UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER

Título del proyecto:
Diseño de políticas de Ciberseguridad enfocadas a una institución de nivel superior caso Instituto Rumiñahui
Línea de Investigación:
Ciencias de la ingeniería aplicadas a la producción, sociedad y desarrollo sustentable
Campo amplio de conocimiento:
Tecnologías de la Información y la Comunicación (TIC)
Autor/a:
Marco Xavier Nacimba Nacimba
Tutor/a:
Mg. Renato Mauricio Toasa G PhD. Maryory Urdaneta

Quito – Ecuador

2024

APROBACIÓN DEL TUTOR

Yo, Mg. Renato Mauricio Toasa G con C.I: 1804724167 en mi calidad de Tutor del proyecto de investigación titulado: Diseño de políticas de Ciberseguridad enfocadas a una institución de nivel superior caso Instituto Rumiñahui.

Elaborado por: Marco Xavier Nacimba Nacimba, de C.I: 1723400014, estudiante de la Maestría en Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2024

Firmado electrónicamente por:
RENATO MAURICIO
TOASA GUACHI

_____

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Marco Xavier Nacimba Nacimba con C.I: 1723400014, autor/a del proyecto de titulación denominado: Diseño de políticas de Ciberseguridad enfocadas a una institución de nivel superior caso Instituto Rumiñahui. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., marzo de 2024

Firmado electrónicamente por:
MARCO XAVIER
NACIMBA NACIMBA

_____

Firma

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

La ciberseguridad se ha convertido en un campo de vital importancia en la era digital y de la información en la que vivimos. La constante evolución de las amenazas cibernéticas plantea un desafío significativo para las organizaciones, que deben mantenerse a la vanguardia de las últimas tendencias y técnicas utilizadas por los actores maliciosos. Esta investigación se propone abordar este desafío mediante un enfoque integral y exhaustivo de las amenazas emergentes en ciberseguridad.

La importancia de este estudio radica en su enfoque basado en tres principios fundamentales: inteligencia, prevención y respuesta. La inteligencia de amenazas se centra en la recopilación y análisis de información para identificar y comprender las amenazas emergentes. La prevención se enfoca en implementar controles y defensas adaptables para mitigar estos riesgos. La respuesta se refiere a la capacidad de las organizaciones para responder de manera efectiva a los ataques cibernéticos mediante la implementación de procesos y procedimientos claros.

El Instituto Rumiñahui es una institución educativa ubicada en el cantón Rumiñahui reconocida por su compromiso con la excelencia académica y la formación integral de sus estudiantes. Con una larga trayectoria en el ámbito educativo, el Instituto Rumiñahui se distingue por su enfoque en el desarrollo personal, académico y cultural de sus alumnos, así como por su compromiso con la innovación pedagógica y tecnológica.

La institución ofrece apertura para la investigación al permitir el uso de herramientas para la prueba de posibles vulnerabilidades adicional puede colaborar facilitando entrevistas con personal técnico, administrativo y docente que estén familiarizados con la seguridad cibernética en el entorno educativo.

Problema de investigación

A pesar del creciente reconocimiento de la importancia de la ciberseguridad en el entorno educativo, muchas instituciones enfrentan desafíos para identificar, comprender y mitigar las amenazas emergentes en ciberseguridad, lo que pone en riesgo la integridad de los datos, la privacidad de los usuarios y la continuidad de las operaciones. En el caso del Instituto Rumiñahui, se desconoce la naturaleza y la magnitud de las amenazas cibernéticas que enfrenta la institución, así como la efectividad de las medidas de seguridad implementadas actualmente.

Este problema se deriva de la necesidad de:

1. Identificar las amenazas emergentes específicas que afectan al Instituto Rumiñahui en el contexto de su entorno educativo.

2. Comprender cómo estas amenazas pueden impactar la integridad, confidencialidad y disponibilidad de los datos y sistemas del instituto.

3. Evaluar la efectividad de las medidas de seguridad existentes para mitigar estas amenazas.

4. Proporcionar recomendaciones específicas para mejorar la postura de ciberseguridad del Instituto Rumiñahui y proteger sus activos digitales y su comunidad educativa.

Con lo cual el problema de investigación que surge es:

¿Cuáles son las amenazas emergentes a la ciberseguridad que afectan al Instituto Rumiñahui en el contexto de su entorno educativo?

Objetivo general

Elaborar políticas de seguridad en base a un análisis de ataques y vulnerabilidades detectadas, en una institución de nivel superior, con el fin de fortalecer su resiliencia ante amenazas emergentes, garantizando así la protección de su infraestructura, datos y recursos digitales.

Objetivos específicos

- Contextualizar los fundamentos teóricos sobre amenazas emergentes en ciberseguridad en el contexto de instituciones educativas, incluyendo las últimas tendencias y desarrollos en el campo de la seguridad cibernética.
- Diagnosticar el estado actual de la ciberseguridad en el Instituto Rumiñahui, determinando las amenazas cibernéticas más relevantes y sus posibles impactos en los sistemas y datos de la institución.
- Diseñar las políticas propuestas para mitigar posibles amenazas.
- Validar la efectividad y pertinencia de las medidas de seguridad propuestas para el Instituto Rumiñahui a través de la retroalimentación y revisión por parte de expertos en ciberseguridad, con el fin de garantizar su idoneidad frente a las amenazas identificadas y las necesidades institucionales.

Vinculación con la sociedad y beneficiarios directos:

La ciberseguridad es un tema crítico para las instituciones educativas. Las amenazas emergentes a la ciberseguridad representan un riesgo significativo para los datos y sistemas de estas instituciones. Por ello, es importante realizar investigaciones para identificar, evaluar y mitigar estas amenazas.

El tema de proyecto "Análisis de Amenazas Emergentes en Ciberseguridad dentro de una Institución Educativa, caso de estudio Instituto Rumiñahui" tiene el potencial de contribuir a mejorar la ciberseguridad de las instituciones educativas en Ecuador. La investigación proporcionará información valiosa sobre las amenazas emergentes a la ciberseguridad que afectan al Instituto Rumiñahui. Esta información beneficiará a los siguientes beneficiarios directos:

El Instituto Rumiñahui: La investigación proporcionará al instituto información valiosa sobre las amenazas emergentes a la ciberseguridad que lo afectan. Esto permitirá al instituto tomar medidas para mitigar estas amenazas y proteger sus datos y sistemas.

La investigación ayudará al Instituto Rumiñahui a comprender mejor los riesgos a los que está expuesto. Esto le permitirá implementar medidas de seguridad específicas para mitigar estos riesgos. Por ejemplo, la investigación podría identificar que el Instituto Rumiñahui está expuesto a un mayor riesgo de ataques. En este caso, el instituto podría implementar medidas de seguridad como la formación de empleados en ciberseguridad, la implementación de copias de seguridad de datos y la utilización de soluciones de seguridad avanzadas.

La comunidad educativa del Instituto Rumiñahui: La investigación ayudará a proteger a los estudiantes, profesores y personal administrativo del instituto de los ataques cibernéticos. Esto garantizará que la comunidad educativa pueda continuar aprendiendo, enseñando y trabajando de forma segura.

La investigación ayudará a concienciar a la comunidad educativa sobre las amenazas cibernéticas. Esto ayudará a los estudiantes, profesores y personal administrativo a tomar medidas para proteger sus datos y sistemas. Por ejemplo, la investigación podría proporcionar información sobre cómo crear contraseñas seguras, evitar el phishing y proteger los dispositivos móviles.

La sociedad en general: La investigación contribuirá a mejorar la ciberseguridad de las instituciones educativas en Ecuador. Esto ayudará a proteger los datos sensibles de los estudiantes, profesores y personal administrativo de estas instituciones.

La investigación proporcionará información valiosa sobre las amenazas emergentes a la ciberseguridad que afectan a las instituciones educativas en Ecuador. Esta información podría ser utilizada por otras instituciones educativas para mejorar su ciberseguridad.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

La ciberseguridad ha adquirido una importancia cada vez mayor en el mundo moderno, ya que estamos constantemente expuestos a nuevas amenazas en el entorno digital, y ello debido a la creciente interconexión de miles de millones de dispositivos en línea (Cisco Networking Academy, s.f.), es fundamental comprender los conceptos básicos de la ciberseguridad y cómo protegernos en línea.

1.1. Contextualización general del estado del arte

La seguridad informática en el ámbito educativo es un tema de creciente relevancia en la actualidad, dado el constante avance de la tecnología y la creciente digitalización de los procesos educativos. En este contexto, resulta fundamental abordar la importancia de la protección de datos y sistemas.

Ciberseguridad

Se define como la práctica o medidas necesarias de protección y cuidado de los sistemas cibernéticos, especialmente aquella información confidencial que pudiera ser vulnerable ante posibles ataques digitales que puedan darse dentro o fuera de las organizaciones, también es conocida como seguridad de las tecnologías de la información creada para combatir las amenazas a los sistemas en red o aplicaciones (IBM, s.f.).

Definición de amenazas emergentes en ciberseguridad

A medida que la tecnología avanza, también lo hacen las tácticas y técnicas utilizadas por los actores malintencionados para comprometer la seguridad de los sistemas y datos. Algunas de las amenazas emergentes en ciberseguridad son:

1. Inteligencia Artificial (IA) generativa: “La capacidad de los sistemas de IA para generar contenido, como texto, audio e imágenes, con un nivel de calidad cada vez más alto, plantea desafíos en términos de detección de contenido falso y manipulación de información” (Stanford University, 2021).

