Tecnológico de Estudios Superiores de Cuautitlán Izcalli

Organismo Público Descentralizado del Estado de México

MAESTRÍA

“DISEÑO DE PROTOCOLO DE SEGURIDAD PARA UN SISTEMA DE INFORMACIÓN DE EDUCACIÓN DE NIVEL SUPERIOR”

TESIS

MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

PRESENTA:

Ing. FILIBERTO TENEISTE HERNANDEZ

DIRECTOR(A) DE TESIS:

M. en C. MARÍA DEL CONSUELO MACIAS GONZÁLEZ

CUAUTITLÁN IZCALLI, EDO. DE MÉXICO SEPTIEMBRE 2024

AUTORIZACIÓN

GOBIERNO DEL ESTADO DE MÉXICO | ESTADO DE MÉXICO ¡El poder de servir! | EDUCACIÓN SECRETARÍA DE EDUCACIÓN, CIENCIA, TECNOLOGÍA E INNOVACIÓN | TECNOLÓGICO DE ESTUDIOS SUPERIORES DE CUAUTITLÁN IZCALLI

"2024. Año del Bicentenario de la Erección del Estado Libre y Soberano de México".

Tecnológico de Estudios Superiores de Cuautitlán Izcalli
Dirección Académica
Subdirección de Apoyo y Desarrollo Académico
Departamento de Investigación y Desarrollo Tecnológico

Cuautitlán Izcalli, Estado de México a 18 de septiembre de 2024
TESCI/DIDT/217/IX/24

DIRECCIÓN ACADÉMICA
DEPARTAMENTO DE INVESTIGACIÓN Y DESARROLLO TECNOLÓGICO
COORDINACIÓN DE POSGRADO

INGENIERO
FILIBERTO TENEISTE HERNANDEZ
P R E S E N T E

Por este conducto me permito informarle que puede proceder a la digitalización del Trabajo de Tesis titulado:

"DISEÑO DE PROTOCOLO DE SEGURIDAD PARA UN SISTEMA DE INFORMACIÓN DE EDUCACIÓN DE NIVEL SUPERIOR"

Ya que la comisión encargada de revisar el trabajo que se presenta para efectos de titulación, han dado su autorización conforme a lo estipulado en el Lineamiento para la operación de los Estudios de Posgrado en el Sistema Nacional de Institutos Tecnológicos.

Sin nada más que agregar, quedo a sus órdenes para cualquier aclaración.

A T E N T A M E N T E

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE CUAUTITLÁN IZCALLI
UNIDAD DE POSGRADO

MTRA. ERIKA EMILIA CANTERA
DEPARTAMENTO DE INVESTIGACIÓN Y DESARROLLO TECNOLÓGICO
COORDINACIÓN DE POSGRADO

c.c.p. Archivo
Departamento de Titulación
Expediente del alumno

Av. Nopaltepec s/n, Col. La Perla, C. P. 54740, Cuautitlán Izcalli, Estado de México.
Tels.: 55 5864 31 70 y 55 5864 31 71 Página web: tesci.edomex.gob.mx

AGRADECIMIENTOS

Yo, FILIBERTO TENESTE HERNANDEZ quiero expresar mi más profundo agradecimiento a todas aquellas personas que, de una u otra manera, me acompañaron en esta etapa profesional:

A mi directora de tesis, Mtra. María del Consuelo Macias González, por su orientación, paciencia y compromiso en cada etapa de este proceso. Su conocimiento y apoyo fueron fundamentales para el desarrollo de este trabajo.

A mis profesores y compañeros del Tecnológico de Estudios Superiores de Cuautitlán Izcalli, por sus valiosos aportes, comentarios y motivación constante a lo largo de estos años de formación.

A todas las personas y entidades que colaboraron de manera directa o indirecta en la recolección de datos, facilitación de recursos y conocimientos.

A todos, ¡gracias!

DEDICATORIA

Dedico esta tesis a mi familia, especialmente a mi hermano, por su apoyo incondicional, comprensión y ánimo en los momentos más difíciles. Sin su respaldo, esta meta no habría sido posible, han sido mi mayor fuente de inspiración y fortaleza. Cada logro alcanzado es también suyo.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

LISTA DE ABREVIATURAS Y TABLA DE SÍMBOLOS

NIST: National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología).

ISO/IEC 27001: International Organization for Standardization / International Electrotechnical Commission 27001 (Norma de Sistemas de Gestión de la Seguridad de la Información).

OWASP: Open Web Application Security Project (Proyecto de Seguridad en Aplicaciones Web Abiertas).

OCTAVE: Operationally Critical Threat, Asset, and Vulnerability Evaluation (Evaluación Operativa de Amenazas, Activos y Vulnerabilidades Críticas).

COBIT: Control Objectives for Information and Related Technologies (Objetivos de Control para Información y Tecnologías Relacionadas).

RBAC: Role-Based Access Control (Control de Acceso Basado en Roles).

ISO/IEC: International Organization for Standardization / International Electrotechnical Commission (Organización Internacional de Normalización / Comisión Electrotécnica Internacional).

TIC: Tecnologías de la Información y la Comunicación.

RESUMEN

Este trabajo presenta el diseño de un protocolo de seguridad para un sistema de información dentro de una institución educativa de nivel superior, con el objetivo de proteger la integridad, confidencialidad y disponibilidad de los datos manejados por la organización. La investigación se centra en identificar las amenazas y vulnerabilidades con un análisis y evaluación de riesgos más comunes, y en desarrollar un conjunto de políticas y procedimientos que mitiguen estos riesgos. El protocolo propuesto incluye la implementación de medidas técnicas, así como la formación y concienciación del personal en temas de seguridad informática.

Por lo que en el capítulo I se presenta el contexto general, la problemática que aborda la investigación, y se definen los objetivos generales y específicos. También se justifica la relevancia de la investigación, destacando los alcances y limitaciones.

Mientras que en el capítulo II, se aborda la seguridad de la Información, que describe la importancia de los protocolos de seguridad, los riesgos y amenazas en entornos de nivel superior, y el desarrollo de un protocolo de seguridad. Se revisan normativas y estándares internacionales, y se discuten metodologías de análisis de riesgos, así también los tópicos específicos que son los que se abordan temas como autenticación, autorización, confidencialidad, integridad, disponibilidad, cifrado, firewalls, antivirus, monitoreo y registro, control de acceso basado en roles (RBAC), pruebas de penetración, educación y concienciación en seguridad, y gestión de identidades.

En el capítulo III se revisan diferentes metodologías para la seguridad de la información, incluyendo NIST, ISO/IEC 27001, OWASP, OCTAVE, y COBIT. Estas metodologías guiaran el análisis y la implementación de medidas de seguridad.

En base al capítulo anterior, la evaluación y Análisis de Riesgo se describe como el proceso de identificación, valoración y clasificación de activos según su criticidad, así como la identificación y evaluación de riesgos asociados, también las políticas y Medidas de Seguridad, medidas técnicas, control de acceso, concientización y formación, gestión de incidentes, auditorías, y la mejora continua en la gestión de seguridad, ampliándolo en el capítulo 4.
Derivado de ello, el capítulo V se realiza el análisis de Aplicación, donde se presentan resultados y se justifican. Incluyen los resultados de la evaluación y análisis de riesgos, implementación de políticas y controles de seguridad, medidas técnicas, cifrado de bases de datos, y concientización. También se discuten la gestión de incidentes, auditorías internas y la mejora continua.

Como conclusión, el desarrollo de un protocolo de seguridad efectivo no solo requiere la implementación de herramientas tecnológicas, sino también la creación de una cultura de seguridad dentro de la institución. La concienciación y formación del personal, junto con una evaluación continua de los riesgos y la mejora de las políticas de seguridad, son fundamentales para garantizar la protección integral de los sistemas de información en una institución educativa de nivel superior.

Palabras clave.
Análisis de riesgos**,** Confidencialidad**,** Disponibilidad**,** Evaluación de riesgos, Integridad de datos, Medidas técnicas, Protocolo de seguridad**,** Sistema de información**,** Seguridad de la información, Vulnerabilidades.

ABSTRACT

This paper presents the design of a security protocol for an information system within a higher education institution, with the objective of protecting the integrity, confidentiality, and availability of the data managed by the organization. The research focuses on identifying threats and vulnerabilities through an analysis and assessment of common risks, and on developing a set of policies and procedures to mitigate these risks. The proposed protocol includes the implementation of technical measures, as well as staff training and awareness on information security topics.

Chapter I presents the general context, the problem addressed by the research, and defines the general and specific objectives. The relevance of the research is also justified, highlighting its scope and limitations.

Chapter II covers Information Security, describing the importance of security protocols, risks and threats in higher education environments, and the development of a security protocol. It reviews international regulations and standards and discusses risk analysis methodologies, along with specific topics such as authentication, authorization, confidentiality, integrity, availability, encryption, firewalls, antivirus, monitoring and logging, role-based access control (RBAC), penetration testing, security awareness and education, and identity management.

Chapter III reviews different methodologies for information security, including NIST, ISO/IEC 27001, OWASP, OCTAVE, and COBIT. These methodologies guide the analysis and implementation of security measures.

Based on the previous chapter, Risk Assessment and Analysis is described as the process of identifying, valuing, and classifying assets according to their criticality, as well as identifying and assessing associated risks. It also covers security policies and measures, technical measures, access control, awareness and training, incident management, audits, and continuous improvement in security management, which is expanded upon in Chapter IV.

In Chapter V, the Application Analysis is carried out, where results are presented and justified. These include the results of the risk assessment and analysis, implementation of security policies and controls, technical measures, database encryption, and awareness. Incident management, internal audits, and continuous improvement are also discussed.

In conclusion, developing an effective security protocol not only requires the implementation of technological tools but also the creation of a security culture within the institution. Staff awareness and training, along with continuous risk assessment and the improvement of security policies, are essential to ensuring comprehensive protection of information systems in a higher education institution.

Keywords.
Availability, Confidentiality, Data integrity, Information system, Information security, Risk analysis, Risk assessment, Security protocol, Technical measures, Vulnerabilities.

INTRODUCCIÓN

En la era digital actual, y en el ámbito de la gestión de la seguridad dentro de los sistemas de información se ha convertido en una prioridad crítica para cualquier organización. La creciente dependencia de las tecnologías de la información y la comunicación (TIC) ha hecho que los sistemas sean cada vez más vulnerables a una amplia gama de amenazas y ataques cibernéticos, por lo que se visto en la necesidad de la implementación de protocolos de seguridad robustos ya que es esencial para proteger la integridad, confidencialidad y disponibilidad de los datos, así como para garantizar la continuidad operativa. El diseño de un protocolo de seguridad eficaz requiere una comprensión profunda de los riesgos específicos que enfrenta el sistema y la adopción de un enfoque sistemático para mitigar estos riesgos.

Según García y Martínez (2018), un protocolo de seguridad debe incluir mecanismos de prevención, detección y respuesta ante incidentes, adaptándose continuamente a las nuevas amenazas emergentes. Además, la norma ISO/IEC 27001 establece un marco para la gestión de la seguridad de la información que puede servir como guía para el desarrollo de políticas y procedimientos de seguridad. La importancia de un protocolo de seguridad bien diseñado se subraya en estudios recientes que demuestran que las brechas de seguridad pueden tener consecuencias devastadoras tanto financieras como reputacionales para las organizaciones.

López y Pérez (2020) señalan que una brecha de seguridad puede resultar en la pérdida de confianza por parte de los clientes, así como en sanciones legales y regulatorias. En lo particular durante esta investigación se pretende diseñar un protocolo que puedan adaptarse a medida que evolucionan las amenazas y las tecnologías. Además, considera cumplir con los estándares y regulaciones de seguridad de la información pertinentes para la institución, como ISO 27001. Se abordarán aspectos relevantes del sistema, como la evaluación de riesgos, la implementación de controles de seguridad, la gestión de accesos, la formación y concienciación de los empleados, y la preparación y respuesta ante incidentes. Este enfoque integral asegurará que el protocolo no solo sea eficaz en la protección del sistema, sino también flexible y adaptable a las necesidades cambiantes de la institución.

PROBLEMATICA

En la era digital actual, las instituciones educativas han adoptado sistemas de información para gestionar y almacenar grandes cantidades de datos sensibles. Estos datos incluyen información personal y académica de estudiantes, docentes y personal administrativo, por lo que su protección es una prioridad. La creciente dependencia de estos sistemas ha puesto de relieve la importancia de contar con una infraestructura de seguridad robusta que garantice la confidencialidad, integridad y disponibilidad de la información. Sin un enfoque adecuado en la ciberseguridad, estas organizaciones se enfrentan a riesgos graves como la manipulación de datos, daños a su reputación y violaciones a la privacidad.

Ante la creciente dependencia de la institución en el sistema que actualmente utiliza para almacenar y gestionar datos sensibles, surge la necesidad de reforzar su infraestructura de seguridad. El sistema almacena información crucial como nombres, direcciones, números de teléfono, datos académicos como calificaciones y expedientes, así como información financiera de pagos de matrícula. Esto coloca a la institución en riesgo de sufrir ataques que comprometan la integridad de los datos, afecten su reputación o resulten en violaciones a la privacidad de los usuarios.

Recientemente, la institución ha identificado varios incidentes que podrían comprometer la seguridad de esta información. Como respuesta, se ha considerado indispensable diseñar un protocolo de seguridad que contemple medidas preventivas, correctivas y un monitoreo continuo. Este protocolo tiene como objetivo abordar las amenazas potenciales y garantizar la protección de los datos que gestiona la institución, mediante estrategias que refuercen la seguridad y reduzcan los riesgos relacionados con el uso de su sistema de información.

CAPÍTULO 1.

