocupación debido a la ausencia de un instrumento legal específico que ofrezca directrices para resguardar la infraestructura crítica. Sin embargo, según el documento [18], con la introducción de la Política Nacional de Ciberseguridad, se busca establecer un marco que coordine y coopere con diversos sectores. Esto incluye el público, privado, académico y la sociedad civil, con el objetivo principal de garantizar un ciberespacio seguro y promover la confianza digital.

1.3.5 Amenazas y Riesgos en la Universidad

Identificar y comprender las amenazas y riesgos específicos para la UTMACH es esencial para establecer medidas de protección adecuadas.

Estas son algunas de las amenazas más frecuentes que enfrentan las instituciones hoy en día. Desde intentos de manipular a los usuarios para que brinden información confidencial hasta ataques que buscan interrumpir los servicios, es crucial estar preparado y protegido contra estas amenazas.

Phishing

El phishing es una forma de ciberdelincuencia que ha proliferado en la era digital, amenazando tanto a individuos como a organizaciones. Este tipo de ataque involucra la suplantación de identidad y la creación de sitios web falsos con el propósito de engañar a las víctimas para que revelen información confidencial, como contraseñas y datos financieros. El phishing ha evolucionado con el tiempo, y la detección efectiva de estos ataques es esencial para la seguridad cibernética. Según [18], los ataques de phishing han dado lugar al desarrollo de algoritmos y conjuntos de datos, como PhiKitA, que permiten analizar y clasificar las técnicas utilizadas por los atacantes, brindando una comprensión más profunda de este problema y posibilitando la adopción de medidas de prevención y mitigación.

Malware

El malware, o software malicioso, es un tipo de programa informático diseñado para infiltrarse o dañar sistemas y dispositivos sin el conocimiento ni el consentimiento del usuario. Como se ha discutido en el artículo [19], el malware puede adoptar diversas formas y estrategias para evadir la detección de soluciones de seguridad, lo que lo convierte en una amenaza persistente en el mundo digital.

Ataque DDoS

Según Dong y Sarem [20] en su investigación sobre la detección de ataques DDoS en redes definidas por software (SDN) , los ataques de denegación de servicio distribuidos, comúnmente conocidos como ataques DDoS, representan una de las amenazas más significativas para la seguridad de las redes. Estos ataques comprometen la disponibilidad de los servicios en línea al inundar un objetivo con una sobrecarga abrumadora de tráfico malicioso, lo que resulta en la inaccesibilidad de los recursos y la interrupción de los servicios. La creciente complejidad de estos ataques y su capacidad para eludir las soluciones de seguridad convencionales hacen que la detección efectiva de DDoS sea una prioridad crítica la seguridad de la red.

Vulnerabilidades de Software

Según la información proporcionada en la investigación [21], las vulnerabilidades de software representan una preocupación crítica en la seguridad informática. Estas vulnerabilidades se refieren a debilidades o fallos en el código de software que pueden ser explotados por actores maliciosos para comprometer la integridad, confidencialidad o disponibilidad de sistemas y datos. En el contexto de la ciberseguridad, identificar y clasificar estas vulnerabilidades es esencial para mitigar los riesgos asociados a posibles ataques.

Riesgos Internos

Los riesgos internos de seguridad son amenazas dentro de una organización, como acceso no autorizado o fuga de datos, causadas por empleados u otros con acceso a sus recursos. Para prevenirlos, se requieren políticas de seguridad, capacitación y controles adecuados.

1.3.6 Control de Acceso

El control de acceso es una parte fundamental de la seguridad, garantizando que solo las personas con acceso autorizado puedan acceder a la información y recursos específicos.

Autenticación

Los mecanismos de autenticación, como las contraseñas y la biometría, verifican la identidad de un usuario antes de permitirle acceder a un sistema o recurso.

- **Contraseña**

  La necesidad de robustecer la seguridad de las contraseñas en el ciberespacio es más crucial que nunca. En este contexto, se ha desarrollado un esquema de autenticación de dos factores que aprovecha tanto contraseñas como la verificación mediante lector de tarjetas, según lo documentado en "An Efficient and Secure Two-Factor Password Authentication Scheme With Card Reader/Terminal Verification" [22]. Este método no solo mejora la resistencia contra ataques malintencionados, sino que también emplea criptografía de curva elíptica para optimizar la eficiencia sin comprometer la seguridad, brindando así una solución efectiva para la protección de datos en entornos con recursos computacionales limitados.

- **Biometría**
  La biometría se refiere al uso de rasgos distintivos físicos o comportamentales de una persona, como las impresiones dactilares, el reconocimiento facial o los patrones de voz, para confirmar quién es esa persona de manera única. Este enfoque es crucial para la autenticación en varios campos, desde sistemas de acceso a dispositivos móviles hasta aplicaciones gubernamentales, y se espera que siga desempeñando un papel fundamental en la protección de la seguridad de los datos.

Autorización

Una vez autenticado, los sistemas de autorización determinan qué recursos o datos puede acceder un usuario, basándose en roles y permisos predefinidos.

- **Roles**
  Según la investigación presentada en [24], los roles desempeñan un papel fundamental en el control de accesos fundamentados en los roles (RBAC) y representan un enfoque clave para gestionar la autorización en sistemas de seguridad. En lugar de asignar permisos directamente a usuarios individuales, RBAC asigna roles a usuarios y define qué permisos tiene cada rol. Este modelo de autorización se basa en la estructura organizativa de una entidad y simplifica la gestión de permisos y usuarios, mejorando la seguridad y la eficiencia en el control de acceso.

- **Permisos**
  Según la investigación presentada [25], los permisos en el contexto de aplicaciones Android se consideran como autorizaciones otorgadas por los usuarios para que las aplicaciones accedan a recursos específicos del dispositivo. Estos permisos desempeñan un papel crucial en la seguridad y la privacidad de las

aplicaciones móviles al determinar qué funciones y datos pueden utilizar. El análisis de permisos se ha convertido en un enfoque esencial para evaluar la confiabilidad y la integridad de las aplicaciones, ya que garantiza que las aplicaciones solo accedan a recursos para los que tienen permiso explícito, lo que contribuye a mitigar riesgos potenciales asociados con el abuso de permisos no autorizados.

1.3.7 Herramientas y Tecnologías de Seguridad

Las herramientas y tecnologías ofrecen soluciones para resguardar los sistemas y la información ante posibles peligros y ataques.

Estas herramientas y tecnologías actúan como barreras y detectores, protegiendo los sistemas contra intrusiones, malware y otras amenazas, y asegurando que los datos estén cifrados y protegidos.

Firewall

Aunque los firewalls desempeñan un papel crucial como barrera protectora contra amenazas, es relevante subrayar que, tal como lo indican Kim y su equipo de investigación [26], estas amenazas pueden abarcar desde intrusiones maliciosas hasta ataques de denegación de servicio. Estos dispositivos de seguridad brindan la capacidad de gestionar y supervisar el flujo de tráfico en la red, garantizando que únicamente el tráfico seguro y autorizado pueda acceder a los recursos internos.

Antivirus

Los antivirus desempeñan un papel esencial en la seguridad cibernética al proteger los sistemas informáticos contra amenazas de software malicioso. En palabras de Yin et al. (2018) [27], estos programas, diseñados para detectar, prevenir y eliminar virus, gusanos, troyanos y otras formas de malware, constituyen una barrera fundamental en la defensa de los sistemas y la integridad de información. Funcionan al identificar patrones de código malicioso y supervisar comportamientos sospechosos en tiempo real. A medida que la ciberdelincuencia evoluciona constantemente, la investigación y desarrollo en esta área son cruciales para mantener la seguridad en el ciberespacio.

Software de Cifrado

El cifrado de software, un componente crucial en la protección de información y la seguridad de esta se elige un sistema de defensa inquebrantable. De acuerdo con YAO [28], mediante el uso de algoritmos avanzados, este tipo de software transforma información legible en un formato ininteligible, asegurando así que solo aquellos poseedores de la clave adecuada puedan descifrarla. Esta capacidad de ocultar datos sensibles es esencial para salvaguardar la confidencialidad de la información. Además, el cifrado de software preserva la integridad de la información durante su tránsito por redes o su resguardo en dispositivos y servicios de almacenamiento en la nube. Su relevancia en la seguridad cibernética es innegable, contribuyendo de forma efectiva a prevenir el acceso no autorizado y a contrarrestar las amenazas en línea.

1.3.8 Políticas y Procedimiento en la Universidad

Las políticas y procedimientos establecen las reglas y directrices que rigen cómo se debe manejar y proteger la información dentro una Universidad

Estas políticas y procedimientos específicos abordan temas como el uso de dispositivos personales, el acceso seguro a la red, y cómo y cuándo se deben aplicar actualizaciones y parches de seguridad.

BYOD (Bring Your Own Device)

Bring Your Own Device o BYOD es una estrategia propuesta por el director de seguridad y privacidad de Intel, Rahat Afreen [29]. Después de observar que la mayoría de los empleados traen sus propios teléfonos inteligentes, tabletas y dispositivos de almacenamiento móviles al trabajo, en lugar de preocuparse por la pérdida de seguridad de los datos empresariales y la productividad de los empleados, propuso una política para adoptar esta tendencia y utilizarla como un medio para reducir costos y aumentar la productividad.

VPN (Virutal Private Network)

Las Redes Privadas Virtuales (VPN) son una tecnología esencial en la era digital actual. Según la investigación [30], las VPN permiten a las organizaciones establecer conexiones de red seguras a través de Internet o redes públicas, asegurando la privacidad y la integridad de la información que se envía. Esta tecnología ha transformado la manera en que tanto organizaciones como individuos pueden acceder a recursos en línea de forma segura y eficaz.

Acceso Remoto

El concepto de laboratorios remotos ha generado interés en la comunidad académica y científica que se centra en la educación en línea y la utilización de Tecnologías de la Información y Comunicación (TIC) en el ámbito educativo. Por eso, es importante desarrollar y poner en marcha plataformas que posibiliten la gestión y supervisión a distancia de los laboratorios en las instituciones educativas, dentro de la enseñanza y la colaboración científica. Según Montoya y Olarte [31],"El presente artículo describe la creación de una plataforma en línea para laboratorios remotos de instrumentación física avanzada. Esta plataforma ofrece herramientas para facilitar diversas etapas del proceso en un laboratorio, como la reserva de experimentos, acceso a los contenidos y dispositivos, ejecución del experimento y gestión administrativa de los laboratorios." La declaración destaca cómo esta plataforma se basa para expandir el acceso remoto a laboratorios en Colombia por Internet y otras redes académicas de alta velocidad, lo que constituye un progreso en la educación y la ciencia del país.

1.3.9 Cultura de Seguridad

La cultura de seguridad hace relevancia a la mentalidad y actitud de una organización entorno a la seguridad, y es tan importante como las herramientas y políticas.
Estas iniciativas buscan educar y preparar a los empleados y miembros de la organización para enfrentar y responder adecuadamente a las amenazas y situaciones de seguridad.

Capacitación

La formación constante en seguridad informática es vital para fortalecer los protocolos de seguridad en las organizaciones. A continuación, se discute cómo esta capacitación es implementada y su impacto en las empresas de Chihuahua, México.

Este artículo destaca la problemática prevalente en las entidades y corporaciones del ámbito productivo en Chihuahua, México, donde la gestión de las Tecnologías de Información y Comunicación (TIC) es crucial en las organizaciones. Según Villagran-Vizcarra et al. (2018), se señala la necesidad de proporcionar formación continua al personal para fomentar una cultura de seguridad informática que contribuya a optimizar los procedimientos de seguridad en la empresa, y minimice las vulnerabilidades relacionadas con la gestión de la información.

Concienciación

La concienciación en seguridad implica entender y adherirse a las normativas para prevenir riesgos. Es esencial educar y comunicar continuamente sobre las prácticas seguras para fomentar un entorno protegido.

Simulacros

Los simulacros de emergencia, por otro lado, son ejercicios prácticos que preparan a las personas para responder eficazmente en situaciones adversas. Permiten identificar áreas de mejora y asegurar que los procedimientos de evacuación y respuesta sean conocidos y efectivos.

1.3.10 Respuestas a Incidentes

La capacidad de responder rápida y eficazmente a los incidentes de seguridad puede marcar la diferencia entre una pequeña interrupción y una gran brecha.

Estos elementos garantizan que, en caso de un incidente, la organización tenga un plan claro y efectivo para abordar la situación, minimizar el daño y recuperar la operación normal lo más rápido posible.

Protocolos

Enfocado en la seguridad informática, es crucial tener mecanismos robustos para enfrentar los desafíos que surgen de los ataques cibernéticos. En este contexto, los Equipos que responden a cualquier incidente suscitado de seguridad informática (CSIRT) desempeñan un papel fundamental. Según el documento revisado [32], Proporcionando servicios y conocimientos para enfrentar de manera eficiente dichos ataques de seguridad. Estos equipos proporcionan no solo una respuesta rápida ante incidentes de seguridad, sino también una estructura organizada que permite una gestión eficaz de los riesgos. La creación y operación eficiente de los CSIRT es un paso esencial para asegurar la integridad de los sistemas informáticos y garantizar la continuidad de sus actividades dentro de las organizaciones. Por lo tanto, es vital entender y aplicar los protocolos adecuados que guíen las respuestas a incidentes, lo que a su vez contribuye a una gestión de seguridad informática más sólida y resiliente.

Equipos de Respuesta

Los Equipos de Respuesta Táctica (ERT) son esenciales en la gestión de incidentes de seguridad, proporcionando una respuesta organizada ante situaciones adversas. A continuación, se detalla el papel del ERT en el Departamento de Gestión Tecnológica de la Universidad Santiago de Cali, ilustrando su importancia y funciones.

Se expone el papel del Equipo de Respuesta Táctica (CERT) como una unidad funcional esencial dentro del Departamento de Gestión Tecnológica para manejar de manera

integral los incidentes vinculados a la protección de datos. Según lo descrito por Carlos, la meta principal del CERT es cambiar de una postura reactiva a una proactiva lo más pronto posible [33]. Entre las responsabilidades típicas del CERT se encuentran la administración de la seguridad, manejo de incendios, control del origen del incidente y protección de la infraestructura tecnológica. Además, la composición del ERT se determinará según la naturaleza y envergadura del incidente, así como del tipo y cantidad de tareas que se requieran.

Planes de Contingencia

En situaciones de desastres mayores, tales como incendios, inundaciones, terremotos, tornados, o robos en la empresa, es esencial seguir un protocolo específico. Según Ferruzola Gómez et al., "En caso de un evento catastrófico como incendios, inundaciones, terremotos, tornados, o robo a la empresa, se deben seguir las directrices definidas en el plan de contingencia para desastres de gran escala." [34]. Este procedimiento es crucial para mitigar los daños y asegurar una recuperación eficaz post-desastre.

Recuperación de Datos

La esencia de la recuperación de datos radica en revertir la pérdida de estos. Tal pérdida puede originarse por varias razones, lo que a su vez puede llevar a diferentes métodos para su recuperación en la mayoría de las situaciones. Según Fernando Madrigal y Jessica Tortolero [35], " La recuperación de datos ocurre cuando se produce la pérdida de estos, la cual puede ser causada por diversos factores y puede implicar el uso de varios métodos para su recuperación, lo cual es común en la mayoría de los casos." En este concepto, hay varios factores que pueden hacer que se recupere información, como la eliminación accidental de archivos por errores humanos o la detección de un virus en la computadora que el software antivirus no pudo eliminar, entre otros problemas comunes. En consecuencia, la recuperación de datos involucra métodos y herramientas diseñadas para recuperar datos que contienen información crucial para realizar ciertas tareas.

1.4. Antecedentes Contextuales

En una institución, la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) es esencial para salvaguardar la confidencialidad y la integridad de los datos estudiantiles, de investigación y administrativos. Este sistema asegura la disponibilidad de la información, disminuye las amenazas de ciberataques y garantiza el cumplimiento de las regulaciones, lo que contribuye a crear un entorno de aprendizaje y trabajo seguro y confiable.

Según Calderón y Sánchez [36], esta revisión anual asegura que el sistema sigue siendo pertinente y eficiente. A partir de esta perspectiva, se consideran diversos factores, como los resultados de auditorías, comentarios de las partes interesadas, y cualquier avance técnico que pueda mejorar el SGSI. Además, se evalúan las vulnerabilidades o amenazas previamente no abordadas y se revisan las mediciones de eficacia. Cualquier cambio que pueda influir en el SGSI es también tomado en cuenta, junto con las recomendaciones para su mejora. De esta manera, la institución no solo establece un SGSI robusto, sino que también se asegura de que evolucione con el tiempo y las circunstancias cambiantes.

