Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), septiembre-octubre 2024,
Volumen 8, Número 5.

https://doi.org/10.37811/cl_rcm.v8i5

CARACTERIZACIÓN GNOSEOLÓGICA, METODOLÓGICA, SOCIOLÓGICA Y TECNOLÓGICA LA SEGURIDAD DE REDES

EPISTEMOLOGICAL, METHODOLOGICAL, SOCIOLOGICAL AND TECHNOLOGICAL CHARACTERIZATION OF NETWORK SECURITY

Alex Enrique Blacio Roca
Instituto Superior Tecnológico Ismael Pérez Pazmiño, Ecuador

Cristhian Javier Ordoñez Cárdenas
Instituto Superior Tecnológico Ismael Pérez Pazmiño, Ecuador

Gabriel Gustavo Narváez Chiliguano
Instituto Superior Tecnológico Ismael Pérez Pazmiño, Ecuador

Jajayra Lisbeth Castillo Castillo
Instituto Superior Tecnológico Ismael Pérez Pazmiño, Ecuador

DOI: https://doi.org/10.37811/cl_rcm.v8i5.13643

Caracterización Gnoseológica, Metodológica, Sociológica y Tecnológica la Seguridad de Redes

Alex Enrique Blacio Roca[1]
alex.blacio@instipp.edu.ec
https://orcid.org/0009-0001-1270-3307
Instituto Superior Tecnológico
Ismael Pérez Pazmiño
Machala - Ecuador

Cristhian Javier Ordoñez Cárdenas
cristhian.ordonez@instipp.edu.ec
https://orcid.org/0009-0007-2031-0363
Instituto Superior Tecnológico
Ismael Pérez Pazmiño
Machala - Ecuador

Gabriel Gustavo Narváez Chiliguano
gabriel.narvaez@instipp.edu.ec
https://orcid.org/0009-0008-7223-3432
Instituto Superior Tecnológico
Ismael Pérez Pazmiño
Machala – Ecuador

Jajayra Lisbeth Castillo Castillo
jajayra.castillo@instipp.edu.ec
https://orcid.org/0009-0001-6999-7676
Instituto Superior Tecnológico
Ismael Pérez Pazmiño
Machala - Ecuador

RESUMEN

Esta investigación se centra en distintas maneras de caracterización de la seguridad de redes permitiendo conocer a profundidad la relevancia que conlleva una eficiente gestión de seguridad de redes en el "Instituto Superior Tecnológico Ismael Pérez Pazmiño campus José Ochoa León". En sentido gnoseológico, brinda los fundamentos filosóficos que afirman la importancia de la seguridad de redes, además considera teorías y modelos que explican los sucesos de vulnerabilidad y protección en ambientes tecnológicos. En este planteamiento se establece una ideología que brinda el conocimiento y la implementación de medidas de seguridad, lo cual además permite entender cómo se pueden mitigar las amenazas en los laboratorios del Instituto Ismael Pérez Pazmiño. La metodología MAGERIT se utilizará en el laboratorio del Instituto para evaluar y mejorar la seguridad de redes, identificando y clasificando amenazas, e implementando medidas de seguridad. Esta metodología es parte del "Proceso de Gestión de Riesgos" y facilita la toma de decisiones sobre los riesgos relacionados con el uso de tecnologías de la información. Al caracterizar de forma sociológica y tecnológica, la seguridad de redes se interpreta el impacto de la sociedad con el manejo en la tecnología, por ello, este proceso es relevante para la creación de estrategias de seguridad eficientes.

***Palabras Clave*:** gnoseológica, tecnológicos, seguridad, filosóficos, instituto superior Ismael Pérez Pazmiño

[1] Autor principal
Correspondencia: alex.blacio@instipp.edu.ec

Epistemological, Methodological, Sociological and Technological Characterization of Network Security

ABSTRACT

This research focuses on different ways of characterizing network security, allowing us to understand in depth the relevance of efficient network security management at the “Instituto Superior Tecnológico Ismael Pérez Pazmiño campus José Ochoa León”. In an epistemological sense, it provides the philosophical foundations that affirm the importance of network security, and also considers theories and models that explain vulnerability and protection events in technological environments. This approach establishes an ideology that provides knowledge and implementation of security measures, which also allows us to understand how threats can be mitigated in the laboratories of the Ismael Pérez Pazmiño Institute. The MAGERIT methodology will be used in the Institute's laboratory to evaluate and improve network security, identifying and classifying threats, and implementing security measures. This methodology is part of the "Risk Management Process" and facilitates decision-making on risks related to the use of information technologies. By characterizing network security in a sociological and technological, the impact of society with management on technology is interpreted, therefore, this process is relevant for the creation of efficient security strategies.