MARCO CONTEXTUAL

OBJETIVOS DE LA INVESTIGACIÓN

Objetivo General:

Diseñar un protocolo de seguridad para proteger el sistema de información de la institución.

Objetivos Específicos:

Identificar las principales amenazas y vulnerabilidades en el sistema actual.

Desarrollar políticas y procedimientos de seguridad adecuados.

Implementar medidas técnicas para mitigar riesgos.

Evaluar la efectividad del protocolo diseñado.

Justificación

El diseño de un protocolo de seguridad en un sistema de información en una institución de nivel superior se fundamenta en la necesidad de proteger la integridad, confidencialidad y disponibilidad de los datos, que son activos críticos para la operación y prestigio de la institución. Las instituciones de educación superior manejan una vasta cantidad de información sensible, que incluye datos personales de estudiantes y empleados, resultados académicos, investigaciones, y otros registros esenciales que, si se ven comprometidos, podrían generar consecuencias graves, como pérdida de confianza, sanciones legales, y daños financieros.

Además, estas instituciones son objetivos atractivos para ciberataques debido a la valiosa información que almacenan y al uso intensivo de tecnología en sus operaciones diarias. Un protocolo de seguridad bien diseñado no solo protege contra accesos no autorizados y ataques externos, sino que también asegura que el personal esté capacitado para manejar correctamente los sistemas y responder de manera eficaz a incidentes de seguridad.

Asimismo, la implementación de este protocolo es crucial para el cumplimiento de normativas legales y estándares internacionales en materia de protección de datos. Esto no solo garantiza la conformidad con las leyes vigentes, sino que también fortalece la reputación institucional al demostrar un compromiso con la seguridad y la privacidad.

La importancia del ISO

El diseño de un protocolo de seguridad en sistemas de información de instituciones de nivel superior es esencial para proteger la integridad, confidencialidad y disponibilidad de los datos críticos que manejan. La norma ISO/IEC 27001 juega un papel fundamental en este contexto, ya que proporciona un marco internacionalmente reconocido para la gestión de la seguridad de la información. La implementación de este estándar asegura que la institución adopte un enfoque sistemático para gestionar los riesgos, protegiendo los activos sensibles contra amenazas internas y externas.

La importancia de ISO 27001 radica en su capacidad para ayudar a las instituciones a cumplir con las normativas legales y a garantizar la seguridad de los datos, lo que es vital para evitar sanciones legales, mantener la confianza de estudiantes y personal, y prevenir daños reputacionales o financieros. Además, el estándar fomenta una cultura de seguridad dentro de la institución, asegurando que el personal esté capacitado para enfrentar incidentes de seguridad y mantenga buenas prácticas de manejo de la información. Esto no solo refuerza la protección contra ciberataques, sino que también mejora la eficiencia operativa, la reputación y el cumplimiento normativo de la institución.

Alcances Y Limitaciones

El protocolo diseñado se enfocará en el resguardo y manejo de datos académicos y administrativos dentro de la institución, abarcando tanto aspectos técnicos como administrativos. Las limitaciones incluyen el alcance temporal del estudio y la disponibilidad de recursos para implementar todas las medidas propuestas.

CAPÍTULO 2.

MARCO TEÓRICO

Introducción

En el marco teórico de la seguridad de la información, es esencial destacar la protección de los sistemas y datos ante accesos no autorizados, mal uso, divulgación, alteración o destrucción. Los pilares fundamentales de esta seguridad incluyen la confidencialidad, que garantiza que solo usuarios autorizados accedan a la información; la integridad, que asegura la exactitud y completitud de los datos; y la disponibilidad, que garantiza que los recursos estén accesibles cuando se necesiten.

Las amenazas representan cualquier circunstancia que pueda causar daño a un sistema, mientras que las vulnerabilidades son debilidades que pueden ser explotadas por estas amenazas. En este contexto, los protocolos de seguridad juegan un papel clave para mitigar riesgos y proteger la continuidad de las operaciones.

En entornos de nivel superior, como universidades, donde se manejan grandes cantidades de datos sensibles, el diseño e implementación de un protocolo de seguridad se vuelve esencial. Este protocolo debe estar basado en un análisis de riesgos, adoptando normativas internacionales como ISO/IEC 27001 o NIST SP 800-53, que proporcionan marcos para gestionar la seguridad de la información.

Asimismo, las metodologías de análisis de riesgos como OCTAVE e ISO 31000 permiten evaluar y gestionar los riesgos de manera integral. El desarrollo de políticas de autenticación y autorización, junto con técnicas de cifrado, uso de firewalls, antivirus, y monitoreo, son medidas esenciales para garantizar la seguridad de los sistemas y la protección de los datos.

Seguridad de Información

La seguridad de la información se define como la protección de la información y los sistemas de información contra accesos no autorizados, usos indebidos, divulgación, alteración o destrucción. Los pilares de la seguridad de la información son:

Confidencialidad: Garantiza que la información solo sea accesible a las personas autorizadas.

Integridad: Asegura que la información sea precisa y completa, y que no haya sido alterada de manera no autorizada.

Disponibilidad: Garantiza que la información esté disponible cuando se la necesite.

Amenazas y Vulnerabilidades: Una amenaza es cualquier circunstancia o evento con el potencial de causar daño a un sistema de información. Las vulnerabilidades son debilidades en un sistema que pueden ser explotadas por amenazas.

Importancia de los Protocolos de Seguridad

Según Stallings (2017), "la seguridad de los sistemas de información debe ser un esfuerzo integral que incluya medidas preventivas, detectivas y correctivas para proteger los activos de información de la organización". En este sentido, el diseño de un protocolo de seguridad efectivo es esencial para mitigar riesgos y asegurar la continuidad de las operaciones.

Riesgos y Amenazas en Entornos de Nivel Superior

Las instituciones de nivel superior, como universidades y centros de investigación, manejan una gran cantidad de datos sensibles que incluyen información personal de estudiantes y personal, resultados de investigaciones, y propiedad intelectual. A medida que estos datos se digitalizan y se almacenan en sistemas de información, se incrementa el riesgo de ciberataques. Como señala Whitman y Mattord (2019), "las organizaciones deben reconocer que las amenazas internas y externas son constantes y que la seguridad no es un estado estático, sino un proceso continuo".

Desarrollo de un Protocolo de Seguridad

El diseño de un protocolo de seguridad en un sistema de información debe basarse en un análisis exhaustivo de riesgos y en la implementación de controles adecuados. De acuerdo con Siponen y Willison (2009), "los protocolos de seguridad deben estar alineados con la normativa vigente y las mejores prácticas de la industria, además de ser adaptativos para responder a nuevas amenazas".

Normativas y Estándares Internacionales

ISO/IEC 27001

La norma ISO/IEC 27001 es un estándar internacional que especifica los requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI). Esta norma proporciona un marco sistemático para la gestión continua de la seguridad de la información.

NIST SP 800-53

El NIST Special Publication 800-53 proporciona un catálogo de controles de seguridad y privacidad para todos los sistemas de información federales en los Estados Unidos. Es ampliamente utilizado como referencia para la implementación de medidas de seguridad.

Metodologías de Análisis de Riesgos

Metodología OCTAVE

La metodología OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) es un enfoque de evaluación de riesgos desarrollado por el Software Engineering Institute (SEI) de la Universidad Carnegie Mellon. OCTAVE permite a las organizaciones evaluar sus riesgos de seguridad y diseñar planes de mitigación adecuados.

Análisis de Riesgos de ISO 31000

ISO 31000 proporciona directrices sobre la gestión del riesgo, incluyendo principios y una estructura de gestión del riesgo. Esta norma es aplicable a cualquier tipo de organización y facilita un enfoque integral para la gestión del riesgo, incluyendo la seguridad de la información.

Autenticación

La autenticación es el proceso mediante el cual se verifica la identidad de un usuario o sistema antes de permitirle el acceso a recursos protegidos. La autenticación puede basarse en algo que el usuario sabe (como una contraseña), algo que el usuario tiene (como un token) o algo que el usuario es (como una huella dactilar) (González, 2018).

Autorización

Una vez autenticado, la autorización determina los permisos y accesos que tiene el usuario dentro del sistema. La autorización se implementa mediante políticas de control de acceso que especifican qué recursos pueden ser accedidos y qué operaciones pueden realizarse (Martínez y López, 2019).

Confidencialidad

La confidencialidad asegura que la información sensible sea accesible solo para las personas autorizadas. Esto se logra a través de técnicas de cifrado, donde los datos se transforman en un formato que solo puede ser leído por quienes posean la clave de descifrado (Pérez, 2020).

Integridad

La integridad de los datos implica que la información no ha sido alterada de manera no autorizada. Los mecanismos de hash y las firmas digitales son herramientas comunes para verificar la integridad de los datos (Ramírez y Hernández, 2017).

Disponibilidad

La disponibilidad garantiza que los sistemas y datos estén accesibles para los usuarios autorizados cuando sea necesario. Las técnicas para asegurar la disponibilidad incluyen la redundancia, los sistemas de respaldo y los planes de recuperación ante desastres (Fernández, 2016).

Cifrado

El cifrado es el proceso de transformar información legible en una forma codificada que solo puede ser descifrada por alguien que tenga la clave adecuada. El cifrado protege la confidencialidad y la integridad de los datos (López, 2019).

Firewalls

Un firewall es una barrera de seguridad que controla el tráfico de red entrante y saliente basado en reglas de seguridad predefinidas. Los firewalls pueden ser hardware o software y son esenciales para proteger redes internas de accesos no autorizados (Sánchez, 2015).

Antivirus

Los programas antivirus son herramientas diseñadas para detectar y eliminar software malicioso, como virus, gusanos y troyanos. Los antivirus ayudan a proteger la integridad y disponibilidad del sistema (Navarro, 2020).

Monitoreo y Registro

El monitoreo y registro involucra la vigilancia continua de actividades en el sistema y el registro de eventos importantes. Esto es crucial para detectar y responder a incidentes de seguridad en tiempo real (Álvarez, 2017).

Control de Acceso Basado en Roles (RBAC)

El control de acceso basado en roles es un enfoque para restringir el acceso a sistemas en función de los roles asignados a los usuarios. RBAC simplifica la administración de permisos y mejora la seguridad al limitar el acceso a lo mínimo necesario para realizar tareas (Castro, 2018).

Pruebas de Penetración

Las pruebas de penetración son simulaciones de ataques realizadas por expertos en seguridad para identificar y corregir vulnerabilidades en el sistema. Estas pruebas ayudan a fortalecer la seguridad al anticipar posibles vectores de ataque (Mendoza, 2019).

Educación y Concienciación en Seguridad

La educación y concienciación en seguridad son fundamentales para que los usuarios comprendan y adopten prácticas seguras. La capacitación continua ayuda a prevenir errores humanos que pueden comprometer la seguridad del sistema (Vega, 2020).

Gestión de Identidades

La gestión de identidades es el proceso de administrar la información de usuario y los permisos asociados a sus identidades. Esto incluye la creación, mantenimiento y eliminación de cuentas de usuario y la implementación de autenticación multifactorial para aumentar la seguridad (Rodríguez, 2017).

CAPÍTULO 3.

MARCO METODOLÓGICO

Introducción

El desarrollo de este protocolo ha involucrado una evaluación exhaustiva de los riesgos potenciales y la identificación de las mejores prácticas de seguridad. A través de un enfoque sistemático y estructurado, este protocolo busca proporcionar una guía clara y efectiva para proteger el sistema de la institución contra cualquier tipo de amenaza.

En las secciones siguientes, se detallarán los componentes clave del protocolo de seguridad, incluyendo las políticas de seguridad, los procedimientos de respuesta a incidentes, las herramientas y tecnologías a utilizar, y el plan de implementación y monitoreo continuo.

El diseño de la investigación se basará en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001:2013. Esta norma proporciona un enfoque sistemático para gestionar información sensible de la empresa, garantizando su confidencialidad, integridad y disponibilidad.

Metodología para fases de la metodología

Para diseñar un protocolo de seguridad para sistemas de información implica establecer una serie de procedimientos y normas que protejan los datos y recursos de una institución contra amenazas. Cada una de estas metodologías ofrece un enfoque estructurado para diseñar y mantener un protocolo de seguridad robusto para sistemas de información. La elección de una metodología específica puede depender del contexto organizacional, los recursos disponibles y las necesidades particulares de seguridad. En muchos casos, las organizaciones pueden combinar elementos de varias metodologías para crear un protocolo de seguridad integral y adaptado a sus requisitos específicos. A continuación, se describen algunas metodologías y enfoques comunes que se utilizan para desarrollar dichos protocolos:

Metodología NIST (National Institute of Standards and Technology)

Proporciona un marco de trabajo completo para gestionar riesgos de ciberseguridad en su documento NIST SP 800-53. Los pasos clave incluyen:

Identificación: Identificar los sistemas, activos, datos y capacidades esenciales para la organización.

Protección: Implementar medidas de protección para asegurar la entrega de servicios críticos.

Detección: Desarrollar y aplicar actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad.

Respuesta: Desarrollar y aplicar actividades apropiadas para tomar acción con respecto a un incidente de ciberseguridad detectado.

Recuperación: Implementar planes para la resiliencia y restaurar capacidades o servicios que fueron afectados por un incidente.

ISO/IEC 27001

La norma ISO/IEC 27001 es un estándar internacional que describe cómo gestionar la seguridad de la información. Los pasos fundamentales incluyen:

Contexto de la organización: Comprender la organización y su contexto.

Liderazgo: Asegurar el compromiso de la dirección y establecer políticas de seguridad.

Planificación: Identificar riesgos y oportunidades, y planificar cómo abordarlos.

Soporte: Proveer recursos necesarios, competencia, concienciación y comunicación.