En concordancia con esto, el documento de la Universidad Técnica de Ambato menciona que " El modelo actual de seguridad (SGSI) debe ser sometido a un análisis y evaluación continuos en intervalos planificados para asegurar que esté cumpliendo con sus funciones

previstas. Esto garantiza una excelente gestión de la seguridad de la información en la institución." [37] .

1.4.1. Ámbito de aplicación

La presente investigación se centra en la propuesta y la creación de un sistema de gestión de seguridad de la información (SGSI). diseñado para la Universidad Técnica de Machala (UTMACH). El estudio se delimita a las siguientes condiciones y características:

Institución: La investigación se circunscribe exclusivamente a la Universidad Técnica de Machala (UTMACH), ubicada en Ecuador. No se abordan otras instituciones educativas, aunque los resultados podrían ser extrapolables.
Objetivo: El propósito principal es fortalecer la protección de los activos informáticos de la UTMACH mediante la implementación de un SGSI basado en estándares ISO y mejores prácticas.
Diagnóstico: Se realiza un diagnóstico inicial del estado actual de seguridad de la información en la UTMACH, identificando las brechas y vulnerabilidades presentes.
Adaptación de Estándares: Aunque se toman como referencia estándares internacionales como los de la ISO, estos se adaptan y personalizan al contexto y necesidades específicas de la UTMACH.
Implementación: Se seleccionan e implementan controles de seguridad en áreas físicas, técnicas y administrativas. Además, se desarrollan programas de concientización para promover una cultura de seguridad en la universidad.
Evaluación: Una vez implementado el SGSI, se evalúa su efectividad y se proponen mejoras si es necesario.
Beneficiarios: Si bien el principal beneficiario es la UTMACH, los resultados y propuestas pueden beneficiar indirectamente a estudiantes, personal académico y administrativo, y a la comunidad universitaria en general.
Consideraciones éticas: Se tiene especial cuidado en el manejo y resguardo de datos sensibles, velando por la privacidad y derechos de los individuos involucrados.
Temporalidad: Aunque la investigación se desarrolla en un periodo específico, no se menciona una fecha exacta. Sin embargo, se entiende que los datos, análisis y propuestas son relevantes para el momento en que se realiza el estudio.

1.4.2. Establecimiento de requerimientos

1. Metodología:

La norma ISO/IEC 27001 es ampliamente reconocida y empleada globalmente para la gestión de la seguridad de la información. Este estándar define los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI) y se fundamenta en un enfoque de gestión de riesgos.

El Ciclo Deming [38], El ciclo PDCA, también llamado Planificar-Hacer-Verificar-Actuar, está vinculado a la norma ISO 27001. Esta metodología es utilizada para la mejora continua de la gestión de la calidad y debe ser empleada para implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) de acuerdo con los requisitos de la norma ISO 27001. La Figura 5 se grafica las etapas, y a continuación se describe las distintas etapas del ciclo PDCA:

- **Planificar:** Durante esta fase, los objetivos y procesos necesarios para entregar resultados se establecen en función de los requisitos del cliente y las políticas organizacionales. Esto conlleva a identificar los requisitos de seguridad de la información, evaluar los riesgos y definir los controles necesarios para mitigar o gestionar esos riesgos.
- **Hacer:** Implementar el proceso definido durante la fase de planificación. Esto sugiere implementar los controles y otras medidas definidas durante la fase de planificación.
- **Evaluar:** Supervise y mida los procesos y resultados en comparación con políticas, objetivos y requisitos, e informe los resultados. Esto requiere monitorear y revisar el desempeño del SGSI, incluida la revisión de incidentes de seguridad de la información y la efectividad de los controles.
- **Actuar:** Tomar medidas para mejorar continuamente el rendimiento del proceso. Esto refleja tomar medidas para resolver no conformidades e identificar oportunidades de mejora para mejorar continuamente la eficacia y eficiencia del SGSI.

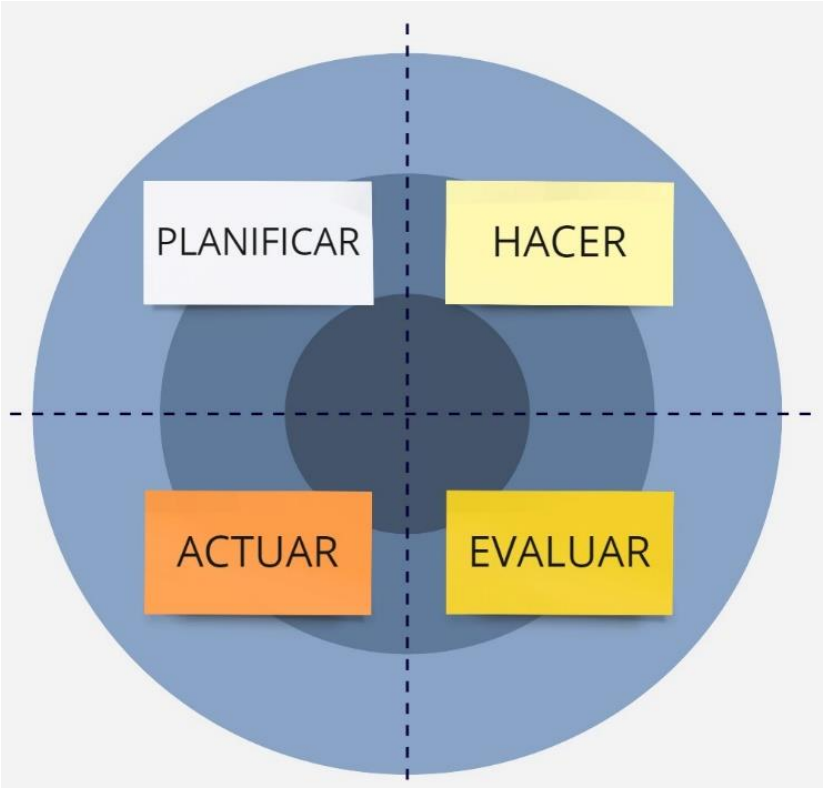


Figura 5 Etapas del Ciclo Deming

La aplicación del ciclo PDCA ayuda a las organizaciones a garantizar que su SGSI sea eficaz y se mantenga al tanto de los cambios en los riesgos de seguridad de la información y otros factores relevantes.

Respecto a la matriz de riesgos que se realizó, esta lleva a cabo la metodología ISO 31000, que fue adaptado paralas necesidades del Politécnico Colombiano Jaima Isaza Cadavid [39], esta institución pone a disposición los mapas de riesgos en su administración de riesgos.

Respecto a la Metodología: La metodología destinada a la gestión del riesgo demanda una evaluación preliminar vinculada con la situación presente de la estructura de riesgos y su administración en la entidad, comprendiendo la misma desde una perspectiva estratégica mediante la ejecución de tres (3) pasos esenciales para su evolución. Además, implica la formulación e implementación de estrategias de comunicación que se extienden a lo largo de toda la entidad, para así poder manifestar su eficacia. A continuación, en la Figura 6, se presenta la estructura integral junto con sus fundamentos básicos:

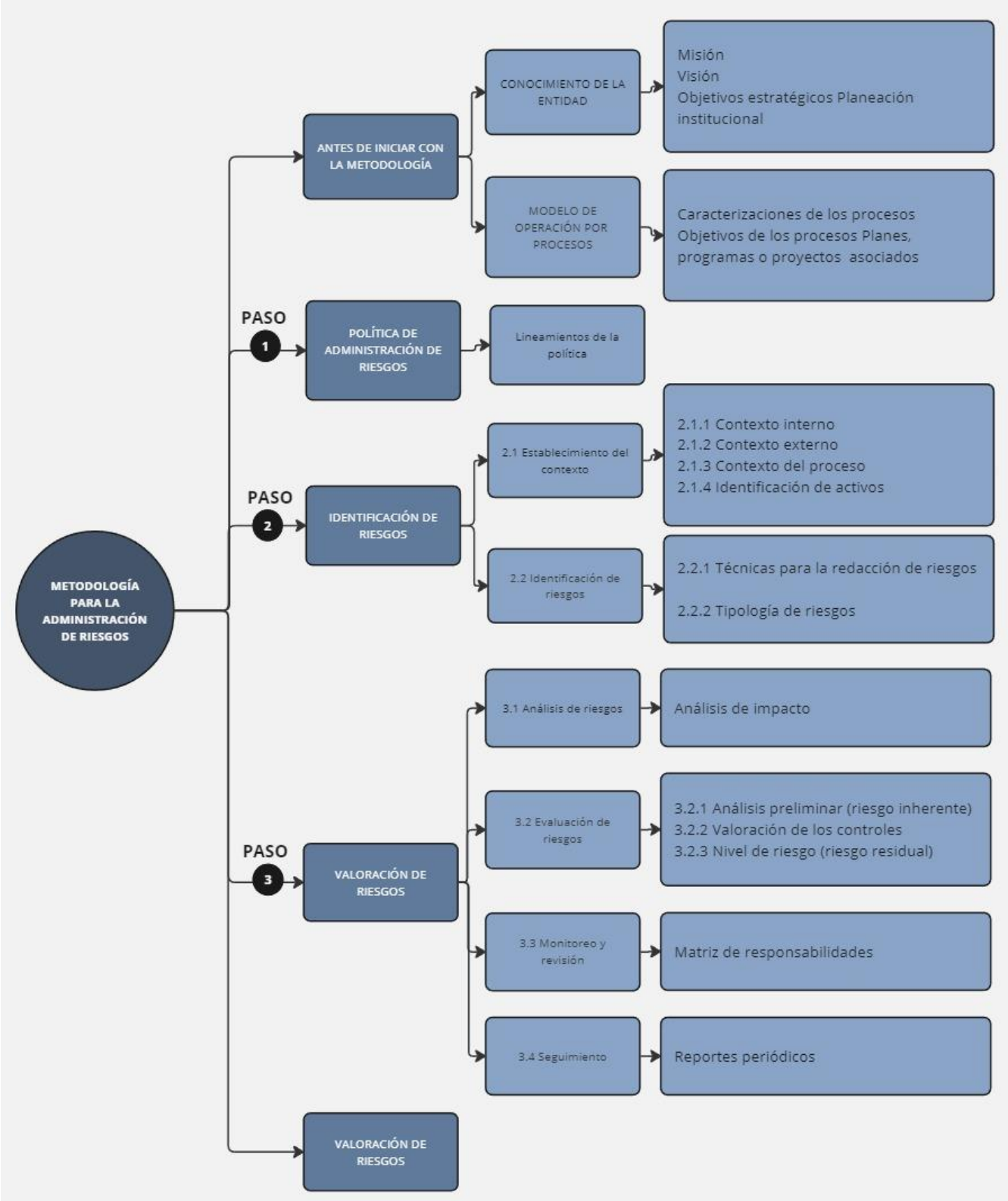


Figura 6 Metodología para la administración del riesgo [39]

2. Identificar necesidades:

Luego de una serie de entrevistas con personal clave de la Universidad Técnica de Machala (UTMACH), incluyendo a responsables técnicos y administrativos, así como un exhaustivo análisis de la literatura relevante, se identifican necesidades críticas:

- **Protección de Información Sensible:** La UTMACH alberga datos confidenciales que requieren salvaguarda contra amenazas, tanto externas como internas. Este aspecto subraya la importancia de un sistema de seguridad robusto.
- **Alineación con Estándares Internacionales:** Podría existir una preocupación acerca de que los sistemas actuales no cumplan con los estándares internacionales de seguridad, lo cual podría representar riesgos significativos.
- **Conciencia de Seguridad en la Comunidad Universitaria:** Se detecta una posible falta de conocimiento o información entre profesores, estudiantes y personal acerca de las prácticas recomendadas de seguridad, lo que podría incrementar la vulnerabilidad a ataques o errores.

3. Definir criterios:

Con base en las necesidades identificadas, se establecen los siguientes requerimientos:

- Evaluar y documentar los sistemas actuales y sus vulnerabilidades.
- Seleccionar estándares internacionales adecuados para la UTMACH
- Elaborar un plan para la implementación de las mejores prácticas identificadas.

4. Priorizar:

Dada la importancia de proteger la información desde ya, se decide que la identificación de vulnerabilidades en los sistemas actuales es prioritaria. Seguido de la implementación de buenas prácticas.

5. Documentar:

Se redacta un documento integral que detalla todos los requerimientos y criterios, incluyendo descripciones específicas de cada uno. Además, se establece un orden de prioridades para abordar los diferentes aspectos identificados.

6. Revisar y ajustar:

Ante los hallazgos obtenidos durante la fase inicial de evaluación de los sistemas actuales en la Universidad Técnica de Machala (UTMACH), se propone una revisión y ajuste estratégico del plan de seguridad de la información.

2. CAPÍTULO II. DESARROLLO DEL PROTOTIPO

2.1. Definición del prototipo

Nombre: Sistema de Gestión de Seguridad de la Información (SGSI) para la UTMACH
Descripción: El prototipo consistirá en una propuesta de Sistema de Gestión de Seguridad de la Información adaptado específicamente a las necesidades y contexto de la Universidad Técnica de Machala. Este SGSI incluirá los siguientes componentes fundamentales:

- **Políticas y procedimientos de seguridad:** Se formularán políticas, estándares y procedimientos que regulen las prácticas de seguridad de la información en la UTMACH basándose en la Política de Ciberseguridad del Ecuador.
- **Análisis y evaluación de riesgos:** Se realizará un análisis de riesgos exhaustivo considerando activos, amenazas, vulnerabilidades, impacto y probabilidad, fundamentado en la ISO 31000 adaptado a la matriz de riesgos del Politécnico Colombiano Jaima Isaza Cadavid.
- **Selección de controles de seguridad:** Se seleccionarán y propondrán controles de seguridad administrativos, técnicos y físicos apropiados para la UTMACH, estos controles se basarán en la INEN-ISO/IEC 27002 sección 10, sobre la base del análisis de riesgos.
- **Gestión de continuidad y contingencia a incidentes:** Se desarrollarán planes de continuidad y contingencia a incidentes de seguridad apoyándose en la sección 14 de la INEN-ISO/IEC 27002.

Tecnologías:

- El prototipo se apoyará substancialmente en la utilización de documentos de texto, hojas de cálculo, software de elaboración de presentaciones, y herramientas dedicadas al modelado de procesos. Estos recursos serán fundamentales para la estructuración y representación de la información, así como para la delineación precisa de los procesos involucrados en el desarrollo del prototipo.
- Durante las fases de desarrollo, se hará uso de plataformas virtuales para facilitar las reuniones de trabajo colaborativo. Estas plataformas permitirán la interacción en tiempo real entre los miembros del equipo, promoviendo un entorno colaborativo y eficiente, lo cual es crucial para el avance coherente y coordinado del proyecto.
- En lo que respecta a la integridad y seguridad del prototipo, se proponen algunos controles técnicos que podrían incorporar tecnologías de seguridad avanzadas. Entre estas tecnologías de cifrado, que asegurarán la confidencialidad y la integridad de la información manejada.

En la Figura 6, se ilustra de manera gráfica el proceso de definición del prototipo, tomando en consideración los aspectos tecnológicos mencionados anteriormente. Esta representación visual facilita la comprensión del enfoque adoptado para el desarrollo del prototipo, y cómo las tecnologías seleccionadas se integran en cada etapa del proceso, contribuyendo así al éxito del proyecto.

Figura 7 Esquema grafico de la definición del prototipo

2.2. Metodología de desarrollo del prototipo

2.2.1. Enfoque, alcance y diseño de investigación

Enfoque de la investigación

La investigación acerca de la gestión de seguridad de la información en la UTMACH se llevará a cabo utilizando un enfoque de investigación mixto. Este enfoque integra métodos cuantitativos y cualitativos, con el fin de brindar un panorama amplio y detallado del fenómeno objeto de estudio.

Desde una perspectiva cuantitativa, el presente estudio se enfocará en la recopilación de información numérica que permitirá evaluar la efectividad de los sistemas de seguridad implementados. Este proceso se llevará a cabo mediante la utilización de indicadores tales como el número de incidentes de seguridad, la frecuencia y tipos de amenazas, y el grado de cumplimiento de las normativas. Asimismo, se evaluará el impacto de los estándares y buenas prácticas, realizando una comparación entre los datos obtenidos antes y después del análisis.

Desde una perspectiva cualitativa, se llevará a cabo la recolección con análisis textuales y discursivos con el objetivo de comprender las experiencias, percepciones y opiniones. Para lograr esto, se realizarán encuestas en profundidad, grupos de discusión y análisis de documentos de política. Este enfoque permitirá comprender cómo los estándares y buenas prácticas pueden adaptarse y aplicarse de manera efectiva en el contexto específico de la UTMACH.