2. Industria 4.0 y el Internet de las cosas (IoT): “El aumento de la conectividad y la interconexión de dispositivos en la industria 4.0 y el IoT también conlleva riesgos de seguridad. Las vulnerabilidades

en los dispositivos y sistemas conectados pueden ser explotadas por actores maliciosos para acceder a información confidencial o interrumpir operaciones críticas" (Mora Sánchez & Marín Guerrero, 2020).

3. Amenazas futuras y riesgos emergentes: La evolución constante del panorama de amenazas cibernéticas hace que sea necesario anticiparse a las amenazas futuras y los riesgos emergentes. Esto implica estar al tanto de las nuevas técnicas de ataque, como el ransomware, el phishing avanzado y los ataques dirigidos, y desarrollar estrategias de defensa adecuadas (Heavey, 2022).

4. Ciberseguridad en la inteligencia artificial y el aprendizaje automático: A medida que la IA y el aprendizaje automático se vuelven más omnipresentes, también aumenta el peligro de seguridad asociado a la posibilidad de ataques de adversarios que operan modelos de IA, el aprovechamiento de vulnerabilidades en algoritmos de aprendizaje automático y la privacidad de los datos utilizados para entrenar los modelos (Mosquera Chere, 2021).

Estas son solo algunas de las amenazas emergentes en ciberseguridad que los investigadores y profesionales en el campo están estudiando y abordando. Es importante tener en cuenta que el panorama de amenazas cibernéticas evoluciona constantemente, por lo que es fundamental mantenerse actualizado sobre las últimas tendencias y mejores prácticas en ciberseguridad.

Importancia de la exploración y comprensión de las amenazas emergentes en ciberseguridad

La importancia de la exploración y comprensión de las amenazas emergentes en ciberseguridad radica en la necesidad de anticiparse y estar preparados para los nuevos desafíos y riesgos que surgen constantemente en el entorno digital. Al comprender y explorar estas amenazas emergentes, se pueden desarrollar estrategias y medidas de prevención y respuesta más efectivas.

La exploración del entorno brinda información esencial para identificar oportunidades emergentes y posibles amenazas (FIDE, s.f.). Al estar al tanto de las últimas tendencias y técnicas utilizadas por los actores malintencionados, las organizaciones pueden anticipar cambios y ajustar sus estrategias de manera proactiva para mantener su competitividad.

La comprensión de las amenazas emergentes permite a las empresas implementar sistemas avanzados de detección de amenazas y adelantarse a los posibles ataques (US Energy Solutions, 2023), esto es crucial para salvaguardar las operaciones y proteger los activos digitales de las organizaciones. Además, la exploración y comprensión de las amenazas emergentes en ciberseguridad ayudan a identificar las vulnerabilidades y debilidades existentes en los sistemas y a tomar medidas para mitigar los riesgos. Esto implica adoptar las mejores prácticas en ciberseguridad y estar al tanto de las regulaciones y marcos regulatorios relevantes.

La exploración y comprensión de las amenazas emergentes en ciberseguridad son fundamentales para mantenerse actualizado, anticiparse a los riesgos y desarrollar estrategias efectivas de prevención y respuesta. Esto permite proteger los activos digitales, salvaguardar las operaciones y mantener la competitividad en un entorno digital en constante evolución.

Según (Llano Casa, Gaibor Gavilanez, Cruz Caiza, & Cadena Moreano, 2021-08-19) en su artículo denominado "Importancia de políticas de seguridad Informática de acuerdo a las ISO 27001 para pequeñas y medianas empresas del Ecuador", se evidencia una preocupante falta de medidas de seguridad informática en las instituciones analizadas. Los datos recopilados de una muestra representativa de empresas revelaron los siguientes hallazgos significativos:

- Ninguna de las empresas implementa acuerdos que garanticen la confidencialidad de la información, lo que expone sus datos a posibles amenazas y violaciones de seguridad.
- Se observó un nivel alarmantemente bajo de seguridad en el control de acceso a los equipos informáticos, lo que aumenta la vulnerabilidad de las empresas a intrusiones y ataques cibernéticos.
- Sorprendentemente, ninguna de las empresas cuenta con un plan de contingencia ante desastres naturales, lo que las deja vulnerables a la pérdida total de datos en caso de eventos catastróficos.

El análisis de riesgos realizado en el estudio indica que las empresas enfrentan un riesgo significativo en áreas clave como la seguridad física de los equipos de cómputo y el control de acceso

a los sistemas de información. Estos hallazgos subrayan la urgente necesidad de implementar políticas de seguridad informática robustas y basadas en estándares reconocidos, como la ISO 27001, para proteger los activos digitales de las empresas y garantizar la continuidad del negocio frente a posibles amenazas cibernéticas.

Según (Coloma Baños & Cañizares Galarza, 2022) en su investigación destaca la importancia de proteger la integridad, confidencialidad y disponibilidad de la información y los servicios proporcionados a la comunidad educativa. Se identifican problemas como la falta de políticas y procedimientos de seguridad, la entrega de credenciales de acceso a plataformas institucionales sin control y la carencia de medidas de seguridad en la conexión de dispositivos extraíbles. La propuesta en su artículo incluye la aplicación del modelo PDCA (Planificar, Hacer, Verificar y Actuar) y la adopción de normas ISO/IEC 27000 para la gestión de la seguridad de la información.

1.2. Proceso investigativo metodológico

El enfoque metodológico adoptado para esta investigación es de naturaleza mixta, tanto cualitativa como cuantitativa, puesto que se realizaron encuestas para obtener datos estadísticos y se realizaron entrevistas con el personal técnico del área. Estos datos se pueden utilizar para evaluar la efectividad de las medidas de seguridad existentes y para identificar las amenazas emergentes que tienen un mayor impacto en la integridad, confidencialidad y disponibilidad de los datos y sistemas del instituto.

La metodología de investigación mixta que se utilizó en este trabajo fue desarrollada en etapas secuenciales y rigurosas, incluyendo:

1. Encuestas

Como parte de la recolección de datos se ejecutó una encuesta dirigida hacia el personal técnico de la institución (ver anexo 1) la cual buscaba obtener información referente a las principales amenazas que ha enfrentado la organización en el campo de la seguridad informática además de determinar si existe o no una cultura de ciberseguridad.

2. Entrevistas en profundidad

Se llevaron a cabo entrevistas en profundidad con personal técnico dentro de la institución, los cuales fueron seleccionados cuidadosamente. Las entrevistas se realizaron utilizando un protocolo estructurado y permitieron obtener información detallada sobre las amenazas emergentes en la institución, así como las estrategias y enfoques utilizados para enfrentarlas. (Ver Análisis de resultados)

3. Análisis de vulnerabilidades

Se implementaron varias herramientas para probar la seguridad interna de la organización utilizando un enfoque de análisis cuantitativo. Este enfoque incluyó la categorización sistemática de los datos para identificar patrones, temas emergentes y relaciones significativas. El análisis se realizó de manera rigurosa y transparente, siguiendo los principios de la investigación.

4. Triangulación

Se llevó a cabo la triangulación de los hallazgos obtenidos. Esto implicó comparar y contrastar los resultados de las entrevistas con la revisión de literatura y los resultados de los test de vulnerabilidades. Además, se realizaron consultas a expertos adicionales para verificar la validez de los resultados obtenidos.