Operación: Implementar y controlar los procesos.

Evaluación del desempeño: Monitorizar, medir, analizar y evaluar el desempeño.

Mejora: Implementar acciones para mejorar continuamente.

Metodología OWASP (Open Web Application Security Project)

OWASP es conocido por su lista de los diez riesgos de seguridad más críticos para aplicaciones web. Una metodología basada en OWASP podría incluir:

Identificación de riesgos: Utilizar la lista OWASP Top 10 para identificar y priorizar riesgos de seguridad.

Evaluación de amenazas: Analizar las amenazas potenciales y su impacto.

Implementación de controles: Desarrollar y aplicar medidas para mitigar los riesgos identificados.

Pruebas de seguridad: Realizar pruebas periódicas de seguridad, como pruebas de penetración y análisis de vulnerabilidades.

Educación y formación: Capacitar al personal en prácticas seguras de desarrollo y uso de sistemas.

Metodología OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

OCTAVE es una metodología de gestión de riesgos desarrollada por CERT que se enfoca en la evaluación de amenazas, activos y vulnerabilidades. Los pasos incluyen:

Identificación de activos críticos: Determinar qué activos son críticos para la organización.

Identificación de amenazas: Identificar posibles amenazas para esos activos.

Evaluación de vulnerabilidades: Analizar las vulnerabilidades que podrían ser explotadas.

Desarrollo de estrategias de mitigación: Crear planes para mitigar los riesgos identificados.

Implementación y monitoreo: Implementar las estrategias y monitorear su efectividad.

Metodología COBIT (Control Objectives for Information and Related Technologies)

COBIT proporciona un marco para la gobernanza y gestión de la TI empresarial. Los pasos incluyen:

Evaluación del entorno de control: Identificar el entorno de control de TI actual.

Desarrollo de objetivos de control: Definir objetivos de control alineados con las necesidades del negocio.

Implementación de controles: Aplicar controles específicos para gestionar riesgos.

Monitoreo y evaluación: Revisar y evaluar los controles para asegurarse de que funcionan según lo esperado.

Mejora continua: Actualizar y mejorar continuamente los controles y procesos.

En conclusión, el desarrollo de un protocolo de seguridad efectivo requiere la adopción de una metodología estructurada que se ajuste a las necesidades específicas de la organización. Las metodologías NIST, ISO/IEC 27001, OWASP, OCTAVE y COBIT proporcionan marcos sólidos y prácticas que ayudan a gestionar riesgos, identificar amenazas y proteger los activos críticos de una institución. Cada una ofrece un enfoque único para mitigar riesgos y garantizar la seguridad de la información. La combinación de estas metodologías puede crear un protocolo integral, garantizando un monitoreo continuo y mejoras en la gestión de seguridad a lo largo del tiempo.

Descripción de las fases

En este capítulo se describen cada uno de las fases que se contemplan para poder diseñar un protocolo que se adapte a las necesidades y posibilidades dentro de la institución, por lo que el diseño de la investigación se basará en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001:2013. Esta norma proporciona un enfoque sistemático para gestionar información sensible de la empresa, garantizando su confidencialidad, integridad y disponibilidad, así, como se muestra en el siguiente esquema con las diferentes etapas que abarca para un completo diseño del protocolo de seguridad.

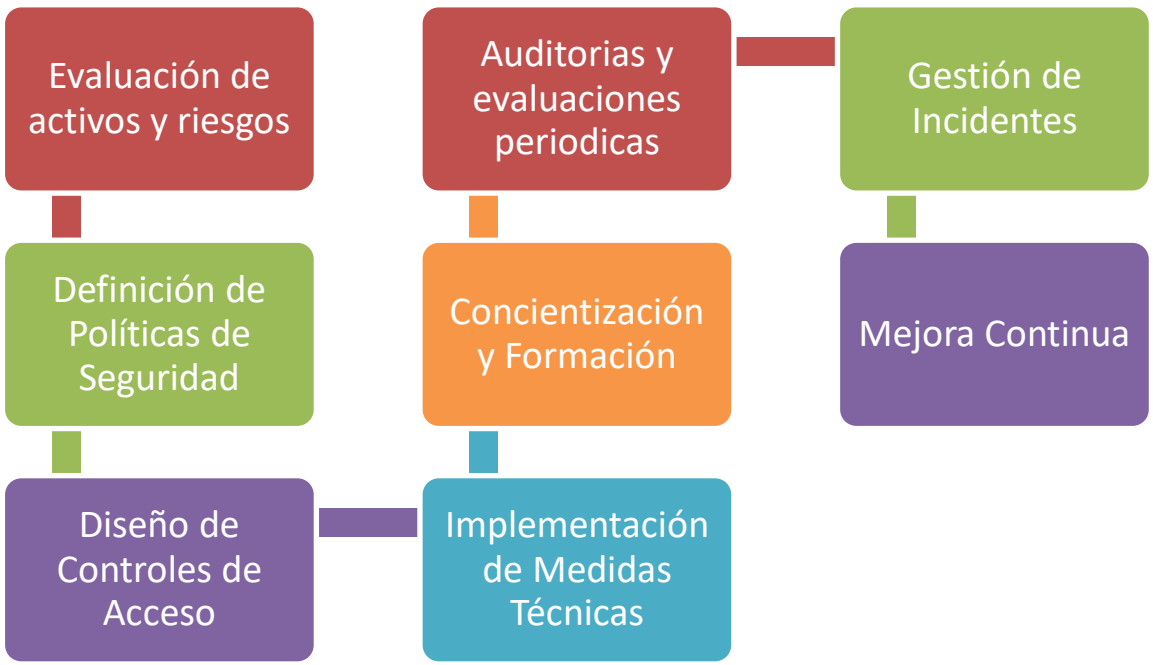


Ilustración 1 Proceso de diseño de metodología

Evaluación y Análisis de riesgos

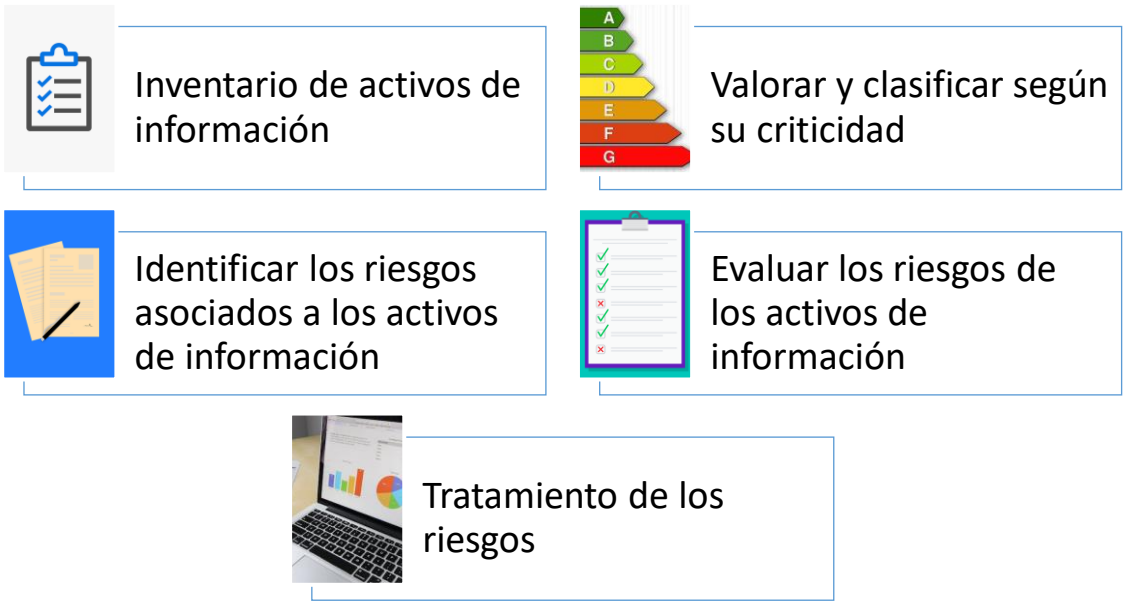


Ilustración 2 Evaluación de riesgos

Identificar y Realizar Inventario de Activos

El primer paso crucial de la evaluación y el análisis de riesgos es identificar y realizar un inventario de todos los activos digitales valiosos dentro de la institución. Los activos pueden incluir hardware (servidores, ordenadores), software (aplicativos, bases de datos) y cualquier otro recurso que tenga valor para la organización. Es esencial crear un inventario detallado que incluya la descripción de cada activo, su ubicación, el propietario responsable y la relación con otros activos. Este inventario sirve como base para las siguientes etapas del proceso de gestión de riesgos. En la siguiente tabla se muestra los conceptos que se consideran para realizar el inventario.

No.	Nombre	Descripción	Propietario	Custodio	Ubicación

Tabla 1 Inventario de activos

No. (Número): Se asigna como un único identificador a cada activo dentro del inventario, ya que este número ayuda a organizar y referenciar los activos de manera ordenada y evita confusiones.

Nombre: Es el título o nombre asignado al activo de información, este debe ser conciso, pero suficientemente descriptivo para que cualquier persona pueda identificar de qué activo se trata.

Descripción: Es un resumen detallado que explica qué es el activo, su función, y cualquier otra información relevante que ayude a entender su propósito y uso dentro de la organización.

Propietario: Es la persona o departamento dentro de la institución que tiene la responsabilidad última del activo. El propietario es responsable de las decisiones relacionadas con el uso y protección del activo.
Custodio: Es la persona o grupo encargado del manejo, mantenimiento y protección diaria del activo, el custodio garantiza que el activo esté disponible y en buen estado.
Ubicación: Hace referencia al lugar físico o lógico donde se encuentra el activo.

Valorar y Clasificar según su Criticidad

Una vez identificados los activos, el siguiente paso es valorarlos y clasificarlos según su criticidad. La valoración implica determinar la importancia de cada activo para la organización, lo que puede basarse en factores como el impacto financiero, la confidencialidad, la integridad y la disponibilidad. Los activos se clasifican en niveles de criticidad (por ejemplo, crítico, alto, medio, bajo) según su importancia. Esta clasificación ayuda a priorizar los esfuerzos de seguridad y recursos hacia los activos más críticos.

No.	Tipo	Descripción	Criticidad

Tabla 2 Clasificación de activos

No. (Número): Es un código único asignado a cada activo, el identificador facilita el seguimiento y la gestión de los activos dentro del inventario.
Tipo: El tipo se refiere a la clasificación general del activo, ayuda a organizar el inventario y a aplicar políticas de seguridad específicas según la naturaleza de los activos.
Descripción: Proporciona información detallada sobre el activo. Esta información incluye características clave, funcionalidades y cualquier otro detalle relevante que ayude a identificar y entender el activo.
Criticidad: Evalúa la importancia del activo en función de su impacto en la organización. Este concepto mide cuán crucial es el activo para la operación y seguridad de la organización.

Identificar los Riesgos de los Activos

La identificación de riesgos implica analizar las amenazas potenciales que pueden afectar a cada activo. Estas amenazas pueden ser internas (errores humanos, fallos técnicos) o externas (ciberataques, desastres naturales). Durante este proceso, se consideran las vulnerabilidades

específicas de cada activo y cómo estas pueden ser explotadas por amenazas. El resultado es una lista de posibles riesgos asociados con cada activo del inventario.

No.	Vulnerabilidad	Amenaza	Riesgo	Probabilidad	Impacto	Nivel de riesgo

Tabla 3 Riesgos en activos

No. (Número): El número o identificador es un código único asignado a cada activo.
Vulnerabilidad: Refiere una debilidad en un activo o en un conjunto de controles de seguridad que puede ser explotada por una amenaza para causar daño o pérdida.
Amenaza: Es cualquier circunstancia o evento con el potencial de causar daño a un sistema de información a través de la explotación de vulnerabilidades.
Riesgo: Es la combinación de la probabilidad de que ocurra un evento amenazante y el impacto que dicho evento tendría sobre la organización.
Probabilidad: Es la medida de la posibilidad de que una amenaza específica explote una vulnerabilidad. Se puede expresar en términos cualitativos o cuantitativos.
Impacto: Es la medida del daño que podría resultar si una amenaza explota una vulnerabilidad.
Nivel de riesgo: Es una valoración combinada de la probabilidad y el impacto, proporcionando una medida del riesgo total asociado con una amenaza y vulnerabilidad específica.

Evaluar los Riesgos de los Activos

La evaluación de riesgos se centra en determinar la probabilidad y el impacto de cada riesgo identificado. La probabilidad se refiere a la posibilidad de que ocurra una amenaza, mientras que el impacto mide las consecuencias potenciales para la organización. A menudo, se utiliza una matriz de riesgos para visualizar y priorizar los riesgos en función de su probabilidad e impacto. Los riesgos con alta probabilidad y alto impacto son los que requieren atención inmediata.

Impacto \ Probabilidad	Muy Baja (1)	Baja (2)	Media (3)	Alta (4)	Muy Alta (5)
Muy Alto (5)					
Alto (4)					
Medio (3)					
Bajo (2)					

Muy Bajo (1)					

Tabla 4 Evaluación de riesgos en impacto y probabilidad

Dicha tabla describe la estimación del impacto que tendría el riesgo si se materializara, contemplando los siguientes parámetros:

Muy Bajo: Riesgo insignificante, no requiere atención.

Bajo: Riesgo reducido, vigilar de forma periódica.

Medio: Riesgo aceptable, se considera planificar medidas de respuesta.

Alto: Riesgo significativo, se deben implementar medidas de mitigación.

Muy Alto: Riesgo severo, se deben tomar acciones inmediatas.

Crítico: Riesgo crítico, se debe dar prioridad máxima en la gestión de riesgos.

