Revista Nexos Científicos
Enero-Junio 2024 pp. 1-11
Volumen 8, Número 1
Fecha de recepción: abril 2024

ISSN: 2773-7489
Correo: editor@istvidanueva.edu.ec
URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index
Fecha de aceptación: mayo 2024

Metodología Magerit para la evaluación de riesgos de activos de información, caso Instituto Superior Tecnológico Nelson Torres

Páez Padilla Mónica[1]; Portilla Martínez Diego [2]

[1,2] Instituto Superior Tecnológico Nelson Torres — Carrera de Desarrollo de Software, Cayambe – Ecuador
monica.paez@intsuperior.edu.ec

Resumen: Este estudio presenta un análisis completo de los riesgos de los sistemas de tecnología de la información del Instituto Nelson Torres de Cayambe, con el propósito de mejorar las medidas de seguridad de la información de la institución. Utilizando la metodología MAGERIT, que se basa en los principios de confidencialidad, integridad y disponibilidad, esta investigación identifica los activos críticos de TI, evalúa las posibles amenazas y vulnerabilidades, y propone estrategias efectivas de mitigación. El enfoque de esta investigación combina métodos cualitativos y cuantitativos, incluyendo entrevistas en profundidad con el personal administrativo y docente, encuestas estructuradas distribuidas entre la comunidad educativa y administrativa, y observación directa de la infraestructura de TI del instituto. Los datos recopilados se analizan utilizando estadísticas descriptivas e inferenciales para descubrir patrones y relaciones entre los incidentes de seguridad y las medidas de protección existentes. Los resultados resaltan riesgos significativos y proponen medidas de mitigación adaptadas para reducirlos al mínimo. Este análisis no solo busca mejorar la seguridad de TI del Instituto Nelson Torres de Cayambe, sino que también sirve como modelo para instituciones educativas similares que enfrentan desafíos similares. Este estudio enfatiza la importancia de la gestión continua de riesgos y la implementación de prácticas sólidas de seguridad de la información para proteger los datos educativos críticos y garantizar el correcto funcionamiento de los procesos académicos y administrativos.
Palabras clave: Seguridad informática, análisis de riesgos, metodología MAGERIT, gestión de riesgos

Abstract

Magerit Methodology for the Risk Assessment of Information Assets: Case Study of the Nelson Torres Higher Technological Institute

This study presents a complete analysis of the risks of the information technology systems of the Nelson Torres Institute of Cayambe, with the purpose of improving the institution's information security measures. Using the MAGERIT methodology, which is based on the principles of confidentiality, integrity and availability, this research identifies critical IT assets, evaluates potential threats and vulnerabilities, and proposes effective mitigation strategies. The approach of this research combines qualitative and quantitative methods, including in-depth interviews with administrative and teaching staff, structured surveys distributed among the educational and administrative community, and direct observation of the institute's IT infrastructure. The collected data is analyzed using descriptive and inferential statistics to discover patterns and relationships between security incidents and existing protection measures.

The results highlight significant risks and propose tailored mitigation measures to minimize them. This analysis not only seeks to improve the IT security of the Nelson Torres Institute of Cayambe, but also serves as a model for similar educational institutions facing similar challenges. This study emphasizes the importance of continuous risk management and the implementation of strong information security practices to protect critical educational data and ensure the proper functioning of academic and administrative processes.
Key Words: Informatic security, risk analysis, MAGERIT methodology, risk management

Revista Nexos Científicos
Enero-Junio 2024 pp. 1-11
Volumen 8, Número 1
Fecha de recepción: abril 2024
ISSN: 2773-7489
Correo: editor@istvidanueva.edu.ec
URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index
Fecha de aceptación: mayo 2024

1. INTRODUCCIÓN

Hoy en día, las tecnologías de la información y la comunicación juegan un papel clave en el funcionamiento y la administración de las instituciones educativas. El Instituto Nelson Torres de Cayambe no es una excepción, ya que en gran medida se basa en sus sistemas informáticos para realizar sus procesos administrativos y educativos, desafortunadamente, el uso generalizado de la tecnología también lo hace vulnerable a una cantidad de riesgos informáticos que pueden atentar contra la confidencialidad, integridad y disponibilidad de información crítica (Sánchez-Aguilar, 2021). Por lo tanto, un análisis de riesgos informáticos adecuado es fundamental para identificar y tratar las amenazas potenciales.