***Keywords*:** epistemology, technological, security, philosophical, Ismael Pérez Pazmiño higher institute

Artículo recibido 08 agosto 2024

Aceptado para publicación: 12 septiembre 2024

INTRODUCCIÓN

Actualmente la gestión de la seguridad de la información es el área de la ciberseguridad que se centra en la protección de las redes informáticas frente a las amenazas y vulnerabilidades de la red, brinda funciones, tales como; impedir el acceso no autorizado a los recursos de la red, detectar y neutralizar los ciberataques y las violaciones de la seguridad, garantizar que los usuarios autorizados tengan un acceso seguro a los recursos de la red de ser necesario. (IBM, 2020)

Con la creación de redes de comunicación y, especialmente, a partir del nacimiento de Internet, surgieron los ciberataques, transformando radicalmente el panorama de la seguridad informática. Antes, los atacantes necesitaban acceso físico a los dispositivos para comprometerlos, pero con la interconexión global, empezaron a operar de forma remota, superando las barreras geográficas.

Este cambio marcó el inicio de una nueva era en la protección de la información y los sistemas. El concepto de seguridad de la información comenzó a tomar forma en la década de 1960, en respuesta al creciente uso de tecnologías informáticas en instituciones gubernamentales y militares. En 1967, la Agencia de Seguridad Nacional (NSA) del Departamento de Defensa de Estados Unidos, junto con la Corporación RAND, fue pionera al desarrollar un informe que alertaba sobre las amenazas emergentes contra la seguridad de la información. (ESCRIBÁ, 2013)

La finalidad principal de la seguridad en redes es proteger los activos informáticos, un concepto que abarca no solo la información, sino también la infraestructura tecnológica y los usuarios que interactúan con ella. La seguridad, por lo tanto, no solo busca resguardar los datos que se almacenan y se transmiten a través de las redes, sino también garantizar que estos estén disponibles cuando se necesiten, sean íntegros y no hayan sido alterados, y que solo puedan ser accedidos por personas autorizadas.

Estos principios clave de la confidencialidad, integridad y disponibilidad (CIA) constituyen el eje central de cualquier estrategia de seguridad de la información. En este contexto, es vital implementar medidas que minimicen la vulnerabilidad de los datos y los equipos ante amenazas externas, como hackers y amenazas internas, como empleados malintencionados o negligencias. (ISOTools)

Además de proteger los sistemas y datos, la ciberseguridad también contempla planes de contingencia para la recuperación ante desastres, mediante la creación de copias de seguridad (**backups**) y estrategias que permitan la restauración de operaciones en caso de fallos críticos. Estas acciones aseguran que, aun

ante un ataque o incidente, las organizaciones puedan reanudar sus actividades con el menor impacto posible.

La evolución de los ataques informáticos ha obligado a que las organizaciones adopten una postura proactiva frente a las amenazas, invirtiendo en tecnologías, como la detección de intrusiones, la autenticación, entre otros, para anticipar y mitigar riesgos. La seguridad de la red y la información ya no es un elemento secundario, sino una prioridad estratégica para la protección de los datos, la continuidad del negocio y la confianza en el entorno digital. (VALENCIA, 2017)

Es por ello que en el contexto específico de los laboratorios del campus José Ochoa León, la seguridad de los equipos tecnológicos es importante debido a los beneficios que implica su aplicación, puesto que existen mil maneras de exponer a los recursos físicos, lógicos y humanos a vulnerabilidades por la falta de conocimientos necesarios para el correcto manejo.

En pocas palabras, este objetivo busca brindar los conocimientos, tanto como; gnoseológico, metodológico, sociológico y tecnológico que permitan al personal estudiantil y docente optar por soluciones de protección para los elementos que constituye la parte del software y hardware dentro del centro de cómputo garantizando integridad, confidencialidad y disponibilidad de la información en un ambiente educativo y de investigación.

La caracterización gnoseológico, metodológico, sociológico y tecnológico permite comprender de una manera amplia y con un mayor entendimiento sobre cómo administrar correctamente métodos de seguridad en la red, sin arriesgarse con la implementación innecesaria de medios obsoletos, los cuales en lugar de brindar seguridad perjudica el entorno tecnológico.