Tratamiento de Riesgos

El tratamiento de riesgos implica decidir cómo gestionar cada riesgo identificado. Las estrategias de tratamiento incluyen la mitigación (implementación de controles para reducir la probabilidad o impacto), la transferencia (trasladar el riesgo a un tercero, como un seguro), la aceptación (aceptar el riesgo si está dentro de los límites tolerables) y la evitación (eliminar la actividad que causa el riesgo). Cada riesgo debe ser abordado con un plan de acción específico que detalle las medidas a tomar, los recursos necesarios y los responsables de su implementación.

Amenaza	Medidas	Tratamiento	Prioridad

Tabla 5 Tratamiento de riesgos

Amenaza: Es cualquier circunstancia o evento potencial que puede explotar una vulnerabilidad y causar daño a un activo, resultando en una pérdida o compromiso de la seguridad de la información. Las amenazas pueden ser de naturaleza humana, tecnológica o ambiental.

Medidas: Las medidas o controles de seguridad son las acciones, procedimientos que se implementan para reducir, mitigar o eliminar un riesgo de seguridad.

Tratamiento: Es el proceso de seleccionar e implementar medidas de seguridad para reducir los riesgos a un nivel aceptable.

Prioridad: Se refiere a la clasificación de los riesgos según su nivel de severidad (combinación de probabilidad e impacto) y la urgencia de abordar cada riesgo.

Monitorización y Revisión

La última etapa es la monitorización y revisión continua de los riesgos y controles implementados. El entorno digital está en constante cambio, lo que puede introducir nuevos riesgos o alterar los existentes. La monitorización implica la supervisión continua de los activos, amenazas y controles, mientras que la revisión periódica evalúa la eficacia de las medidas de seguridad. Los informes de auditoría y las revisiones regulares ayudan a mantener la relevancia y efectividad del programa de gestión de riesgos.

Políticas de Seguridad

Las políticas de seguridad son un conjunto de directrices y reglas que definen cómo proteger los activos de información de una organización. Estas políticas establecen el marco general para la seguridad, incluyendo roles y responsabilidades, así como los procedimientos para manejar y proteger la información.

Para esta investigación se contemplan los conceptos que se muestran en la siguiente figura:

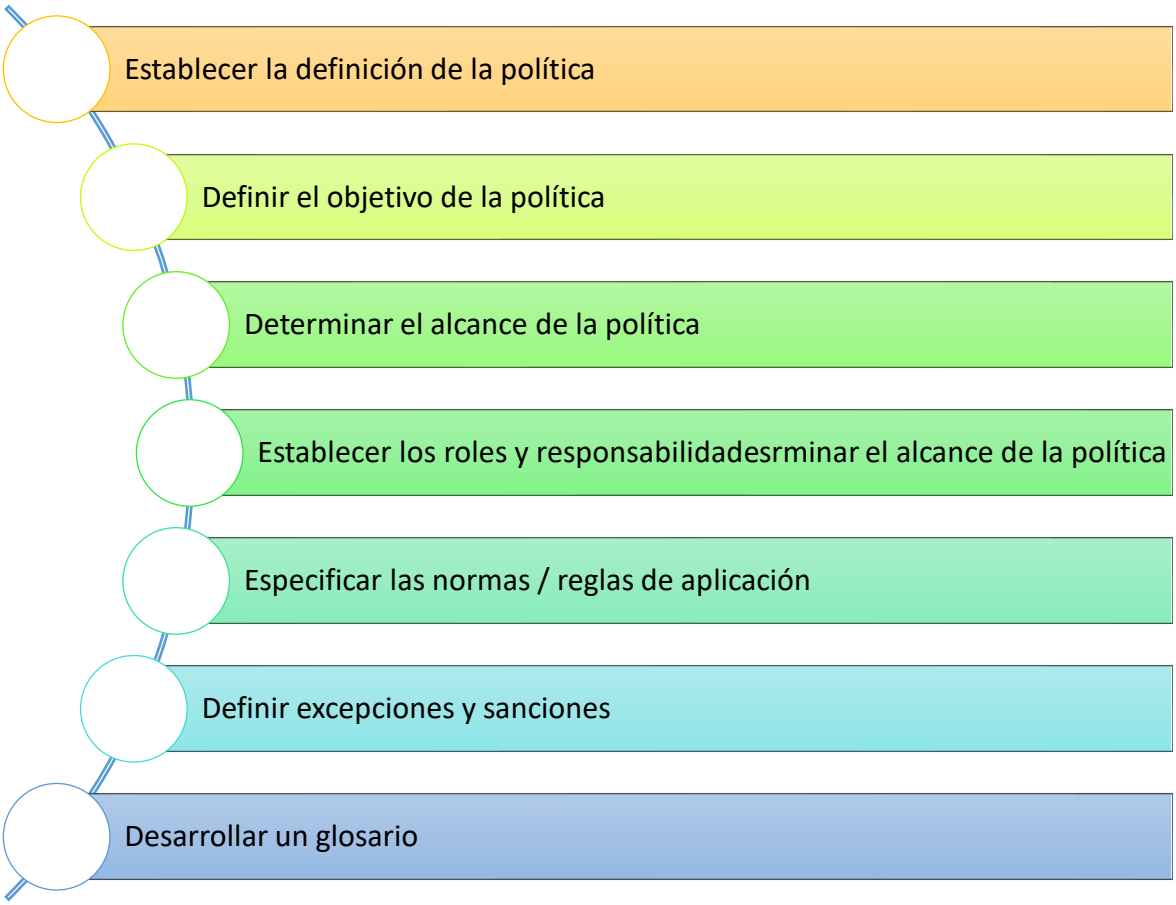


Ilustración 3 conceptos de política de seguridad

Nombre de la política de seguridad: Es el título o denominación oficial de la política de seguridad, este nombre debe ser claro y reflejar el propósito principal de la política.

Objetivo: Se refiere a la meta principal que busca alcanzar la política, describe el propósito de la política y los beneficios esperados de su implementación. Suele incluir aspectos como la protección de la información, la prevención de incidentes de seguridad y el cumplimiento de regulaciones legales.

Alcance: Describe a quién y a qué se aplica la política de seguridad, incluye las áreas, departamentos, sistemas, datos, y personas que estarán bajo la cobertura de esta política.

Roles y responsabilidades: Especifica las funciones y obligaciones de las diferentes personas o entidades involucradas en la implementación y el mantenimiento de la política de seguridad. Esto puede incluir a empleados, directivos, administradores de sistemas, equipo de seguridad, entre otros.

Reglas de aplicación: Explica las directrices y procedimientos específicos que deben seguirse para cumplir con la política de seguridad. Estas reglas detallan las acciones permitidas y prohibidas, así como los controles y medidas de seguridad que deben implementarse.

Excepciones y sanciones: Describe las circunstancias bajo las cuales se pueden hacer excepciones a la política y el proceso para obtener dichas excepciones. También detalla las sanciones y consecuencias para aquellos que violen la política, incluyendo medidas disciplinarias y legales.

Glosario: Es un listado de términos y definiciones que se utilizan en la política de seguridad, este glosario ayuda a garantizar que todos los lectores entiendan claramente el lenguaje y los conceptos específicos mencionados en la política.

Medidas Técnicas

Las medidas técnicas son soluciones tecnológicas utilizadas para proteger los sistemas y datos contra amenazas y vulnerabilidades. Estos Incluyen software, hardware y procedimientos técnicos, dependerá de las necesidades de la institución.

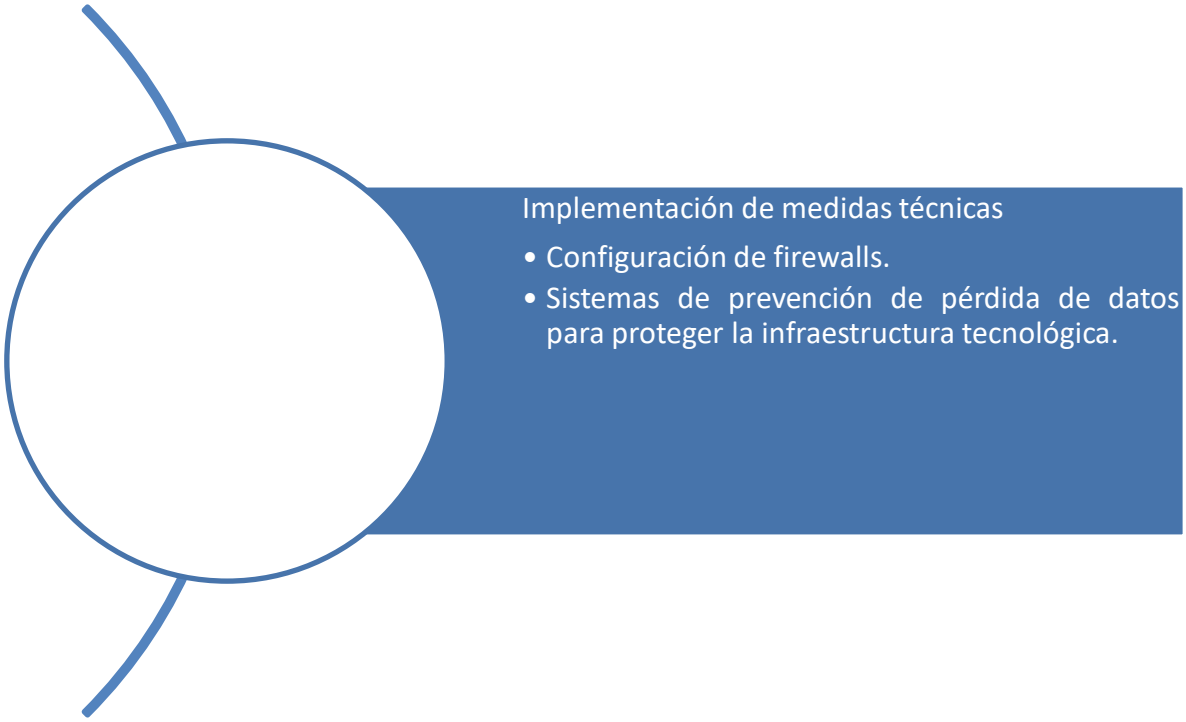


Ilustración 4 Medidas técnicas

Control de Acceso

Los controles de acceso son mecanismos que regulan quién puede ver o usar los recursos en un entorno informático. Estos controles aseguran que solo las personas autorizadas tengan acceso a determinados datos y sistemas.

Implementación de Control de Acceso basado en roles

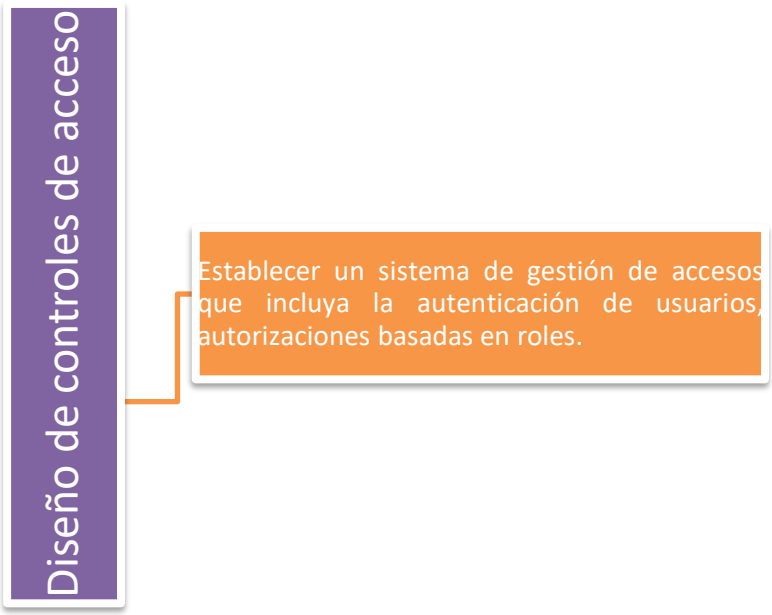


Ilustración 5 Control de acceso

Descripción: El control de acceso se refiere a las políticas, procedimientos y herramientas utilizadas para restringir el acceso a recursos, sistemas y datos únicamente a personas autorizadas. Esto incluye tanto el acceso físico a instalaciones como el acceso lógico a sistemas informáticos y datos.

Objetivo de Control de Acceso: Describe el objetivo principal del control de acceso basándose en proteger la confidencialidad, integridad y disponibilidad de los recursos y datos.

Alcance: Abarca todos los recursos, sistemas, datos y personas dentro de la organización, incluyendo sistemas de TI, aplicaciones, bases de datos, archivos físicos, instalaciones y cualquier otro activo que requiera protección. Además, puede extenderse a empleados, contratistas, proveedores y cualquier otra entidad que interactúe con los recursos de la organización.

Proceso de Implementación: Describe los pasos para implementar el control de acceso, contemplando las diferentes etapas clave

Monitoreo y Auditoría: Describe las actividades continuas que aseguran la eficacia de los controles de acceso.

Beneficios del Control de Acceso: Describe la implementación efectiva del control de acceso y los beneficios que se obtiene al tener una completa implementación del control.

Concientización y Formación

La concientización y formación consisten en educar a los empleados sobre la importancia de la seguridad de la información y cómo comportarse de manera segura en el entorno digital. Esto incluye la capacitación continua sobre las mejores prácticas de seguridad.

Concientización: Proceso continuo que busca mantener a los empleados informados sobre las políticas de seguridad, las amenazas actuales y emergentes, y la importancia de cumplir con las prácticas de seguridad. Incluye campañas, recordatorios y comunicaciones regulares.

Formación: Proceso estructurado y planificado que proporciona a los empleados los conocimientos y habilidades necesarios para proteger la información y cumplir con las políticas de seguridad. Incluye cursos, talleres, simulaciones y certificaciones.

