Fundamentos de Seguridad Informática y Ciberseguridad

Clara Pozo

Raúl Saed Reascos

R. Wladimir Minaya

EDICIONES GESICAP

TODOS LOS DERECHOS RESERVADOS:

Texto arbitrado bajo la modalidad doble par ciego.
El Carmen, Manabí, Ecuador
https://edicionesgesicap.com

ISBN: 978-9942-626-25-7

Depósito Legal: 1ra Edición: Ediciones Gesicap, Calle 24 de julio y Ave. 3 de julio, El Carmen, Manabí, Ecuador.

CÓMO CITAR ESTE LIBRO:

Pozo Hernández, C.G; Reascos Pinchao, R.S; Minaya Macías, R.W. (2025). Fundamentos de seguridad informática y ciberseguridad. Ediciones GESICAP. 77 pp.

EQUIPO EDITORIAL:

Edición y Maquetación: Sergio Alejandro Rodríguez Hernández
Revisión y Corrección: Xenia Pedraza González
Diseño de Portada: Sergio Alejandro Rodríguez Hernández.

Toda la información relacionada al contenido del texto es responsabilidad de los autores.

Fundamentos de Seguridad Informática y Ciberseguridad

Pozo Hernández Clara Guadalupe
Universidad Laica Eloy Alfaro de Manabí
Clara.pozo@uleam.edu.ec
Orcid: https://orcid.org/0000-0002-7903-4312

Reascos Pinchao Raúl Saed
Universidad Laica Eloy Alfaro de Manabí
raul.reascos@uleam.edu.ec
Orcid: https://orcid.org/0000-0002-7903-4312

Minaya Macías Renelmo Wladimir
Universidad Laica Eloy Alfaro de Manabí
renelmo.minaya@uleam.edu.ec
Orcid: https://orcid.org/0000-0002- 0418-6864

Prólogo

En la era digital actual, la seguridad de la información y la ciberseguridad se han convertido en pilares fundamentales para la protección de datos y sistemas en todo el mundo. Este libro, “Fundamentos de Seguridad Informática y Ciberseguridad”, está diseñado para proporcionar una comprensión integral de los conceptos clave y las mejores prácticas en esta área. A través de sus capítulos, se exploran definiciones generales, principios y dimensiones de la seguridad de la información, así como conceptos esenciales como riesgo, vulnerabilidad y amenaza.

El libro también aborda el control de acceso, detallando los mecanismos y tipos de autenticación, incluyendo la autenticación multifactor, y la autorización. Además, se profundiza en la ciberseguridad, analizando las fases de ciberseguridad, ciberataques y ciberatacantes, y ofreciendo estrategias para protegerse contra ellos. Se dedica una sección detallada al malware y a las técnicas de ingeniería social, proporcionando una visión clara de cómo proteger los recursos del sistema.

Finalmente, se presenta la gestión de riesgos de seguridad de la información, incluyendo la identificación, análisis, evaluación y tratamiento de riesgos, y se exploran los componentes de un Sistema de Gestión de Seguridad de la Información (SGSI). Se destaca la importancia de la norma ISO 27001 en la gestión de la seguridad de la información y se detallan sus requisitos. Este libro es una guía esencial para profesionales y estudiantes que buscan profundizar en la seguridad informática y la ciberseguridad, contribuyendo a fortalecer la protección de la información en sus respectivas organizaciones.

Contenidos

6 SGSI SEGÚN ISO 27001 / 68

TABLAS

ÍNDICE DE ILUSTRACIONES

capítulo uno

INTRODUCCIÓN

1 / INTRODUCCIÓN

En el ámbito de la seguridad informática, es fundamental comprender ciertos conceptos y definiciones que serán recurrentes a lo largo de este documento. Este capítulo tiene como objetivo proporcionar una base sólida de términos clave que permitirán al lector entender mejor los temas más complejos que se abordarán posteriormente. Desde la definición de seguridad en un sentido amplio hasta los principios específicos de la seguridad de la información, esta sección sentará las bases para una comprensión integral de las medidas y prácticas necesarias para proteger la información en el entorno digital.

1.1 / DEFINICIONES GENERALES

Antes de abordar la seguridad de la información, es importante considerar algunos términos y sus definiciones que se mencionarán con frecuencia en diferentes apartados de este documento.