El análisis de riesgos informáticos es un procedimiento sistemático que permite a las organizaciones identificar las amenazas que pueden afectar a sus activos informáticos, evaluar las vulnerabilidades existentes y determinar el impacto potencial de los incidentes de seguridad. MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), desarrollada por el Ministerio de Administraciones Públicas de España. ofrece un marco estructurado para evaluar y gestionar los riesgos, asistiendo a las organizaciones en la toma de decisiones informadas sobre las medidas de seguridad a implementar.

La metodología MAGERIT se fundamenta en tres principios esenciales: la confidencialidad, la integridad y la disponibilidad de la información, su aplicación implica diversas etapas: la identificación de activos, amenazas y vulnerabilidades; la evaluación del impacto y la probabilidad de los riesgos; y la gestión de dichos riesgos a través de la implementación de medidas de mitigación. Esta metodología resulta especialmente apropiada para entornos educativos como el Instituto Nelson Torres de Cayambe, donde la protección de la información y la continuidad de los servicios son de vital importancia.

En este artículo, el objetivo principal es identificar los activos informáticos críticos de la institución, evaluar las amenazas y vulnerabilidades a las que están expuestos y proponer medidas de mitigación adecuadas para reducir los riesgos a niveles mínimos. Este análisis no solo contribuirá a mejorar la seguridad informática del instituto, sino que también servirá como un modelo para otras instituciones educativas que enfrentan desafíos similares.

2. METODOLOGÍA

Para obtener una comprensión completa y detallada de los riesgos informáticos en el Instituto Nelson Torres de Cayambe, la investigación empleará un enfoque mixto que combina métodos cualitativos y cuantitativos, al integrar la interpretación subjetiva de experiencias y percepciones con el análisis

ISSN: 2773-7489
Correo: editor@istvidanueva.edu.ec
URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index
Fecha de aceptación: mayo 2024

objetivo de datos numéricos, se obtendrá una perspectiva más robusta y comprehensiva. El tipo de investigación para este proyecto está basado en la investigación descriptiva se enfoca en realizar un análisis minucioso de los riesgos informáticos específicos que impactan al Instituto Nelson Torres de Cayambe. Este enfoque permitirá identificar con precisión las amenazas y vulnerabilidades presentes en los sistemas de información de la institución. A través de métodos como entrevistas detalladas, encuestas estructuradas y análisis estadísticos, se obtendrá una comprensión clara de la frecuencia y el impacto de los incidentes de seguridad.

Los resultados de esta investigación serán esenciales para diseñar estrategias efectivas de mitigación de riesgos y mejorar las prácticas de seguridad informática en el instituto, así como para establecer un marco sólido para la implementación de políticas y procedimientos que fortalezcan la protección de datos y sistemas críticos. Esta estrategia asegura un enfoque sistemático y fundamentado para hacer frente a los desafíos actuales en seguridad informática, proporcionando un entorno más seguro y confiable para toda la comunidad educativa del Instituto. Se realizó un análisis de la literatura concerniente con la seguridad informática, se utilizaron artículos científicos, libros especializados, normativas y estándares reconocidos como ISO 27001 y metodología MAGERIT. Esta estrategia proporcionó un sólido marco teórico actualizado sobre las mejores prácticas en la gestión de riesgos informáticos, de esta manera el estudio se basó en el conocimiento y la experiencia previa de la comunidad académica y profesional. Los instrumentos empleados fueron, entrevista al director del área de Tic, con una muestra representativa del personal administrativo y docente del instituto. Los participantes compartieron sus opiniones sobre temas de seguridad informática, las políticas de seguridad existentes y las áreas que requieren mejoras.