Objetivo de la Concientización y Formación: Definición: El objetivo principal es crear una cultura de seguridad dentro de la organización, donde todos los empleados comprendan su papel en la protección de la información y actúen de manera proactiva para prevenir incidentes de seguridad. Se busca reducir el riesgo de errores humanos que puedan comprometer la seguridad.

Alcance: Definición: La concientización y formación en seguridad de la información deben abarcar a todos los empleados, desde la alta dirección hasta el personal de línea. También puede extenderse a contratistas, proveedores y cualquier persona que tenga acceso a los sistemas y datos de la organización.

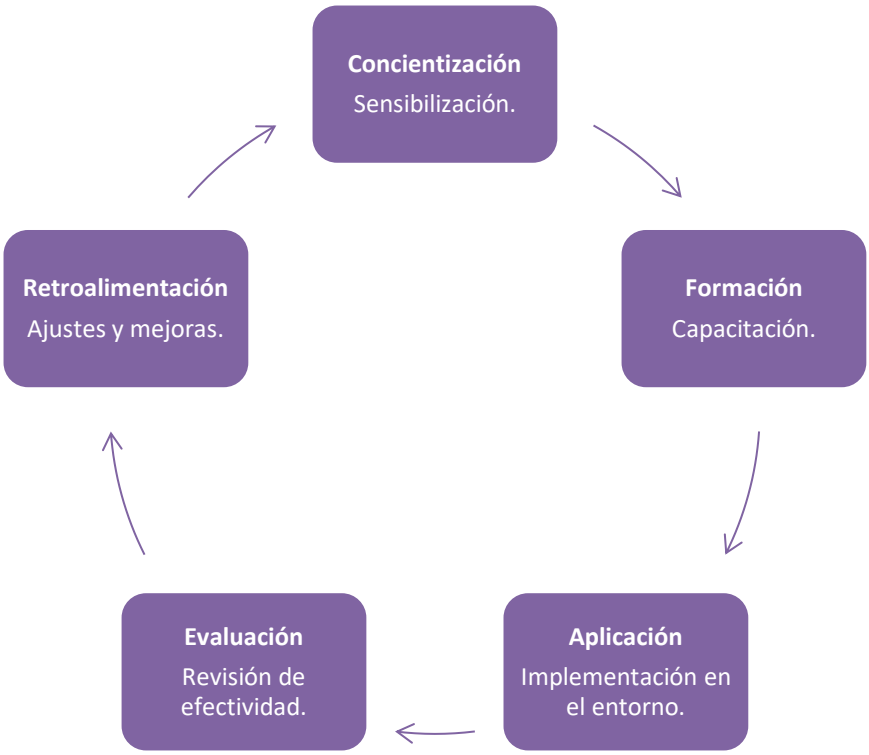


Ilustración 6 Proceso de concientización y formación

Gestión de incidentes

La gestión de incidentes implica la preparación y respuesta ante incidentes de seguridad, como violaciones de datos o ataques cibernéticos. Esto incluye la identificación, contención, erradicación, y recuperación de incidentes de seguridad.

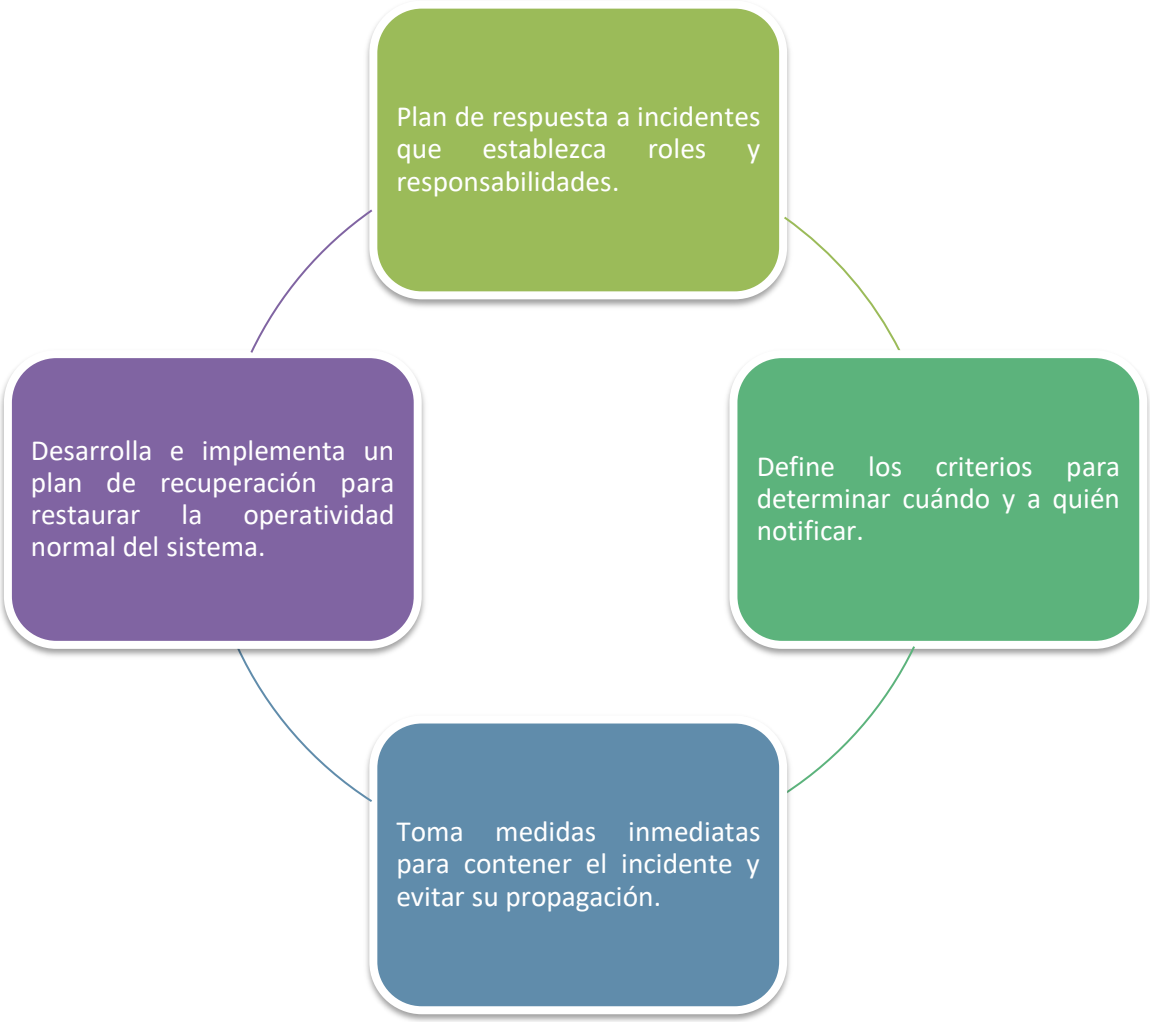


Ilustración 7 Gestión de incidentes

Auditorias y evaluaciones periódicas

Las auditorías y evaluaciones periódicas son revisiones sistemáticas y regulares de los sistemas y políticas de seguridad para asegurar que cumplen con los estándares establecidos y son eficaces en la protección contra amenazas.

Ilustración 8 Auditorias y evaluaciones

Mejora continua

La mejora continua es el proceso de evaluar y mejorar constantemente las políticas, procedimientos y tecnologías de seguridad para adaptarse a nuevas amenazas y cambios en el entorno empresarial.

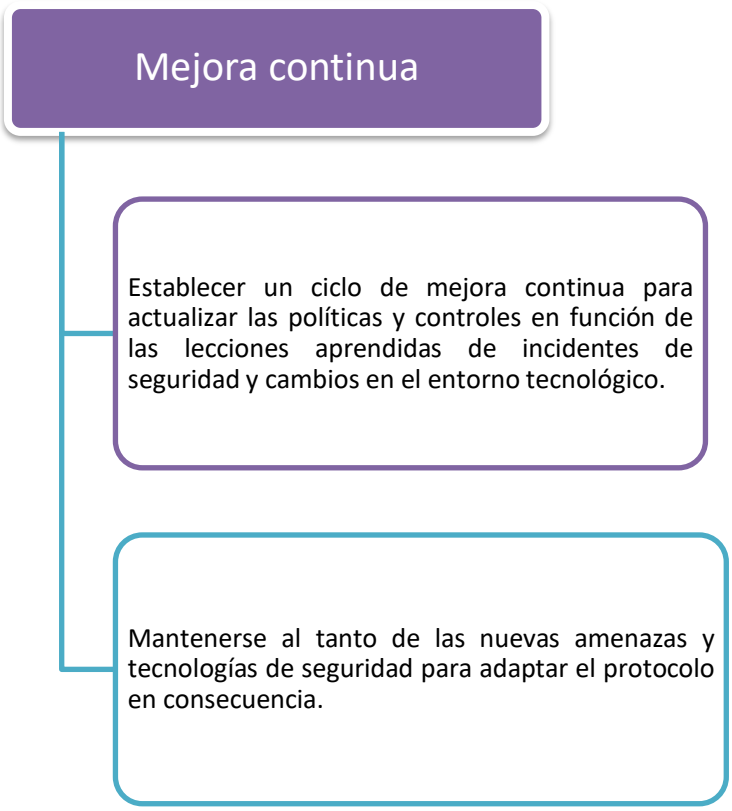


Ilustración 9 Mejora continua

CAPÍTULO 4.

APLICACIÓN DE LA METODOLOGÍA Y DISCUSIÓN DE RESULTADOS

Resultados de Evaluación y Análisis de riesgos

En esta primera etapa consistió en identificar los activos digitales y realizar un inventario detallado para entender de aquellos elementos que necesitan protección y cuál es el valor dentro de la organización, este inventario es la base de las siguientes etapas en este proceso de análisis de riesgos, a continuación, se muestra detallado los conceptos en la siguiente tabla:

Tabla 6 Inventario de activos identificados

No.	Nombre	Descripción	Propietario	Custodio	Ubicación
1	Base de Datos	Almacena y gestiona grandes cantidades de datos de manera centralizada.	Universidad	Jefe del departamento	Cómputo y telemática
2	Visual Studio	Software de entorno de desarrollo	Universidad	Jefe del departamento	Cómputo y telemática

Tabla 7 Inventario de activos identificados

Posteriormente y una vez identificados los activos, en este paso, se valora y clasifican según la criticidad, ya que con esto se prioriza los esfuerzos de seguridad y recursos hacia los más críticos.

No	Tipo	Descripción	Criticidad
1	Información	Datos y conocimientos utilizados por una organización para tomar decisiones informadas, planificar y operar.	Alta
2	Hardware	Componentes físicos y dispositivos utilizados para el procesamiento, almacenamiento y transmisión de datos.	Media
3	Software	Programas y aplicaciones que permiten realizar tareas específicas en una computadora o dispositivo.	Baja

Tabla 8 Clasificación de activos identificados

Durante este proceso, se consideran las vulnerabilidades específicas que pueden afectar a los activos y como pueden ser explotadas por amenazas, el resultado consiste en una lista de posibles riesgos asociados con cada activo del inventario.

No	Vulnerabilidad	Amenaza	Riesgo	Probabilidad	Impacto	Nivel de riesgo
1	Falta de equipo	Cortes o sobrecargas de energías	Perdida de información, daños en los equipos, pérdida de tiempo en procesos	Media (3)	Medio (3)	Medio
2	Software sin licencia	virus, programa maligno	Destrucción de sistemas operativos, modificación de aplicaciones, mal funcionamiento del sistema	Muy Baja (1)	Bajo (2)	Medio
3	Deficiente control de acceso al sistema	Suplantación de identidad	Robo, alteración de datos, robo de claves de acceso	Alta (4)	Alto (4)	Muy Alto

Tabla 9 Riesgos en activos identificados

La evaluación de riesgos se centra en determinar en términos de probabilidad y el impacto de cada riesgo identificado, en esta etapa, se utiliza una matriz de riesgos para describir y visualizar los riesgos en función de su probabilidad e impacto, cabe mencionar que el valor del riesgo se determina entre la intersección de la probabilidad y el impacto, así como se muestra en la matriz.

Tabla 10 Descripción de matriz de riesgos

Impacto \ Probabilidad	Muy Baja (1)	Baja (2)	Media (3)	Alta (4)	Muy Alta (5)
Muy Alto (5)	Medio	Alto	Muy Alto	Crítico	Crítico
Alto (4)	Medio	Alto	Muy Alto	Crítico	Crítico
Medio (3)	Bajo	Medio	Alto	Muy Alto	Crítico
Bajo (2)	Bajo	Bajo	Medio	Alto	Muy Alto
Muy Bajo (1)	Muy Bajo	Bajo	Medio	Medio	Alto

Tabla 11 Descripción de matriz de riesgos

El tratamiento de riesgos implica en decidir la forma en que se gestionaran cada riesgo identificado, en esta etapa, la manera más viable se trata de poner en marcha estrategias para mitigarlos, esto mediante la implementación de controles o políticas de seguridad, con la finalidad de reducir la probabilidad o el impacto.

Tabla 12 Tratamiento de riesgos identificados

Amenaza	Medidas	Tratamiento	Prioridad
Cortes o sobrecargas de energías	UPS (Sistema de Alimentación Ininterrumpida): Proporcionan energía de respaldo en caso de cortes eléctricos.	Política para respaldos de información	Media
	Reguladores de voltaje: Ayudan a mantener un suministro eléctrico constante a pesar de fluctuaciones en la corriente, evitando daños a tus dispositivos electrónicos.		
	Control de acceso: Limitar el acceso a la información solo a las personas autorizadas.	Administración de usuarios y	Media

Manipulación de información	Encriptación: Utilizar técnicas de encriptación para proteger los datos mientras están en tránsito.	gestión de contraseñas	
Suplantación de identidad	Implementar sistemas de monitoreo y revisión para rastrear quién accede a la información, qué cambios se realizan y cuándo, y detectar cualquier actividad sospechosa.	Modificación de datos Y Capacitación de usuarios	Baja
	Educar a los empleados sobre las mejores prácticas de seguridad de la información y cómo reconocer y evitar las amenazas cibernéticas, como el phishing y la ingeniería social.		