Seguridad: Es una palabra que significa estar libre de cualquier peligro o daño. Puede considerarse como la garantía que tienen las personas de estar libres de daño, amenaza, peligro o riesgo en cualquier situación de la vida (Tamilarasan, Srinivasan, Dhivya, Subramanian, & Govindasamy, 2023).

1.1.1 / SEGURIDAD INFORMÁTICA

Cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema de red informática, cuyos efectos pueden conllevar daños sobre la misma y comprometer su confidencialidad, autenticidad o integridad (Gómez Vieites, 2017).

1.1.2 SEGURIDAD DE LA INFORMACIÓN

Condición que permite tener libertad ante el peligro, cuyo principal objetivo es la protección contra los adversarios (Samaniego Mena & Ponce Ordoñez, 2021).

Información: Resultado del procesamiento de datos, todo aquello susceptible de ser aprendido o que puede transmitir un conocimiento (Turban, Sharda, & Delen, 2011).

Seguridad de la Información puede definirse como:

Estado de cualquier tipo de información (informática o no) que indica que ese sistema está libre de peligro, daño o riesgo.

Otras definiciones para considerar

La seguridad de la información es la protección de la integridad, disponibilidad y confidencialidad de la información, según el nivel requerido para los objetivos de negocio de la empresa (Pérez, 2015).

Es la protección de la información y de los sistemas de información del acceso, uso, divulgación y destrucción no autorizada a través de estándares, procesos, procedimientos, estrategias, recursos informáticos, recursos educativos y recursos humanos (Avenía Delgado, 2017).

- Un proceso para eliminar los riesgos asociados a la confidencialidad, integridad y disponibilidad de uno de los recursos empresariales más valiosos: la información.

Ilustración 1. Seguridad de la información (Generado en Copilot)

- Preservación de la confidencialidad, integridad y disponibilidad de la información, pudiendo además abarcar otras propiedades como autenticidad, responsabilidad o el no repudio (ISO 27001).

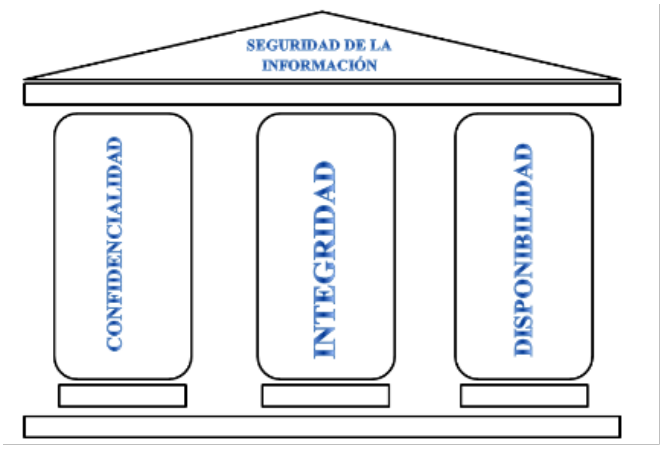


Ilustración 2. Principios de seguridad de la información

1.1.3 / PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

Se considera un sistema seguro cuando el software y hardware garantizan la protección del usuario y de su información. Para ello, deben cumplir tres principios pilares básicos de seguridad.

Confidencialidad: También conocida como privacidad, es la necesidad de que la información sea conocida solo por las personas autorizadas, garantizando que los datos no se propaguen de manera fortuita o

deliberada. Existen datos que, por su carácter delicado, no pueden ser divulgados (Merkow & Breithaupt, 2014). Por ejemplo:

- En el área de salud: Los médicos tienen la obligación de mantener en reserva los datos de sus pacientes, así como los diagnósticos y tratamientos. Esta información no puede ser compartida ni divulgada por ningún medio sin el consentimiento del paciente.

- Área Financiera: Es responsabilidad de bancos, cooperativas y entidades financieras proteger los datos de sus clientes, como detalles de transacciones, estados de cuenta y números de tarjetas de crédito. La divulgación de alguno de estos datos podría infringir leyes de privacidad y conllevar sanciones para la entidad.

- Área empresarial: El departamento de recursos humanos de cada empresa debe proteger la información personal y profesional de sus empleados, como roles de pago, evaluaciones de desempeño, historial laboral y salarios. Deben asegurarse de compartir dicha información solo con personal autorizado.