Por otro lado, se diseñaron y distribuyeron encuestas estructuradas a una muestra aleatoria de la comunidad educativa y administrativa del instituto, conocedores del tema. Las encuestas recopilaron datos cuantitativos sobre la percepción de riesgos, la frecuencia de incidentes reportados y la efectividad de las medidas de seguridad implementadas. Los resultados de las encuestas proporcionaron información estadísticamente significativa sobre el panorama general de la seguridad informática en el Instituto.

3. RESULTADOS Y DISCUSIÓN

4.1 LISTA DE ACTIVOS

Tabla 1.

Lista de Activos

[D] DATOS / INFORMACIÓN	**COPIA DE RESPALDO DATOS DE ACCESO A USUARIOS**
[IS] SERVICIOS INTERNOS	SERVICIO DE INTERNET SERVICIO DE TELEFONÍA SERVICIO DE MANTENIMIENTO WORLD WIDE WEB

Revista Nexos Científicos
Enero-Junio 2024 pp. 1-11
Volumen 8, Número 1
Fecha de recepción: abril 2024
ISSN: 2773-7489
Correo: editor@istvidanueva.edu.ec
URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index
Fecha de aceptación: mayo 2024

[SW] SOFTWARE (APLICACIONES INFORMÁTICAS)	SERVICIO DE INTERNET SERVICIO DE TELEFONÍA ENTORNO VIRTUAL DE APRENDIZAJE (EVA) SISTEMA DE GESTION ACADEMICA (SIGA)
[HW] HARDWARE (EQUIPO INFORMÁTICOS)	COMPUTADORAS DE ESCRITORIO COMPUTADORAS PERSONALES IMPRESORAS SWITCH ROUTER
[COM] REDES DE COMUNICACIONES	ACCESS POINT TELEFONIA IP RED LAN RED WIFI INTERNET
[COM] REDES DE COMUNICACIONES	TELEFONIA IP RED LAN RED WIFI INTERNET
[AUX] EQUIPOS AUXILIARES	CABLEADO UPS FUENTE DE ALIMENTACIÓN
[P] PERSONAL	DIRECTOR TIC LIDER SIGA

Nota. La tabla contiene todos los activos informáticos que posee el Instituto Nelson Torres. Fuente (INT, 2024

4.2. VALORACION DE ACTIVOS

Una vez que se identifican los activos informáticos, se utiliza un modelo de valoración para relacionarlos con las dimensiones especificadas por la norma ISO 27001:2005. Para ello, se emplea la metodología Magerit. Las dimensiones de seguridad de la información consideradas incluyen la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad del servicio.

Tabla 2

Escala Likert para valoración de activos

Nivel de daño	Ponderación	Descripción
Muy Alto (MA)	10	Daño muy grave pérdida total
Alto (A)	7 a 9	Daño grave
Medio (M)	4 a 6	Daño importante
Bajo (B)	1 a 3	Daño menor o leve
Despreciable (D)	0	Daño irrelevante

Nota. La tabla utilizada para valorar los activos ha sido extraída del Catálogo de elementos del Libro II de la metodología MAGERIT.

Tabla 3.

Criterios de Valoración

Valor	Criterio
10	Interrupciones en el funcionamiento de la Institución. Alteración del orden público Cierre de la Institución Publicidad negativa Incumplimiento de una ley o regulación
7 a 9	Amenazar la vida de uno o más individuos Interrumpir la operación Institucional ı Inconvenientes en la relación con el cliente
4 a 6	Afectar a un individuo o grupo de individuos Quebrantar la ley o reglamento de protección de información personal Manifestaciones o presiones significativas
1 a 3	Daños menores a un individuo o grupo de individuos Impedir parte de la operación de la empresa Afectar las relaciones internas de la organización
0	Afectar la confianza dentro de la Institución Afectar la seguridad de las personas Incidentes leves entre los implicados

Nota: La tabla de criterios detalla las valoraciones correspondientes a la Escala Likert

Aspectos o características de los datos

Cada activo será evaluado bajo las siguientes dimensiones o variables:

- ✓ [D] Disponibilidad
- ✓ [I] Integridad
- ✓ [C] Confidencialidad
- ✓ [A] Autenticidad
- ✓ [T] Trazabilidad

Revista Nexos Científicos
Enero-Junio 2024 pp. 1-11
Volumen 8, Número 1
Fecha de recepción: abril 2024
ISSN: 2773-7489
Correo: editor@istvidanueva.edu.ec
URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index
Fecha de aceptación: mayo 2024

Tabla 4.