Por último, se procederá a la integración y análisis de los datos cuantitativos y cualitativos recopilados. A través de esta integración, se podrán realizar inferencias más exhaustivas y sólidas, se brindarán recomendaciones prácticas y respaldadas por evidencia para mejorar la protección de la información en la universidad. En términos generales, el objetivo de esta aproximación mixta es proporcionar una visión más amplia y contextualizada del fenómeno en estudio, y generar recomendaciones efectivas y viables para la aplicación práctica.

Alcance de la investigación

En el presente estudio se ha decidido adoptar un enfoque mixto, utilizando diversas etapas de alcance de investigación, con el propósito de abordar de manera integral.

La primera fase del proyecto, se llevará a cabo un enfoque exploratorio y descriptivo. El propósito de esta etapa es adquirir conocimiento sobre la situación, con el fin de obtener una comprensión más profunda de las condiciones actuales y destacar posibles áreas de riesgo y vulnerabilidad. Para lograr este objetivo, se recopilarán y analizarán datos tanto cualitativos como cuantitativos. Los datos cualitativos se obtendrán a través de del análisis de documentos existentes y entrevistas realizadas al personal, lo que permitirá describir las prácticas actuales y ofrecer una perspectiva detallada de las percepciones y actitudes. Además, los datos cuantitativos se obtendrán mediante encuestas, lo cual proporcionará medidas objetivas.

En la segunda fase se adopta un enfoque correlacional y explicativo. Proponiendo las políticas de seguridad, y a un plan de contingencia que ayude en el control de

problemas de seguridad de la información dentro del Área de TIC's. El objetivo en esta etapa es comprender las relaciones entre distintos aspectos, como, por ejemplo, la relación entre el nivel de capacitación del personal, o la relación entre los controles específicos de seguridad y la percepción de seguridad de la información. Este enfoque nos permite determinar la magnitud y dirección de las relaciones entre las variables, así como inferir posibles relaciones causales.

Diseño de la investigación

El presente estudio sigue un diseño secuencial explicativo con un componente concurrente. Este diseño ha sido seleccionado con el objetivo de optimizar la comprensión del fenómeno de estudio y garantizar la recopilación y análisis de datos de forma sistemática y coherente.

En la primera fase del diseño secuencial, se realiza el componente cualitativo del estudio. Esta fase inicial permite explorar en profundidad las prácticas y percepciones actuales. Los hallazgos de este componente cualitativo informarán la elaboración de la encuesta cuantitativa, que se utiliza en la segunda fase del diseño secuencial para recoger datos de una muestra más amplia. Esta secuencia permite validar y generalizar los hallazgos cualitativos, proporcionando un panorama más amplio y representativo del estado de la seguridad.

Durante el transcurso de este proceso, también se implementa un enfoque concurrente en el diseño. Esto implica que, mientras se recolectan y analizan los datos cuantitativos, se continúa con los datos cualitativos a través de entrevistas y análisis de documentos. Esta estrategia posibilita que los descubrimientos cualitativos emergentes puedan contribuir a la explicación de los resultados cuantitativos, mejorando de esta manera la comprensión del fenómeno y permitiendo una interpretación más detallada y precisa de los resultados.

Este enfoque mixto y diseño de investigación permiten un abordaje integral. Este diseño también es adecuado para manejar la complejidad y los múltiples aspectos de SGSI en la UTMACH, ofreciendo una comprensión sólida y detallada que puede informar decisiones futuras.

2.2.2. Unidades de análisis

Población (universo)

La población de este estudio se define como todas las partes interesadas relevantes y los sistemas informáticos dentro la UTMACH. Esta población se divide en tres categorías principales:

1. Personal de la universidad: Este grupo de la población engloba a todos los miembros del personal de la UTMACH, desde el personal docente hasta el personal administrativo y el equipo de soporte técnico. Cada individuo que forma parte de esta categoría tiene algún nivel de interacción con la información de la universidad. El personal administrativo, por ejemplo, tiene acceso a los datos académicos, mientras que el personal administrativo y técnico interactúa con una variedad de

datos que pueden incluir datos financieros, datos personales de estudiantes y personal, entre otros.

2. Usuarios de los sistemas: Este grupo abarca a todos los usuarios de los sistemas y servicios de información, desde estudiantes hasta personal docente y administrativo. Como usuarios, su comportamiento y entendimiento de las políticas son cruciales para el estado general de la seguridad.
3. Sistemas de información de la universidad: Esta categoría incluye todas las infraestructuras de TI y sistemas de información utilizados para manejar, almacenar, transmitir y recuperar la información en la universidad. Esto puede incluir desde sistemas de administración de bases de datos hasta redes informáticas y servidores.

Muestra

No se consiguió muestra, ya que se operó con el total de integrantes de la población.

2.2.3. Técnicas e instrumentos de recopilación de datos

Tabla 4 Técnicas e instrumentos de recopilación de datos

TÉCNICA	INSTRUMENTO
ENTREVISTAS	Guía de entrevista
ENCUESTAS	Cuestionario
OBSERVACIÓN	Lista de verificación
REUNIONES	Puntos de discusión en la reunión

Cada uno de estos instrumentos de la Tabla 4, será diseñado y refinado para adaptarse a las necesidades específicas de esta investigación, asegurando que se recopile información precisa y útil que contribuya a alcanzar los objetivos del estudio.

2.2.4. Técnicas de procesamiento de datos para la obtención de resultados

Tabla 5 Técnicas de procesamiento de datos para la obtención de resultados

TÉCNICA	CONCEPTO
ANÁLISIS DE ENCUESTAS	Los datos obtenidos a través de las encuestas se procesarán y analizarán utilizando herramientas estadísticas. Inicialmente, se realizará una limpieza de datos para asegurar la calidad y precisión de los datos recogidos. Esto incluirá el uso de: • Cuadros de frecuencias absolutas y relativas: Se usarán para obtener una descripción general del conjunto de datos, resumiendo la información y permitiendo la identificación de patrones y tendencias. • Gráficos de barras simples: Permitirán visualizar de manera efectiva la frecuencia de las respuestas y comparar categorías diferentes de respuestas.

	• Estadísticos principales: Se calcularán la media, la desviación estándar, la varianza, el rango y el coeficiente de variación para las respuestas cuantitativas en las encuestas, proporcionando una comprensión clara de la distribución de los datos. • Pruebas de preguntas de investigación: Dependiendo del objetivo de la investigación, se podrían utilizar pruebas para comparar las respuestas de diferentes grupos de la población (por ejemplo, personal administrativo vs. docentes), o para evaluar la relación entre diferentes variables.
ANÁLISIS DE ENTREVISTAS	• Las entrevistas se grabarán y transcribirán para un análisis detallado. Se utilizará el análisis de contenido para identificar temas y patrones recurrentes en las respuestas de los entrevistados. • Este proceso se realizará de manera iterativa, donde los temas se identificarán y refinados a medida que se analicen más entrevistas. Se crearán códigos para representar estos temas. • Se realizarán análisis adicionales para identificar cualquier relación entre los temas y para explorar cualquier diferencia en las respuestas de diferentes grupos de participantes.
ANÁLISIS DE OBSERVACIONES	• Las observaciones se realizarán utilizando un instructivos de pasos de observación estructurada, que se utilizará para registrar comportamientos • Estos datos serán analizados cualitativamente para identificar patrones y tendencias en los comportamientos observados. • Además, los datos de las observaciones pueden ser codificados y analizados cuantitativamente si es apropiado.
ANÁLISIS DE REUNIONES	• Las notas de las reuniones y las grabaciones (si están disponibles) se revisarán para identificar los temas de discusión, las decisiones tomadas y cualquier acción identificada. • Este análisis informará sobre el progreso del proyecto y ayudará a identificar cualquier problema o barrera que pueda necesitar ser abordada.
TÉCNICAS DE APRENDIZAJE AUTOMÁTICO	• Si los datos recogidos son suficientemente grandes y variados, se podrían aplicar técnicas de aprendizaje automático para identificar patrones y relaciones que podrían no ser

	evidentes a través del análisis estadístico tradicional. • Por ejemplo, podrían aplicarse técnicas de análisis de sentimientos a las respuestas de texto libre en las encuestas para obtener una comprensión más matizada de las actitudes de los encuestados. • Además, los algoritmos de aprendizaje automático pueden ser útiles para predecir el comportamiento futuro basándose en los datos históricos, lo que puede ser útil para anticipar y mitigar los riesgos.

Todos los análisis de la Tabla 5, se llevarán a cabo utilizando software estadístico, como Microsoft Forms, Excel, SPSS, R, Python y/o NVivo, y se seleccionarán en función de la naturaleza de los datos y los objetivos de la investigación.

2.2.5. Metodología o métodos específicos

Con el fin de alcanzar los objetivos planteados en este estudio y desarrollar un sistema integral, se empleará una combinación de la metodología de análisis y gestión de riesgos, y el marco de gestión de seguridad de la información propuesto por estándares y buenas prácticas, teniendo también en cuenta la familia de la ISO 27000 además de otros estándares como la ISO 31000 y la normativa de ciberseguridad del Ecuador. Estas metodologías son ampliamente reconocidas a nivel internacional y habitualmente utilizadas en la gestión de la seguridad de la información.

1. Fase de Análisis y Evaluación de Riesgos

    - Identificación de los Activos de Información: En esta etapa se identificarán y clasificarán los activos de información que son críticos para la universidad. Esto incluye tanto los activos tangibles como los intangibles.
    - Identificación de Amenazas y Vulnerabilidades: Una vez identificados plenamente los activos, la siguiente parte a seguir es identificar las amenazas y vulnerabilidades que podrían impactar en estos activos. Las amenazas pueden ser tanto internas como externas, y las vulnerabilidades pueden ser debilidades inherentes o debilidades introducidas por deficiencias en los controles de seguridad existentes.
    - Evaluación de Riesgos: procederemos a llevar a cabo la pertinente evaluación de riesgos. Dicha evaluación consistirá en determinar la probabilidad de que una amenaza llegue a explotar una vulnerabilidad y el impacto potencial que ello supondría para los activos de información pertenecientes a nuestra institución universitaria. Mediante la realización de esta evaluación de riesgos, lograremos establecer una jerarquía en cuanto a los riesgos de seguridad de la información, estableciendo claramente cuáles son aquellos que demandan una atención inmediata.

2. Fase de evaluación y Gestión

- Formación y Sensibilización: Se realizarán actividades de formación y sensibilización para el personal y los usuarios de la universidad. El objetivo es crear una cultura de seguridad sólida en toda la universidad.
- Establecimiento de un Marco de Respuesta a Incidentes de Seguridad de la Información: Se desarrollará un marco de respuesta a incidentes de seguridad de la información.

2.2.6. Herramientas y/o Materiales

Para lograr los objetivos de la investigación, será fundamental contar con una serie de herramientas y/o materiales que faciliten la recolección de datos, El estudio, la divulgación y la valoración de las propuestas. Las herramientas se dividen en las siguientes categorías:

1. Herramientas Software:
    - Software de Encuestas: Plataformas como Microsoft Forms, SurveyMonkey o Typeform serán esenciales para crear y distribuir cuestionarios en línea a la población de estudio. Estas herramientas también proporcionan funciones útiles para recopilar y analizar las respuestas.
    - Herramientas de Análisis de Datos: Se utilizarán aplicaciones como Microsoft Excel para organizar, clasificar y analizar los datos recolectados. Además, el software estadístico como SPSS o R será útil para realizar análisis más complejos, como la correlación y regresión, que podrían ser necesarios para entender completamente la información recolectada.
    - Herramientas de Videoconferencia: Las herramientas de videoconferencia como Zoom, Microsoft Teams o Google Meet permitirán llevar a cabo entrevistas de manera remota, lo que facilita la participación de aquellos que se encuentran en diferentes ubicaciones o que tienen horarios de trabajo apretados.
    - Software de Grabación de Audio: Aplicaciones como Audacity o Voice Recorder se utilizarán para grabar las entrevistas, ya sea en persona o a través de videoconferencias, para asegurar la precisión y permitir un análisis posterior más detallado.
    - Gestión de Proyectos y Herramientas de Colaboración: Herramientas como Microsoft Teams, Trello, Asana, Slack u One Drive ayudarán a coordinar y monitorear el progreso del proyecto, facilitar la comunicación entre el equipo de investigación, y organizar documentos y recursos.

2. Materiales Físicos:
    - Dispositivo de Grabación de Audio: Un grabador de audio de alta calidad será útil para grabar las entrevistas en persona, asegurando que todos los detalles se capturen claramente para su posterior análisis.
    - Equipos Informáticos: Ordenadores portátiles y de escritorio con acceso a internet y software relevante serán necesarios para llevar a cabo la investigación.
    - Material de Oficina: Se requerirán diversos suministros de oficina, como papel, bolígrafos, lápices, carpetas, y equipos de impresión y escaneo, para

documentar la investigación, organizar la información, y preparar informes y presentaciones

3. Recursos Humanos:
    - Personal: El personal jugará un papel crucial en la recogida de datos a través de entrevistas y encuestas.
    - Equipo de investigación: El equipo de investigación, formado por el investigador principal y posiblemente otros miembros, será responsable de llevar a cabo la investigación.

4. Recursos Documentales:
    - Normativas de la familia ISO 27000, ISO 31000 y el marco de ciberseguridad del Ecuador: Estas normas internacionales proporcionará la estructura y las directrices. Se requerirá copias completas y actualizada de las normas para su consulta durante la investigación.
    - Documentos internos de la Universidad: Los documentos internos de la universidad, como las políticas y procedimientos existentes, los planes estratégicos y los informes de auditoría, serán valiosos para entender el contexto actual.
    - Estas herramientas y materiales no solo facilitarán la recopilación y el análisis de los datos, sino que también ayudarán a que el sistema de gestión de seguridad de la información propuesto sea relevante, aplicable y eficaz para la Universidad Técnica de Machala.

2.3. Desarrollo del prototipo

El desarrollo de la propuesta del Sistema de Gestión de Seguridad de la Información (SGSI) para la UTMACH, se desarrolló la matriz de riesgos y los controles, esta se llevó a cabo en varias fases:

Fase 1 - Diagnóstico inicial:

Se realizó un diagnóstico un análisis detallado de la situación actual de la seguridad de la información en la UTMACH, que incluyó las técnicas y los activos de la Tabla 6:

Tabla 6 Técnicas y activos del diagnóstico inicial

TÉCNICA	ACTIVOS
REVISIÓN	Políticas y procedimientos de seguridad existentes.
ANÁLISIS	Documentos y registros para detectar debilidades y oportunidades de mejora.
ENTREVISTAS	Personal clave para comprender procesos y controles actuales.
ENCUESTAS	Personal para conocer su percepción y cumplimiento de medidas de seguridad.
EVALUACIÓN	Técnica de infraestructura informática para identificar vulnerabilidades. Los hallazgos permitieron tener una línea base sólida para diseñar el SGSI requerido.

Fase 2 - Adaptación de estándares y análisis de riesgos:

Se seleccionó la familia de estándares ISO 27000 como marco de referencia para el SGSI, ISO 31000 como marco de referencia para la matriz de riesgos y vulnerabilidades, y el marco de ciberseguridad del Ecuador para las políticas. Estos estándares internacionales fueron cuidadosamente adaptados a la realidad de la UTMACH. Sobre esta base se realizó un análisis de riesgos exhaustivo, evaluando en detalle la probabilidad e impacto de diversas amenazas y vulnerabilidades sobre los principales activos informáticos.

Este análisis de riesgos fue crucial para determinar los controles de seguridad requeridos.

Fase 3 - Selección y propuesta de controles de seguridad:

Considerando las necesidades específicas de la UTMACH y los resultados del análisis de riesgos, se seleccionaron controles de seguridad administrativos, técnicos y físicos apropiados, descritas en la Tabla 7:

Tabla 7 Tipos de controles de seguridad

CONTROLES DE SEGURIDAD
Políticas y procedimientos para clasificación y manejo de información sensible.
Tecnologías de protección perimetral (firewalls, ips).
Autenticación y autorización robusta de usuarios.
Soluciones de respaldo y recuperación ante desastres.
Controles de acceso físico a centros de datos.
Cifrado de información crítica.
Monitoreo y detección de amenazas.

Fase 4 – Concientización y capacitación:

Se diseñó un programa de concientización, definidos en la Tabla 8, en seguridad de la información dirigido a todos los miembros de la comunidad universitaria. Este incluyó:

Tabla 8 Programa de Concientización

PROGRAMA DE CONCIENTIZACIÓN
Campañas informativas para resaltar la importancia y responsabilidades compartidas en seguridad de la información.
Capacitaciones presenciales y virtuales sobre políticas y buenas prácticas de seguridad.
Evaluaciones periódicas para medir efectividad y retroalimentación.