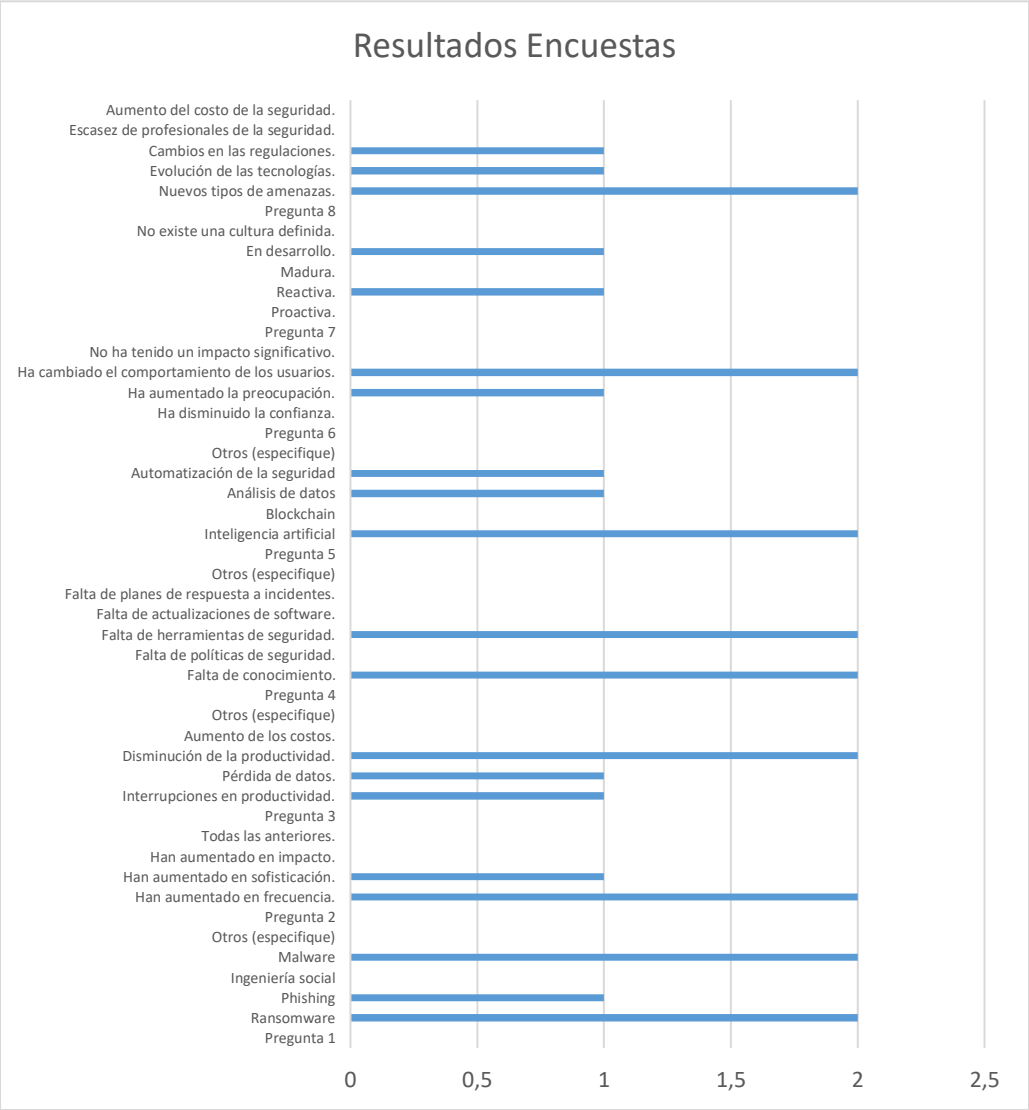
1.3. Análisis de resultados

Como parte de este estudio Se ha llevado a cabo una encuesta al personal administrativo encargado de plataformas, arrojando los siguientes resultados:

Este resumen representa la recopilación de todos los datos obtenidos en la investigación, mostrando un potencial prometedor para su aplicación a nivel general. A continuación, se exponen algunos de los resultados obtenidos en las encuestas:

Figura 1

Resultado de las encuestas realizadas al personal administrativo



Nota. Análisis basado en la encuesta realizada.

Como se muestra en la figura 1, al analizar las respuestas se ha podido identificar varios indicadores clave relacionados con la ciberseguridad:

Tipos de amenazas identificadas: Ransomware y Malware fueron mencionados como amenazas por múltiples participantes.

Tendencias en las amenazas: Se observa un consenso en que las amenazas han aumentado en frecuencia y sofisticación, lo que indica una evolución preocupante en el panorama de ciberseguridad.

Impacto en la organización: La interrupción y disminución de la productividad, así como la pérdida de datos, son aspectos críticos que afectan directamente a la operatividad y seguridad de la organización.

Causas de vulnerabilidades

La falta de conocimiento y herramientas de seguridad son factores identificados por múltiples participantes como desafíos clave que deben abordarse para fortalecer la ciberseguridad.

Tecnologías emergentes relevantes: La importancia de la inteligencia artificial en ciberseguridad es resaltada por varios participantes, junto con el análisis de datos y la automatización de la seguridad.

Impacto en la cultura organizacional: Se observa un cambio en el comportamiento de los usuarios y un aumento en la preocupación por parte de algunos participantes, lo que sugiere una mayor conciencia sobre los riesgos de seguridad.

Cultura de Seguridad: Se mencionan diferentes niveles de madurez en la cultura de seguridad, desde proactiva hasta en desarrollo, e incluso se señala la falta de una cultura definida.

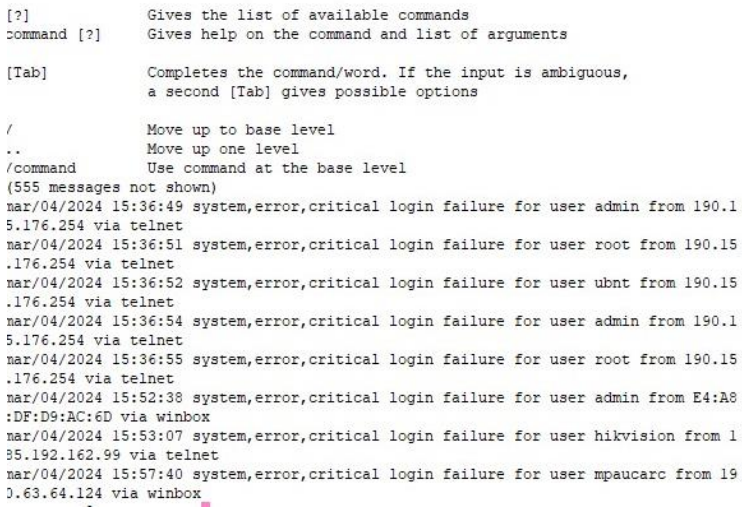
Estos puntos destacados reflejan las áreas críticas que requieren atención y acción para fortalecer la postura de ciberseguridad dentro de la organización, abordando tanto las amenazas actuales como las tendencias emergentes en el ámbito de la seguridad informática.

En base a la información preliminar recopilada para llegar a determinar las políticas más acordes en la institución se realizaron distintos tests de seguridad tomando en cuenta 3 áreas críticas:

Infraestructura

Figura 2

Registro de ataque escaneo de puertos

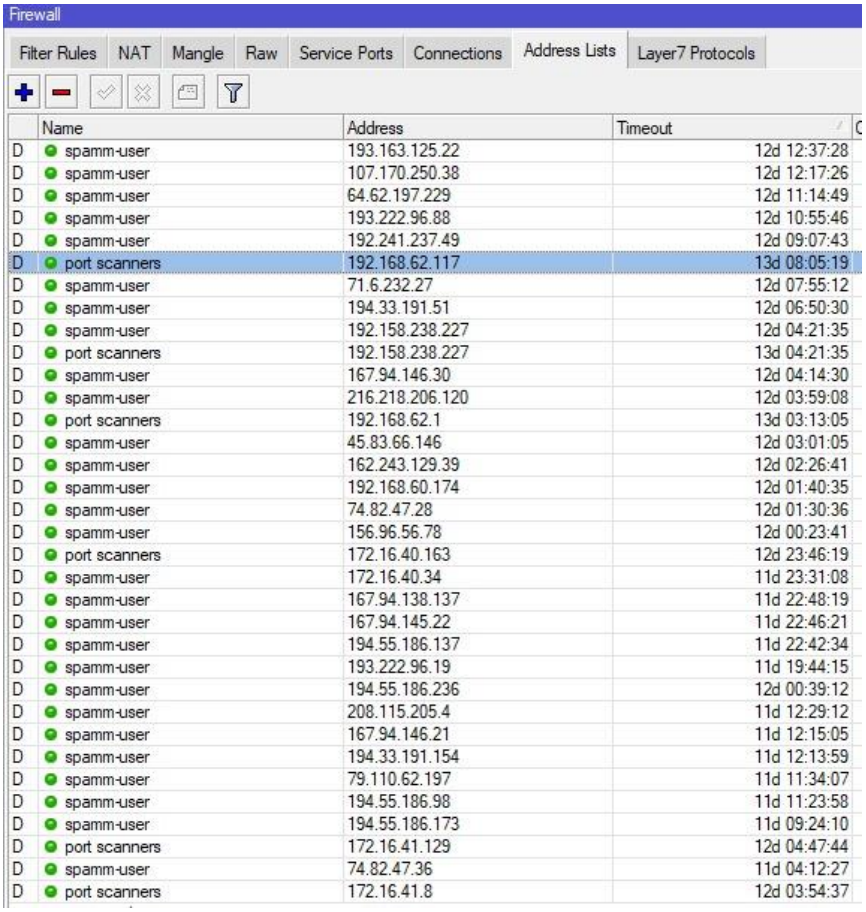


Nota. Basado en análisis propios.

Se simuló un ataque de fuerza bruta hacía la infraestructura de red como se puede apreciar en la figura 2, mediante la aplicación nmap, es importante resaltar que esto no comprometió la integridad de los activos en la institución, sin embargo, se detectó la vulnerabilidad de ciertos puertos.

Figura 3

Registro de Ataques internos y externos



	Name	Address	Timeout
D	spamm-user	193.163.125.22	12d 12:37:28
D	spamm-user	107.170.250.38	12d 12:17:26
D	spamm-user	64.62.197.229	12d 11:14:49
D	spamm-user	193.222.96.88	12d 10:55:46
D	spamm-user	192.241.237.49	12d 09:07:43
D	port scanners	192.168.62.117	13d 08:05:19
D	spamm-user	71.6.232.27	12d 07:55:12
D	spamm-user	194.33.191.51	12d 06:50:30
D	spamm-user	192.158.238.227	12d 04:21:35
D	port scanners	192.158.238.227	13d 04:21:35
D	spamm-user	167.94.146.30	12d 04:14:30
D	spamm-user	216.218.206.120	12d 03:59:08
D	port scanners	192.168.62.1	13d 03:13:05
D	spamm-user	45.83.66.146	12d 03:01:05
D	spamm-user	162.243.129.39	12d 02:26:41
D	spamm-user	192.168.60.174	12d 01:40:35
D	spamm-user	74.82.47.28	12d 01:30:36
D	spamm-user	156.96.56.78	12d 00:23:41
D	port scanners	172.16.40.163	12d 23:46:19
D	spamm-user	172.16.40.34	11d 23:31:08
D	spamm-user	167.94.138.137	11d 22:48:19
D	spamm-user	167.94.145.22	11d 22:46:21
D	spamm-user	194.55.186.137	11d 22:42:34
D	spamm-user	193.222.96.19	11d 19:44:15
D	spamm-user	194.55.186.236	12d 00:39:12
D	spamm-user	208.115.205.4	11d 12:29:12
D	spamm-user	167.94.146.21	11d 12:15:05
D	spamm-user	194.33.191.154	11d 12:13:59
D	spamm-user	79.110.62.197	11d 11:34:07
D	spamm-user	194.55.186.98	11d 11:23:58
D	spamm-user	194.55.186.173	11d 09:24:10
D	port scanners	172.16.41.129	12d 04:47:44
D	spamm-user	74.82.47.36	11d 04:12:27
D	port scanners	172.16.41.8	12d 03:54:37

Nota. Se obtiene del reporte de ataques del firewall.