Es la propiedad de prevenir la revelación y divulgación intencionada o no intencionada de información a personas o sistemas no autorizados

Para garantizar el principio de confidencialidad, las empresas pueden implementar medidas o controles como:

- Cifrar datos, de modo que, en caso de acceso no autorizado, la información no sea entendible sin las claves para descifrarla.
- Establecer roles para limitar el acceso a la información confidencial solo a aquellas personas que necesiten trabajar con ella.
- Implementar controles de acceso físico a los lugares donde se encuentran los equipos con información confidencial y controles lógicos como mecanismos de

Ilustración 3. Confidencialidad de la Información (generado en Copilot)

autenticación para acceso a sistemas.

- Firmar acuerdos de confidencialidad con aquellos usuarios que manejan información delicada.

Integridad: Se refiere a que la información (almacenada o enviada) no ha sido manipulada por terceros con mala intención, asegurando que solo los usuarios autorizados puedan modificarla. Esto garantiza que los datos recibidos o recuperados sean exactamente los que fueron enviados o almacenados, sin modificaciones, asegurando la exactitud y fiabilidad de la información (Anderson, 2010). La integridad de los datos es vital, por ejemplo:

Ilustración 4. Integridad de la Información (Generado en Copilot)

- **Área de salud:** La información y las historias clínicas de los pacientes incluyen datos sensibles. Un error en un diagnóstico, como cambiar datos sobre alergias, puede ocasionar que se suministre un medicamento que afecte gravemente al paciente, llevando al médico a tomar decisiones incorrectas sobre el tratamiento.

- **Área financiera:** Las entidades financieras deben garantizar que los saldos en las cuentas de sus clientes no sean alterados por transacciones no realizadas por los propietarios.

- **Área empresarial:** Si la integridad de los datos del inventario se ve comprometida por errores en la base de datos, fallos del sistema o manipulación no autorizada, las cantidades de productos pueden estar equivocadas, lo que puede llevar a decisiones empresariales erróneas y a la imposibilidad de cumplir con los clientes al comprometer una venta sin stock suficiente.

La integridad de la información no sólo es proteger datos de acciones externas como acceso de hackers o malware, también cubre aspectos internos como errores humanos, de diseño o programación.

Es la característica que asegura que los datos permanezcan sin alteraciones no autorizadas

Para garantizar la integridad de los datos, las empresas pueden implementar medidas o controles como:

- Limitar permisos de usuarios sobre el uso de información.
- Utilizar hashing de los datos para asegurar que no han sido modificados.
- Gestionar la configuración de los sistemas para asegurar que no ha sido cambiada sin autorización.
- Gestionar cambios para asegurar la integridad de los procesos.
- Implementar controles de acceso físico a las instalaciones y lógico a la información, los sistemas y aplicaciones, así como a la red.
- Utilizar firmas digitales en la información.
- Realizar auditorías de seguridad.

Disponibilidad: Un sistema está disponible cuando sus usuarios legítimos pueden utilizarlo para realizar funciones legítimas, es decir, para realizar el trabajo necesario para el negocio. Esto implica un acceso permanente y la posibilidad de recuperación en caso de incidente (Gallacher & Morris, 2012). No tener acceso a información en el momento oportuno puede resultar muy perjudicial, por ejemplo:

- Área de salud: Los profesionales de la salud necesitan acceso a la información digital de sus pacientes en casos de emergencia. No es posible esperar para revisar la historia clínica, ya que esto puede ocasionar retrasos en el tratamiento, errores médicos involuntarios por falta de información y complicaciones éticas y legales.

- Área financiera: Los clientes de empresas financieras necesitan realizar transacciones en el momento que lo requieran. Si una plataforma deja de funcionar cuando un cliente intenta efectuar un pago de su tarjeta de crédito, préstamo u otra obligación financiera, la imposibilidad de completar la transacción a tiempo puede resultar en multas o recargos por incumplimiento de contrato.

- Área empresarial: Las empresas que venden productos en línea dependen de que los clientes puedan acceder a sus plataformas para realizar compras. Si un servidor deja de funcionar, la plataforma puede volverse inaccesible, lo que puede resultar en pérdidas económicas.

Es la propiedad de la información de estar disponible para los usuarios autorizados, ya sean personas, procesos o aplicaciones.