Fase 5 – Evaluación y mejora continua:

Una vez que la propuesta del SGSI se presentó en el área de TIC, se realizó una evaluación integral mediante una encuesta a expertos para determinar su efectividad, La metodología de valoración por expertos se centra en seleccionar especialistas con experiencia y conocimiento en la administración de seguridad informática.

Estos expertos investigan y analizan el prototipo, aportando puntos de vista, comentarios y sugerencias derivados de su bagaje profesional. Dicha metodología resulta efectiva para este género de prototipos gracias a su aproximación objetiva y cimentada en experiencias

y conocimientos previos, y utilizando la escala de Likert, que es adecuada para este tipo de evaluación porque permite medir actitudes y percepciones de manera detallada, lo que facilita una evaluación exhaustiva y completa del esquema propuesto, midiendo el cumplimiento de políticas y procedimientos, objetivos de control, e indicadores como cantidad de incidentes o vulnerabilidades detectadas.

Sobre esta base se desarrolló un plan de mejora continua, que incluye revisiones regulares, auditorías, actualización de controles y capacitaciones de refuerzo. Esto asegura que el SGSI se mantenga alineado con las mejores prácticas y la evolución de amenazas.

2.4. Ejecución del prototipo

La presentación del prototipo del Sistema de Gestión de Seguridad de la Información (SGSI) para la UTMACH se realizó en reuniones, Anexo1, detallando los aspectos de la matriz con sus respectivos puntos a tomar en cuenta. Se realizo la matriz de riesgos usando los activos del área de TI, además su respectivo análisis de riesgo con sus controles, que se pueden revisar en el Anexo 4.

El prototipo del SGSI para la UTMACH, como se detalla en el Anexo 3, abarca una estructura integral que define el propósito y alcance del documento, alineándose con las normativas pertinentes. En el contexto de la organización, se abordan aspectos cruciales como el entendimiento de la organización y su contexto, las necesidades y expectativas de las partes interesadas, y la definición del alcance del SGSI. El inventario de activos es exhaustivo, clasificando y asignando propiedad a cada activo de información. La sección de análisis y evaluación de riesgos se centra en identificar amenazas y vulnerabilidades, evaluar impactos y probabilidades, y determinar niveles de riesgo. Esto conduce a un tratamiento de riesgos meticuloso, proponiendo controles específicos. La operación del SGSI implica políticas de seguridad propuestas y aprobadas, y mejoras continuas. Finalmente, se aborda la gestión de contingencia y la continuidad del negocio, crucial para la resiliencia organizacional.

El Plan de Contingencia, presentado en el Anexo 4, Se centra en garantizar la continuidad y la integridad de los procesos tecnológicos críticos de la UTMACH. La evaluación de riesgos tecnológicos es fundamental al permitir la identificación y la mitigación proactiva de los posibles riesgos. Se elaboran estrategias de contingencia detalladas, que incluyen la identificación de equipos y recursos necesarios para una respuesta eficaz.

3. CAPÍTULO III. EVALUACIÓN DEL PROTOTIPO

3.1. Plan de evaluación

PLAN DE CONFORMIDAD DEL PROTOTIPO

Tema de trabajo de titulación: Gestión de la seguridad y protección de la información de la UTMACH mediante estándares y buenas prácticas.
Autores: Diaz Quezada Iván Fabricio, Ramirez Samaniego Elian Josué
Tutor: Ing. Loja Mora Nancy Loja, Mg. Sc.
Cotutor: Ing. Sist. Rivas Asanza Wilmer Braulio, Phd

Objetivo General

Desarrollar un plan de conformidad para el prototipo de Sistema de Gestión de Seguridad de la Información (SGSI) en la Universidad Técnica de Machala (UTMACH), asegurando su alineación con las buenas prácticas.

Objetivos Específicos

- Evaluación de Contexto y Alcance: Determinar el alcance de la implementación del SGSI (Sistema de Gestión de Seguridad de la Información) según las necesidades específicas de la UTMACH.
- Evaluación de Controles: Revisar y evaluar las mejoras en los controles propuestos de seguridad.
- Cumplimiento y Mejora Continua: Evaluar el cumplimiento del SGSI con los y establecer un proceso de plan de contingencia.
- Elaborar un Informe de Evaluación: Documentar los hallazgos, recomendaciones y áreas de mejora identificadas durante la evaluación, proporcionando una visión clara del estado actual de seguridad de la información en la UTMACH.

Planificación

Actividades	Semana 10 15-01-2024 19-01-2024	Semana 11 22-01-2024 26-01-2024	Semana 12 29-01-2024 02-02-2024	Semana 13 05-02-2024 09-02-2024
Definir objetivos, cronograma, herramientas y técnicas del plan de evaluación. Seleccionar el grupo de expertos. Diseñar las encuestas a utilizar y distribuirlas.				
Recopilar, revisar y analizar las respuestas de las encuestas, con la finalidad de identificar preocupaciones comunes y recomendaciones.				
Entrevistar a algunos expertos con el objetivo de profundizar en sus respuestas y recomendaciones.				
Redactar los hallazgos de las encuestas y entrevistas en el capítulo III del trabajo de titulación.				

Alcance del SGSI

Este documento tiene como propósito establecer un marco formal para el Sistema de Gestión de Seguridad de la Información (SGSI) de la Universidad Técnica de Machala. El objetivo es proteger la confidencialidad, integridad y disponibilidad de los datos estudiantiles, de investigación y administrativos, minimizar los riesgos de seguridad y asegurar el cumplimiento de las normativas aplicables.

Referencias Normativas

El Sistema de Gestión de Seguridad de la Información (SGSI) se basa en las directrices y normas reconocidas por la ISO/IEC 27001. Se siguen los principios para gestionar riesgos, elegir controles de seguridad y promover mejoras continuas, tal como lo establece la ISO 27002. Esto garantiza un enfoque organizado y sólido para proteger la información. Al igual que se fundamenta en la ISO 31000 para el desarrollo de la matriz de riesgos, donde se evalúo los activos

para determinar su nivel de riego, a los activos de mayor riesgo se propuso controles que ayuden a mitigar el riesgo del activo, y el marco de ciberseguridad de telecomunicaciones del Ecuador para su propuesta de políticas que ayuden al área de TIC a minimizar y controlar las actividades dentro del negocio.

Contexto de la Organización

La falta de un sistema de gestión de seguridad pone a la UTMACH en riesgo, expuesta a vulnerabilidades y riesgos que podrían poner en peligro la confidencialidad, integridad y accesibilidad de los datos institucionales. Además, esta situación podría conducir a consecuencias perjudiciales como el acceso no autorizado, la pérdida de datos, la interrupción de servicios, el daño a su reputación y posibles repercusiones legales.

Liderazgo y Compromiso:

Política de seguridad de la información

La política de seguridad de la información articula el compromiso de la institución con la seguridad de la información. Define el marco para establecer objetivos de seguridad y establece la dirección general para la protección de la información.

La Universidad Técnica de Machala (UTMACH) dispone de un departamento de Tecnologías de la Información y Comunicación (TIC) encargado de administrar la infraestructura tecnológica asociada a los sistemas y recursos de información. Sin embargo, este departamento enfrenta una falta de documentación y procedimientos estandarizados para la gestión y mantenimiento de la seguridad de dicha infraestructura y los activos de información. Asimismo, se identifica la ausencia de un sistema de gestión de seguridad de la información, planes de contingencia y continuidad de negocio ante incidentes o desastres que puedan impactar la confidencialidad, integridad y disponibilidad de los activos de información.

Roles, responsabilidades y autoridades en la organización

El Departamento de Tecnologías de la Información y Comunicación ha establecido su misión, visión y estrategias para garantizar el uso eficiente de sus recursos y la entrega oportuna y efectiva de las tecnologías de la información. El personal colaboró en este documento, según se detalla en el punto 3.2 del Sistema de Gestión de Seguridad de la Información de la Universidad Técnica de Machala, a través de sus líderes de área, capacitados para responder efectivas a las consultas institucionales.

Gestión de Activos

Los activos se recolectaron mediante la documentación de las respectivas Unidades del Departamento de TIC’s, en esta labor ayudaron los respectivos jefes de área a brindar detalladamente la información de los activos para que se pueda llevar a cabo el prototipo de SGSI. Los activos documentados hasta diciembre del 2023 en funciones, estos activos están definidos en el punto 4.1 del Sistema de Gestión de Seguridad de la Información de la Universidad Técnica de Machala.

Evaluación de Riesgos y Análisis

La evaluación de riesgos y análisis se detalla en los puntos 5 y 6 del Sistema de Gestión de Seguridad de la Información de la Universidad Técnica de Machala.

Controles de Seguridad

Se propone una serie de medidas de control basadas en la normativa ISO/IEC 27002. Esta norma internacional proporciona un conjunto extenso de controles de seguridad detallados en los puntos

7 y 8 del Sistema de Gestión de Seguridad de la Información de la Universidad Técnica de Machala, organizados en diferentes secciones, para la gestión efectiva de los riesgos de seguridad de la información. Especialmente relevante para la UTMACH es la Sección 10, dedicada a la Gestión de Comunicaciones y Operaciones. Esta sección ofrece un marco de referencia para identificar y aplicar los controles de seguridad adecuados en el ámbito de la gestión de las operaciones y las comunicaciones. Por tanto, se sugiere que la UTMACH evalúe y considere estos controles específicos, con el objetivo de fortalecer su infraestructura de TIC y asegurar la integridad, disponibilidad y confidencialidad de su información.

Políticas de Seguridad y Operación del SGSI

La descripción de las políticas y procedimientos del SGSI se encuentra detallada en el punto 9 del Sistema de Gestión de Seguridad de la Información de la Universidad Técnica de Machala.

Gestión de Incidentes y Mejoras

Detallado en el punto 10 del Sistema de Gestión de Seguridad de la Información de la Universidad Técnica de Machala.

Herramientas y Técnicas

La evaluación de conformidad se centra en recolectar la debida aprobación dentro del departamento de TIC. De manera preferencial a los jefes de cada unidad, estos investigan y analizan el prototipo, aportando puntos de vista, comentarios y sugerencias derivados de su bagaje profesional. Dicha evaluación resulta efectiva para este género de prototipos, gracias a su aproximación objetiva y cimentada en experiencias y conocimientos previos, lo que facilita una evaluación exhaustiva y completa del esquema propuesto.

Criterios de evaluación:

La escala de Likert es adecuada para este tipo de evaluación porque permite medir actitudes y percepciones de manera detallada. Ofrece una gama de opciones que van desde el acuerdo total hasta el desacuerdo total, permitiendo a los encuestados expresar su opinión con precisión. Esta escala es útil para analizar tendencias y patrones en las respuestas, facilitando la identificación de áreas de fortaleza y mejora en la implementación del SGSI. Además, los datos recopilados mediante esta metodología pueden ser fácilmente cuantificados y analizados estadísticamente, proporcionando una base sólida para decisiones informadas y estratégicas.

- Totalmente en desacuerdo
- En desacuerdo
- Un poco de acuerdo
- De acuerdo
- Totalmente de acuerdo

Instrumentos para la recolección de datos:

Identificación y Clasificación de Activos

¿En qué medida está conforme con la clasificación y registro de activos identificados en la unidad a la cual pertenece usted dentro del departamento de TI, en caso de **NO** estar **"Totalmente de acuerdo"** indique el por qué?

1	2	3	4	5

Identificación de Vulnerabilidades

¿Está conforme con la identificación de vulnerabilidades propuesta en la unidad a la cual pertenece usted dentro del departamento de TI, en caso de **NO** estar **"Totalmente de acuerdo"** indique el por qué?

1	2	3	4	5

Evaluación de Riesgos

¿Está conforme con la precisión y exhaustividad del análisis de riesgos propuesta en la unidad a la cual pertenece usted dentro del departamento de TI, en caso de **NO** estar **"Totalmente de acuerdo"** indique el por qué?

1	2	3	4	5

Aplicabilidad de Controles

¿Está de acuerdo con la propuesta de los controles técnicos y administrativos para proteger los activos en la unidad a la cual pertenece usted dentro del departamento de TI, en caso de **NO** estar **"Totalmente de acuerdo"** indique el por qué?

1	2	3	4	5

Políticas de Seguridad y Cumplimiento

¿Está de acuerdo que las políticas y procedimientos de seguridad de la información son adecuados y están alineadas con las necesidades de departamento de TIC, en caso de **NO** estar **"Totalmente de acuerdo"** indique el por qué?

1	2	3	4	5

Gestión de Incidentes y Plan de Contingencia

¿Está de acuerdo con la preparación y capacidad de respuesta del plan de contingencia frente a incidentes de seguridad de la información en el departamento de TI, en caso de **NO** estar **"Totalmente de acuerdo"** indique el por qué?

1	2	3	4	5

Formación y Concienciación del Personal

¿Está de acuerdo a su consideración con la efectividad de las iniciativas de formación y concienciación sobre seguridad de la información para el personal del departamento de TIC, en caso de **NO** estar **"Totalmente de acuerdo"** indique el por qué?

1	2	3	4	5

Revisión y Mejora Continua

¿Está de acuerdo a su consideración con la eficacia del proceso de revisión y mejora continua del SGSI, en caso de **NO** estar **"Totalmente de acuerdo"** indique el por qué?

1	2	3	4	5

Apoyo y Compromiso de la Dirección

¿Está de acuerdo con el proceso (recolección de información, encuestas, entrevistas) realizado dentro su unidad del departamento de TIC para la realización del SGSI, en caso de **NO** estar **"Totalmente de acuerdo"** indique el por qué?

1	2	3	4	5

Gestión de Cambios en el SGSI

¿Está de acuerdo con el punto **IX (**Mantenimiento y actualización), del *Plan de Contingencia de Procesos Tecnológicos – UTMACH,* en caso de **NO** estar **"Totalmente de acuerdo"** indique el por qué?

1	2	3	4	5

3.2. Resultados de la evaluación

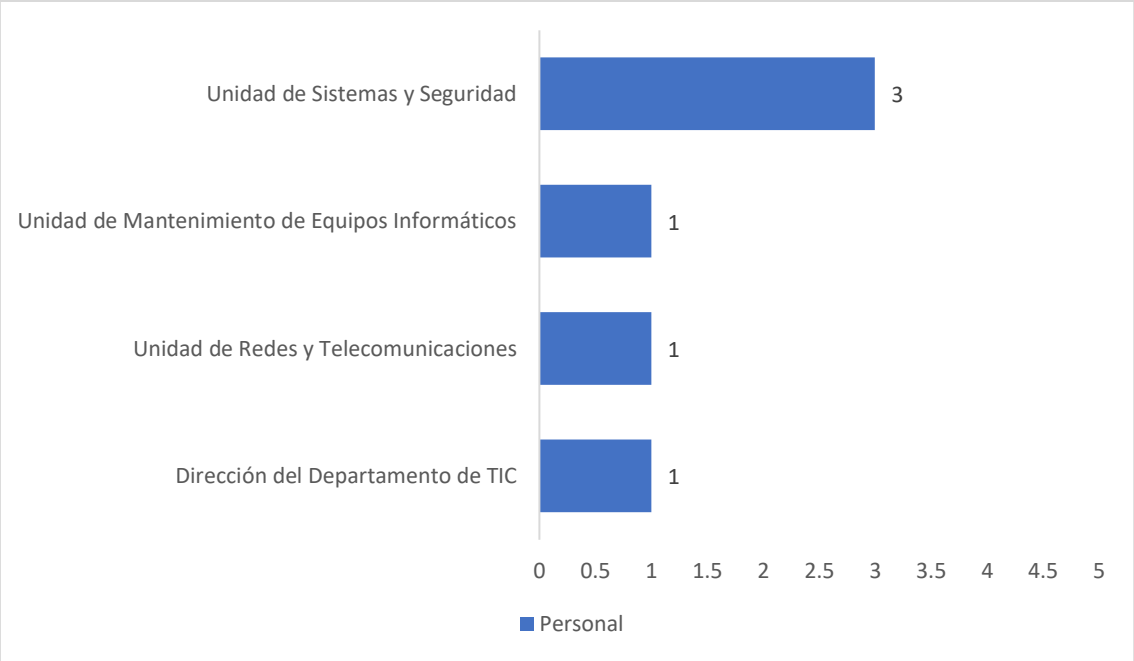
Correo Institucional

- lpazmino@utmachala.edu.ec
- bpachucho@utmachala.edu.ec
- bramirez@utmachala.edu.ec
- jcelleri@utmachala.edu.ec
- kavalarezo@utmachala.edu.ec
- jceras@utmachala.edu.ec