Valoración de los Activos

ITEM	DESCRIPCIÓN DEL ACTIVO	VALORACIÓN					VALORACIÓN TOTAL
		[C]	[I]	[D]	[A]	[T]	
					[D] DATOS / INFORMACIÓN		
1	COPIA DE RESPALDO	9	9	9	8	9	44
2	DATOS DE ACCESO A USUARIOS	8	9	9	8	9	43
					[IS] SERVICIOS INTERNOS		
3	SERVICIO DE INTERNET	8	8	9	7	7	39
4	SERVICIO DE TELEFONÍA	7	8	7	7	7	36
5	SERVICIO DE MANTENIMIENTO	7	9	9	7	7	39
6	WORLD WIDE WEB	9	9	8	8	8	42
					[SW] SOFTWARE (APLICACIONES INFORMÁTICAS)		
7	OFIMÁTICA	6	7	7	6	7	33
8	ANTIVIRUS	6	7	7	6	8	34
9	SISTEMA DE GESTION EVA	7	6	6	7	6	32
10	SISTEMA DE GESTION SIGA	7	6	6	6	8	33
					[HW] HARDWARE (EQUIPOS INFORMÁTICOS)		
11	COMPUTADORAS DE ESCRITORIO	6	9	8	7	8	38
12	COMPUTADORAS PERSONALES	4	9	9	6	8	36
13	IMPRESORAS	5	8	8	6	6	33
14	SWITCH	5	8	7	7	7	34
15	FIREWALL	6	7	8	8	8	37
16	ROUTER	7	8	7	7	9	38
17	ACCESS POINT	6	8	7	8	8	37
					[COM] REDES DE COMUNICACIONES		
18	RED LAN	6	8	6	8	8	36
19	RED WIFI	6	8	7	8	7	36
20	INTERNET	7	8	7	8	8	38
					[AUX] EQUIPOS AUXILIARES		
21	CABLEADO	6	6	8	0	0	20
22	UPS	7	7	6	0	0	20
23	FUENTE DE	6	5	5	0	0	16

Revista Nexos Científicos
Enero-Junio 2024 pp. 1-11
Volumen 8, Número 1
Fecha de recepción: abril 2024

ISSN: 2773-7489
Correo: editor@istvidanueva.edu.ec
URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index
Fecha de aceptación: mayo 2024

	ALIMENTACION						
[I] INSTALACIONES							
28	OFICINAS	0	0	9	0	0	9
[P] PERSONAL							
29	COORDINADOR DE SISTEMAS INFORMÁTICOS	8	9	9	0	0	26
30	TÉCNICOS OPERATIVOS	7	8	8	0	0	23
31	COORDINADOR DE VENTAS	7	5	8	0	0	20
32	COORDINADOR DE MARKETING	7	7	8	0	0	22
33	TÉCNICO DE MANTENIMIENTO	8	6	9	0	0	23