Para asegurar la disponibilidad de la información, las empresas pueden implementar medidas o controles como:

- Realizar copias de seguridad de la información (backups de datos y configuraciones).
- Crear imágenes de discos.
- Implementar sistemas RAID de discos.
- Implementar sistemas en clúster.
- Configurar conmutación por error entre sistemas.
- Balancear la carga entre máquinas/sistemas.
- Asegurar redundancia en las líneas eléctricas y de datos.

1.1.4 / DIMENSIONES DE SEGURIDAD DE LA INFORMACIÓN

Además de los tres principios de seguridad, la información debe cumplir con otras características o cualidades que, al sumarse a las anteriores, constituyen las dimensiones de seguridad:

Ilustración 5. Dimensiones de seguridad de la Información

Autenticación: Es el proceso que permite verificar si un documento o hecho es genuino. En informática, consiste en revisar la identidad de los participantes en una comunicación y asegurar que son quienes dicen ser, permitiendo verificar la identidad de las personas que manejan la información. Generalmente, un usuario demuestra su identidad proporcionando sus credenciales, como una contraseña, un PIN, la respuesta a una pregunta personal, etc.

Ilustración 6. Autenticación (Generado en Copilot)

Trazabilidad-No Repudio: Garantiza que las actuaciones de una entidad pueden ser imputadas única e inequívocamente a dicha entidad.

1.1.5 / RIESGO

Es la posibilidad de ocurrencia de un evento no deseado con consecuencias negativas, especialmente en el contexto de la seguridad de los recursos de información.

1.1.6 / VULNERABILIDAD

Es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información, permitiendo que un atacante comprometa su integridad, disponibilidad o confidencialidad (Vega Briceño E. , 2021).

1.1.7 / AMENAZA

Es una causa potencial de un incidente no deseado que puede provocar daños a un sistema u organización. Cualquier acción que aproveche una vulnerabilidad para comprometer la seguridad de un sistema de información se considera una amenaza, ya sea accidental o intencionada (Avenía Delgado, 2017).

1.2 / OBJETIVOS DE LA SEGURIDAD INFORMÁTICA

La información es un activo valioso para las organizaciones, por lo que es necesario protegerla y garantizar su seguridad. Los principales objetivos de la seguridad informática incluyen:

- Confidencialidad de datos: Garantizar que la información sea accesible únicamente para usuarios, dispositivos y procesos autorizados.

- Integridad: Se refiere a la protección contra alteraciones, adiciones o destrucciones no autorizadas. Asegurar la integridad es esencial, especialmente cuando la información es valiosa y no debe perderse, o cuando los datos podrían ser modificados intencionalmente para engañar al receptor. Normalmente, la información se resguarda contra el borrado mediante métodos que garantizan la confidencialidad y la realización de copias de seguridad. Además, la integridad se verifica mediante técnicas de hashing para asegurar que no haya distorsiones.
  - Integridad de los datos: Protección contra cambios o manipulación no autorizada.
  - Integridad del sistema: Asegurar que el sistema funcione según lo esperado.

- Disponibilidad: Garantizar el acceso oportuno y confiable a la información y a los

servicios de información. Las violaciones típicas de accesibilidad incluyen fallos de software/hardware y ataques de denegación de servicio distribuido (DDoS). El sistema de información se protege contra deficiencias eliminando sus causas y contra ataques DDoS bloqueando el tráfico no deseado.

- Autenticidad: La capacidad de identificar de manera única al autor o la fuente de información es crucial. La autenticidad de los datos electrónicos se verifica frecuentemente mediante firmas digitales, lo que garantiza que el recurso, ya sea una persona o una máquina, es realmente quien afirma ser. Estas firmas digitales actúan como una huella digital única que valida la identidad del remitente y asegura que la información no ha sido alterada durante la transmisión. Además, el uso de certificados digitales y criptografía avanzada refuerza esta autenticidad, proporcionando un nivel adicional de confianza y seguridad en las comunicaciones electrónicas. Este proceso es fundamental para prevenir fraudes y asegurar la integridad de las transacciones y comunicaciones en el entorno digital.

- No rechazo: Garantiza que no se pueda negar la autoría de la información ni el hecho de su envío o recepción. Esto se asegura mediante firmas digitales y otros medios y protocolos criptográficos, proporcionando prueba de que se realizó una transacción o se envió/recibió un mensaje. Es relevante en sistemas de licitación electrónica, garantizando la responsabilidad entre vendedores y compradores.