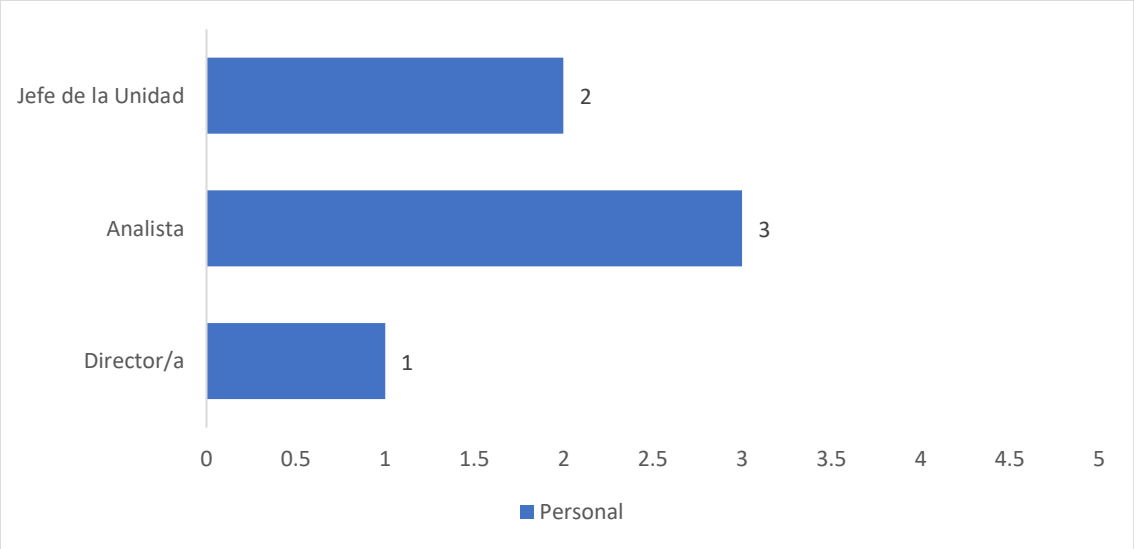
Nombres y Apellidos

- Leslie Howard Pazmiño Carrión
- Betty Pachucho Hernández
- Byron Fabricio Ramírez Carrillo
- Jennifer Celleri
- Kevin Adrián Valarezo Paz
- Jazmin Cecibel Eras López

Seleccione la Unidad donde realiza sus actividades laborales

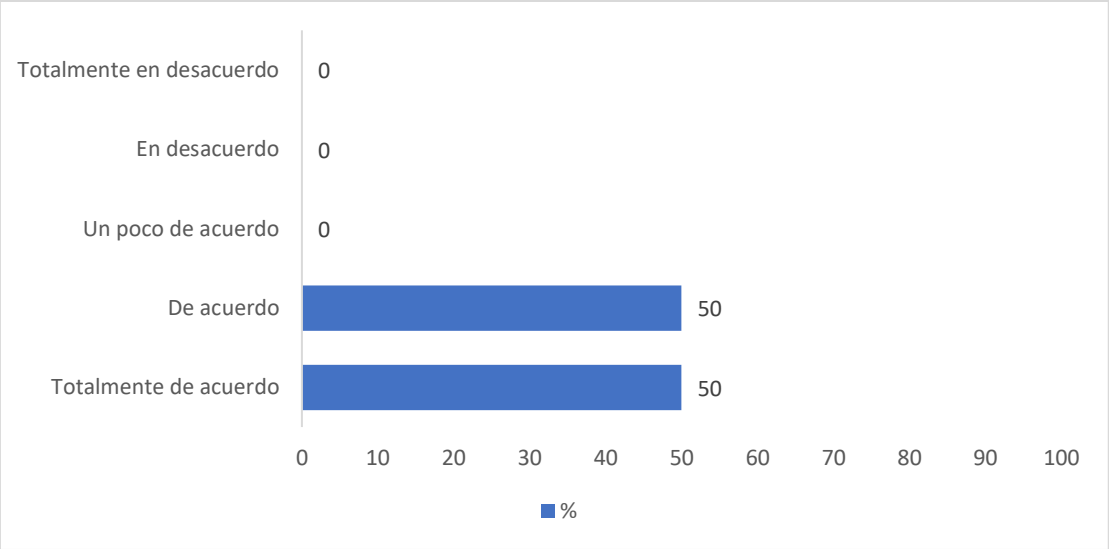


Seleccione el Rol que desempeña dentro de la Unidad anteriormente seleccionada



Identificación y Clasificación de Activos

¿En qué medida está conforme con la clasificación y registro de activos identificados en la unidad a la cual pertenece usted dentro del departamento de TI?

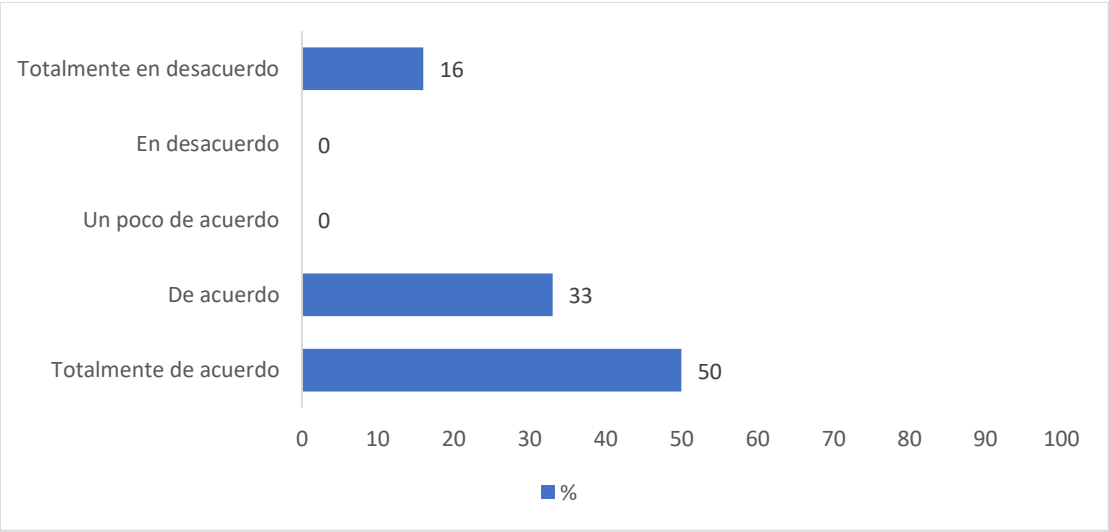


En caso de **NO** estar **"Totalmente de acuerdo"** indique el por qué

Unidad	Encuestado	Respuesta
Unidad de Sistemas y Seguridad	Jazmin Cecibel Eras López	El listado de activos (plataformas) esta desactualizado
Unidad de Redes Y Telecomunicaciones	Byron Fabricio Ramirez Carrillo	Se menciona información correcta parcialmente, de las subredes en el inventario, sin considerar los equipos (LAN, WAN y WIFI), y servidores.

Identificación de Vulnerabilidades

¿Está conforme con la identificación de vulnerabilidades propuesta en la unidad a la cual pertenece usted dentro del departamento de TI?

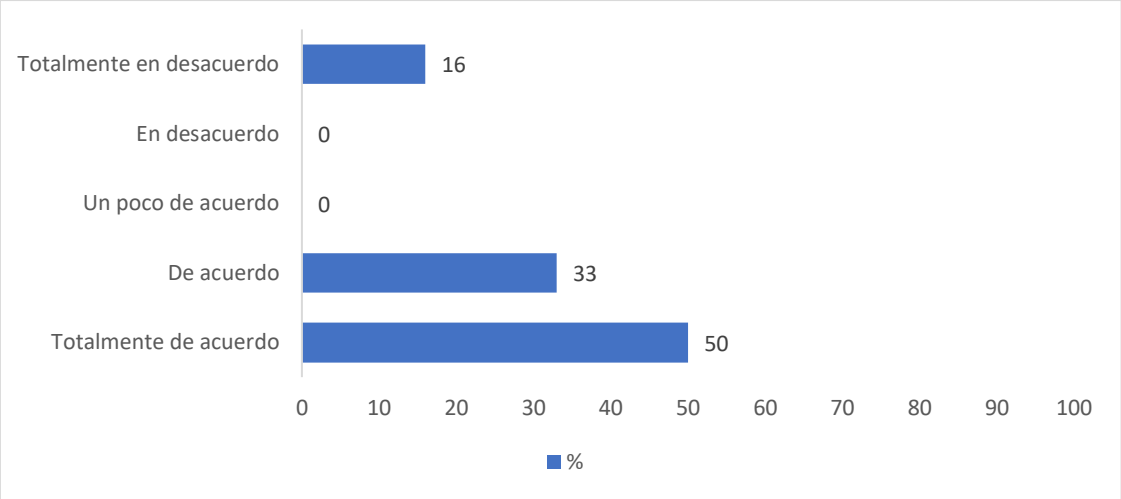


En caso de **NO** estar **"Totalmente de acuerdo"** indique el por qué

Unidad	Encuestado	Respuesta
Unidad de Redes Y Telecomunicaciones	Byron Fabricio Ramirez Carrillo	Identificación de vulnerabilidades para activos como equipos y servidores, general.

Evaluación de Riesgos

¿Está conforme con la precisión y exhaustividad del análisis de riesgos propuesta en la unidad a la cual pertenece usted dentro del departamento de TI?

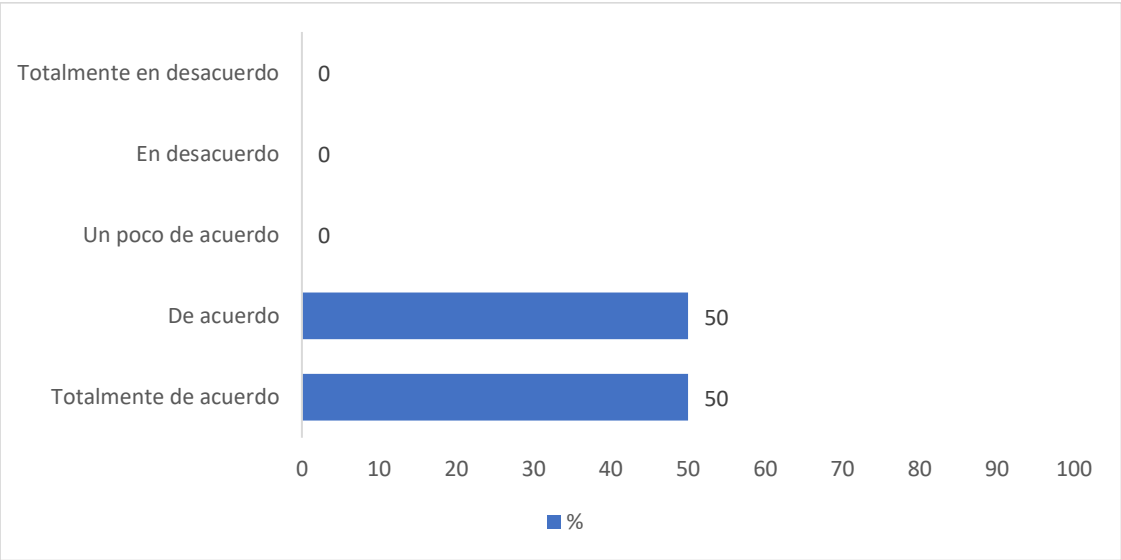


En caso de **NO** estar **"Totalmente de acuerdo"** indique el por qué

Unidad	Encuestado	Respuesta
Unidad de Redes Y Telecomunicaciones	Byron Fabricio Ramirez Carrillo	El análisis se realizó a nivel general.

Aplicabilidad de Controles

¿Está de acuerdo con la propuesta de los controles técnicos y administrativos para proteger los activos en la unidad a la cual pertenece usted dentro del departamento de TI?

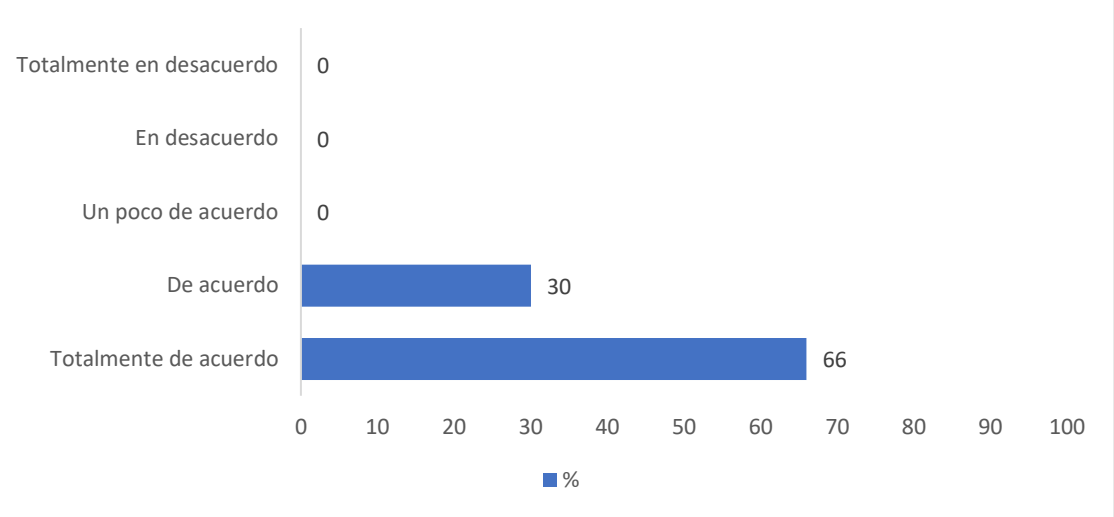


En caso de **NO** estar **"Totalmente de acuerdo"** indique el por qué

Unidad	Encuestado	Respuesta
Unidad de Sistemas y Seguridad	Jazmin Cecibel Eras Lopez	Se debe incluir en la propuesta la planificación de recursos para minimizar el riesgo por fallas
Unidad de Redes Y Telecomunicaciones	Byron Fabricio Ramirez Carrillo	Se proponen controles que ya existen actualmente (WAF, cifrado, antivirus y firewall, etc...), pero que no fueron considerador en el análisis por ser general.

Políticas de Seguridad y Cumplimiento

¿Está de acuerdo que las políticas y procedimientos de seguridad de la información son adecuados y están alineadas con las necesidades de departamento de TIC?

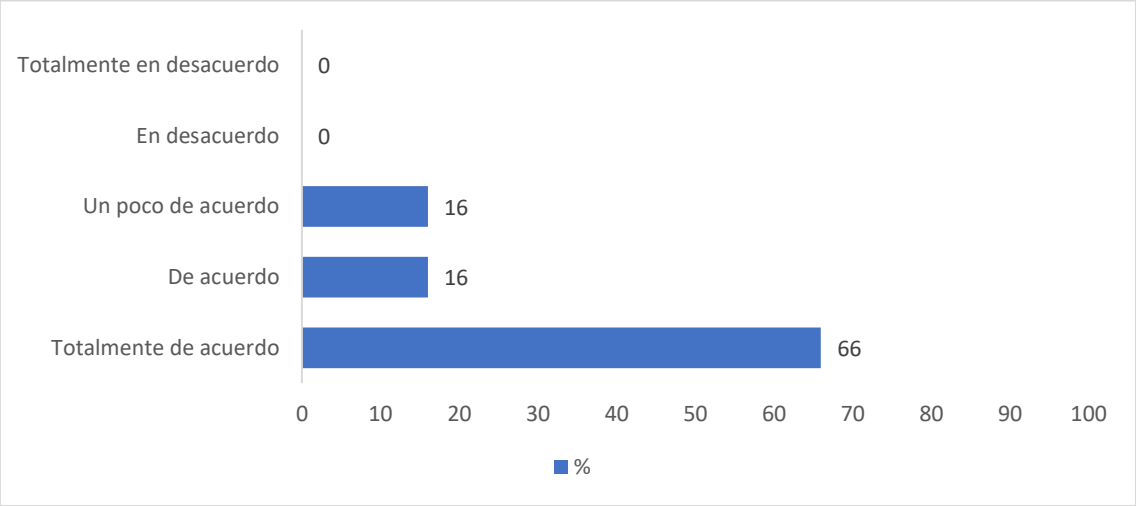


En caso de **NO** estar **"Totalmente de acuerdo"** indique el por qué

Unidad	Encuestado	Respuesta
Unidad de Sistemas y Seguridad	Jazmin Cecibel Eras Lopez	En la 1ra Politica de control de acceso y autenticación, se menciona implementar MFA con al menos tres métodos independientes. Mediante el servicio de Microsoft solo se tiene configuración para 2 métodos por el momento.

Gestión de Incidentes y Plan de Contingencia

¿Está de acuerdo con la preparación y capacidad de respuesta del plan de contingencia frente a incidentes de seguridad de la información en el departamento de TI?