Es importante el destacar que durante la entrevista con el administrador de la red este indicó que la institución sufre constantes ataques tanto internos como externos, entre los cuales se detallan escaneo y búsqueda del puerto para envió de correos lo que se puede visualizar en la figura 3.

Plataformas

Figura 4

Resultado test de Seguridad Moodle

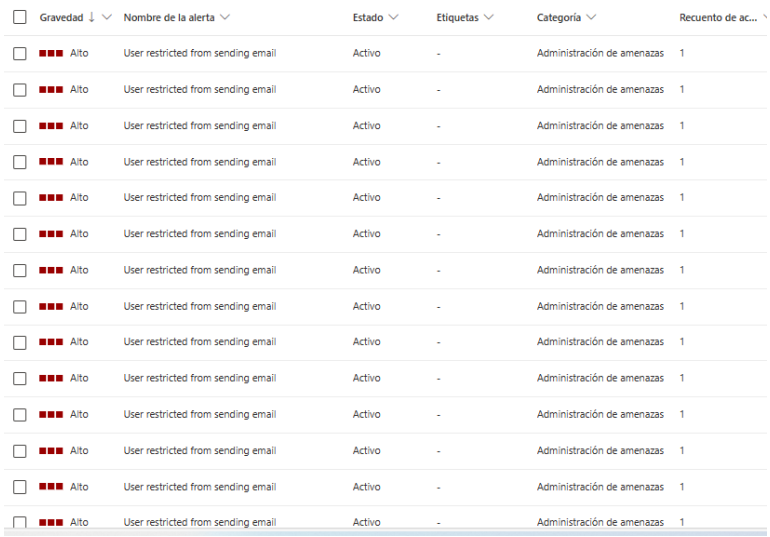
Nota. Se obtiene del reporte de seguridad de Moodle LMS.

Una vez realizado un test de seguridad en la plataforma educativa principal de la institución mediante la misma aplicación Moodle se encontraron ciertos incidentes como se puede apreciar en la figura 4, cabe destacar que varios de los mismos son críticos, los cuales radican principalmente en archivos que son accesibles desde la web. Esto presenta grandes riesgos frente a ataques, además de denotar vulnerabilidades en el servidor puesto que la institución centraliza sus plataformas y sitios web en un hosting con lo cual ante una inyección de código malicioso todo el servidor podría ser infectado.

Durante la entrevista con el administrador de plataformas manifestó que previamente tuvieron una infección en el hosting por lo cual implementaron el antivirus ImunifyAV como medida de protección.

Figura 5

Reporte Microsoft Defender ataques



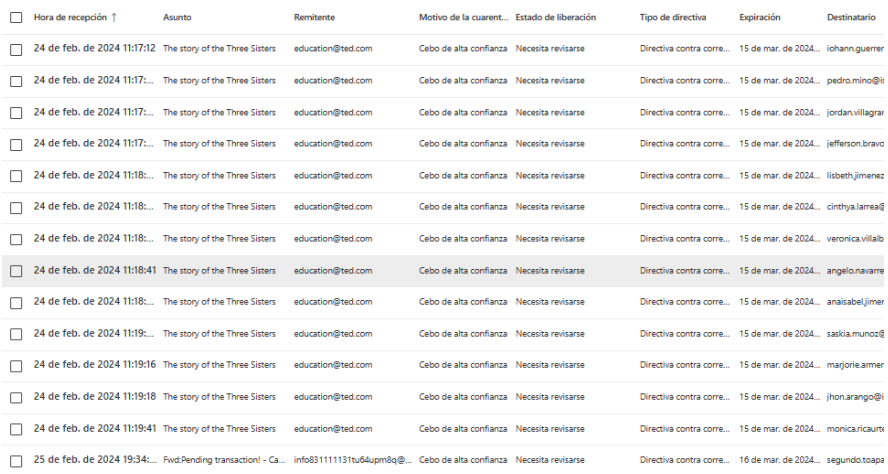
Gravedad	Nombre de la alerta	Estado	Etiquetas	Categoría	Recuento de ac...
Alto	User restricted from sending email	Activo	-	Administración de amenazas	1
Alto	User restricted from sending email	Activo	-	Administración de amenazas	1
Alto	User restricted from sending email	Activo	-	Administración de amenazas	1
Alto	User restricted from sending email	Activo	-	Administración de amenazas	1
Alto	User restricted from sending email	Activo	-	Administración de amenazas	1
Alto	User restricted from sending email	Activo	-	Administración de amenazas	1
Alto	User restricted from sending email	Activo	-	Administración de amenazas	1
Alto	User restricted from sending email	Activo	-	Administración de amenazas	1
Alto	User restricted from sending email	Activo	-	Administración de amenazas	1
Alto	User restricted from sending email	Activo	-	Administración de amenazas	1
Alto	User restricted from sending email	Activo	-	Administración de amenazas	1
Alto	User restricted from sending email	Activo	-	Administración de amenazas	1
Alto	User restricted from sending email	Activo	-	Administración de amenazas	1

Nota. Imagen extraída del reporte de Microsoft Defender para Office365.

Al realizar la entrevista con el responsable de Plataformas, este indicó que actualmente presentan un serio problema con el correo institucional, puesto que los ataques e infecciones de malware son constantes. Se realizó un test con Microsoft Defender lo cual mostró varios ataques perpetrados por usuarios infectados como se muestra en la figura 5.

Figura 6

Reporte Microsoft Defender Spam



Hora de recepción	Asunto	Remitente	Motivo de la cuarent...	Estado de liberación	Tipo de directiva	Expiración	Destinatario
24 de feb. de 2024 11:17:12	The story of the Three Sisters	education@ted.com	Cebo de alta confianza	Necesita revisarse	Directiva contra corre...	15 de mar. de 2024...	iohann.guerrer
24 de feb. de 2024 11:17:...	The story of the Three Sisters	education@ted.com	Cebo de alta confianza	Necesita revisarse	Directiva contra corre...	15 de mar. de 2024...	pedro.mino@i
24 de feb. de 2024 11:17:...	The story of the Three Sisters	education@ted.com	Cebo de alta confianza	Necesita revisarse	Directiva contra corre...	15 de mar. de 2024...	jordan.villagrar
24 de feb. de 2024 11:17:...	The story of the Three Sisters	education@ted.com	Cebo de alta confianza	Necesita revisarse	Directiva contra corre...	15 de mar. de 2024...	jefferson.bravo
24 de feb. de 2024 11:18:...	The story of the Three Sisters	education@ted.com	Cebo de alta confianza	Necesita revisarse	Directiva contra corre...	15 de mar. de 2024...	lisbeth.jimenez
24 de feb. de 2024 11:18:...	The story of the Three Sisters	education@ted.com	Cebo de alta confianza	Necesita revisarse	Directiva contra corre...	15 de mar. de 2024...	cinthya.larrea@
24 de feb. de 2024 11:18:...	The story of the Three Sisters	education@ted.com	Cebo de alta confianza	Necesita revisarse	Directiva contra corre...	15 de mar. de 2024...	veronica.villalb
24 de feb. de 2024 11:18:41	The story of the Three Sisters	education@ted.com	Cebo de alta confianza	Necesita revisarse	Directiva contra corre...	15 de mar. de 2024...	angelo.navarre
24 de feb. de 2024 11:18:...	The story of the Three Sisters	education@ted.com	Cebo de alta confianza	Necesita revisarse	Directiva contra corre...	15 de mar. de 2024...	anaisabel.jimer
24 de feb. de 2024 11:19:...	The story of the Three Sisters	education@ted.com	Cebo de alta confianza	Necesita revisarse	Directiva contra corre...	15 de mar. de 2024...	saskia.munoz@
24 de feb. de 2024 11:19:16	The story of the Three Sisters	education@ted.com	Cebo de alta confianza	Necesita revisarse	Directiva contra corre...	15 de mar. de 2024...	marjorie.armer
24 de feb. de 2024 11:19:18	The story of the Three Sisters	education@ted.com	Cebo de alta confianza	Necesita revisarse	Directiva contra corre...	15 de mar. de 2024...	jhon.arango@i
24 de feb. de 2024 11:19:41	The story of the Three Sisters	education@ted.com	Cebo de alta confianza	Necesita revisarse	Directiva contra corre...	15 de mar. de 2024...	monica.ricaurt
25 de feb. de 2024 19:34:...	Fwd:Pending transaction! - Ca...	info831111131tu64upm8q@...	Cebo de alta confianza	Necesita revisarse	Directiva contra corre...	16 de mar. de 2024...	segundo.toapa

Nota. Reporte tomado del dashboard de seguridad de Office 365.