El objetivo principal de este estudio es caracterizar la seguridad de la red, con el fin de brindad una mayor comprensión para la protección en los equipos tecnológicos de los laboratorios del campus José Ochoa León.

Uno de los pilares fundamentales de la seguridad es la protección de la información, lo cual requiere una adecuada identificación y clasificación de los activos. Estos activos incluyen, entre otros, información, datos, servicios, aplicaciones, equipos, comunicaciones, recursos humanos, recursos físicos y recursos administrativos.

Es esencial reconocer que cada uno de estos activos puede estar expuesto a diferentes tipos de amenazas, lo que implica la necesidad de medidas de protección específicas.

El primer paso en la gestión de la seguridad consiste en identificar los activos existentes dentro de la organización. Esta identificación es crucial, ya que las amenazas y las estrategias de protección varían según la naturaleza del activo. Además, es indispensable valorar la importancia de cada uno de estos activos para la organización, es decir, evaluar cuán crítico es protegerlo.

Cuanto mayor sea el valor de un activo, más robustas deben ser las medidas de seguridad que se implementen para su protección. Para valorar los activos, se utilizan principalmente tres dimensiones clave: confidencialidad, integridad y disponibilidad.

La confidencialidad garantiza que la información solo sea accesible por personas o sistemas autorizados; la integridad asegura que los datos no sean alterados de forma no autorizada; y la disponibilidad se refiere a que los activos estén accesibles cuando se necesiten.

Sin embargo, en ciertos casos es necesario evaluar otras dimensiones adicionales, como la autenticidad, que verifica la legitimidad del origen de la información; la trazabilidad del uso del servicio, que permite conocer quién y cuándo ha utilizado un recurso; y la trazabilidad del acceso a los datos, que registra las acciones realizadas sobre la información.

En definitiva, el proceso de valoración y clasificación de los activos no solo ayuda a identificar qué se debe proteger, sino también a establecer las prioridades y asignar los recursos de seguridad de manera eficiente, asegurando así la continuidad de las operaciones y la minimización de riesgos.

METODOLOGÍA

El sistema experimental propuesto tiene como objetivo investigar y comprender la importancia de la seguridad de redes caracterizado de diversas maneras, incluyendo lo filosófico centrándose en la gestión de la seguridad de la información en los equipos tecnológicos de los laboratorios del campus José Ochoa León.

El sistema experimental proporcionará una comprensión profunda acerca de la carnetización, gnoseológico, metodológico, sociológico y tecnológico relacionado con la seguridad de redes en los laboratorios tecnológicos del campus José Ochoa León, así como recomendaciones prácticas para la aplicación de sistemas seguros en la información que se maneja en las instalaciones ya mencionadas.

Se espera que esta investigación permita la concientización sobre la importancia de su aplicación en el entorno tecnológico del campus.

Según el autor Uciber, s.f. gnoseológicamente la seguridad de redes da lugar en historia de su desarrollo, lo cual, se originó en el año de 1970, cuando las redes de computadoras tuvieron un gran impacto su reconocimiento. En dicho entonces, la seguridad se centraba principalmente en la autenticación de usuarios y en la protección de los datos confidenciales.

Debido a que en los 80, surgieron los primeros virus informáticos y los ataques de hackers, lo que hizo que las empresas comenzaran a preocuparse más por la seguridad de sus redes. Fue en esta época cuando se desarrollaron los primeros firewalls y sistemas de detección de intrusiones (IDS, por sus siglas en inglés).

En la década de 1990, con la creciente popularidad de Internet, la seguridad de las redes se convirtió en una preocupación aún mayor. Los ataques de hackers se volvieron más sofisticados y se crearon nuevas amenazas, como el phishing y los ataques de denegación de servicio (DoS). Para hacer frente a estas amenazas, se desarrollaron tecnologías de cifrado más avanzadas, como el SSL y el TLS, y se crearon nuevas herramientas de seguridad, como los antivirus y los sistemas de prevención de intrusiones.

En la década de 2000, la seguridad de las redes se convirtió en una prioridad aún mayor debido a los crecientes riesgos de la seguridad cibernética. Los ataques se volvieron más avanzados y sofisticados, y las empresas tuvieron que adoptar nuevas estrategias de seguridad, como el análisis de seguridad de la red, la gestión de vulnerabilidades y la educación y concienciación de los usuarios.