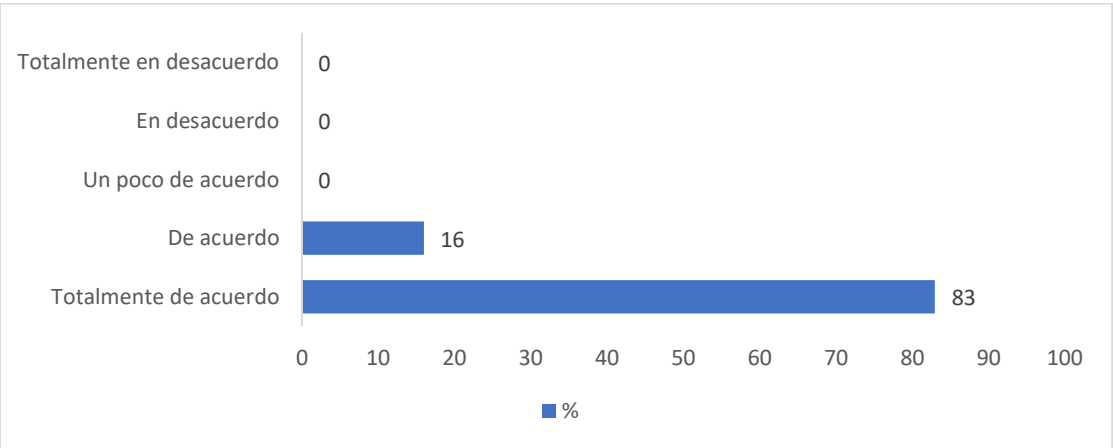


En caso de **NO** estar **"Totalmente de acuerdo"** indique el por qué

Unidad	Encuestado	Respuesta
Unidad de Sistemas y Seguridad	Betty Pachucho Hernández	Esto no se da "• Interrupciones programadas para mantenimiento que no se comunicaron efectivamente a los usuarios." todas las tareas de mantenimiento son comunicadas oportunamente

Formación y Concienciación del Personal

¿Está de acuerdo a su consideración con la efectividad de las iniciativas de formación y concienciación sobre seguridad de la información para el personal del departamento de TIC?

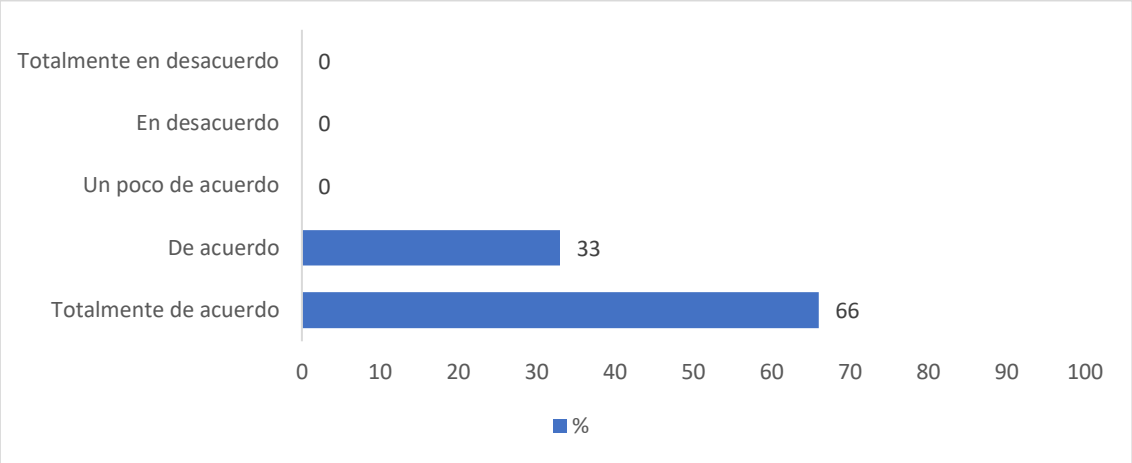


En caso de **NO** estar **"Totalmente de acuerdo"** indique el por qué

Unidad	Encuestado	Respuesta

Revisión y Mejora Continua

¿Está de acuerdo a su consideración con la eficacia del proceso de revisión y mejora continua del SGSI?

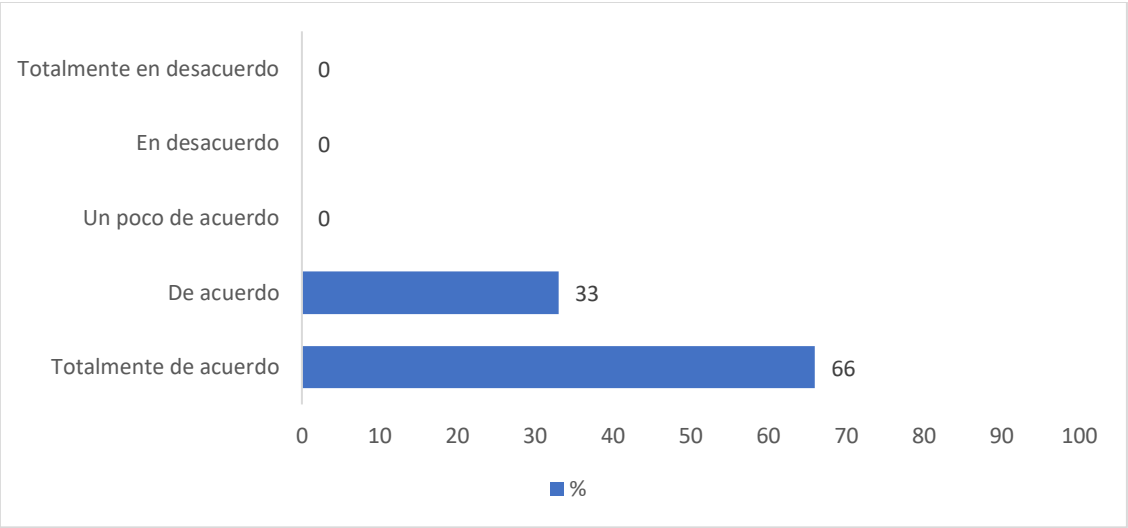


En caso de **NO** estar **"Totalmente de acuerdo"** indique el por qué

Unidad	Encuestado	Respuesta
Unidad de Sistemas y Seguridad	Jazmin Cecibel Eras Lopez	Se debe considerar una revisión anual previo a incidentes para detección de los mismos.

Apoyo y Compromiso de la Dirección

¿Está de acuerdo con el proceso (recolección de información, encuestas, entrevistas) realizado dentro su unidad del departamento de TIC para la realización del SGSI?

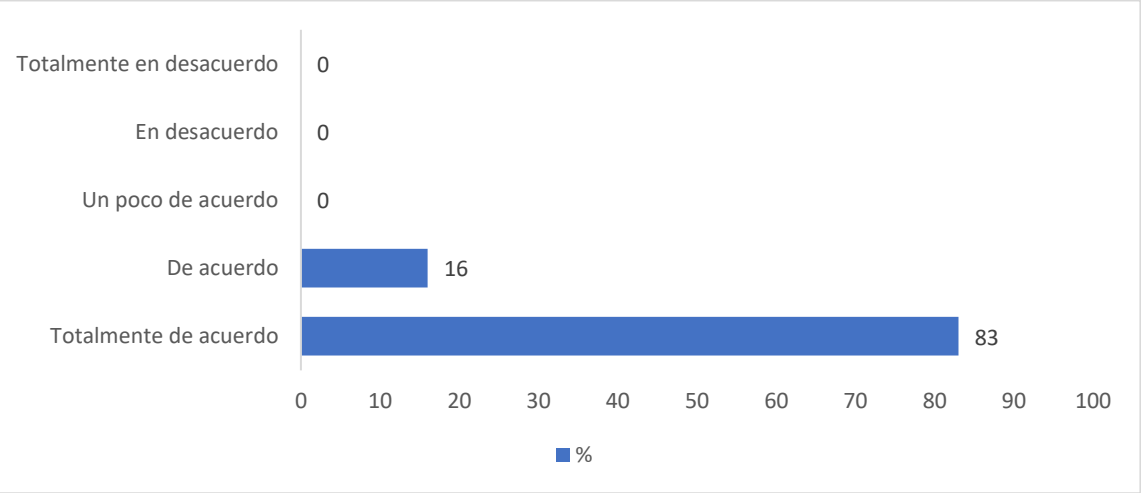


En caso de **NO** estar **"Totalmente de acuerdo"** indique el por qué

Unidad	Encuestado	Respuesta
Unidad de Redes Y Telecomunicaciones	Byron Fabricio Ramirez Carrillo	Se realizo muy general

Gestión de Cambios en el SGSI

¿Está de acuerdo con el punto **IX (**Mantenimiento y actualización), del *Plan de Contingencia de Procesos Tecnológicos – UTMACH?*



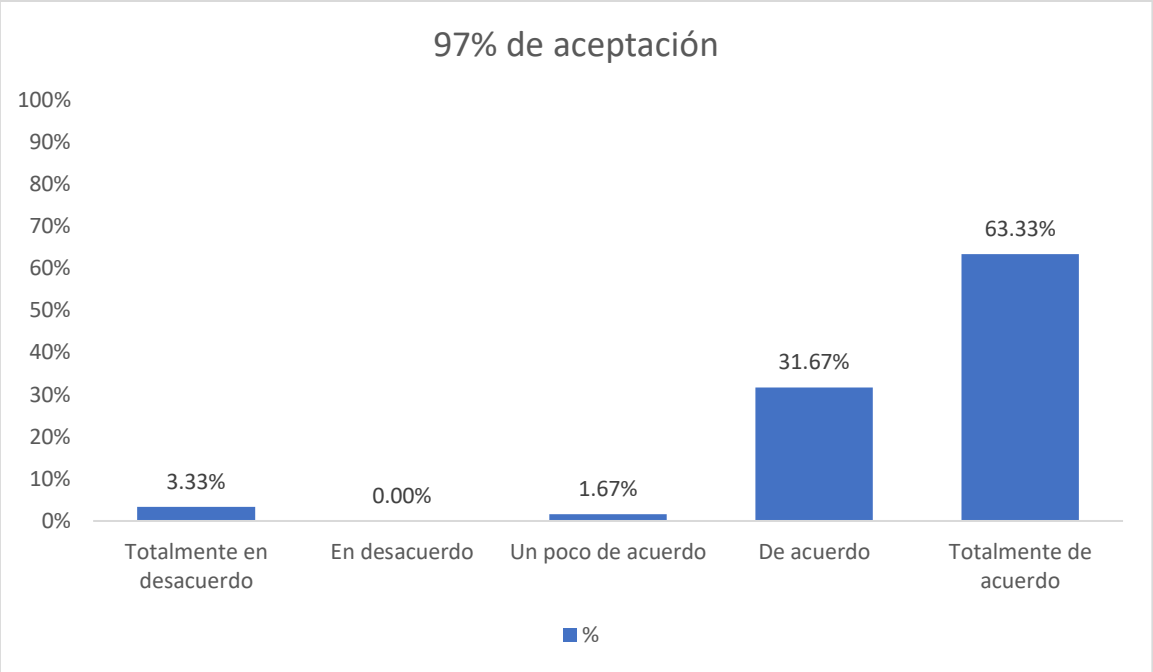
En caso de **NO** estar **"Totalmente de acuerdo"** indique el por qué

Unidad	Encuestado	Respuesta

Total

Preguntas	Totalmente en desacuerdo	En desacuerdo	Un poco de acuerdo	De acuerdo	Totalmente de acuerdo
¿En qué medida está conforme con la clasificación y registro de activos identificados en la unidad a la cual pertenece usted dentro del departamento de TI?	0	0	0	3	3
¿Está conforme con la identificación de vulnerabilidades propuesta en la unidad a la cual pertenece usted dentro del departamento de TI?	1	0	0	2	3
¿Está conforme con la precisión y exhaustividad del análisis de riesgos propuesta en la unidad a la cual pertenece usted dentro del departamento de TI?	1	0	0	2	3
¿Está de acuerdo con la propuesta de los controles técnicos y administrativos para proteger los activos en la unidad a la cual pertenece usted dentro del departamento de TI?	0	0	0	3	3
¿Está de acuerdo que las políticas y procedimientos de seguridad de la información son adecuados y están alineadas con las	0	0	0	2	4

necesidades de departamento de TIC?					
¿Está de acuerdo con la preparación y capacidad de respuesta del plan de contingencia frente a incidentes de seguridad de la información en el departamento de TI, en caso de NO estar "Totalmente de acuerdo" indique el por qué?	0	0	1	1	4
¿Está de acuerdo a su consideración con la efectividad de las iniciativas de formación y concienciación sobre seguridad de la información para el personal del departamento de TIC?	0	0	0	1	5
¿Está de acuerdo a su consideración con la eficacia del proceso de revisión y mejora continua del SGSI?	0	0	0	2	4
¿Está de acuerdo con el proceso (recolección de información, encuestas, entrevistas) realizado dentro su unidad del departamento de TIC para la realización del SGSI?	0	0	0	2	4
¿Está de acuerdo con el punto IX (Mantenimiento y actualización), del Plan de Contingencia de Procesos Tecnológicos – UTMACH?	0	0	0	1	5
Total suma	**2**	**0**	**1**	**19**	**38**
Total %	**3%**	**0%**	**2%**	**32%**	**63%**
Suma % positivo					**97%**



CONCLUSIONES

La realización de este proyecto ha cumplido con el objetivo general de elaborar una propuesta para la gestión de la seguridad y protección de la información en la Universidad Técnica de Machala (UTMACH) empleando estándares y buenas prácticas. A través del desarrollo del marco teórico, se ha establecido una base sólida que aborda la gestión de la seguridad de la información dentro del contexto universitario, identificando vulnerabilidades y desarrollando un conjunto de políticas, procedimientos y controles de seguridad adecuados. Además, se han llevado a cabo actividades de sensibilización, promoviendo una cultura de seguridad informática robusta en la comunidad de la UTMACH. En la evaluación de conformidad, existe un alto nivel de conformidad y acuerdo con el SGSI propuesto en el departamento TIC, especialmente en: el proceso recolección de información, el plan de contingencia, formación y concienciación, proceso de revisión y mejora continua. Las áreas con mayor nivel de conformidad son las relacionadas con preparación y respuesta ante contingencias y, formación y concienciación en seguridad de la información con 5 puntos en total aprobación. No se reportan respuestas de desacuerdo total en ninguno de los ítems evaluados. Solo un 1 punto de total desacuerdo en los ítems de análisis de riesgos y la identificación de vulnerabilidades.

4. RECOMENDACIONES

De acuerdo a los comentarios y retroalimentación brindados por los ingenieros de las unidades técnicas del departamento TIC, se recomienda realizar una revisión integral del Sistema de Gestión de Seguridad de la Información focalizándose en actualizar el inventario de activos para incluir todos los equipos de red, servidores y demás elementos, así mismo de asegurarse de mantenerlo siempre actualizado. Continuando con la realización de análisis de vulnerabilidades y evaluación de riesgos más exhaustivos, considerando específicamente los activos críticos como equipos de red y servidores. No quedarse solo en un análisis general. Revisar la propuesta de controles considerando aquellos que ya existen actualmente y no fueron incluidos. Verificar su efectividad. El ajuste de las políticas de control de acceso y autenticación para que se alineen con las capacidades tecnológicas actuales de MFA. Mejorar la comunicación de tareas de mantenimiento programadas para minimizar la afectación a los usuarios. Involucrar más directamente a los ingenieros de cada unidad en el proceso de recolección de información y

retroalimentación para enriquecer el SGSI. Mantener actualizado el plan de contingencia tecnológica alineado con los cambios en el SGSI. Establecer indicadores de desempeño del SGSI y monitorearlos periódicamente. Fomentar una cultura de mejora continua de la seguridad de la información en el departamento. Esta recomendación permitirá robustecer el SGSI incorporando las necesidades específicas de las unidades y el personal técnico del departamento TIC.

5. REFERENCIAS BIBLIOGRÁFICAS

[1] S. Bauer, E. W. N. Bernroider, and K. Chudzikowski, "Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks," *Comput. Secur.*, vol. 68, pp. 145–159, Jul. 2017, doi: 10.1016/j.cose.2017.04.009.

[2] A. Da Veiga and N. Martins, "Defining and identifying dominant information security cultures and subcultures," *Comput. Secur.*, vol. 70, pp. 72–94, Sep. 2017, doi: 10.1016/j.cose.2017.05.002.

[3] Y. He and C. Johnson, "Challenges of information security incident learning: An industrial case study in a Chinese healthcare organization," *Inform. Health Soc. Care*, vol. 42, no. 4, pp. 393–408, Oct. 2017, doi: 10.1080/17538157.2016.1255629.