Tabla 13 tratamiento de riesgos identificados

En la fase de monitoreo y revisión se emplea un formato que ayude a obtener datos de los incidentes que han ocurrido históricamente, ya que con ella se gestionan y documentan adecuadamente los eventos que puedan comprometer los activos de una organización, esto por el constante cambio en los entornos digitales, por lo que se pueden presentar nuevos riesgos y alterar los existente. Este documento permite registrar, rastrear y analizar incidentes que ocurren dentro de la institución, facilitando la identificación de patrones, la evaluación de riesgos y la implementación de medidas correctivas, a continuación, se muestra la propuesta del formato en mención que proporciona una estructura clara y completa para documentar todos los aspectos relevantes de un incidente, desde los detalles iniciales hasta las acciones correctivas y preventivas tomadas. La implementación de un formato así no solo ayuda a gestionar los incidentes de manera más eficiente, sino que también contribuye a mejorar la seguridad general mediante la identificación y mitigación de riesgos.

FORMATO DE REGISTRO DE INCIDENCIAS

Encabezado del documento

Nombre de la Organización: Nombre de la organización
Título del Documento: Registro de Incidencias de Seguridad de la Información
Fecha de Creación: Fecha
Versión del Documento: Versión

Detalles de la incidencia

ID de Incidencia: Número único de identificación
Fecha y Hora de Detección: Fecha y hora exacta
Detectado por: Nombre y cargo del detector
Fuente de Detección: Sistema de detección, empleado, auditoría, etc.

Descripción de la Incidencia

Descripción Detallada: Descripción completa de la incidencia
Tipo de Incidencia: Phishing, malware, acceso no autorizado, etc.
Impacto: Confidencialidad, integridad, disponibilidad
Gravedad: Alto, Medio, Bajo

Análisis de la Incidencia

Causa Raíz: Descripción de la causa raíz del incidente
Métodos Utilizados: Métodos o técnicas utilizadas por el atacante
Vulnerabilidades: Vulnerabilidades específicas explotadas

Respuesta y Mitigación

Acciones Inmediatas: Acciones tomadas inmediatamente después de la detección
Medidas de Contención: Medidas implementadas para contener el incidente
Medidas Correctivas: Medidas a largo plazo para corregir y prevenir futuros incidentes
Fecha de Resolución: Fecha en que la incidencia fue resuelta

Impacto y Recuperación

Evaluación del Impacto: Descripción del impacto en la organización
Tiempo de Inactividad: Duración del tiempo de inactividad, si aplica
Coste Estimado: Coste estimado del incidente en términos de recursos, tiempo, y dinero

Lecciones Aprendidas

Análisis de Lecciones: Lecciones aprendidas del incidente
Recomendaciones: Recomendaciones para evitar futuros incidentes similares

Revisión y Cierre

Revisado por: Nombre y cargo del revisor
Fecha de Revisión: Fecha de la revisión final
Comentarios Adicionales: Comentarios adicionales sobre la incidencia

Anexos

Documentación de Soporte: Archivos adicionales, capturas de pantalla, logs, etc.

Ilustración 10 Formato de incidencias

Resultados de Implementación de Política de Seguridad

En la fase de implementar una política de seguridad, se diseña la política de respaldos o copias de seguridad. Como se muestra en la Ilustración 2 conceptos de política de seguridad, y como refiere a la definición a un conjunto de directrices, reglas y prácticas diseñadas para proteger la información sensible y garantizar la confidencialidad, integridad y disponibilidad de los datos dentro de una organización. Esta política establece cómo se debe gestionar, proteger y distribuir la información y define las responsabilidades de los empleados en relación con la seguridad de la información. A continuación, se estable una política para su implementación, este contempla los aspectos que definen una política de seguridad.

Nombre de la política de seguridad: Respaldos o copias de seguridad

Objetivo:

Proteger y preservar la información valiosa de la organización o individuo frente a posibles pérdidas de datos. Estas pérdidas pueden ocurrir debido a diversos factores, tales como fallos del hardware, errores humanos, ataques cibernéticos, desastres naturales, o software malicioso.

Alcance:

Se prioriza asegurar las bases de datos, las aplicaciones y los sistemas operativos dentro de la institución por si es necesario una recuperación completa.

Aspectos que deben considerarse para garantizar que la estrategia de respaldo cumpla con las necesidades de protección de datos y recuperación ante desastres:

1. Datos a respaldar (Tipo de datos, Ubicación).
2. Frecuencia de respaldo (programación, ventanas de respaldo).
3. Métodos de respaldo (Tipos de respaldo, medios de almacenamiento).
4. Retención y Ciclo de Vida de los Datos de Respaldo (Tiempo de conservación, Remplazo de medios de respaldo).
5. Seguridad de respaldo (Solo personal autorizado).
6. Procedimiento de recuperación (Planes de recuperación).
7. Documentación y registro (Registro de actividades).
8. Cumplimiento y normativas (Auditorías internas).

Roles y responsabilidades:

Equipo de TI: Determina quién es responsable de realizar, monitorear y mantener las copias de seguridad.

Planes de Recuperación: Define los pasos a seguir y los responsables en caso de una restauración de datos.

Ilustración 11 Formato de política de seguridad

Resultados de Implementación de Controles de Seguridad

En la implementación de controles de seguridad, se propone un mecanismo de control de acceso basado en roles, en este proceso se establece un mecanismo de control de acceso que sirve para asignar permisos a usuarios basados en sus roles dentro de la institución, los roles representan conjuntos de acciones o tareas que un usuario específico está autorizado a realizar. La propuesta de la implementación efectiva de RBAC implica los siguientes conceptos como se muestra a continuación:

Es una estrategia eficaz para gestionar los permisos de acceso a recursos en una organización, asignando derechos y privilegios en función de las responsabilidades y roles de los empleados. A continuación, se describe una propuesta para la implementación de RBAC en una organización:

Nombre del control: Implementación de Control de Acceso Basado en Roles

Descripción:
Es un mecanismo de seguridad que restringe el acceso a los sistemas y datos en función de los roles asignados a los usuarios dentro de una organización. Cada rol tiene permisos específicos que definen a qué recursos pueden acceder y qué acciones pueden realizar.

Objetivo del Control de Acceso:
Garantizar que solo las personas autorizadas tengan acceso a los datos sensibles y sistemas críticos, reduciendo así el riesgo de acceso no autorizado y potenciando la seguridad de la información.

Alcance:
Este control de acceso se aplica a todos los sistemas de información y bases de datos de la institución que manejan datos sensibles, incluyendo datos académicos como datos personales.

Proceso de implementación:
Paso 1: Identificación de Roles y Permisos
Acción: Identificar y definir los roles dentro de la institución (Administrador, Administrativo, Docente y estudiante).
Permisos: Asignar permisos específicos a cada rol.
Ejemplos:
Administrador: Acceso completo a todos los sistemas y datos.
Administrativo: Acceso a datos y sistemas relacionados con datos académicos.
Docente: Acceso limitado a los datos y módulos necesarios para su uso diario.
Estudiante: Acceso a su historial académico.

Paso 2: Asignación de Roles a Usuarios
Acción: Asignar roles a cada usuario en función de su posición y responsabilidades dentro de la institución.

Paso 3: Configuración de Políticas de Acceso
Acción: Configurar políticas de acceso en los sistemas de información que refuercen los permisos definidos para cada rol.
Ejemplo de Política: Solo los usuarios con el rol de "Administrador" pueden modificar la configuración del sistema.

Ilustración 12 Formato de control de acceso

En la siguiente tabla se muestra un ejemplo de la manera que puede tener una estructura de control de acceso que se explica anteriormente.

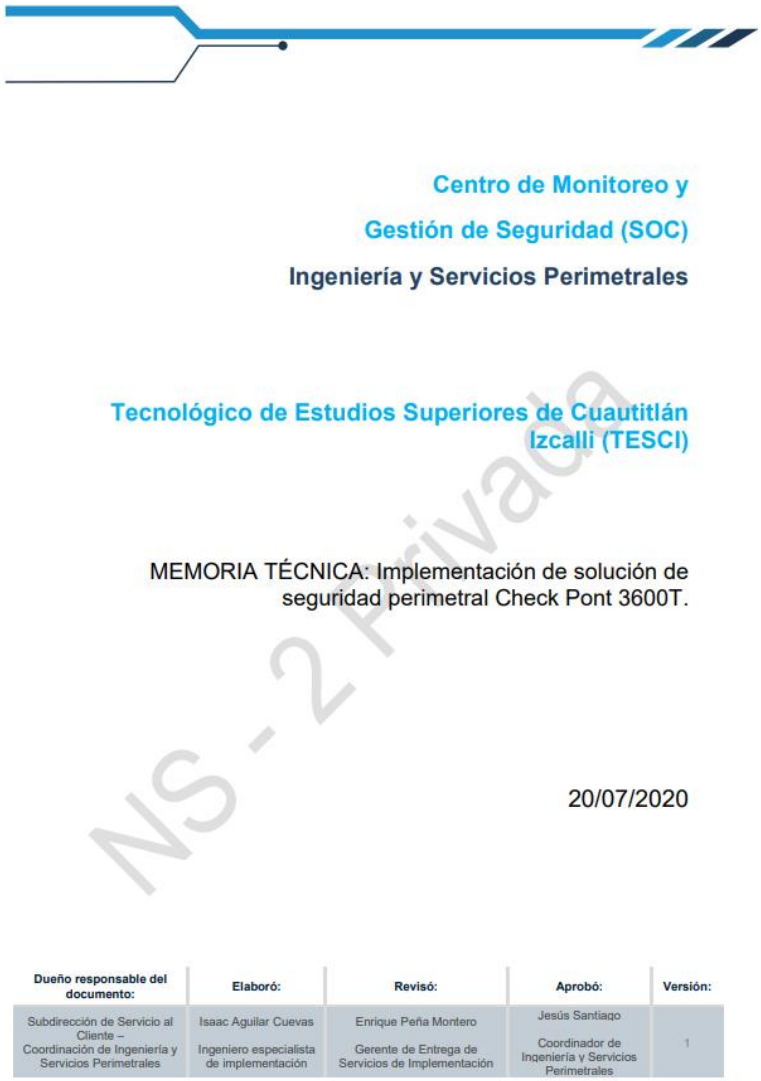
Tabla 14 Roles y permisos

Rol	Permiso 1	Permiso 2	Permiso 3	Permiso 4	Permiso 5
Administrador	Leer	Escribir	Modificar	Borrar	Configurar
Usuario común	Leer	-	-	-	-
Auditor	Leer	-	-	-	Informes
Gerente de Proyecto	Leer	Escribir	Modificar	-	-

Resultados de Implementación de Medidas Técnicas

En la implementación de una medida técnica, y que actualmente está en funcionamiento en la institución, se trata de una solución de seguridad perimetral Check Pont 3600T.

La implementación de soluciones de seguridad perimetral, como el Check Point 3600T, se refiere al proceso de configurar y poner en funcionamiento este dispositivo específico para proteger el perímetro de la red institucional. El Check Point 3600T es un firewall de próxima generación que proporciona funciones avanzadas de seguridad, incluyendo inspección de paquetes, filtrado de contenidos, prevención de intrusiones, y VPN (Redes Privadas Virtuales), entre otras capacidades. La implementación implica instalar físicamente el dispositivo, configurar las reglas de seguridad según las políticas de la organización, asegurarse de que las actualizaciones de firmas de amenazas estén al día, y probar el sistema para garantizar su efectividad y cumplimiento con los requisitos de seguridad establecidos.



Centro de Monitoreo y
Gestión de Seguridad (SOC)
Ingeniería y Servicios Perimetrales

Tecnológico de Estudios Superiores de Cuautitlán Izcalli (TESCI)

MEMORIA TÉCNICA: Implementación de solución de seguridad perimetral Check Pont 3600T.

20/07/2020

Dueño responsable del documento:	Elaboró:	Revisó:	Aprobó:	Versión:
Subdirección de Servicio al Cliente – Coordinación de Ingeniería y Servicios Perimetrales	Isaac Aguilar Cuevas Ingeniero especialista de implementación	Enrique Peña Montero Gerente de Entrega de Servicios de Implementación	Jesús Santiago Coordinador de Ingeniería y Servicios Perimetrales	1

Ilustración 13 Formato de medida técnica

El documento describe el proceso de la implementación de la solución de seguridad perimetral, describiendo el objetivo, la infraestructura de seguridad que involucra, la representación grafica de la red, además, de los detalles sobre las licencias necesarias para operar los componentes de la infraestructura y el protocolo de pruebas que se utilizan para probar su efectividad junto a las recomendaciones o sugerencias de las mejores prácticas en su aplicación.

Implementación de base de datos cifradas

Otra medida técnica que está en funcionamiento actualmente es la implementación de cifrar la base de datos. En este proceso se configura y aplican técnicas de cifrado para proteger la información almacenada. Esto implica encriptar los datos de manera que solo las personas autorizadas puedan acceder a ellos, incluso si alguien más obtiene acceso no autorizado al sistema de bases de datos. El cifrado se realiza a nivel de columna, tabla o base de datos completa, dependiendo de los requisitos de seguridad y cumplimiento.