También se detectaron recepción de flujos masivos de spam, el mismo que fue colocado en cuarentena por Microsoft Defender como se muestra en la figura 6, diferentes ataques de spam de los últimos 30 días enviados al servidor de correo. Los resultados de las pruebas de penetración revelaron:

- Existen vulnerabilidades importantes en los sistemas informáticos del Instituto.
- Los sistemas informáticos del Instituto necesitan mayor a tensión para asegurar la protección contra ataques informáticos.

Análisis de riesgos

- Se realizó un análisis de riesgos para identificar, evaluar y priorizar los riesgos de seguridad informática en el Instituto.

Los resultados del análisis de riesgos revelaron:

- Los principales riesgos de seguridad informática en el Instituto son:
- Acceso no autorizado a la información confidencial
- Interrupción del servicio educativo

Pérdida de Productividad

- Afectación en la imagen de los servicios en línea de la institución

Análisis documental

Se revisó la documentación existente en el Instituto relacionada con la seguridad informática, incluyendo:

- Políticas de seguridad informática
- Planes de seguridad informática
- Informes de auditorías de seguridad
- Registros de incidentes de seguridad

Los resultados del análisis documental revelaron:

- No existe una política de seguridad informática formal y actualizada.

- No se ha realizado un análisis de riesgos de seguridad informática.
- No se han implementado medidas de control de acceso adecuadas.
- No se ha realizado un plan de formación en seguridad informática para el personal.
- No se ha implementado un plan de respuesta a incidentes de seguridad.

Entrevistas

Se realizaron entrevistas a personal administrativo del Instituto de las áreas de:

- Redes
- Plataformas

Los resultados de las entrevistas revelaron:

- El personal tiene una baja percepción del riesgo de seguridad informática.
- El personal no tiene suficiente conocimiento sobre las medidas de seguridad informática.
- No existe una cultura de seguridad informática en el Instituto.

CAPÍTULO II: PROPUESTA

2.1. Fundamentos teóricos aplicados

Análisis de Vulnerabilidades:

El análisis de vulnerabilidades es una herramienta crucial para identificar las debilidades en los sistemas informáticos que pueden ser explotadas por los atacantes.

La propuesta se basa en una combinación de técnicas de análisis de vulnerabilidades, incluyendo análisis de amenazas, evaluación de riesgos y pruebas de penetración (Valencia Lomas, 2023).

Desarrollo de Políticas:

Las políticas de seguridad son esenciales para establecer un marco de trabajo claro y consistente para la protección de la información.

La propuesta se basa en la norma ISO/IEC 27001, que proporciona un marco para la elaboración de políticas de seguridad.

Adicionalmente, se consideran las recomendaciones del SANS Top 25 y los CIS Controls, que ofrecen listas de las vulnerabilidades más comunes y las medidas de seguridad recomendadas.

Implementación y Capacitación:

La implementación y la capacitación son dos aspectos críticos para el éxito de cualquier iniciativa de seguridad.

La propuesta se basa en el uso de guías de buenas prácticas, manuales de seguridad y técnicas de aprendizaje experiencial para asegurar una implementación efectiva de las medidas de seguridad.

Monitoreo y Evaluación:

El monitoreo y la evaluación son esenciales para asegurar que las medidas de seguridad implementadas sean efectivas y para identificar áreas de mejora.

La propuesta se basa en la norma ISO 27001 y el NIST Cybersecurity Framework, que ofrecen marcos para la monitorización y evaluación de la seguridad.

Adicionalmente, se propone la utilización de análisis de métricas y auditorías de seguridad para evaluar el estado de la seguridad del sistema.

Marco Normativo:

La propuesta se ajusta a la Ley Orgánica de Telecomunicaciones, que protege los datos de los estudiantes, docentes y personal administrativo del Instituto Rumiñahui.

Adicionalmente, se toma como referencia la norma ISO 27001, que proporciona un marco para la gestión de la seguridad de la información.

2.2. Descripción de la propuesta

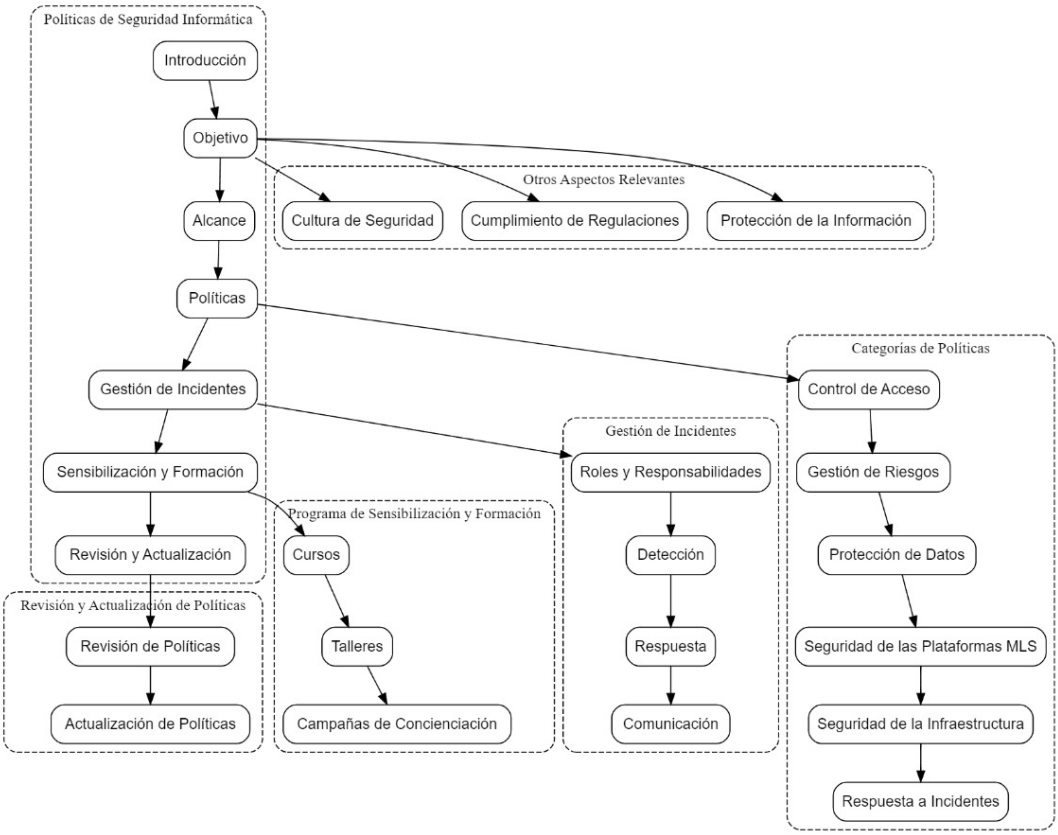
En la actualidad, la seguridad informática es esencial para garantizar el adecuado funcionamiento de cualquier institución educativa. La protección de la información confidencial, la continuidad de los servicios educativos y la confianza de la comunidad educativa dependen en gran medida de la implementación de políticas de seguridad robustas y efectivas. Con este fin, se presenta la siguiente propuesta de políticas de seguridad informática para el Instituto Rumiñahui, con el objetivo de proteger los activos informáticos, garantizar la confidencialidad de la información, asegurar la continuidad del servicio educativo y cumplir con las regulaciones vigentes:

a. Estructura general

En el siguiente cuadro (figura 7) se presenta una propuesta de políticas de seguridad informática diseñadas para el Instituto Rumiñahui. Esta propuesta tiene como objetivo primordial proteger los activos informáticos, garantizar la confidencialidad de la información, asegurar la continuidad de las operaciones educativas y cumplir con las normativas vigentes en materia de seguridad.

Figura 7

Diagrama estructura general de la propuesta



Nota. Elaboración propia.

b. Explicación del aporte

El objetivo principal de estas políticas es establecer un marco integral para la gestión de la seguridad informática en el Instituto Rumiñahui. A través de su implementación, se busca: Proteger la información confidencial y sensible del Instituto, incluyendo datos personales de estudiantes, profesores y personal administrativo.

Garantizar la disponibilidad, integridad y confidencialidad de los sistemas informáticos y los datos que estos contienen.

Prevenir, detectar y responder a incidentes de seguridad informática de manera oportuna y eficaz.

Promover una cultura de seguridad informática entre el personal docente, administrativo y estudiantes.

Cumplir con las leyes y regulaciones vigentes en materia de seguridad informática. (ver anexo 3)

Alcance

- Se aplican a todos los usuarios de los sistemas informáticos del Instituto Rumiñahui, incluyendo:
- Personal docente: Profesores, tutores, investigadores y demás personal con acceso a los sistemas informáticos del Instituto.
- Personal administrativo: Directivos, secretarios, personal de apoyo y demás personal con acceso a los sistemas informáticos del Instituto.
- Estudiantes: Alumnos matriculados en el Instituto que utilizan los sistemas informáticos para fines académicos o administrativos.