[4] C. Vorakulpipat, S. Sirapaisan, E. Rattanalerdnusorn, and V. Savangsuk, "A Policy-Based Framework for Preserving Confidentiality in BYOD Environments: A Review of Information Security Perspectives," *Secur. Commun. Netw.*, vol. 2017, pp. 1–11, 2017, doi: 10.1155/2017/2057260.

[5] P. B. Lowry, T. Dinev, and R. Willison, "Why security and privacy research lies at the centre of the information systems (IS) artefact: proposing a bold research agenda," *Eur. J. Inf. Syst.*, vol. 26, no. 6, pp. 546–563, Nov. 2017, doi: 10.1057/s41303-017-0066-x.

[6] A. Erceg, "Information security: threat from employees," *Teh. Glas.*, vol. 13, no. 2, pp. 123–128, Jun. 2019, doi: 10.31803/tg-20180717222848.

[7] A. Shelupanov, O. Evsyutin, A. Konev, E. Kostyuchenko, D. Kruchinin, and D. Nikiforov, "Information Security Methods—Modern Research Directions," *Symmetry*, vol. 11, no. 2, p. 150, Jan. 2019, doi: 10.3390/sym11020150.

[8] "Security Information System, Based on Fingerprint Biometrics," *Acta Polytech. Hung.*, vol. 16, no. 5, Aug. 2019, doi: 10.12700/APH.16.5.2019.5.6.

[9] H. C. Pham, L. Brennan, and S. Furnell, "Information security burnout: Identification of sources and mitigating factors from security demands and resources," *J. Inf. Secur. Appl.*, vol. 46, pp. 96–107, Jun. 2019, doi: 10.1016/j.jisa.2019.03.012.

[10] H. Paananen, M. Lapke, and M. Siponen, "State of the art in information security policy development," *Comput. Secur.*, vol. 88, p. 101608, Jan. 2020, doi: 10.1016/j.cose.2019.101608.

[11] W. Jiang, G. Xiong, X. Ding, Z. Chang, and N. Sang, "Confidentiality-aware message scheduling for security-critical wireless networks," *J. Syst. Eng. Electron.*, vol. 21, no. 1, pp. 154–160, Feb. 2010, doi: 10.3969/j.issn.1004-4132.2010.01.025.

[12] Y. Wang, J. Li, S. Zhao, and F. Yu, “Hybridchain: A Novel Architecture for Confidentiality-Preserving and Performant Permissioned Blockchain Using Trusted Execution Environment,” *IEEE Access*, vol. 8, pp. 190652–190662, 2020, doi: 10.1109/ACCESS.2020.3031889.

[13] Z. Liu, Y. Liu, X. Yang, and X. Li, “Integrity Auditing for Multi-Copy in Cloud Storage Based on Red-Black Tree,” *IEEE Access*, vol. 9, pp. 75117–75131, 2021, doi: 10.1109/ACCESS.2021.3079143.

[14] H. Yan and W. Gui, “Efficient Identity-Based Public Integrity Auditing of Shared Data in Cloud Storage With User Privacy Preserving,” *IEEE Access*, vol. 9, pp. 45822–45831, 2021, doi: 10.1109/ACCESS.2021.3066497.

[15] M. Mirtsch, J. Kinne, and K. Blind, “Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis,” *IEEE Trans. Eng. Manag.*, vol. 68, no. 1, pp. 87–100, Feb. 2021, doi: 10.1109/TEM.2020.2977815.

[16] F. R. Moreira, D. A. Da Silva Filho, G. D. A. Nze, R. T. de Sousa Júnior, and R. R. Nunes, “Evaluating the Performance of NIST’s Framework Cybersecurity Controls Through a Constructivist Multicriteria Methodology,” *IEEE Access*, vol. 9, pp. 129605–129618, 2021, doi: 10.1109/ACCESS.2021.3113178.

[17] J. Oh, J. Hong, C. Lee, J. J. Lee, S. S. Woo, and K. Lee, “Will EU’s GDPR Act as an Effective Enforcer to Gain Consent?,” *IEEE Access*, vol. 9, pp. 79477–79490, 2021, doi: 10.1109/ACCESS.2021.3083897.

[18] F. Castaño, E. F. Fernañdez, R. Alaiz-Rodríguez, and E. Alegre, “PhiKitA: Phishing Kit Attacks Dataset for Phishing Websites Identification,” *IEEE Access*, vol. 11, pp. 40779–40789, 2023, doi: 10.1109/ACCESS.2023.3268027.

[19] B. Jin, J. Choi, J. B. Hong, and H. Kim, “On the Effectiveness of Perturbations in Generating Evasive Malware Variants,” *IEEE Access*, vol. 11, pp. 31062–31074, 2023, doi: 10.1109/ACCESS.2023.3262265.

[20] S. Dong and M. Sarem, “DDoS Attack Detection Method Based on Improved KNN With the Degree of DDoS Attack in Software-Defined Networks,” *IEEE Access*, vol. 8, pp. 5039–5048, 2020, doi: 10.1109/ACCESS.2019.2963077.

[21] G. Huang, Y. Li, Q. Wang, J. Ren, Y. Cheng, and X. Zhao, “Automatic Classification Method for Software Vulnerability Based on Deep Neural Network,” *IEEE Access*, vol. 7, pp. 28291–28298, 2019, doi: 10.1109/ACCESS.2019.2900462.

[22] W. Xiong, F. Zhou, R. Wang, R. Lan, X. Sun, and X. Luo, “An Efficient and Secure Two-Factor Password Authentication Scheme With Card Reader(Terminal) Verification,” *IEEE Access*, vol. 6, pp. 70707–70719, 2018, doi: 10.1109/ACCESS.2018.2869535.

[23] K. Ntalianis and N. Tsapatsoulis, “Remote Authentication via Biometrics: A Robust Video-Object Steganographic Mechanism Over Wireless Networks,” *IEEE Trans. Emerg. Top. Comput.*, vol. 4, no. 1, pp. 156–174, Jan. 2016, doi: 10.1109/TETC.2015.2400135.

[24] Q. Liu, H. Zhang, J. Wan, and X. Chen, “An Access Control Model for Resource Sharing Based on the Role-Based Access Control Intended for Multi-Domain Manufacturing Internet of Things,” *IEEE Access*, vol. 5, pp. 7001–7011, 2017, doi: 10.1109/ACCESS.2017.2693380.

[25] Z. Wu, X. Chen, M. U. Khan, and S. U.-J. Lee, “Enhancing Fidelity of Description in Android Apps With Category-Based Common Permissions,” *IEEE Access*, vol. 9, pp. 105493–105505, 2021, doi: 10.1109/ACCESS.2021.3100118.

[26] S. Kim, S. Yoon, J. Narantuya, and H. Lim, “Secure Collecting, Optimizing, and Deploying of Firewall Rules in Software-Defined Networks,” *IEEE Access*, vol. 8, pp. 15166–15177, 2020, doi: 10.1109/ACCESS.2020.2967503.

[27] X. Yin, X. Chen, L. Chen, G. Shao, H. Li, and S. Tao, “Research of Security as a Service for VMs in IaaS Platform,” *IEEE Access*, vol. 6, pp. 29158–29172, 2018, doi: 10.1109/ACCESS.2018.2837039.

[28] Y. Yao, Z. Zhai, J. Liu, and Z. Li, “Lattice-Based Key-Aggregate (Searchable) Encryption in Cloud Storage,” *IEEE Access*, vol. 7, pp. 164544–164555, 2019, doi: 10.1109/ACCESS.2019.2952163.

[29] R. Siddiqui, “Bring Your Own Device (BYOD) in Higher Education: Opportunities and Challenges,” *Int. J. Emerg. Trends Technol. Comput. Sci. IJETTCS*, vol. 3, pp. 233–236, Mar. 2014.

[30] Z. Zhang, Y.-Q. Zhang, X. Chu, and B. Li, “An Overview of Virtual Private Network (VPN): IP VPN and Optical VPN,” *Photonic Netw. Commun.*, vol. 7, no. 3, pp. 213–225, May 2004, doi: 10.1023/B:PNET.0000026887.35638.ce.

[31] J. C. Montoya and T. O. Hernández, “a instrumentación física avanzada”.

[32] C. A. R. Agudelo, “Arquitectura para automatizar respuesta a incidentes de seguridad de la información relacionados con ataques internos mediante la ejecución de técnicas spoofing”.

[33] C. E. R. Escobar, “DESARROLLO DE LA NORMATIVA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN EN EL DEPARTAMENTO DE GESTIÓN TECNOLÓGICA DE LA UNIVERSIDAD SANTIAGO DE CALI,” 2013.

[34] E. Ferruzola Gómez, J. Duchimaza S., J. Ramos Holguín, and M. Alejandro Lindao, “Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología MAGERIT,” *Rev. Científica Tecnológica UPSE*, vol. 6, no. 1, pp. 34–41, Jun. 2019, doi: 10.26423/rctu.v6i1.429.

[35] F. Madrigal Patiño and J. Y. Tortolero Martines, “Protección y recuperación de datos,” Dec. 2009, Accessed: Sep. 22, 2023. [Online]. Available: http://tesis.ipn.mx/xmlui/handle/123456789/5543

[36] D. O. Calderón Merchán and D. A. Sánchez Meza, “Desarrollo de un sistema de gestión de seguridad de la información (SGSI) para la empresa Comware S.A. en la ciudad de Quito, aplicando la norma Iso / Iec 27001,” bachelorThesis, 2012. Accessed: Sep. 21, 2023. [Online]. Available: http://dspace.ups.edu.ec/handle/123456789/3901

[37] “Repositorio Universidad Técnica de Ambato: Gestión de la Seguridad de la Información basado en la Norma ISO/IEC 27001 y su incidencia en las Instituciones de Educación Superior de la ciudad de Machala.” Accessed: Sep. 22, 2023. [Online]. Available: https://repositorio.uta.edu.ec/handle/123456789/29844

[38] Prisma, “El ciclo Deming: en qué consiste y cómo aplicarlo,” Eurofins Environment Testing Spain. Accessed: Sep. 26, 2023. [Online]. Available: https://www.eurofins-environment.es/es/el-ciclo-deming-que-consiste-y-como-ayuda-gestion-procesos/

[39] Departamento Administrativo de la Función Pública, “Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital,” *Oct. 2018*.

6. ANEXOS

6.1. Anexo 1: Reunión de revisión del Trabajo de Proyecto de Integración Curricular

6.2. Anexo 2: Reunión de revisión del Trabajo de Proyecto de Integración Curricular con la Unidad de Mantenimiento de Equipos Informáticos

6.3. Anexo 3: Matriz de consistencia

Tabla 9 Matriz de consistencia

Problema, objeto y campo	**Objetivo**	**Marco Teórico**	**Preguntas de investigación**	**Metodología**
Problema: La falta de un sistema de gestión de seguridad pone a la UTMACH en riesgo, expuesta a vulnerabilidades y amenazas que podrían comprometer la confidencialidad, integridad y disponibilidad de la información institucional. Además, esta situación podría conducir a consecuencias perjudiciales como el acceso no autorizado, la pérdida de datos, la interrupción de servicios, el daño a su reputación y posibles repercusiones legales. **Problemas específicos:** • ¿Cuáles son los estándares y marcos de trabajo más adecuados para gestionar la seguridad de la información en una institución educativa como la Universidad Técnica de Machala?	**Objetivo General** • Elaborar una propuesta para la gestión de la seguridad y protección de la información en la UTMACH mediante estándares y buenas prácticas que sirva de guía para la mitigación de incidentes informáticos. **Objetivos específicos** • Desarrollar el marco teórico de la investigación a través de la revisión de antecedentes históricos, teóricos y contextuales sobre la gestión de seguridad de la información en el ámbito de la UTMACH, que permita establecer los requerimientos para la propuesta del sistema de gestión. • Identificar vulnerabilidades y desarrollar políticas, procedimientos y controles de seguridad de la información para la UTMACH según	**Antecedentes históricos a nivel internacional y nacional del objeto, campo:** Para elaborar los antecedentes del presente trabajo sobre seguridad de la información en la UTMACH, se realizó una Revisión Sistemática de Literatura con el objetivo de identificar, analizar e interpretar evidencia científica previa sobre gestión de seguridad de la información, uso de estándares y buenas prácticas aplicadas en instituciones de educación superior. Mediante este proceso se examinaron estudios relacionados que aportaron insumos valiosos para enmarcar la investigación actual, contextualizando adecuadamente los antecedentes del problema con base en el conocimiento y experiencias de trabajos previos, según la metodología de Revisión Sistemática.	**Hipótesis General:** • ¿Cuáles son las vulnerabilidades y riesgos específicos relacionados con la seguridad de la información que enfrenta la UTMACH? • ¿Cómo se pueden identificar y evaluar de manera sistemática dichas vulnerabilidades y riesgos en la universidad? • ¿Qué normativas, métodos y medidas de protección de datos deben desarrollarse e implementarse fortalecer la protección de los activos informáticos en el área de TIC de la UTMACH? • ¿Qué protocolos y procedimientos deben establecerse para una reacción y restauración efectivas frente a situaciones de brechas de protección de datos en la institución académica?	**Enfoque:** La investigación acerca de la gestión de seguridad de la información en la UTMACH se llevará a cabo utilizando un enfoque de investigación mixto. Este enfoque integra métodos cuantitativos y cualitativos, con el fin de brindar un panorama amplio y detallado del fenómeno objeto de estudio. **Alcance:** En el presente estudio se ha decidido adoptar un enfoque mixto, utilizando diversas etapas de alcance de investigación, con el propósito de abordar de manera integral. La primera fase del proyecto, se llevará a cabo un enfoque exploratorio y descriptivo. El propósito de esta etapa es adquirir conocimiento sobre la situación. En la segunda fase se adopta un enfoque correlacional y explicativo. Proponiendo las políticas de seguridad, y a un plan de contingencia que ayude en el control de problemas de seguridad de la información dentro del Área de TIC's. **Diseño:** El presente estudio sigue un diseño secuencial explicativo con un componente concurrente. Este diseño ha sido seleccionado

• ¿Cuáles son las principales vulnerabilidades y peligros más relevantes en materia de seguridad de la información a los que se expone la Universidad Técnica de Machala? • ¿Cómo se pueden identificar y evaluar de manera sistemática los riesgos de seguridad de la información en la universidad? • ¿Cuáles son las mejores prácticas para los controles de protección de datos efectivos en la UTMACH (Universidad Técnica de Machala)? • ¿Qué medidas de concienciación y capacitación en seguridad de la información son necesarias para el personal y los usuarios de la universidad? • ¿Cómo se puede establecer un marco de respuesta y recuperación ante incidentes de seguridad de la información en la Universidad Técnica de Machala? • ¿Cuáles son los recursos y la infraestructura	estándares y necesidades específicas. • Realizar actividades de sensibilización y establecer un marco de respuesta ante riesgos en protección de datos para fomentar una cultura de seguridad sólida en la UTMACH. • Evaluar el esquema de seguridad basado en estándares y buenas prácticas.			con el objetivo de optimizar la comprensión del fenómeno de estudio y garantizar la recopilación y análisis de datos de forma sistemática y coherente. **Unidades de análisis:** **Población:** La población de este estudio se define como todas las partes interesadas relevantes y los sistemas informáticos dentro de la Universidad Técnica de Machala (UTMACH). **Muestra:** No se consiguió muestra ya que se operó con el total de integrantes de la población. **Técnicas e instrumentos de recolección de datos:** Entrevistas: Guía de entrevista Encuestas: Cuestionario Observación: Lista de verificación Reuniones: Puntos de discusión en la reunión **Técnicas de procesamiento de datos:** Análisis de encuestas: Los datos recogidos a través de las encuestas se procesarán y analizarán utilizando herramientas estadísticas Análisis de entrevistas: Las entrevistas se grabarán y transcribirán para un análisis detallado. Análisis de observaciones: Las observaciones se realizarán utilizando una guía de observación

necesarios para mantener un sistema de gestión de seguridad de la información robusto y eficiente en la universidad? • ¿Cuál es el impacto financiero y la viabilidad de un sistema de estándares y buenas prácticas en la gestión de la seguridad de la información en la Universidad Técnica de Machala? **Objeto de estudio** • Sugerir gestión de protección de datos en UTMACH. • Evaluar políticas y riesgos en seguridad de información de UTMACH. • Investigar y adaptar estándares ISO 27000 a UTMACH. • Proponer sistema de protección de activos TIC en UTMACH. Campo de acción • El Mejorar la seguridad de la información en el área TIC de la UTMACH mediante el análisis, evaluación de riesgos y propuesta de soluciones prácticas basadas en estándares y buenas prácticas.				estructurada, que se utilizará para registrar comportamientos Análisis de reuniones: Las notas de las reuniones y las grabaciones (si están disponibles) se revisarán para identificar los temas de discusión, las decisiones tomadas y cualquier acción identificada. Técnicas de aprendizaje automático: Si los datos recogidos son suficientemente grandes y variados, se podrían aplicar técnicas de aprendizaje automático para identificar patrones y relaciones que podrían no ser evidentes a través del análisis estadístico tradicional.