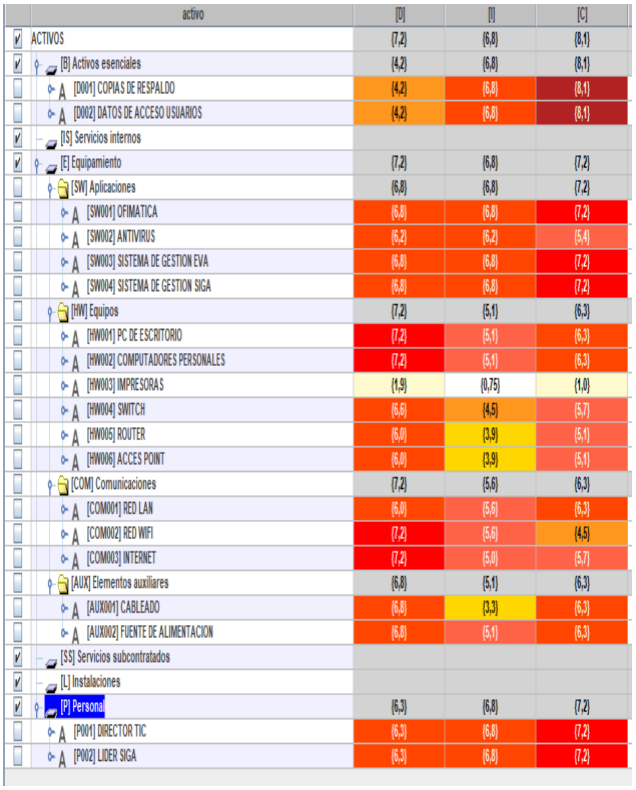
Nota: Realizada en Pilar 5.2.9 por el autor en base a los datos del Instituto Nelson Torres.

4.3 Análisis y evaluación de riesgos

En esta sección se detalla cada uno de los activos y el valor de riesgo al que se encuentran expuestos.

Figura 1.

Riesgo de los Activos



Nota: Valoración de riesgos establecidas en software por el autor.

4.4 Evaluación de Salvaguardas y medidas de protección

En esta sección se proporciona un detalle de las salvaguardas de cada uno de los activos y se evalúa el nivel de criticidad.

Revista Nexos Científicos
Enero-Junio 2024 pp. 1-11
Volumen 8, Número 1
Fecha de recepción: abril 2024

ISSN: 2773-7489
Correo: editor@istvidanueva.edu.ec
URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index
Fecha de aceptación: mayo 2024

Figura 2.

Salvaguardas de los Activos

Nota. Salvaguardas establecidas en software por el autor

Medidas de protección

Luego del análisis de activos y salvaguardas se propone controles para mitigar el riesgo de cada uno de los activos, a continuación, la Tabla 2. expone el tipo de activo y salvaguarda sugerida.

Figura 3.

Activos y Medidas de protección

Tipo de Activos	Controles Sugeridos
COPIAS DE RESPALDO **[D] DATOS**	Implementar copias de respaldo automatizadas y encriptadas, almacenadas externamente, para garantizar la disponibilidad y la integridad de los datos en situaciones de pérdida o corrupción.
CONTROL, DE ACCESO A USUARIOS **[D] DATOS**	Implementar un sistema de gestión de accesos basado en roles y privilegios, con autenticación multifactorial y auditorías regulares para asegurar que solo usuarios autorizados tengan acceso a los recursos críticos del sistema.
OFIMÁTICA **[SW] SOFTWARE**	Configurar permisos y actualizaciones frecuentes para proteger la suite ofimática contra vulnerabilidades y garantizar prácticas seguras de gestión de documentos y correos.
SISTEMA DE GESTIÓN EVA**[SW] SOFTWARE**	Implementar controles de acceso y revisiones regulares para asegurar la integridad y disponibilidad del sistema de gestión del entorno virtual de aprendizaje.
SISTEMA DE GESTIÓN SIGA**[SW] SOFTWARE**	Implementar controles de acceso y revisiones regulares para asegurar la integridad y disponibilidad del sistema de gestión del entorno virtual de aprendizaje.
ANTIVIRUS**[SW] SOFTWARE**	Implementar un software antivirus con configuraciones avanzadas de detección y prevención, asegurando la protección proactiva contra malware y amenazas cibernéticas en entornos de sistemas y redes.
COMPUTADORES	Implementar políticas de acceso, mantener software antivirus

ISSN: 2773-7489
Correo: editor@istvidanueva.edu.ec
URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index
Fecha de aceptación: mayo 2024