Políticas

Las políticas de seguridad informática se dividen en las siguientes categorías:

- Control de acceso: Define los mecanismos para controlar el acceso a las plataformas MLS e infraestructura informática, incluyendo la clasificación de la información, la asignación de permisos de acceso y la realización de auditorías de acceso.
- Gestión de riesgos: Establece el proceso para identificar, evaluar y mitigar los riesgos de seguridad informática, con especial atención a las amenazas específicas que pueden afectar a las plataformas MLS e infraestructura.
- Protección de datos: Define las medidas para proteger la confidencialidad, integridad y disponibilidad de los datos, incluyendo la clasificación de la información, el cifrado de datos sensibles y la implementación de medidas para prevenir la fuga de datos.
- Seguridad de las plataformas MLS: Define las medidas específicas para proteger las plataformas MLS, como la implementación de controles de acceso granulares, la segregación de redes y la monitorización de la actividad.
- Seguridad de la infraestructura: Define las medidas para proteger la infraestructura informática, como la instalación de firewalls y sistemas de detección de intrusiones, la

realización de copias de seguridad y la implementación de planes de recuperación ante desastres.

Respuesta a incidentes: Define el plan de acción para responder a incidentes de seguridad informática, incluyendo:

- Definición de roles y responsabilidades para la detección, contención, erradicación, recuperación y lecciones aprendidas en incidentes de seguridad, especialmente aquellos que involucren plataformas MLS o infraestructura crítica.
- Sensibilización y formación: Establece el programa de formación en seguridad informática para el personal del Instituto, incluyendo sesiones específicas sobre el manejo de información clasificada en plataformas MLS y las medidas de seguridad asociadas a la infraestructura.

Revisión y actualización: Define el proceso para la revisión y actualización periódica de las políticas de seguridad informática, teniendo en cuenta los avances tecnológicos, las nuevas amenazas y las regulaciones vigentes, especialmente aquellas relacionadas con la seguridad de la información clasificada y la infraestructura crítica.

Gestión de incidentes

Se establece un plan de respuesta a incidentes de seguridad informática que define los siguientes aspectos:

- Roles y responsabilidades: Se definen los roles y responsabilidades de cada persona en caso de un incidente de seguridad.
- Detección: Se establecen mecanismos para la detección temprana de incidentes de seguridad.
- Respuesta: Se definen las acciones a tomar en caso de un incidente de seguridad, incluyendo la contención del daño, la recuperación de los datos y la investigación del incidente.
- Comunicación: Se establece un plan de comunicación para informar a los usuarios y a las autoridades sobre los incidentes de seguridad. (ver anexo 3)

Sensibilización y formación

Se implementa un programa de formación en seguridad informática para el personal del Instituto, que incluye:

Cursos

Se ofrecen cursos de formación en seguridad informática para el personal docente, administrativo y estudiantes. Los cursos cubrirán temas como:

- Conceptos básicos de seguridad informática
- Amenazas y riesgos de seguridad informática
- Medidas de seguridad para proteger la información
- Buenas prácticas en el uso de los sistemas informáticos
- Responsabilidades en materia de seguridad informática

Talleres

Se realizan talleres prácticos para que el personal pueda aplicar los conocimientos adquiridos en los cursos. Los talleres se enfocarán en:

- Simulaciones de ataques informáticos
- Prácticas de configuración de seguridad en equipos
- Ejercicios de respuesta a incidentes de seguridad

Campañas de concienciación

Se realizan campañas de concienciación para promover una cultura de seguridad informática en el Instituto. Las campañas se realizarán a través de:

- Charlas informativas
- Material informativo (folletos, posters, vídeos)
- Correos electrónicos
- Intranet del Instituto

Para el éxito del programa de formación en seguridad informática, se considera fundamental:

- Involucrar a la alta dirección del Instituto en el programa.

- Designar un responsable de la seguridad informática.
- Destinar recursos humanos y financieros para la implementación del programa.
- Evaluar la efectividad del programa de forma regular.
- La sensibilización y formación en seguridad informática es un proceso continuo que debe ser parte de la cultura del Instituto Rumiñahui.

Beneficios de la sensibilización y formación en seguridad informática

- Mejora la capacidad del personal para identificar y prevenir riesgos de seguridad informática.
- Reduce la probabilidad de que ocurran incidentes de seguridad informática.
- Minimiza el impacto de los incidentes de seguridad informática.
- Fomenta una cultura de responsabilidad en materia de seguridad informática.
- Protege la información confidencial del Instituto.
- Garantiza la continuidad del servicio educativo.

Revisión y actualización

Las políticas de seguridad informática serán revisadas y actualizadas periódicamente para asegurar que se mantienen vigentes y se adaptan a los cambios en el contexto tecnológico y legal.

La implementación de las políticas de seguridad informática es fundamental para proteger los activos informáticos del Instituto Rumiñahui, garantizar la confidencialidad de la información, asegurar la continuidad del servicio educativo y cumplir con las regulaciones vigentes.

La propuesta de políticas de seguridad informática presentada en este documento es un marco integral que puede ser adaptado a las necesidades específicas del Instituto. Se recomienda que la implementación de las políticas sea un proceso gradual y participativo, con el fin de asegurar la comprensión y el compromiso de todos los usuarios de los sistemas informáticos del Instituto.

c. Estrategias y/o técnicas

Al diseñar e implementar un plan integral de seguridad informática, es crucial considerar varios aspectos clave para garantizar su efectividad y éxito a largo plazo. Estos incluyen la implementación

gradual de políticas, la sensibilización y formación del personal, la monitorización y evaluación constante, la revisión periódica de las políticas, la comunicación efectiva de las mismas y la promoción de una cultura de seguridad informática en toda la institución. Cada uno de estos elementos desempeña un papel fundamental en fortalecer las defensas cibernéticas y proteger los activos digitales de manera proactiva.

Implementación gradual: Descripción de un plan para la implementación gradual de las políticas y priorización de las medidas de seguridad más críticas.

Sensibilización y formación: Detalle de los diferentes métodos para sensibilizar y formar al personal en seguridad informática. Ejemplos de materiales de formación y actividades de concienciación.

Monitorización y evaluación: Descripción del plan para monitorizar y evaluar la eficacia de las políticas. Definición de indicadores clave de rendimiento (KPIs).

Revisión y actualización: Especificación del proceso para la revisión y actualización periódica de las políticas. Consideración de cambios en el contexto tecnológico y legal.

Comunicación efectiva: Descripción de las estrategias para comunicar las políticas a toda la comunidad educativa. Ejemplos de canales de comunicación y materiales informativos.

Cultura de seguridad: Detalle de las estrategias para promover una cultura de seguridad informática en el instituto. Ejemplos de actividades para fomentar la responsabilidad individual y colectiva.

2.3. Validación de la propuesta

Metodología

Para la validación de la propuesta se utilizó el método de criterios de especialistas, en el que se seleccionaron a un grupo de expertos correspondientes a cada área técnica dentro de la institución educativa, los cuales mediante entrevistas y encuestas corroboraron el aporte del presente trabajo para la organización como se puede constatar en el anexo 2 y 3.

Criterios de evaluación

Los criterios de evaluación utilizados fueron:

Viabilidad técnica

Factibilidad de implementar las políticas con la tecnología actual del instituto.

Necesidad de recursos adicionales para la implementación.

Eficacia

Robustez de las políticas para proteger la información.

Adecuación de las políticas a las necesidades del instituto.

Aceptación

Claridad y facilidad de comprensión de las políticas para la comunidad educativa.

Aceptación de las políticas por parte de los diferentes grupos de la comunidad educativa.

Cumplimiento normativo:

Cumplimiento de las leyes y regulaciones aplicables.

Adecuación de las políticas a los estándares de seguridad informática.

Resultados

Mediante las encuestas y entrevistas aplicadas a los expertos de la organización dentro de su área respectiva se destaca lo siguiente. Ver anexo 1.

Análisis de la evaluación del Experto 1. Criterios de evaluación:

- Impacto
- Aplicabilidad
- Conceptualización
- Actualidad
- Calidad técnica
- Factibilidad
- Pertinencia

Puntuación. Experto 1: 29/35 puntos

Conclusiones. El Experto 1 acepta la propuesta con una calificación positiva.

La propuesta cumple con los criterios de evaluación, aunque con algunas observaciones.

La seguridad informática es esencial para la organización.

Se recomienda implementar las políticas de forma inmediata.

Observaciones. La propuesta se adapta a los requerimientos de la organización, con algunas modificaciones.

Se debe crear una cultura de seguridad de la información dentro de la institución como un proceso continuo y con el apoyo de todos los miembros de la organización.

Puede haber resistencia al cambio por parte de algunos miembros de la institución, por lo que es importante realizar una campaña de sensibilización y capacitación.

Análisis de la evaluación del Experto 2. Criterios de evaluación:

- Impacto
- Aplicabilidad
- Conceptualización
- Actualidad
- Calidad técnica
- Factibilidad
- Pertinencia

Puntuación. Experto 2: 31/35 puntos

Conclusiones. El Experto 2 acepta la propuesta.

La propuesta cumple con los criterios de evaluación.

La seguridad informática es esencial para las unidades educativas.

Se recomienda implementar las políticas de forma inmediata.

Observaciones. La seguridad informática es una parte integral de la gestión educativa moderna.

Se debe crear una cultura de seguridad de la información dentro de la institución.

Puede haber resistencia al cambio por parte de los miembros de la institución.

Viabilidad técnica. Las políticas se pueden implementar con la tecnología actual del instituto.

Se requieren algunos recursos adicionales para la implementación, como capacitación del personal y adquisición de software especializado.

Eficacia. Las políticas son suficientemente robustas para proteger la información.

Las políticas se ajustan a las necesidades del instituto, con algunas recomendaciones para mejorar su cobertura.