En la actualidad, la seguridad de las redes sigue siendo un reto, debido la evolución de las amenazas y los riesgos de la seguridad informática, por ello los centros de cómputo tienen que estar constantemente actualizando y mejorando sus estrategias de seguridad para mantenerse protegidas. Para entender a profundidad la seguridad de redes, a continuación, se explica la evolución que ha tenido:

Periodo de seguridad de las comunicaciones (1940s)

La seguridad de los sistemas de información se limitaba a la seguridad física de la información y a la seguridad basada en cifrado de la comunicación (principalmente cifrado de flujo). Es decir, la información se almacenaba en un lugar relativamente seguro y se prohibía el acceso a la información a usuarios no autorizados; se utilizaban tecnologías criptográficas para garantizar la seguridad de

diferentes procesos de intercambio de información como el teléfono, el telégrafo y el fax, garantizando así la seguridad de los datos.

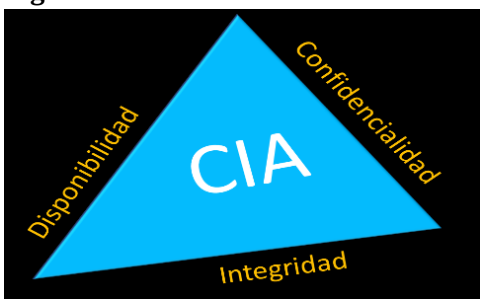
Figura 1. Evolución de la seguridad

Elaborado por: https://interactivasys.com/blog/sabes-que-es-una-politica-de-referencia-web/

Período de seguridad de la información (1970 – 1980)

La aplicación de tecnologías informáticas y de redes entró en una fase de uso práctico y a gran escala, y la transmisión de datos pudo completarse a través de redes informáticas. Aquí se garantizaba la integridad, disponibilidad y confidencialidad.

Figura 2. CIA



Elaborado por: https://interactivasys.com/blog/sabes-que-es-una-politica-de-referencia-web

Período de garantía de la información (1990s)

Las tecnologías de red entraron en la fase práctica y se concedió gran importancia a la confidencialidad, integridad y disponibilidad de la información. La controlabilidad y el no repudio se convirtieron en el nuevo objetivo de la seguridad de la información.

Período de auditoría de la información (2005s)

La norma ISO 27001 es un estándar internacional que define los requisitos para implementar, mantener y mejorar continuamente un Sistema de Gestión de la Seguridad de la Información (SGSI). Este sistema tiene como objetivo proteger la confidencialidad, integridad y disponibilidad de la información. ISO 27001 proporciona un marco estructurado que permite a las organizaciones identificar, evaluar y gestionar eficazmente los riesgos relacionados con la seguridad de la información, garantizando así su protección frente a amenazas tanto internas como externas.

La norma ISO 27001 es aplicable a cualquier tipo de organización, independientemente de su tamaño, ya sean pequeñas y medianas empresas, grandes corporaciones, instituciones gubernamentales o entidades sin fines de lucro. Además, puede implementarse en diversos sectores, como tecnología de la información, finanzas, salud y servicios públicos. El proceso de implementación de la norma ISO 27001 se organiza en cuatro fases principales: planificación, implementación, evaluación y mejora continua.

Figura 3. Certificación ISO

Elaborado por: https://www.normaiso27001.es/

Fase de Planificación

Durante esta fase, la organización identifica sus necesidades de seguridad de la información y diseña un plan estratégico para implementar el Sistema de Gestión de la Seguridad de la Información (SGSI).

Fase de Implementación

En la fase de implementación, se desarrollan las políticas, procedimientos y controles necesarios para proteger la información, asegurando que todos los aspectos de la seguridad estén cubiertos.

Fase de Evaluación

La fase de evaluación implica analizar la efectividad del SGSI, identificando posibles áreas de mejora para garantizar que los controles implementados funcionen correctamente.

Fase de Mejora Continua

En esta fase, la organización se centra en identificar y aplicar mejoras a los procesos y controles del SGSI, asegurando su evolución y adaptación frente a nuevos riesgos.

Una vez implementado y certificado, el SGSI debe revisarse y actualizarse periódicamente para asegurar su cumplimiento continuo con los requisitos de seguridad de la información.

Aunque la certificación ISO 27001 no es obligatoria, puede mejorar significativamente la imagen de la organización y aumentar la confianza de los clientes, ya que demuestra un compromiso sólido con la protección de la información, respaldado por una entidad certificadora independiente.