Mantener las Bases de Datos Cifradas

El cifrado de bases de datos es una práctica esencial para proteger datos sensibles contra accesos no autorizados y brechas de seguridad. A continuación, se detalla la metodología para implementar y mantener bases de datos cifradas.

1. Evaluación y Planificación

a. Identificación de Datos Sensibles:

Clasificación de Datos: Determinar qué tipos de datos deben cifrarse, como información personal identificable.

Mapeo de Datos: Identificar todas las ubicaciones donde se almacenan los datos sensibles, tanto en tránsito como en reposo.

b. Selección de Algoritmos de Cifrado:

Estándares de Cifrado: Elegir algoritmos de cifrado robustos y estándares de la industria, como AES-256, que es ampliamente reconocido por su alta seguridad.

Compatibilidad: Asegurar que los algoritmos seleccionados sean compatibles con las tecnologías y sistemas de base de datos existentes.

2. Implementación del Cifrado

a. Cifrado en Reposo:

Cifrado a Nivel de Columna: Cifrar datos sensibles específicos dentro de las tablas de la base de datos. Esto es útil para proteger información particularmente crítica sin cifrar toda la base de datos.

Cifrado a Nivel de Archivo: Utilizar sistemas de archivos cifrados para proteger toda la base de datos. Ejemplos incluyen el uso de Transparent Data Encryption (TDE) en bases de datos SQL Server.

b. Cifrado en Tránsito:

TLS/SSL: Asegurar que todas las conexiones a la base de datos estén protegidas mediante TLS/SSL para evitar la intercepción de datos durante la transmisión.

VPN: Utilizar redes privadas virtuales (VPN) para proteger la comunicación entre servidores y clientes que acceden a la base de datos.

Ilustración 14 Formato de cifrado de datos

Este proceso se ejecuta acorde a las características del sistema actual dentro de la institución, y cubre las necesidades más sensibles para mantener protegido la información almacenada.

Justificación de la implementación

Categoría	Aspecto	Descripción
Protección de Datos Sensibles	Confidencialidad	El cifrado asegura que solo los usuarios autorizados puedan acceder a los datos sensibles, protegiendo la confidencialidad de la información.
	Cumplimiento Normativo	Ayuda a cumplir con las normativas y estándares de protección de datos.
Reducción de Riesgos	Minimización de Impacto	En caso de una brecha de seguridad, los datos cifrados son inutilizables para los atacantes sin las claves de cifrado, minimizando el impacto del incidente.
	Integridad de Datos	Protege los datos contra modificaciones no autorizadas y asegura que la información permanece intacta y confiable.
Mejora de la Confianza	Confianza del Cliente	Implementar cifrado robusta mejora la confianza de los clientes y socios comerciales, demostrando un compromiso con la seguridad de sus datos.
	Reputación de la Empresa	Mantener prácticas de cifrado adecuadas contribuye positivamente a la reputación de la empresa, mostrando que se toman en serio las preocupaciones de seguridad.

Tabla 15 Justificación de implementación

Implementar y mantener el cifrado de bases de datos es una medida fundamental para proteger la información sensible contra accesos no autorizados y brechas de seguridad, proporcionando una capa adicional de defensa crítica en la estrategia general de seguridad de una organización.

Concientización y formación

Se diseña una guía rápida para proporcionar a los usuarios y empleados una referencia fácil de entender y accesible que detalla las acciones y prácticas esenciales para proteger la información y los sistemas de la organización. Esta guía sirve como una herramienta práctica que complementa las políticas y procedimientos más detallados, ayudando a garantizar que las medidas de seguridad se implementen de manera efectiva y eficiente, además de que propicia una cultura de uso de los accesos que se disponen dentro del sistema.

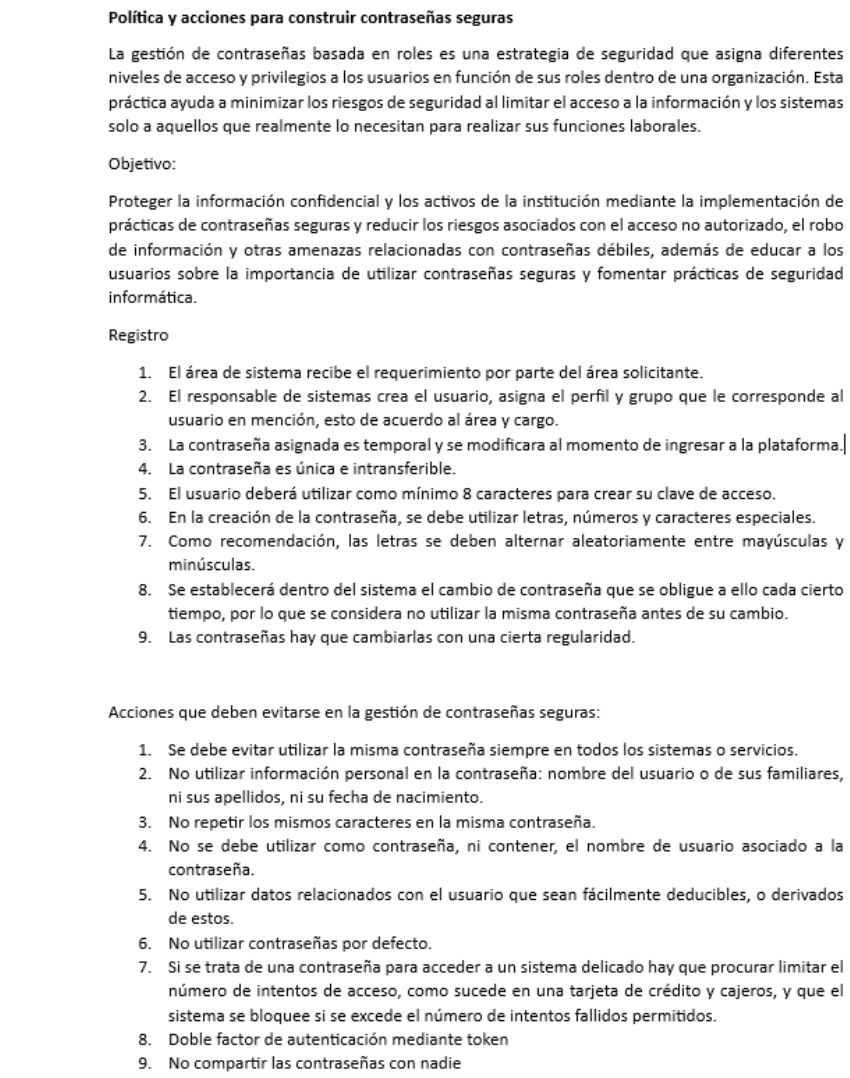
Ilustración 15 Guía rápida

Diseñar una guía rápida para un sistema de información puede proporcionar varios resultados beneficiosos. A continuación, se detallan algunos de los resultados clave que se obtienen:

1. Facilitar la comprensión y el uso del sistema
2. Reducir el tiempo de capacitación
3. Con una guía rápida, los usuarios pueden encontrar rápidamente las funciones y características que necesitan, lo que mejora su productividad y eficiencia en el uso del sistema.
4. Se reduce la probabilidad de que los usuarios cometan errores o se sientan frustrados al intentar utilizar el sistema.
5. Soporte en la resolución de problemas comunes.

6. Proporcionar una guía rápida ayuda a asegurar que todos los usuarios utilicen el sistema de manera consistente y conforme a las mejores prácticas establecidas.
7. Mejorar la comunicación interna:

8. Una guía rápida puede ser una herramienta de comunicación efectiva entre los desarrolladores del sistema y los usuarios finales, asegurando que todos comprendan las capacidades y limitaciones del sistema.
9. Una guía rápida puede ser fácilmente actualizada para reflejar nuevas características y mejoras del sistema, manteniendo a los usuarios informados y al día con los cambios.



Política y acciones para construir contraseñas seguras

La gestión de contraseñas basada en roles es una estrategia de seguridad que asigna diferentes niveles de acceso y privilegios a los usuarios en función de sus roles dentro de una organización. Esta práctica ayuda a minimizar los riesgos de seguridad al limitar el acceso a la información y los sistemas solo a aquellos que realmente lo necesitan para realizar sus funciones laborales.

Objetivo:

Proteger la información confidencial y los activos de la institución mediante la implementación de prácticas de contraseñas seguras y reducir los riesgos asociados con el acceso no autorizado, el robo de información y otras amenazas relacionadas con contraseñas débiles, además de educar a los usuarios sobre la importancia de utilizar contraseñas seguras y fomentar prácticas de seguridad informática.

Registro

1. El área de sistema recibe el requerimiento por parte del área solicitante.
2. El responsable de sistemas crea el usuario, asigna el perfil y grupo que le corresponde al usuario en mención, esto de acuerdo al área y cargo.
3. La contraseña asignada es temporal y se modificara al momento de ingresar a la plataforma.
4. La contraseña es única e intransferible.
5. El usuario deberá utilizar como mínimo 8 caracteres para crear su clave de acceso.
6. En la creación de la contraseña, se debe utilizar letras, números y caracteres especiales.
7. Como recomendación, las letras se deben alternar aleatoriamente entre mayúsculas y minúsculas.
8. Se establecerá dentro del sistema el cambio de contraseña que se obligue a ello cada cierto tiempo, por lo que se considera no utilizar la misma contraseña antes de su cambio.
9. Las contraseñas hay que cambiarlas con una cierta regularidad.

Acciones que deben evitarse en la gestión de contraseñas seguras:

1. Se debe evitar utilizar la misma contraseña siempre en todos los sistemas o servicios.
2. No utilizar información personal en la contraseña: nombre del usuario o de sus familiares, ni sus apellidos, ni su fecha de nacimiento.
3. No repetir los mismos caracteres en la misma contraseña.
4. No se debe utilizar como contraseña, ni contener, el nombre de usuario asociado a la contraseña.
5. No utilizar datos relacionados con el usuario que sean fácilmente deducibles, o derivados de estos.
6. No utilizar contraseñas por defecto.
7. Si se trata de una contraseña para acceder a un sistema delicado hay que procurar limitar el número de intentos de acceso, como sucede en una tarjeta de crédito y cajeros, y que el sistema se bloquee si se excede el número de intentos fallidos permitidos.
8. Doble factor de autenticación mediante token
9. No compartir las contraseñas con nadie

Ilustración 16 Formato de guía rápido

Política de acceso

El diseño de un manual de usuario en este protocolo de seguridad es proporcionar a los usuarios finales y al personal de la institución una guía clara y detallada sobre cómo operar de manera segura dentro del entorno de información. Este manual sirve como una herramienta educativa y de referencia que promueve el cumplimiento de las políticas de seguridad y asegura la correcta implementación de las medidas de protección de datos, a continuación, se muestra el manual que fue diseñado para el uso de los módulos que tienen a su disposición los usuarios dentro de la institución.

MANUAL DE USUARIO DEL SISTEMA DE INFORMACIÓN "SITESCI" PARA JEFATURAS DE DIVISION

Ilustración 17 Manual de usuario

Gestión de incidentes

Plan ante desastres naturales, en este plan de continuidad, se describen un conjunto detallado de los procedimientos y estrategias diseñadas para asegurar que la institución pueda mantener sus operaciones y recuperarse de manera inmediata en caso de enfrentar interrupciones graves o ante desastres que afectes los sistemas informáticos. El objetivo principal es garantizar que la institución pueda seguir operando de manera efectiva. Proporcionando un marco estructurado para gestionar crisis y minimizar interrupciones, asegurando así la estabilidad y la capacidad de respuesta ante situaciones adversas, para ello como se muestra en la figura siguiente, el plan de recuperación y de continuidad dentro de la institución que se describe, sigue las pautas más importantes para su conocimiento en el entorno donde se tiene el sistema de información y la infraestructura tecnológica.

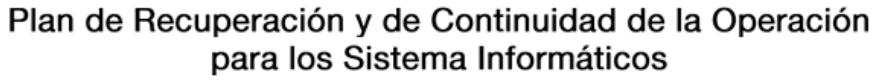


Ilustración 18 Formato de plan de incidentes

Acceso y modificación de datos

Otro apartado en la gestión de incidentes, es contar con un formato claro y conciso para mantener registrados los eventos que se realizan dentro del sistema, y para ello, se plantea un proceso para acceder y modificar datos dentro de la plataforma que utiliza la institución, esto para que se haga de una forma más efectiva y no se cometan acciones erróneas o indebidas que comprometan la integridad de los datos que se almacenan dentro de la institución.

A continuación, se describe de manera general en la siguiente ilustración.

Proceso de Modificación de Calificaciones

1. Descripción General del Proceso:
Este proceso permite a los docentes y administradores realizar cambios en las calificaciones de los estudiantes, asegurando que los ajustes se realicen de manera precisa, segura y conforme a las normativas académicas.

2. Objetivo del Proceso:
Garantizar que las calificaciones de los estudiantes se modifiquen de manera adecuada, con trazabilidad, control de acceso y seguridad, para mantener la integridad y confidencialidad de los datos académicos.

3. Alcance:
Este proceso aplica a todos los cursos y estudiantes registrados en el sistema. Involucra a los docentes, administradores académicos y personal autorizado.

4. Flujo del Proceso:
Paso 1: Solicitud de Modificación
El docente o jefe de área inicia una solicitud de modificación de calificaciones a través de la interfaz del sistema.
Datos Requeridos: Identificación del curso, nombre del estudiante, calificación actual y nueva calificación.
Validación: Verificación de permisos del usuario y autenticación de identidad mediante un sistema de autenticación de dos factores (2FA).

Paso 2: Revisión y Aprobación
La Dirección Académica o responsable revisa la solicitud de modificación y verifica la justificación y la autenticidad de la solicitud.
Datos requeridos: documentación justificativa, historial académico del estudiante, y registro de la calificación anterior.
Validación: Aprobación basada en la normativa interna y la normativa académica vigente.