Aceptación. Las políticas son claras y fáciles de entender para la comunidad educativa.

Se recomienda realizar una campaña de sensibilización para asegurar la comprensión y aceptación de las políticas.

Cumplimiento normativo. Las políticas cumplen con las leyes y regulaciones aplicables.

Se recomienda actualizar algunas políticas para asegurar su total cumplimiento con los últimos estándares de seguridad informática.

Recomendaciones generales propuesta. El grupo de expertos recomendó las siguientes mejoras a la propuesta:

- Incluir un plan de implementación detallado, con cronograma y presupuesto.
- Desarrollar un programa de capacitación para el personal sobre las nuevas políticas.
- Implementar un sistema de monitoreo y evaluación para medir la eficacia de las políticas.
- Revisar y actualizar las políticas periódicamente para asegurar su vigencia y cumplimiento.
- Incluir informe.

2.4. Matriz de articulación de la propuesta

En la presente matriz (tabla 1) se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

Tabla 1
Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Marco Teórico	- Seguridad informática. - Marco legal. - Diseño de políticas (Postigo Palacios, 2020).	- Revisión de literatura. - Análisis documental. - Consulta a expertos.	- Comprensión de conceptos, diagnóstico y riesgos.	- Políticas claras, plan y manuales. - Campañas de sensibilización. - Informes de seguimiento.	- Encuestas, entrevistas, análisis FODA, talleres participativos, análisis de riesgos.
Análisis del Contexto	- Contexto político, social y económico (Baldeon Quishpe, 2021).	- Observación participante. - Análisis de datos.	- Comprensión de factores, actores clave, riesgos y desafíos.	- Políticas adaptadas al contexto. - Plan de implementación con estrategias para la gestión de riesgos.	- Encuestas a stakeholders, entrevistas a expertos, análisis de documentos, grupos focales, talleres participativos.
Diseño de Políticas	- Principios y criterios para el diseño de políticas.	- Análisis de riesgos.	- Políticas efectivas, eficientes y equitativas. -	- Políticas que logran objetivos, optimizan recursos y	- Encuestas a expertos, análisis de

	- Enfoque participativo (Cruz Navarro, 2021).		Plan de implementación y estrategias de seguimiento.	protegen a la comunidad educativa.	documentos, grupos focales, talleres participativos.

Fuente. Elaboración propia**.**

CONCLUSIONES

La investigación realizada permitió comprender como el impacto potencial de las amenazas es fundamental en instituciones educativas para tomar decisiones informadas sobre la inversión en seguridad informática, enfocar recursos en las áreas de mayor riesgo y desarrollar estrategias de prevención y respuesta más efectivas.

Las principales amenazas en el instituto son el phishing, las vulnerabilidades en software y hardware desactualizado, la falta de conciencia sobre seguridad cibernética, las debilidades en la gestión de accesos y permisos, y una infraestructura de red vulnerable.

En el diseño de las políticas se priorizaron de acuerdo con su impacto potencial en la mitigación de las amenazas identificadas, asegurando la implementación gradual y sostenible de las medidas de seguridad.

Las encuestas realizadas a los expertos en las áreas técnicas de la institución demostraron la aceptación de la propuesta puntuando en el primer caso con 29 y en el segundo caso con 31 de los 35 puntos, cabe resaltar que los encuestados manifestaron el interés y la premura en una inmediata adopción de las políticas por parte de la institución.

RECOMENDACIONES

Con base en la investigación realizada, se recomienda que las instituciones educativas implementen un enfoque proactivo en la gestión de la seguridad informática, priorizando la evaluación del impacto potencial de las amenazas.

Para mejorar la seguridad informática del instituto, se recomienda implementar un plan integral que aborde las principales amenazas identificadas: phishing, software y hardware desactualizado, falta de conciencia sobre seguridad cibernética, debilidades en la gestión de accesos y permisos, e infraestructura de red vulnerable. Este plan debe incluir programas de capacitación, control de accesos, actualización de software, protección contra phishing y vulnerabilidades de la red. Al tomar estas medidas, el instituto podrá proteger sus activos críticos y reducir el riesgo de sufrir un ataque cibernético.

Con el fin de asegurar la implementación efectiva y sostenible de las medidas de seguridad, se recomienda priorizar las políticas de acuerdo con su impacto potencial en la mitigación de las amenazas identificadas. Esto permitirá enfocar los recursos disponibles en las áreas de mayor riesgo y garantizar un retorno de la inversión en seguridad informática.

En vista de la alta aceptación de la propuesta de políticas de seguridad informática por parte de los expertos técnicos de la institución, se recomienda su inmediata adopción. La alta puntuación en las encuestas (29 y 31 de 35 puntos) y el interés expresado por los encuestados en una rápida implementación indican que las políticas son relevantes, factibles y tienen un alto potencial para mejorar la seguridad informática de la institución.

BIBLIOGRAFÍA

Álvarez del Carpio, M. J. (s/f). Importancia del análisis de la situación y exploración del entorno en la toma de decisiones empresariales. [Documento en línea]. Disponible: https://www.fide.edu.pe/blog/detalle/importancia-del-analisis-de-la-situacion-y-exploracion-del-entorno-en-la-toma-de-decisiones-empresariales/ [Consulta: 2023, Noviembre 16].

Cisco Networking Academy. (s.f.). *Cómo funciona la ciberseguridad*. Obtenido de Cisco Networking Academy: https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

Coloma Baños, N. C., & Cañizares Galarza, F. P. (2022). La seguridad informática para la toma de decisiones en el distrito de educación 12d03. Mocache-Ecuador. *Dialnet*.

FIDE. (s.f.). Obtenido de Importancia del Análisis de la Situación y Exploración del Entorno en la Toma de Decisiones Empresariales: https://www.fide.edu.pe/blog/detalle/importancia-del-analisis-de-la-situacion-y-exploracion-del-entorno-en-la-toma-de-decisiones-empresariales/

Heavey, M. J. (2022). *Constuyendo la ciberseguridad en Chile.* Valparaíso: Biblioteca del Congreso Nacional de Chile.

IBM. (s.f.). Recuperado el 10 de diciembre de 2023, de ¿Qué es la ciberseguridad?: https://www.ibm.com/es-es/topics/cybersecurity

Llano Casa, A. C., Gaibor Gavilanez, M. L., Cruz Caiza, C. C., & Cadena Moreano, J. A. (2021-08-19). Importancia de políticas de seguridad Informática de acuerdo a las ISO 27001 para pequeñas y medianas empresas del Ecuador. *Ciencias de la Ingeniería y Aplicadas*, 17.

Mora Sánchez, D., & Marín Guerrero, L. (2020). Industria 4.0: el reto en la ruta hacia las organizaciones digitales . *Revista Academica UASB-E*.

Mosquera Chere, S. O. (2021). La vinculación entre la inteligencia artificial y la seguridad cibernética en el. *Polo del Conocimiento*, 20.

Stanford University (2021). Informe Artificial Intelligence Index. Human-Centered Artificial Intelligence. [Documento en línea]. Disponible: https://aiindex.stanford.edu/wp-

content/uploads/2021/05/2021-AI-Index-Report_Spanish-Edition.pdf. [Consulta: 2023, Noviembre 14].

Valencia Lomas, G. A. (2023). ANÁLISIS COMPARATIVO DE SNIFFERS PARA APLICARLOS EN LAS. *Universidad Isarel Dspace*, 24.

ANEXOS

ANEXO 1

ENCUESTA SEGURIDAD INFORMÁTICA

¿Cuáles son las principales amenazas emergentes que afectan a las redes y plataformas del instituto en este momento?

Ransomware

Phishing

Ingeniería social

Malware

Otros (especifique)

¿Cómo han evolucionado las amenazas emergentes en los últimos años?

Han aumentado en frecuencia.

Han aumentado en sofisticación.

Han aumentado en impacto.

Todas las anteriores.

¿Qué impacto tienen las amenazas emergentes en la operación del instituto?

Interrupciones del servicio.

Pérdida de datos.

Disminución de la productividad.

Aumento de los costos.

Otros (especifique)

¿Cuáles son las principales vulnerabilidades que hacen que el instituto sea susceptible a las amenazas emergentes?

Falta de conocimiento.

Falta de políticas de seguridad.

Falta de herramientas de seguridad.

Falta de actualizaciones de software.

Falta de planes de respuesta a incidentes.

Otros (especifique)

¿Qué nuevas tecnologías se podrían implementar para mejorar la seguridad de las redes y plataformas?

Inteligencia artificial

Blockchain

Análisis de datos

Automatización de la seguridad

Otros (especifique)

¿En qué medida las amenazas emergentes han afectado la confianza de los usuarios en las redes y plataformas del instituto?

Ha disminuido la confianza.

Ha aumentado la preocupación.

Ha cambiado el comportamiento de los usuarios.

No ha tenido un impacto significativo.

¿Cómo describiría la cultura de seguridad informática en el instituto?

Proactiva.

Reactiva.

Madura.

En desarrollo.

No existe una cultura definida.

¿Qué desafíos se enfrentarán en el futuro para la seguridad de las redes y plataformas del instituto?

Proactiva.

Reactiva.

Madura.

En desarrollo.

No existe una cultura definida.

ANEXO 2

VALIDACIÓN PROPUESTA EXPERTO 1

INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: Diseño de políticas de Ciberseguridad enfocadas a una institución de nivel superior caso Instituto Rumiñahui.