Además, la norma ISO 27001 puede integrarse con otros estándares y marcos de referencia, proporcionando una gestión más integral y eficaz de la seguridad de la información. Entre estos se incluyen la norma ISO 31000, para el análisis y gestión de riesgos, y la norma ISO 22301, para la gestión de la continuidad del negocio. Sin embargo, aunque es posible la integración, cada estándar tiene un enfoque y objetivos específicos que deben ser considerados de manera individual.

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

MAGERIT es una metodología para el análisis y gestión de riesgos en sistemas de información, desarrollada por el Consejo Superior de Administración Electrónica (CSAE), un organismo dependiente del Ministerio de Hacienda y Administraciones Públicas del Gobierno de España.

Esta metodología fue elaborada y publicada por primera vez en 1997, con un enfoque hacia los riesgos fundamentales en materia de sistemas de información.

La segunda versión fue publicada en 2005 con el fin de realizar una revisión constructiva con respecto a los riesgos de las compañías, involucrando cuestiones más profundas a cerca de la gestión de riesgos.

La tercera versión y ultima busca una nueva adaptación, teniendo en cuenta no solo la experiencia práctica sino también la evolución de las normas internacionales de ISO que constituyen un referente.

Según el Consejo Superior de Administración Electrónica (CSAE) la metodología "MAGERIT" persigue dos tipos de objetivos: directos e indirectos.

Los objetivos directos incluyen

- Estimar los riesgos asociados al uso de las tecnologías de la información y las comunicaciones TIC
- Concienciar a los usuarios y responsables de cada área de la organización sobre la existencia de riesgos y la importancia de gestionarlos adecuadamente.
- Proporcionar un método sistemático para analizar los riesgos derivados tanto del uso de las TIC como de la propia información.
- Planificar el tratamiento de los riesgos, con el objetivo de eliminarlos o, en su defecto, implementar medidas para mitigarlos.

Los objetivos indirectos incluyen

- Preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

MAGERIT se estructura en tres libros fundamentales

- **Método**: Expone el método propuesto para el análisis y la gestión de riesgos, detalla el proceso de gestión de riesgos, los proyectos de análisis, la elaboración del plan de seguridad y el desarrollo de sistemas de información.
- **Catálogo de Elementos:** Proporciona pautas sobre los tipos de activos, las dimensiones de valoración de los activos (como disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad), los criterios para su valoración, las amenazas comunes que afectan a los sistemas de información y las salvaguardas recomendadas para protegerlos.
- **Guía de Técnicas:** Reúne diversas técnicas utilizadas en proyectos de análisis y gestión de riesgos. Estas incluyen técnicas específicas, como análisis mediante tablas, análisis algorítmico y árboles de ataque; así como técnicas generales, como sesiones de trabajo (entrevistas, reuniones, presentaciones) y el método Delphi para valoración.

Método de análisis de riesgos

Indica los pasos a seguir para determinar y evaluar de forma adecuada los riesgos, amenazas y salvaguardas que puede tener y ejecutar la organización.

- Establecer los activos relevantes para la organización, su interrelación y su valor.
- Definir a qué amenazas están expuestos los activos.
- Determinar las salvaguardas hay dispuestas y cuan eficaces son frente al riesgo.
- Estimar el impacto o daño sobre el activo derivado de la materialización de la amenaza.
- Estimar el riesgo y el impacto ponderado con la tasa de ocurrencia de la amenaza.

En la actualidad: 2006-2024

En este contexto, la controlabilidad y el no repudio se han convertido en el nuevo foco de atención de la seguridad de la información, además de los tres principios tradicionales de confidencialidad, integridad y disponibilidad.

Período de seguridad del ciberespacio:

El objetivo es garantizar la seguridad del sistema de todo el ciberespacio, incluidas las instalaciones, los datos, los usuarios y las operaciones.

Se publican normas y reglamentos nacionales (como la Protección Clasificada de la Ciberseguridad) para orientar a las empresas a establecer un sistema de gestión de la seguridad de la información.

Finalmente, caracterizar la seguridad de redes, de forma sociológica y tecnológica, es fundamental puesto que La caracterización sociológica se centra en el estudio de los aspectos humanos y sociales relacionados con la seguridad de redes.

Figura 4. Evolución de la seguridad

elaborado por: https://www.kaspersky.es/resource-center/definitions/what-is-cloud-security

Permite analizar cómo las personas, las organizaciones y la sociedad en general interactúan con las tecnologías de seguridad. Algunos puntos clave incluyen:

Comportamiento de los Usuarios

- Conciencia de Seguridad: Evaluación de cuán informados están los usuarios sobre prácticas seguras y amenazas potenciales.
- Cumplimiento de Políticas: Análisis de la adherencia de los empleados a las políticas de seguridad establecidas por la organización.