Paso 3: Modificación de la Calificación
Una vez autorizada la solicitud, el responsable del sistema actualiza la calificación con los datos requeridos y asentando la nueva calificación.

Ilustración 19 Formato de proceso de modificaciones

Auditorías Internas

Para esta etapa de la investigación se propone las fechas para su ejecución, cada trimestre, se realizará una evaluación integral con el objetivo de asegurar el cumplimiento de las políticas y procedimientos internos de seguridad, es decir, se evaluará el cumplimiento de las políticas y la efectividad de los controles implementados, durante esta auditoría, se llevarán a cabo diversas actividades, incluyendo una revisión exhaustiva de los logs para identificar cualquier actividad inusual o no autorizada. Además, se analizarán los incidentes de seguridad reportados en el período para determinar sus causas y evitar futuras ocurrencias similares. Se verificará el acceso de los usuarios para garantizar que los permisos se otorguen de acuerdo con las políticas de mínimos privilegios y que no haya accesos indebidos. Finalmente, se ejecutarán pruebas de vulnerabilidad internas para identificar y corregir debilidades en el sistema antes de que puedan ser explotadas.

PROCESO PARA EJECUTAR UNA AUDITORÍA INTERNA

Ejecutar una auditoría interna en un sistema de información es un proceso sistemático y organizado que busca evaluar el cumplimiento de las políticas y procedimientos de seguridad, así como identificar posibles vulnerabilidades y áreas de mejora. A continuación, se presenta un proceso detallado para llevar a cabo una auditoría interna:

1. Planificación de la Auditoría

Definición del Alcance:

- Determinar qué áreas y sistemas serán auditados.
- Especificar los objetivos de la auditoría.

Formación del Equipo de Auditoría:

- Seleccionar auditores con experiencia y conocimientos adecuados.
- Asignar roles y responsabilidades dentro del equipo.

Elaboración del Plan de Auditoría:

- Crear un cronograma detallado con las actividades a realizar y los plazos.
- Identificar los recursos necesarios (herramientas, documentación, acceso a sistemas).

2. Recolección de Información

Revisión de Documentación:

- Revisar políticas de seguridad, procedimientos, manuales y registros.
- Obtener una comprensión completa de los controles y procesos existentes.

Entrevistas y Encuestas:

- Realizar entrevistas con personal clave para entender mejor las prácticas y procedimientos.
- Distribuir encuestas si es necesario para recolectar información adicional.

3. Ejecución de Pruebas y Revisión

Revisión de Logs:

- Analizar logs de sistemas, aplicaciones y redes para identificar actividades sospechosas o no conformidades.

Análisis de Incidentes:

- Revisar los incidentes de seguridad reportados para evaluar la respuesta y medidas correctivas adoptadas.

Verificación de Acceso:

- Verificar que los accesos a los sistemas y datos están alineados con las políticas de seguridad y principios de mínimos privilegios.

Pruebas de Vulnerabilidad Internas:

Ilustración 20 Formato de auditoría interna

Mejora continua

Revisión de formatos de incidencias

Con la revisión de Formatos de Incidencias se refiere al proceso sistemático de evaluación y actualización de los documentos y plantillas utilizados para reportar y gestionar incidentes de seguridad dentro de la institución. Este proceso asegura que los formatos de incidencias sean eficaces, completos y estén alineados con las políticas y procedimientos de seguridad establecidos, el siguiente formato contempla las principales características para ejecutar un registro de incidentes de manera adecuada para que se pueda analizar con mayor facilidad en el proceso que lo requiera, y con este análisis se determine que el protocolo se mantenga efectivo o se actualice en caso de cambios en los entornos requeridos.

FORMATO DE REGISTRO DE INCIDENCIAS

Encabezado del documento
Nombre de la Organización: Nombre de la organización
Título del Documento: Registro de Incidencias de Seguridad de la Información
Fecha de Creación: Fecha
Versión del Documento: Versión

Detalles de la incidencia
ID de Incidencia: Número único de identificación
Fecha y Hora de Detección: Fecha y hora exacta
Detectado por: Nombre y cargo del detector
Fuente de Detección: Sistema de detección, empleado, auditoría, etc.

Descripción de la Incidencia
Descripción Detallada: Descripción completa de la incidencia
Tipo de Incidencia: Phishing, malware, acceso no autorizado, etc.
Impacto: Confidencialidad, integridad, disponibilidad
Gravedad: Alto, Medio, Bajo

Análisis de la Incidencia
Causa Raíz: Descripción de la causa raíz del incidente
Métodos Utilizados: Métodos o técnicas utilizadas por el atacante
Vulnerabilidades: Vulnerabilidades específicas explotadas

Respuesta y Mitigación
Acciones Inmediatas: Acciones tomadas inmediatamente después de la detección
Medidas de Contención: Medidas implementadas para contener el incidente
Medidas Correctivas: Medidas a largo plazo para corregir y prevenir futuros incidentes
Fecha de Resolución: Fecha en que la incidencia fue resuelta

Impacto y Recuperación
Evaluación del Impacto: Descripción del impacto en la organización
Tiempo de Inactividad: Duración del tiempo de inactividad, si aplica
Coste Estimado: Coste estimado del incidente en términos de recursos, tiempo, y dinero

Lecciones Aprendidas
Análisis de Lecciones: Lecciones aprendidas del incidente
Recomendaciones: Recomendaciones para evitar futuros incidentes similares

Revisión y Cierre
Revisado por: Nombre y cargo del revisor
Fecha de Revisión: Fecha de la revisión final
Comentarios Adicionales: Comentarios adicionales sobre la incidencia

Anexos
Documentación de Soporte: Archivos adicionales, capturas de pantalla, logs, etc.

Ilustración 21 Formato de incidencias para su análisis

CAPÍTULO 5.

CONCLUSIONES Y PERSPECTIVAS PARA TRABAJOS FUTUROS

Conclusión

La seguridad en un sistema de información para una institución de educación superior es un componente crítico en el mundo digital actual, el diseñar un protocolo de seguridad que cubra las necesidades es un tema que no se debe tomar a la ligera, por tal motivo, al concluir este proceso, es esencial destacar los siguientes aspectos clave que se han abordado para asegurar que el protocolo pueda ser implementado de una manera eficaz dentro de la institución para proteger el sistema. El primer paso en el diseño del protocolo de seguridad fue llevar a cabo una evaluación exhaustiva de riesgos y análisis de vulnerabilidades. Esto implicó identificar y clasificar los activos de información, evaluar las posibles amenazas y analizar las vulnerabilidades existentes. A partir de este análisis, se estableció una comprensión clara de los riesgos a los que está expuesto el sistema, lo cual permitió priorizar las medidas de seguridad necesarias.

Una vez identificados los riesgos, se procedió a la definición de políticas y procedimientos de seguridad. Estas políticas establecen las directrices y normas que deben seguirse para proteger la información y los sistemas. Incluyen aspectos como el control de acceso, la gestión de contraseñas, la encriptación de datos, la seguridad de la red y la protección contra malware. Los procedimientos detallan los pasos específicos que deben seguir los usuarios y administradores para cumplir con estas políticas.

La implementación de controles de seguridad es un paso crucial en el protocolo. Se aplicaron controles técnicos, administrativos y físicos para mitigar los riesgos identificados. Entre los controles técnicos, se incluyeron firewalls, sistemas de detección y prevención de intrusiones (IDS/IPS).

El protocolo de seguridad también incluyó la implementación de sistemas de monitoreo y detección de incidentes. Estos sistemas permiten la vigilancia continua del tráfico de red, los eventos de seguridad y las actividades sospechosas. Se establecieron procedimientos para la respuesta a incidentes, que incluyen la identificación, contención, erradicación y recuperación de cualquier amenaza detectada. La capacidad de detectar y responder rápidamente a los incidentes es esencial para minimizar el impacto de posibles ataques.

Un componente esencial del protocolo fue el desarrollo de un plan de respuesta a incidentes y recuperación de desastres. Este plan asegura que el sistema pueda recuperarse rápidamente de cualquier interrupción, ya sea causada por un ataque cibernético, un fallo técnico o un desastre natural. El plan incluye procedimientos detallados para la continuidad del negocio, la restauración de datos y la comunicación con las partes interesadas durante una crisis.

El protocolo de seguridad no es un documento estático, sino un proceso dinámico que requiere evaluación y mejora continua. Se establecieron mecanismos para la revisión periódica de las políticas y procedimientos de seguridad, así como para la realización de pruebas de penetración y auditorías

de seguridad. La retroalimentación obtenida de estas evaluaciones se utiliza para ajustar y mejorar el protocolo, asegurando que se mantenga actualizado frente a nuevas amenazas y tecnologías emergentes.

La educación y concienciación del personal es un pilar fundamental en la estrategia de seguridad. Se implementan programas de capacitación para todos los empleados, enfocándose en la importancia de la seguridad de la información y las mejores prácticas para proteger los datos. La concienciación constante ayuda a crear una cultura de seguridad dentro de la organización, donde cada miembro comprende su papel y responsabilidad en la protección de la información.

En conclusión, el diseño de un protocolo de seguridad para un sistema de información es un proceso integral que abarca la evaluación de riesgos, la implementación de controles, el monitoreo continuo y la mejora constante. Al seguir un enfoque sistemático y bien documentado, se puede lograr un alto nivel de seguridad que protege los activos de información y asegura la continuidad operativa de la institución.

Pasos Futuras

Las etapas futuras para la implementación del protocolo de seguridad se centran en establecer un plan claro y detallado que garantice su correcta ejecución. El primer paso consiste en la formación del equipo de implementación, designando un grupo de personas que serán responsables de llevar a cabo las tareas relacionadas con el protocolo. Este equipo debe contar con las habilidades y conocimientos necesarios para asegurar una correcta implementación.

A continuación, se debe proceder con el desarrollo del plan de proyecto, que implica la creación de un cronograma. Este cronograma debe incluir hitos clave, especificando plazos, asignación de responsabilidades y la identificación de los recursos que se requerirán a lo largo del proceso.

El siguiente paso es la asignación de recursos, lo cual consiste en garantizar que se cuenten con los recursos humanos, financieros y tecnológicos adecuados para cumplir con las tareas y objetivos del protocolo.

En cuanto al tiempo estimado para la implementación, el proceso se divide en dos fases principales. La primera es la evaluación inicial, que tomará entre una y dos semanas. Durante esta fase, se debe revisar el estado actual del protocolo de seguridad, identificando posibles vulnerabilidades y áreas que necesitan mejora. La segunda fase es la planificación y diseño, que tendrá una duración de entre dos y cuatro semanas. En esta etapa, se desarrollarán las estrategias específicas para la ejecución del protocolo, garantizando que se cumplan los objetivos de seguridad establecidos.

REFERENCIAS

Álvarez, J. (2017). Monitoreo y registro en sistemas de información. Editorial Técnica.

Castro, L. (2018). Control de acceso basado en roles (RBAC). Revista de Seguridad Informática, 12(4), 45-58.

Fernández, M. (2016). Disponibilidad en sistemas críticos. Editorial Universitaria.

García, L., & Martínez, J. (2018). Seguridad informática: Estrategias y técnicas de defensa. Editorial Universitaria.

González, F. (2018). Autenticación en entornos digitales. Editorial Seguridad.

Introducción

ISO 31000: "Gestión del riesgo - Directrices".

ISO/IEC 27001. (2013). Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos. ISO.

ISO/IEC 27001: "Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos".

López, M., & Pérez, R. (2020). Impacto de las brechas de seguridad en las organizaciones. Revista de Seguridad Informática, 15(2), 45-60.

López, P. (2019). Cifrado de datos: Teoría y práctica. Editorial Criptografía.

Marco teórico

Martínez, J., & López, R. (2019). Autorización y control de acceso. Ediciones Informáticas.

Mendoza, S. (2019). Pruebas de penetración: Metodologías y técnicas. Revista de Seguridad Cibernética, 15(2), 123-140.

Navarro, D. (2020). Antivirus y protección de sistemas. Editorial Seguridad Digital.

NIST SP 800-53: "Security and Privacy Controls for Federal Information Systems and Organizations".

Pérez, C. (2020). Confidencialidad en la era de la información. Editorial Seguridad.

Ramírez, H., & Hernández, T. (2017). Integridad de datos y técnicas de verificación. Editorial Informática.

Rodríguez, E. (2017). Gestión de identidades y autenticación multifactor. Editorial Cibernética.

Sánchez, R. (2015). Firewalls: Principios y prácticas. Ediciones de Seguridad.

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. Information & Management, 46(5), 267-270.

Software Engineering Institute: "OCTAVE: Methodology for Information Security Risk Assessments".

Stallings, W. (2017). Computer Security: Principles and Practice. Pearson.

Stallings, W., & Brown, L.: "Seguridad en Redes y Sistemas de Información".

Van Niekerk, J., & Von Solms, R. (2010). Information security culture: A management perspective. Computers & Security, 29(4), 476-486.

Vega, L. (2020). Educación y concienciación en seguridad informática. Revista de Seguridad, 18(3), 70-85.

Whitman, M. E., & Mattord, H. J.: "Principios de Seguridad de la Información".

ANEXOS

Toda la documentación y/o formatos generados al momento de realizar la presente investigación no se adjunta en este apartado, ya que contienen información confidencial de la institución y estos documentos solo deberán estar disponibles después de que se haya aprobado el protocolo de seguridad correspondiente. En su lugar, se hace referencia a ellos en una ilustración de su alojamiento dentro de un repositorio digital para su disposición una vez que se proceda con dicho proceso.

Ilustración 22 Repositorio Digital del Protocolo