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Mg. Carlos Gómez

Título obtenido
Magister en Telemática Mención en Calidad en el Servicio
Cédula de Identidad
1721719696
E- mail
carlos.gomez@ister.edu.ec
Institución de Trabajo
Instituto Universitario Rumiñahui
Cargo
Administrador Plataformas LMS
Años de experiencia en el área
7

1

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque **una X** en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: Diseño de políticas de Ciberseguridad enfocadas a una institución de nivel superior caso Instituto Rumiñahui.

Indicador	*Descripción*	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*		*X*			
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*		***X***			
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*			***X***		
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*		***X***			
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*		***X***			
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*	***X***				
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	*X*				
Total		*10*	*16*	*3*		

Observaciones:

La propuesta es adecuada acorde a las necesidades de la institución, no obstante, por la resistencia al cambio podría tomar algo de tiempo su implementación completa.

Recomendaciones

Es recomendable la implementación de estas políticas de forma inmediata dado que la resistencia al cambio dentro de la organización podría retrasar el proceso.

Lugar, fecha de validación: Sangolquí 09-03-2024

Firma del especialista

2

ANEXO 3

VALIDACIÓN PROPUESTA EXPERTO 2

INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: Diseño de políticas de Ciberseguridad enfocadas a una institución de nivel superior caso Instituto Rumiñahui.

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Ing. Mauricio Paucar MSc.

Título obtenido
Master Universitario en Industria 4.0 MTCNA MTCTCE
Cédula de Identidad
1723118913
E- mail
mauricio.paucar@ister.edu.ec
Institución de Trabajo
Instituto Universitario Rumiñahui
Cargo
Administrador de Infraestructura de red
Años de experiencia en el área
5

1

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque **una X** en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: Diseño de políticas de Ciberseguridad enfocadas a una institución de nivel superior caso Instituto Rumiñahui.

Indicador	*Descripción*	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*	*X*				
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*		***X***			
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*			***X***		
Actualidad	*Los procedimientos actuales y los cambios científicas y tecnológicas considerados en la propuesta*	***X***				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*		***X***			
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*	***X***				
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	*X*				
Total		*20*	*8*	*3*		

Observaciones:

La propuesta es adecuada tomando en cuenta la forma en como se llevan a cabo la gestión de procesos en torno la institución

Recomendaciones

Es recomendable aplicar las políticas de forma inmediata y sistemática de tal forma de disminuir la resistencia al cambio por parte del personal.

Lugar, fecha de validación: Sangolquí 10-03-2024

EDISON MAURICIO PAUCAR CONDOR

_____

Firma del especialista

ANEXO 3

DEFINICIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

En este apartado del documento se plantea un conjunto de directrices de seguridad informática, concebidas como una herramienta para reducir los riesgos a los se encuentran expuestos estudiantes, profesores y administrativos de la Institución.

Políticas de Ciberseguridad para Estudiantes:

Se establecen políticas directas de ciberseguridad dirigidas a los estudiantes del Instituto Rumiñahui. Estas políticas están diseñadas para garantizar la protección de la información personal y promover prácticas seguras en línea dentro del entorno educativo.

1. Control de Acceso:

- Uso exclusivo de cuentas de estudiante asignadas.
- Obligación de mantener la contraseña de acceso segura y confidencial.
- No compartir credenciales de acceso con otros estudiantes.

2. Gestión de Riesgos:

- Educación sobre seguridad informática para concienciar sobre las amenazas potenciales.
- Reporte inmediato de cualquier actividad sospechosa o incidente de seguridad.

3. Protección de Datos:

- Conocimiento y respeto de las políticas de privacidad de la institución.
- Uso responsable de la información y datos proporcionados por la institución.

4. Seguridad de Plataformas LMS:

- Cumplimiento estricto de las políticas de acceso a recursos restringidos.
- Respeto de las políticas de clasificación y manejo de datos clasificados.

5. Seguridad en Infraestructura:

- Uso de dispositivos personales en la red de la institución sujeto a las políticas de seguridad establecidas.

- Actualización de software y aplicaciones instaladas en dispositivos personales utilizados para fines académicos.

6. Respuesta a Incidentes:

- Reporte inmediato de cualquier incidente de seguridad o actividad sospechosa.
- Cooperación con las autoridades y administradores de red en la investigación y resolución de incidentes.

Políticas de Ciberseguridad para Docentes:

Estas políticas establecen directrices claras para ayudar a los docentes a mantener la integridad del proceso educativo y a proteger la confidencialidad de los datos dentro del entorno digital.

1. Control de Acceso:

- Uso exclusivo de cuentas de docente proporcionadas por la institución.
- Mantenimiento de contraseñas seguras y confidenciales.

2. Gestión de Riesgos:

- Concienciación sobre riesgos de seguridad informática entre los estudiantes y colaboradores.
- Reporte de cualquier actividad sospechosa o incidente de seguridad.

3. Protección de Datos:

- Uso responsable de la información y datos de los estudiantes.
- Cumplimiento de las políticas de privacidad de la institución.

4. Seguridad de Plataformas LMS:

- Cumplimiento de las políticas de acceso y manejo de datos clasificados.
- Supervisión activa del acceso a recursos restringidos.

5. Seguridad en Infraestructura:

Cumplimiento de las políticas de seguridad en el uso de la red y sistemas de la institución.

Informar sobre cualquier vulnerabilidad o incidente de seguridad detectado.

6. Respuesta a Incidentes:

- Reporte inmediato de cualquier incidente de seguridad o actividad sospechosa.

- Cooperación con las autoridades y administradores de red en la investigación y resolución de incidentes.

7. Gestión de Contraseñas:

- Implementación de políticas de cambio regular de contraseñas y restricciones sobre la reutilización de contraseñas antiguas.
- Uso de herramientas de gestión de contraseñas para almacenar y proteger contraseñas de forma segura.

Políticas de Ciberseguridad para Personal Administrativo:

En esta sección se presentan políticas de ciberseguridad dirigidas al personal administrativo del Instituto Rumiñahui. Estas políticas proporcionan pautas claras y prácticas para ayudar al personal administrativo a mantener un entorno digital seguro y proteger la confidencialidad e integridad de la información institucional.

1. Control de Acceso:

- Implementación de medidas de autenticación fuertes para acceder a sistemas críticos.
- Restricción de privilegios de acceso según las funciones y responsabilidades del administrativo.

2. Gestión de Riesgos:

- Participación en evaluaciones regulares de riesgos y medidas para mitigarlos.
- Promoción de una cultura de seguridad informática entre el personal administrativo.

3. Protección de Datos:

- Cumplimiento estricto de las políticas de protección de datos de la institución.
- Uso seguro y responsable de la información confidencial de la institución.

4. Seguridad de Plataformas LMS:

- Cumplimiento de las políticas de acceso y manejo de datos clasificados.
- Supervisión activa del acceso a recursos restringidos.

5. Seguridad en Infraestructura:

- Implementación de medidas de seguridad en la red y sistemas de la institución.
- Mantenimiento de software actualizado y parches de seguridad aplicados en todos los sistemas.

6. Respuesta a Incidentes:

- Participación activa en la respuesta a incidentes y en la implementación de medidas correctivas.
- Registro y documentación adecuada de todos los incidentes de seguridad reportados.

7. Gestión de Contraseñas:

- Implementación de políticas de cambio regular de contraseñas y restricciones sobre la reutilización de contraseñas antiguas.
- Uso de herramientas de gestión de contraseñas para almacenar y proteger contraseñas de forma segura.

8. Colaboración Segura:

- Promoción del uso de herramientas seguras y cifradas para la colaboración en línea, como plataformas de gestión de aprendizaje seguras y correo electrónico cifrado.
- Concienciación sobre los riesgos asociados con el intercambio de información confidencial a través de canales no seguros, como el correo electrónico no cifrado.

Aviso de Cumplimiento de Normas de Seguridad Informática

Este aviso tiene el propósito de informar a todos los miembros de la comunidad educativa sobre las normas y políticas de seguridad informática establecidas por el Instituto Universitario Rumiñahui. El incumplimiento de estas normas puede resultar en acciones disciplinarias, incluyendo medidas tomadas contra los responsables de cada área específica, según se detalla a continuación:

1. Estudiantes: En caso de violación de las normas de seguridad informática por parte de estudiantes, se tomará como responsable a los docentes encargados de su supervisión, quienes deberán informar y aplicar las sanciones correspondientes de acuerdo con las políticas institucionales.

2. Docentes: Si un docente no cumple con las normas de seguridad informática, la responsabilidad recaerá en el departamento de dirección docente, que deberá tomar las medidas adecuadas para garantizar el cumplimiento de las políticas establecidas y aplicar las sanciones correspondientes según lo estipulado por la institución.

3. Administrativos: En el caso de violaciones de seguridad informática por parte del personal administrativo, el usuario será responsable directo.

La dirección de talento humano y tecnología serán responsables de analizar el caso y tomar las medidas necesarias para abordar la situación y aplicar las sanciones apropiadas de acuerdo con las políticas internas y los procedimientos establecidos.

Todos los miembros de la comunidad educativa están obligados a cumplir con las normas de seguridad informática establecidas por la institución. Esto incluye, entre otras cosas, el uso adecuado de los recursos informáticos, la protección de la información confidencial y el respeto de los derechos de propiedad intelectual. La cooperación de todos los miembros es esencial para mantener un entorno seguro y protegido digitalmente.