Según el autor revista seguridad360, 2023 la interacción en la red se ha convertido en una parte fundamental de nuestras vidas. Desde compras en línea hasta comunicaciones y relaciones personales, el mundo digital se ha convertido en un espacio importante para la interacción humana.

Sin embargo, también es importante ser consciente de las implicaciones de nuestras acciones en línea, especialmente en lo que se refiere a nuestra identidad digital, nuestra huella digital y nuestra privacidad digital.

La identidad digital se refiere a la forma en que una persona es percibida y representada en línea. Esta identidad puede ser formada por la información que publicamos en redes sociales, los comentarios que hacemos en foros, y otras actividades que realizamos en línea, por ello es relevante ser conscientes de

la forma en que nos representamos en línea, ya que puede tener implicaciones en nuestra vida personal y profesional.

Se debe considerar que nuestra identidad digital es una extensión de nuestra identidad real y que puede ser fácilmente rastreada en línea. Las publicaciones en las redes sociales pueden ser vistas por cualquier persona en todo el mundo y pueden tener implicaciones para nuestra vida personal y profesional.

La huella digital se refiere a la información que dejamos en línea a través de nuestras actividades en línea. Esta información puede ser utilizada para rastrearnos y monitorearnos en línea. Asimismo, es importante ser consciente de la información que compartimos en línea, así como de los sitios web que visitamos y las actividades que realizamos en línea.

La privacidad digital es la capacidad de controlar la información personal que compartimos en línea. Es importante tener en cuenta que cualquier información que compartamos en línea puede ser vista por otras personas, por lo que es fundamental tomar medidas para proteger nuestra privacidad en línea.

Una de las formas de proteger nuestra privacidad en línea es asegurándonos de que nuestra información personal esté protegida. Esto puede incluir el uso de contraseñas seguras, la autenticación de dos factores y la utilización de software antivirus. También es importante ser conscientes de los sitios web que visitamos y de la información que compartimos en línea.

Otra forma de proteger nuestra privacidad en línea es revisando la configuración de privacidad en las redes sociales y otros sitios web. Muchos sitios web permiten a los usuarios controlar quién puede ver su información personal, lo que puede ser útil para proteger la privacidad.

Es importante tener en cuenta que la privacidad en línea es una responsabilidad compartida entre los usuarios y las empresas. Las empresas deben tomar medidas para proteger la privacidad de los usuarios, como la encriptación de datos y la educación de los usuarios sobre cómo proteger su información personal.

Por tanto, en el contexto de la identidad digital, la huella digital y la privacidad digital son aspectos importantes a tener en cuenta al interactuar en línea. Es importante ser conscientes de la forma en que nos representamos en línea, la información que compartimos en línea y la forma en que nuestras actividades en línea pueden ser rastreadas y monitoreadas.

¿Qué sucede cuando los usuarios no protegen su privacidad?

Cuando los usuarios no toman medidas para proteger su privacidad en línea, están expuestos a varios riesgos. Uno de los más comunes es el robo de identidad.

Los delincuentes pueden utilizar información personal, como el número de seguridad social, la fecha de nacimiento o el correo electrónico, para suplantar la identidad de una persona. Esto puede tener consecuencias graves, como la pérdida de dinero y la dificultad para restaurar la reputación y el crédito.

Otro riesgo es el ciberacoso. Las redes sociales y los medios de comunicación digital ofrecen una plataforma para la difusión de rumores y la intimidación, lo que puede tener consecuencias graves en la salud mental de las personas. También se pueden producir estafas en línea, como la venta de productos falsificados o la participación en esquemas de pirámide.

¿Qué medidas de seguridad pueden tomar los usuarios?