PERSONALES **[HW] HARDWARE**	actualizado y aplicar cifrado de datos para asegurar la integridad y confidencialidad de la información en computadores personales.
PC DE ESCRITORIO **[HW] HARDWARE**	Implementar políticas de acceso, mantener software antivirus actualizado y aplicar cifrado de datos para asegurar la integridad y confidencialidad de la información en computadores personales.
SWITCH **[HW] HARDWARE**	Aplicar directivas de seguridad en los switches para gestionar el acceso a la red y reducir riesgos de intrusión o manipulación no autorizada de datos.
ROUTERS **[HW] HARDWARE**	Implementar configuraciones de seguridad en los routers para asegurar la integridad y confidencialidad de las comunicaciones, mitigando riesgos de acceso no autorizado y ataques externos.
ACCES POINT **[HW] HARDWARE**	Configurar seguridad avanzada en los puntos de acceso para proteger redes inalámbricas contra accesos no autorizados y amenazas, garantizando la confidencialidad e integridad de los datos.
RED LAN [**COM] REDES DE COMUNICACIONES**	Implementar firewalls y sistemas de detección de intrusiones para proteger la red LAN contra accesos no autorizados y asegurar la seguridad de los activos críticos.
RED WIFI [**COM] REDES DE COMUNICACIONES**	Implementar WPA3 y cifrado AES, segmentar la red y monitorear constantemente para detectar intrusiones
INTERNET [**COM] REDES DE COMUNICACIONES**	Implementar WPA3 con cifrado AES, segmentar la red interna, monitorear continuamente en busca de intrusiones y añadir una VPN para asegurar conexiones externas
CABLEADO ESTRUCTURADO, FUENTES DE ALIMENTACION, UPS **[AUX] EQUIPOS AUXILIARES**	Implementar cableado estructurado según normativas para asegurar conexiones fiables. Usar fuentes de alimentación redundantes y estables para continuidad operativa. Integrar sistemas UPS para proteger contra cortes eléctricos y asegurar la integridad de datos y equipos críticos
PERSONAL: DIRECTOR TIC LIDER SIGA **[P] PERSONAL**	Para el personal directores de departamento TIC, es fundamental implementar políticas de acceso basadas en roles y privilegios, junto con formación continua en ciberseguridad y concienciación sobre buenas prácticas. Además, establecer protocolos robustos de respuesta a incidentes es esencial para asegurar una gestión efectiva de emergencias de seguridad informática.
PERSONAL DOCENTE Y ADMINISTRATIVO	Personal docente y administrativo debe recibir capacitación regular en seguridad informática y prácticas de manejo de datos. Es fundamental

ISSN: 2773-7489
Correo: editor@istvidanueva.edu.ec
URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index
Fecha de aceptación: mayo 2024

[P] PERSONAL	seguir protocolos estrictos para proteger la información sensible, como usar contraseñas fuertes y mantener actualizados los sistemas y software.

Nota. Controles sugeridos para cada activo crítico del Instituto Tecnológico Nelson Torres

5. DISCUSIÓN

En la era digital, las instituciones educativas se han transformado en centros neurálgicos de información crítica, almacenando datos sensibles de estudiantes, docentes y personal administrativo en sistemas interconectados. Esta dependencia tecnológica impulsa la eficiencia y la innovación educativa, pero también expone a la institución a un amplio espectro de amenazas cibernéticas en constante evolución.

Para mitigar estos riesgos, es crucial implementar una estrategia integral de seguridad informática que abarque tres niveles fundamentales:

5.1. Análisis de Riesgos Informáticos: Utilizando metodologías como MAGERIT, se identifican, evalúan y priorizan las vulnerabilidades en los sistemas de información. Este enfoque permite dirigir los recursos hacia la protección de los activos más críticos de la institución.

5.2. Implementación de Medidas de Seguridad Física y Lógica: Incluye la actualización continua de software y sistemas operativos, el despliegue de firewalls, sistemas de detección y prevención de intrusos (IDS/IPS), la segmentación de redes, el cifrado de datos confidenciales y la realización periódica de copias de seguridad con planes de recuperación ante desastres.

5.3. Capacitación del Personal y Fomento de una Cultura de Seguridad: Educación del personal docente y administrativo sobre amenazas cibernéticas, buenas prácticas de manejo de datos y procedimientos de respuesta a incidentes. Promoción de una cultura organizacional donde la seguridad de la información sea responsabilidad compartida, con campañas de sensibilización y canales claros para reportar incidentes.