- Protección de recursos: Asegura que solo usuarios autorizados puedan acceder a los objetos del sistema. Primero, se definen las categorías de usuarios que pueden ingresar al sistema. Luego, se establece una política de seguridad y se define el tipo de autorización de acceso para cada grupo de usuarios.

- Autorización: Proceso que asegura que la persona o sistema al otro lado de la sesión tiene permiso para hacer la petición. Determina quién o qué puede acceder a los recursos del sistema o realizar determinadas actividades, generalmente en medio de la autenticación.

- Auditoría: Supervisa los eventos asociados con la seguridad, proporcionando un registro de accesos satisfactorios y no satisfactorios. Lista quién realiza cada tarea en los sistemas y detecta intentos de atravesar las barreras de seguridad o problemas de acceso.
  - Minimizar y gestionar riesgos: Detecta posibles problemas y amenazas a la seguridad.
  - Garantizar la adecuada utilización de recursos: Asegura el uso correcto de los recursos y aplicaciones del sistema.

- Limitar pérdidas y recuperación: Facilita la recuperación adecuada del sistema en caso de un incidente de seguridad.
- Cumplimiento legal: Asegura el cumplimiento del marco legal y los requisitos impuestos por los clientes en sus contratos.

1.3 / CASOS DE ESTUDIO PRINCIPIOS DE SEGURIDAD

CASO DE ESTUDIO 1: ATAQUE RANSOMWARE EN UNA COOPERATIVA DE AHORRO Y CRÉDITO EN CUENCA

Contexto:

CoopFinanzas, una cooperativa de ahorro y crédito con sede en Cuenca, Ecuador, ofrece servicios financieros digitales a miles de clientes en el país. La empresa maneja datos sensibles de los usuarios, incluyendo información de cuentas, transacciones y datos personales. Con el crecimiento de su plataforma digital, CoopFinanzas implementó seguridad básica, pero no contaba con un sistema robusto de copias de seguridad.

Incidente:

Un empleado de CoopFinanzas recibió un correo aparentemente legítimo de un proveedor tecnológico con un archivo adjunto titulado “Actualización de Seguridad”. Al descargarlo, un malware tipo ransomware se infiltra en la red interna de la empresa, encriptando bases de datos críticas y dejando un mensaje de los atacantes exigiendo un rescate en criptomonedas para restaurar.

Debido a que no existían copias de seguridad recientes, la empresa quedó paralizada, afectando transacciones bancarias y generando pánico entre los clientes. La incertidumbre aumentó cuando los atacantes amenazaron con filtrar datos sensibles si no se pagaba el respectivo rescate.

Preguntas para análisis:

- ¿Qué tipo de ataque sufrió CoopFinanzas?
- ¿Cómo se relacionan los principios de confidencialidad, integridad y disponibilidad con el tipo de ataque sufrido?
- ¿Cuáles son las implicaciones legales y financieras de este ataque para la cooperativa?

CASO DE ESTUDIO 2: FILTRACIÓN DE DATOS EN UNA EMPRESA DE LOGÍSTICA EN GUAYAQUIL

Contexto:

EcuatransCargo es una empresa de logística con sede en Guayaquil, que maneja envíos nacionales e internacionales. Su plataforma digital permite a los clientes rastrear paquetes, gestionar pagos y acceder a facturas electrónicas. La empresa almacena datos personales de clientes, incluyendo direcciones, cédulas y detalles de pago.

Para mejorar su eficiencia, la empresa contrató a un desarrollador externo para actualizar su sistema de gestión. Sin embargo, no se realizarán auditorías de seguridad tras los cambios en el software.

Incidente:

Semanas después de la actualización, varios clientes reportaron haber recibido correos sospechosos con detalles de sus envíos y enlaces fraudulentos solicitando pagos adicionales. Una investigación interna reveló que un actor malintencionado había accedido a la base de datos de clientes e información filtrada. Se descubrió que la brecha de seguridad provino de una vulnerabilidad en el código introducido por el desarrollador externo, quien sin saberlo dejó expuesta una API sin autenticación.