- La utilización de contraseñas seguras. Las contraseñas deben ser complejas y difíciles de adivinar, y es recomendable cambiarlas periódicamente.
- La utilización de autenticación de dos factores. La autenticación de dos factores es un proceso que requiere que los usuarios ingresen dos formas de autenticación, como una contraseña y un código enviado a su teléfono móvil. Esto aumenta la seguridad de las cuentas y hace que sea más difícil para los delincuentes acceder a ellas.
- Estar al día con las actualizaciones de seguridad. Los sistemas operativos y las aplicaciones pueden tener vulnerabilidades que los delincuentes pueden aprovechar para acceder a la información personal. Por lo tanto, es fundamental mantener el software actualizado.
- Implementar firewalls: Dispositivos y software que controlan el tráfico de red basado en reglas de seguridad predefinidas.
- Criptografía: Métodos para proteger la información mediante el uso de algoritmos criptográficos como AES, RSA, y ECC.
- Protocolos de Seguridad: Se debe implementar protocolos de protección, entre ellos estan: **SSL/TLS, Ipsec, VPN, etc.**

Figura 5. Seguridad de redes caracterizado de forma sociologica y tecnológica

elaborado por: https://informacionytic.com/6-tips-para-compartir-un-recurso-de-manera-mas-inclusiva/

Seguridad de la información con IA (Inteligencia Artificial)

La inteligencia artificial (IA) está transformando la seguridad de la información y la seguridad en la red al permitir a las organizaciones identificar y responder a amenazas de manera más rápida y eficiente. Para ello aplica aprendizaje automático con un alto procesamiento, la IA mejora la prevención, detección y respuesta ante ataques externos e internos.

Además, reduce la necesidad de intervención humana, permitiendo organizar tareas complejas en secuencias automáticas. Esta capacidad de aprendizaje continuo también incrementa su efectividad en áreas como la identificación de phishing, malware y otros tipos de ataques.

Los sistemas de IA también permiten una respuesta más efectiva a incidentes, analizando las causas raíz y mitigando vulnerabilidades. Además, ofrecen predicciones sobre posibles ataques, ayudando a planificar mejor los recursos y mejorar la resiliencia dentro de las organizaciones.

En resumen, la IA está cambiando el panorama de la ciberseguridad, aumentando la eficacia y permitiendo a las organizaciones adaptarse a un entorno de amenazas cada vez más complejo.

RESULTADOS Y DISCUSIÓN

Se realizo una investigación acerca de varios aspectos, tales como; gnoseológica, metodológica, sociológica y tecnológica relacionándolo a la seguridad de redes, por lo que se obtuvieron datos de suma importancia que permitieron comprender, de manera mucho más amplia su funcionalidad, así mismo esta investigación brinda un contexto comprensivo, lo cual entiende la complejidad de un sistema de seguridad en redes fomentando una perspectiva integral y adaptable que permita garantizar la integridad y protección de la información en ámbitos tecnológicos, como lo es el “Instituto Superior Tecnológico Ismael Pere Pazmiño”

Aplicar una seguridad de redes en el campus José Ochoa León garantiza que la información que se maneja en los dispositivos finales e intermediarios cumplan con su función, evitando que usuarios malintencionados entren a los sistemas de redes, con la finalidad de dañar o alterar datos que resulten ser importantes para la evaluación académica del estudiante. Por tanto, la comprensión de varios aspectos en la gestión de seguridad permite aplicar un sistema de seguridad que soluciones las vulnerabilidades que actualmente existen dentro del centro de cómputo.

La norma ISO 27001 es un estándar internacional que permitió conocer y establecer la base de los requisitos para una futura implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI). Este sistema se utilizará para proteger la confidencialidad, integridad y disponibilidad de la información en los equipos de los laboratorios del "Instituto Superior Tecnológico Ismael Pérez Pazmiño".

Es importante conocer y determinar el uso de las diferentes herramientas o metodologías que se utilizan para la gestión de los sistemas de la información, ya que además de ser aplicadas para análisis de activos e información, son bastante útiles y ayudan a lograr eficiencia y eficacia en los sistemas de información mediante la minimización de los riesgos.

El uso de la metodología Magerit, como instrumento de investigación asociado a la ISO27001 puede ser seleccionado para identificar activos, riesgos y amenazas. Además, podemos presentar los resultados en una notación textual y gráfica, que va a ser más fácil de entender para los usuarios.

Si utilizaríamos otra herramienta como Octave, tendríamos que considerar la gran cantidad de anexos que utiliza, lo que hace que el proceso de análisis de vulnerabilidades y definición de riesgos sea más complejo, otra desventaja que presenta es el idioma en el que esta desarrollado y el uso exclusivo para Pymes. Finalmente podemos abarcar parámetros de dimensión de impacto asociando la disponibilidad, confidencialidad, e integridad.