Esta estrategia integral no solo protege los activos críticos de la institución educativa, sino que también prepara a su comunidad para navegar en un entorno digital seguro y resiliente ante las amenazas emergentes.

6. CONCLUSIONES

1.-El inventario y la categorización de los activos de información, así como los riesgos y amenazas asociados, ha proporcionado una base conceptual amplia sobre el panorama del Instituto Nelson Torres, este proceso ha facilitado una comprensión clara de los diversos tipos de activos de información y su importancia relativa dentro de la institución, además, el análisis de riesgos y amenazas ha permitido identificar las vulnerabilidades específicas que afectan a estos activos.

2.-El análisis actual de la gestión de activos de información en el Tecnológico Nelson Torres

ISSN: 2773-7489
Correo: editor@istvidanueva.edu.ec
URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index
Fecha de aceptación: mayo 2024

revela carencias significativas que afectan la seguridad y protección de los datos, la institución carece de políticas estructuradas y un inventario actualizado de activos, lo que dificulta la implementación de estrategias efectivas de protección y respuesta ante incidentes, la falta de capacitación en seguridad informática entre el personal aumenta la vulnerabilidad ante amenazas internas y externas.

3.-La implementación de un protocolo de seguridad o un Plan Operacional de Seguridad (POS) es crucial para el Instituto Nelson Torres, este plan debe incluir directrices claras para la gestión de activos de información, procedimientos de respuesta a incidentes y medidas de protección adecuadas. El POS debe ser revisado y actualizado periódicamente para adaptarse a las nuevas amenazas y cambios en la infraestructura tecnológica. Además, debe incluir programas de capacitación para el personal, asegurando que todos los miembros de la institución estén al tanto de las políticas y procedimientos de seguridad, y sean capaces de actuar de manera efectiva ante cualquier incidente de seguridad.

REFERENCIAS

Abrams, M. (2022). *La guerra en la sombra: Cómo los ciberataques están cambiando el mundo.* Editorial Planeta.

ACLU. (2024). *ACLU.* Obtenido de https://www.aclu.org/: https://www.aclu.org/news/privacy-technology/the-aclu-is-committed-to-protecting-your-personal-information

Carrillo, J. J. (2020). *Proceso de Ciberseguridad: Guía Metodológica para su implementación.* Revista Ibérica de Sistemas e Tecnologias de Informação.

CCN-CER-CNI. (2024). *CENTRO CRIPTOLOGICO NACIONAL*. Obtenido de https://pilar.ccn-cert.cni.es/index.php/recursos/guias-manuales

Chenhan Zhang, Shui Yu,James J Q Yu,Zhiyi Tian. (2023). Generative Adversarial Networks: A Survey on Attack and Defense Perspective. *ACM Computing Surveys*, 1-35.

Dirección General de Modernización Administrativa, P. e. (2012). *MAGERIT – versión 3.0.* © Ministerio de Hacienda y Administraciones Públicas.

Erick Guerra, H. N. (Oct. 2021). Desarrollo de un sistema de gestión para la seguridad de la. *Scientific Electronic Library Online - SciELO*.

ISO/IEC. (2018). Information technology — Security techniques — Information security management systems — Requirements. International Organization for Standardization.

Ministerio de Administraciones Públicas de España. (2024). *Metodología de Análisis y*

ISSN: 2773-7489
Correo: editor@istvidanueva.edu.ec
URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index
Fecha de aceptación: mayo 2024

Gestión de Riesgos de los Sistemas de Información (MAGERIT). Obtenido de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

O'Connor, T. (2022). *Ciberseguridad para todos: Proteja su información en línea.* Ediciones Díaz de Santos.

Pablo Israel Morales-Paredes, R. P. (2021). Ciberseguridad en plataformas educativas institucionales de educación superior de la provincia de Tungurahua - Ecuador. *Dialnet*.

Sánchez-Aguilar, J. A. (2021). Análisis y evaluación de riesgos: aplicado a EMAPAL-EP. *Dominio de las Ciencias* .