Preguntas para análisis:

- ¿Qué principios de seguridad de la información se vieron comprometidos?
- ¿Cuáles fueron las principales vulnerabilidades explotadas?
- ¿Qué controles de seguridad pudo haber implementado EcuatransCargo para prevenir la filtración de datos?
- ¿Cómo debería manejar la empresa la comunicación con sus clientes?

capítulo dos

CONTROL DE ACCESO

2 / CONTROL DE ACCESO

En el ámbito de la seguridad informática, los controles juegan un papel crucial en la protección de los activos de una organización. Estos controles son acciones y mecanismos diseñados para prevenir o reducir el impacto de eventos no deseados que puedan poner en riesgo dichos activos. Su objetivo principal es mitigar los efectos de amenazas o riesgos, asegurando que las operaciones se realicen conforme a los programas, órdenes y principios establecidos.

Ilustración 7. Controles de Acceso (Generado en Copilot)

Este capítulo se centra en la definición y la importancia de los controles, especialmente en el contexto de la informática. Se explorarán los diferentes tipos de controles de acceso, que son esenciales para gestionar y restringir el uso de los recursos del sistema de información y el comportamiento de los usuarios. Además, se abordarán los mecanismos de autenticación, que son fundamentales para garantizar que solo las personas autorizadas puedan acceder a los recursos de la organización, protegiendo así la seguridad y la privacidad de la información.

2.1 / DEFINICIÓN DE CONTROL

Los controles son acciones y mecanismos definidos para prevenir o reducir el impacto de eventos no deseados que ponen en riesgo los activos de una organización. Su objetivo es mitigar los efectos de una amenaza o riesgo. También pueden entenderse como un conjunto de disposiciones metódicas cuyo fin es vigilar las funciones y actitudes de la empresa, permitiendo verificar que todo se realice conforme a los programas adoptados, órdenes impartidas y principios admitidos (Terán, 2014).

En informática un **control de acceso** puede definirse como:

Conjunto de mecanismos y procedimientos que permiten a los gestores de seguridad controlar y restringir el uso de los recursos del sistema de información, así como el comportamiento de los usuarios en relación con el mismo.

Los controles de acceso definen:

- Qué pueden hacer los usuarios.
- A qué recursos pueden acceder.
- Qué operaciones pueden realizar.

2.2 / TIPOS DE CONTROLES DE ACCESO

2.2.1 / AUTENTICACIÓN

La autenticación es el proceso de identificación de un individuo basado en sus credenciales (normalmente nombre de usuario y contraseña). El control de acceso y la autenticación son acciones destinadas a proteger los sistemas informáticos, como servidores y ordenadores. Su objetivo es proporcionar a las empresas mecanismos para gestionar usuarios y datos de identificación, así como controlar el acceso a los recursos. (Areirio Bertolin, 2008)

Ilustración 8. Autenticación (Generado en Copilot)

La autenticación incluye tres pasos:

Identificación: capacidad de identificar de forma exclusiva a un usuario de un sistema

Autenticación: capacidad de demostrar que un usuario o una aplicación es realmente quién dicha persona o aplicación asegura

Autorización: El sistema comprueba que los usuarios tengan permisos para el sistema al que intentan acceder.

En la empresa u organización la autenticación es importante por los siguientes motivos:

- Ayudan a proteger la seguridad de la información.
- Garantizan que solo las personas autorizadas puedan acceder a los recursos de la organización.

- Ayudan a evitar el acceso no autorizado.
- Protegen la privacidad de los datos.
- Garantizan su disponibilidad a las personas autorizadas.
- Aseguran la confidencialidad de los bienes de la empresa.

2.2.2 / MECANISMOS DE AUTENTICACIÓN

La identificación de un usuario es el proceso mediante el cual este afirma ser una persona concreta, es decir, reclama una identidad. La autenticación, por su parte, es el proceso de proporcionar alguna prueba o pruebas de que dicha afirmación es verdadera. La autenticación se basa en algo que solo el usuario legítimo conoce, posee o es.

2.2.3 / TIPOS DE AUTENTICACIÓN

Tabla 1, Tipos de Autenticación

TIPO	DESCRIPCIÓN	EJEMPLO
Tipo 1	Usuario Conoce	Contraseña, PIN, respuesta a una pregunta
Tipo 2	Usuario Tiene	Tarjeta inteligente, mensaje al dispositivo móvil
Tipo 3	Usuario Es, se reconoce alguna característica física del individuo	Técnicas biométricas como: reconocimiento facial, huella dactilar, patrones de voz

En muchas ocasiones, la autenticación no se basa solo en uno de los tipos sino en una combinación.