CONCLUSIÓN

Utilizando el sentido gnoseológico, se identificó la naturaleza y origen de la seguridad de los datos y redes de la información, además se consideró teorías y modelos que explican los sucesos de vulnerabilidad y protección en equipos tecnológicos a través del tiempo, desde 1970 hasta la presente fecha.

El documento permitió establecer una ideología de la seguridad de la información, para la implementación adecuada de medidas de seguridad en una red informática, lo cual además permite entender cómo se generan y mitigan las amenazas.

Caracterizar la norma ISO 27001 ayudó establece un marco sólido para la seguridad de la información, enfocándose en la gestión de riesgos de manera consecuente y anticipándose a los acontecimientos.

Este documento proporcionó información de los principios fundamentales en los que se basa la metodología Magerit haciendo uso de herramientas como la ISO27001, con lo cual se pretende realizar la auditoría de red en los laboratorios del Instituto Ismael Pérez Pazmiño en el cantón Pasaje.

Se determinó que los objetivos directos de la metodología Magerit incluyen, estimar los riesgos asociados al uso de las tecnologías de la información y las comunicaciones, concienciar a los usuarios responsables de cada área, proporcionar un método sistemático y planificar el tratamiento de los riesgos. Mientras que los objetivos indirectos corresponden a preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda el caso.

Se identificó de forma clara el eje central de la estrategia de la seguridad de la información, que corresponden a la confidencialidad, integridad y disponibilidad. Parámetros que deben ser tratados de forma especial para garantizar la seguridad en la red.

En el contexto sociológico, es importante implementar medidas que minimicen la vulnerabilidad de los datos y los equipos ante amenazas externas, internas, con actividades o tareas que se realicen de forma malintencionados o negligencias propias del personal encargado de la red.

La seguridad de redes es un tema complejo por lo que debe ser comprendido desde su origen y como ha sido su evolución frente a nuevas vulnerabilidades y amenazas en la red e integrar enfoques como; metodología, sociológicos y tecnológicos permitió entender la importancia de proteger eficientemente la red, por ello este artículo brinda el conocimiento de como la colaboración entre la tecnología y las personas pueden solventar los problemas que surgen en la red, para hacer uso de dispositivos adecuadamente garantizando la integridad del centro de cómputo y sus involucrados.

REFERENCIAS BIBLIOGRAFICAS

Escribá, G. (2013). Seguridad Informática. España: MACMILLAN, 2013. ISBN 978-84-15656-64-7. Disponible en: https://www.machadolibros.com/libro/seguridad-informatica_528475

IBM. (2020). *IBM*. Obtenido de IBM: https://www.ibm.com/es-es/topics/network-security

ISOTools Excellence. (2017) ¿Seguridad informática o seguridad de la información? Recuperado el 05 de marzo de 2017, de http://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/

Navarro, M. (2017). Guía del PMBOK para la gestión de pruebas de intrusión a aplicaciones web. PMBOK guide for web application penetration testing management Disponible en: https://www.researchgate.net/publication/342545006_Guia_del_PMBOK_para_la_gestion_de_pruebas_de_intrusion_a_aplicaciones_web_PMBOK_guide_for_web_application_penetration_testing_management.

Peña, M. & Anias, C. (2020). Integración de marcos de referencia para gestión de Tecnologías de la Información Integration of frames of reference for information technology. Ingeniería Industrial. ISSN: 1815-5936 Disponible en: https://www.redalyc.org/articulo.oa?id=360464918003.

Revista seguridad 360. (27 de 03 de 2023).

Obtenido de Revistaseguridad360:

https://revistaseguridad360.com/noticias/que-sucede-cuando interactuan-en-la-red/

Rodríguez, A. (2020). Herramientas fundamentales para el hacking ético. Revista Cubana de Informática Médica. ISSN 16x 84-1859 [consulta: 01-Jun-2020] Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1684-18592020000100116&lng=es.

UCIBER (1 de septiembre de 2024). Historia del desarrollo de la seguridad de las redes. https://uciber.com/lessons/historia-del-desarrollo-de-la-seguridad-de-las-redes-2/

Valencia, D (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. Disponible en: https://go.gale.com/ps/i.do?id=GALE%7CA501832208&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=16469895&p=AONE&sw=w&userGroupName=anon%7Ee29ae139&aty=open-web-entry

Veloz, J. & Alcibar, A. (2017). Ethical hacking, una metodología para descubrir fallas de seguridad en sistemas informáticos mediante la herramienta KALI-LINUX. Informática y Sistemas: Revista de Tecnologías de la Informática y las Comunicaciones.