6.4. Anexo 4: Instrumentos de recopilación de datos

Tabla 10 Cuestionario Integral sobre la Seguridad de la Información de la UTMACH

CUESTIONARIO INTEGRAL SOBRE LA SEGURIDAD DE LA INFORMACIÓN EN LA UTMACH					
INFORMACIÓN GENERAL					
Este cuestionario está diseñado para evaluar la seguridad de la información en la Universidad Técnica de Machala, enfocándose en hardware, redes, servidores y software. Su objetivo es identificar vulnerabilidades y oportunidades de mejora en la infraestructura tecnológica, recopilando información sobre las prácticas de seguridad, la capacitación del personal y la eficacia de las políticas actuales. Es una herramienta clave para administradores de sistemas y gestores de seguridad, proporcionando una visión integral para fortalecer la seguridad de la información en la universidad.					
Correo institucional:					
Nombres y apellidos:					
Seleccione la Unidad donde realiza sus actividades laborales					
Unidad de Sistemas y Seguridad	☐	Unidad de Mantenimiento de Equipos Informáticos	☐	Unidad de Redes y Telecomunicaciones	☐
Seleccione el Rol que desempeña dentro de la Unidad anteriormente seleccionada					
Jefe de la Unidad	☐	Analista	☐		
SEGURIDAD DE LA INFORMACIÓN DE HARDWARE EN LA UNIVERSIDAD TÉCNICA DE MACHALA					
Esta sección busca recoger datos de la infraestructura de redes del área de TIC. La información proporcionada en este cuestionario será tratada de forma confidencial y se utilizará exclusivamente con fines de investigación.					
¿De estos controles de acceso físico cuáles está implementado en el área donde se encuentra el hardware?					
Cerraduras tradicionales con llave	❑				
Sistemas de tarjetas de acceso	❑				
Teclados con códigos de seguridad	❑				
Reconocimiento biométrico (huellas dactilares, reconocimiento facial, etc.)	❑				
Guardias de seguridad	❑				
¿Quién tiene acceso autorizado a los equipos de las instalaciones?					
Todo el personal de TI	❑				
Solo administradores de sistemas y redes	❑				
Personal de mantenimiento y soporte técnico	❑				
Profesores y personal académico	❑				

Alta dirección de la universidad	❑
¿Cómo se manejan las llaves o credenciales de acceso en el departamento de TI? (Seleccione todas las opciones que apliquen)	
Se asignan individualmente y se rastrean mediante un registro	❑
Se comparten entre miembros del equipo sin un registro formal	❑
Se almacenan de manera segura cuando no están en uso	❑
Se cambian o actualizan periódicamente	❑
Se revocan inmediatamente después de que un empleado deja la organización o cambia de rol	❑
¿Con qué frecuencia se realiza el mantenimiento del hardware?	
❑ Semanalmente ❑ Mensualmente ❑ Trimestralmente ❑ Semestralmente ❑ Anualmente / Cuando sea necesario	
En caso de fallo del hardware, ¿Qué plan de continuidad de operaciones o recuperación anti-desastres se aplica?	
Activación inmediata de un sitio de respaldo completo	❑
Uso de hardware redundante en el lugar	❑
Reemplazo o reparación del hardware afectado sin plan de continuidad formal	❑
No existe un plan de continuidad de operaciones o recuperación ante desastres	❑
¿Qué tipos de copias de seguridad se realizan para los datos almacenados en los dispositivos usados en el departamento de TI?	
Copias de seguridad locales en unidades externas o servidores internos.	☐
Copias de seguridad en la nube.	☐
Copias de seguridad remotas en un centro de datos secundario.	☐
No se realizan copias de seguridad regularmente.	☐
¿Cómo se reportan y gestionan los incidentes de seguridad relacionados con el hardware?	

Mediante un sistema automatizado de gestión de incidentes	❑
Reporte manual a un equipo o persona específica encargada de la seguridad	❑
Discusión en reuniones regulares de equipo sin un proceso formal de reporte	❑
Los incidentes rara vez se reportan o gestionan de manera formal	❑
Comparta una experiencia donde las medidas de seguridad del hardware hayan sido eficaces o ineficaces	
¿Qué mejoras sugiere para mejorar la seguridad del hardware en su espacio de trabajo?	
SEGURIDAD DE LA INFORMACIÓN DE REDES EN LA UNIVERSIDAD TÉCNICA DE MACHALA	
Esta sección busca recoger datos de la infraestructura de redes del área de TIC. La información proporcionada en este cuestionario será tratada de forma confidencial y se utilizará exclusivamente con fines de investigación.	
¿Existe documentación de los APs (Access point) donde se indique su ubicación y configuración?	
Sí, existe documentación completa que incluye ubicación y configuración detallada	❑
Existe documentación parcial, solo con ubicación o configuración	❑
La documentación es antigua y posiblemente no esté actualizada	❑
No existe documentación formal, pero la información se conoce informalmente dentro del equipo	❑
No existe ningún tipo de documentación sobre los APs	❑
¿Cuál es el primer paso que realizas al iniciar tu jornada laboral para revisar la red en el departamento de TI?	

Revisar los informes y alertas del sistema de monitoreo de red	□
Realizar un chequeo visual o físico de los equipos críticos	□
Revisar los registros (logs) de eventos de seguridad	□
Consultar con el equipo sobre posibles problemas o cambios recientes	□
¿Cuál es tu procedimiento habitual para responder a los informes de posibles incidentes de seguridad en la red en el departamento de TI?	
Verificación inmediata y aislamiento del problema potencial	□
Revisión de los registros de la red para confirmar y evaluar el incidente	□
Notificación a un equipo o persona específica encargada de la seguridad	□
Implementación de medidas preventivas temporales mientras se investiga	□
Si descubres un servicio de red no autorizado funcionando en la infraestructura, ¿cuál es tu procedimiento para abordarlo en el departamento de TI?	
Desconectar o deshabilitar inmediatamente el servicio no autorizado	□
Investigar la fuente y el propósito del servicio antes de tomar medidas	□
Notificar al equipo de seguridad o a un supervisor para obtener más instrucciones	□
Registrar el incidente y monitorear el servicio antes de actuar	□
Implementar medidas de seguridad adicionales para limitar el acceso al servicio	□
De las siguientes políticas de seguridad, marque cuáles están implementadas para el acceso a la red inalámbrica de la UTMACH	
Autenticación mediante usuario y contraseña	□
Uso de encriptación WPA2 o superior	□
Filtrado de direcciones MAC	□
Segmentación de la red para invitados y personal	□
VPN obligatoria para el acceso remoto	□
¿Cómo se gestionan las credenciales de acceso a los APs (creación, distribución, revocación)?	
Manualmente por el personal de TI cuando se solicita	□
Mediante un proceso centralizado y documentado	□

Las credenciales se configuran una vez y raramente se cambian o actualizan	□
No hay un procedimiento establecido para la gestión de credenciales	□
De los siguientes métodos de autenticación y cifrado, marque cual se utilizan en los Access Points (APs) de la UTMACH	
WPA3 (Wi-Fi Protected Access 3)	□
EAP (Extensible Authentication Protocol)	□
RADIUS (Remote Authentication Dial-In User Service)	□
SSL/TLS (Secure Sockets Layer / Transport Layer Security)	□
¿Se realiza un monitoreo proactivo de los Access Points (APs) para detectar actividades sospechosas o no autorizadas en el departamento de TI?	
Sí, mediante un sistema automatizado de detección de intrusiones	□
Sí, mediante revisiones manuales regulares	□
Sí, pero solo cuando se sospecha de un problema	□
No, pero se planea implementarlo en el futuro	□
No, no se realiza monitoreo proactivo de los APs	□
¿Detalle el procedimiento para la actualización y parcheo de seguridad de los APs?	
¿Detalle algún incidente de seguridad relacionado con la red Wi-Fi (como intrusiones no autorizadas, interceptación de datos, ¿etc.)?	
En su rol de gestión de Access Points (APs), ¿ha recibido capacitación específica en seguridad de redes?	
Sí, capacitación formal y completa en seguridad de redes	□
Sí, pero solo capacitación básica o introductoria	□
Sí, capacitación continua y actualizada regularmente	□
No, pero se planea recibir en el futuro	□
No, no he recibido ninguna capacitación específica en seguridad de redes	□
¿Se proporciona formación regular a los usuarios de la red sobre amenazas de seguridad y buenas prácticas de seguridad?	

Sí, se proporciona formación regular y completa a todos los usuarios	□
Sí, pero la formación es solo básica y no cubre todos los aspectos de seguridad	□
Sí, pero solo se dirige a usuarios específicos (como personal de TI)	□
No, pero se planea implementar en el futuro	□
No, no se proporciona formación en seguridad a los usuarios de la red	□

¿Tiene alguna sugerencia específica para mejorar la seguridad de la red Wi-Fi en la universidad?

SEGURIDAD DE LA INFORMACIÓN DE LOS SERVIDORES EN LA UNIVERSIDAD TÉCNICA DE MACHALA

Esta sección busca recoger datos dentro del departamento de servidores en el área de TIC. La información proporcionada en este cuestionario será tratada de forma confidencial y se utilizará exclusivamente con fines de investigación.

¿Ha recibido capacitación específica en seguridad para la gestión de servidores como DS_SRV_MOODLE_HISTORICO, DS_SRV_UAIC_PORTAL, ¿u otros servidores similares en el area de TI?

Sí, capacitación formal y completa específica para estos servidores	□
Sí, pero la capacitación es general y no específica para estos servidores	□
Sí, capacitación continua y actualizada regularmente	□
No, pero se planea recibir en el futuro	□
No, no he recibido capacitación específica para la gestión de estos servidores	□

En una escala del 1 al 5, ¿cómo evaluaría su conocimiento en las prácticas de seguridad aplicadas a los servidores específicos de la universidad (ej. DS_SRV_EDUROAM, DS_SRV_GESCONT)?

□ 1	□ 2	□ 3	□ 4	□ 5

¿Qué políticas de manejo de contraseñas conoce o está familiarizado en el departamento de TI? (Seleccione todas las opciones que apliquen)

Requerimiento de complejidad de la contraseña (combinación de letras, números, símbolos)	□
Cambio periódico de contraseñas (por ejemplo, cada 3 o 6 meses)	□
Uso de gestores de contraseñas para almacenar y generar contraseñas	□
Prohibición de reutilizar contraseñas antiguas	□

¿Qué políticas de respaldo de datos conoce o está familiarizado en el departamento de TI? (Seleccione todas las opciones que apliquen)

Copias de seguridad completas a intervalos regulares	□
Copias de seguridad incrementales	□
Copias de seguridad diferenciales	□

Utilización de almacenamiento en la nube para copias de seguridad	□
¿Con qué frecuencia se aplican estas políticas y procedimientos en la gestión diaria de los activos de servidores en el departamento de TI?	
Constantemente, en todas las operaciones y actividades	□
Diariamente	□
Semanalmente	□
Mensualmente	□
Solo en revisiones periódicas o auditorías	□
¿Recomendaría alguna herramienta o práctica de seguridad específica para implementar en servidores como DS_SRV_TITULACION o DS_SRV_DIRECTORY_2012_GROUP en el departamento de TI?	
Fortalecimiento de las políticas de contraseñas y autenticación	□
Implementación de firewalls y sistemas de detección/preventivos de intrusiones	□
Uso de software antivirus y antimalware actualizado	□
Configuración de VPNs para accesos remotos seguros	□
"¿Qué medidas adicionales considera que podrían fortalecer la seguridad de la información en el área de servidores en el departamento de TI?"	
SEGURIDAD DE LA INFORMACIÓN DE SOFTWARE EN LA UNIVERSIDAD TÉCNICA DE MACHALA	
Esta sección busca recoger datos de la infraestructura de redes del área de TIC. La información proporcionada en este cuestionario será tratada de forma confidencial y se utilizará exclusivamente con fines de investigación.	
De las siguientes herramientas de software, marque cuáles utiliza regularmente en su trabajo (marque todas las que correspondan)	
Sistemas de gestión de bases de datos (por ejemplo, MySQL, SQL Server)	□
Herramientas de monitoreo de redes (como Nagios, Zabbix)	□
Plataformas de virtualización (por ejemplo, VMware, Hyper-V)	□
Herramientas de gestión de proyectos (como Jira, Trello)	□
¿De los siguientes problemas de seguridad de software, ha experimentado alguno en su trabajo en el entorno de desarrollo? (Marque todos los que correspondan)	
Vulnerabilidades de inyección SQL	□
Cross-site scripting (XSS)	□
Fallos de autenticación y gestión de sesiones	□
Exposición de datos sensibles	□

Configuración incorrecta de seguridad	□
En el contexto de su entorno de desarrollo, ¿cuáles de las siguientes medidas de seguridad de la información se implementan regularmente para garantizar la confidencialidad, integridad y disponibilidad de los datos manejados a través de los softwares utilizados?	
Encriptación de datos en tránsito y en reposo	□
Autenticación fuerte y control de acceso	□
Realización de auditorías y revisiones de código regularmente	□
Uso de firewalls y sistemas de detección de intrusiones	□
¿Cuáles de los siguientes protocolos de acceso a software tiene implementados en su área de trabajo? (Marque hasta 5 opciones)	
SSH (Secure Shell) para acceso remoto seguro	□
RDP (Remote Desktop Protocol) para control remoto de escritorio	□
FTP/SFTP (File Transfer Protocol/Secure File Transfer Protocol) para transferencia de archivos	□
VPN (Virtual Private Network) para acceso remoto cifrado	□
¿Se realizan auditorías periódicas de seguridad para los softwares utilizados en su área de trabajo?	
Sí, se realizan auditorías de forma mensual	□
Sí, se realizan auditorías de forma trimestral	□
Sí, se realizan auditorías de forma semestral	□
Sí, se realizan auditorías de forma anual / cuando es necesario	□
No, no se realizan auditorías periódicas de seguridad	□
En su entorno de desarrollo, ¿qué métodos utiliza regularmente para administrar los accesos y permisos en las aplicaciones? (Marque hasta 5 opciones)	
Control de acceso basado en roles (RBAC)	□
Listas de control de acceso (ACLs)	□
Gestión de identidades y accesos (IAM)	□
Autenticación multifactor (MFA)	□
¿Cuáles de las siguientes estrategias para asegurar la privacidad y seguridad de los datos implementa en su entorno de desarrollo? (Marque hasta 5 opciones)	
Encriptación de datos en tránsito y en reposo	□
Uso de redes privadas virtuales (VPN) para el acceso remoto seguro	□
Autenticación multifactor (MFA)	□
Anonimización y pseudonimización de datos sensibles	□

¿Cómo reacciona ante comportamientos inusuales o sospechosos en las aplicaciones que utiliza en su entorno de desarrollo?	
¿Gestionas las actualizaciones de software en tu espacio de trabajo?	
Sí, gestiono todas las actualizaciones de software personalmente	☐
Sí, pero en colaboración con un equipo o departamento específico	☐
No, pero superviso o reviso el proceso realizado por otro equipo o departamento	☐
No, otro equipo o departamento se encarga completamente de ello	☐
No estoy seguro/a de cómo se gestionan las actualizaciones de software en mi espacio de trabajo	☐
¿De los siguientes protocolos para reportar fallos o vulnerabilidades en el software tiene implementado en su espacio de trabajo?	
Sistema de tickets o seguimiento de incidencias	☐
Protocolo de reporte a través de correo electrónico	☐
Reuniones regulares para discutir problemas de seguridad	☐
Herramientas de colaboración en línea para reportar y seguir problemas (como Slack, Teams)	☐
¿Recibe información regular sobre amenazas de seguridad cibernética relacionadas con los softwares utilizados en su entorno de desarrollo?	
Sí, recibo información regularmente de forma constante y en tiempo real	☐
Sí, recibo información regularmente, pero no de forma inmediata	☐
Sí, pero solo en casos de alertas de seguridad críticas o importantes	☐
Ocasionalmente, pero no de forma sistemática o regular	☐
No, raramente o nunca recibo este tipo de información	☐
¿Hay algún aspecto de seguridad de la información que considere que necesita más atención o mejora en su área?	

Muchas gracias por su tiempo y colaboración. Sus respuestas son muy valiosas para esta investigación.