Tabla 2, Ejemplos de técnicas de autenticación

TÉCNICA	DESCRIPCIÓN
Identificador y Contraseña	El identificador y la contraseña es la combinación de autenticación más conocido. Representado por una palabra, frase o secuencia numérica secreta (conocida solo por el usuario). Para autenticar al usuario, solo se requiere un dispositivo de entrada. Los códigos PIN son generalmente aceptados en todo el mundo debido a su amplia adopción por parte de los cajeros automáticos y al uso generalizado de teléfonos móviles.

Certificados PKI sobre tarjeta inteligente o token USB	Los certificados PKI en tarjetas inteligentes o tokens USB utilizan certificados X.509, que emplean tecnología avanzada de cifrado para firmar o calcular mensajes sin necesidad de compartir un secreto. El identificador es un certificado público firmado y respaldado por una autoridad de certificación reconocida. Para utilizar los distintos elementos criptográficos, el usuario debe proporcionar un secreto, como el PIN de su tarjeta o su llave USB. Esto se aplica principalmente durante el proceso de autenticación inicial en aplicaciones de red o servicios de mensajería. Una autenticación se puede aumentar con un token tangible para probar la veracidad. Un usuario puede producir una tarjeta inteligente, un teléfono inteligente, un dispositivo móvil u otro dispositivo, los cuales son más difíciles de delegar. El token de software más conocido es la contraseña/código de acceso generado por un programa único (OTP)
Verificación automática de Firmas	La firma de un documento se coteja con una firma de referencia para comprobar si coincide. Las empresas suelen utilizar este método de verificación para la autenticación de clientes, la protección de datos y la mejora de la seguridad en general.
Técnicas biométricas	La biometría se refiere a la identificación automática de una persona en base a sus características fisiológicas o de comportamiento

2.2.4 / AUTENTICACIÓN MULTI-FACTORES

La multiplicación del número de factores de autenticación aumenta el nivel de seguridad general, pero plantea los siguientes problemas: El ciclo de vida de cada factor debe administrarse: inicialización de las contraseñas y códigos PIN, distribución de las tarjetas inteligentes. (Vega Briceño E. , 2021)

2.2.5 / AUTORIZACIÓN

Entendemos por autorización una parte del sistema operativo que protege los recursos del sistema, permitiendo que solo sean utilizados por aquellos usuarios a quienes se les ha concedido el derecho para ello.

Ilustración 9. Autenticación multifactor (Generado en Copilot)

El proceso de autorización se utiliza para decidir si una persona, programa o dispositivo tiene permiso para acceder a un dato, funcionalidad o servicio específico.

Entre las principales funciones de la autorización están:

- Asegurar que únicamente los usuarios autorizados puedan realizar acciones permitidas con su correspondiente nivel de privilegio.
- Controlar el acceso a recursos protegidos mediante decisiones basadas en el rol o el nivel de privilegio.
- Prevenir ataques de escalada de privilegios, como el uso de funciones administrativas por parte de un usuario anónimo o incluso un usuario autenticado.

2.3 / CASOS DE ESTUDIO CONTROL DE ACCESO

CASO DE ESTUDIO 1: CONTROL DE ACCESO EN PLANTA SOLAR INTELIGENTE DE "ENERSOL ECUADOR SA"

Contexto:

"EnerSol Ecuador SA" es una empresa dedicada a la generación de energía solar, que opera una planta fotovoltaica en una zona rural del sur del país. La planta cuenta con infraestructura crítica (paneles, inversores y subestaciones) y un sistema SCADA para el control y monitoreo de la producción de energía. Conscientes de la importancia de proteger tanto el entorno físico como el digital, la empresa implementó un sistema de control de acceso de múltiples capas:

Acceso físico: Uso de tarjetas RFID para la entrada general y lectores biométricos (huella y retina) en áreas críticas, como salas de control y cuartos de servidores.

Acceso digital: Autenticación multifactor para ingresar a la plataforma SCADA, combinando contraseña, OTP (One Time Password) y verificación biométrica en dispositivos autorizados.

Incidente:

Una mañana, el sistema de monitoreo de "EnerSol Ecuador SA" detectó varios intentos fallidos de acceso en la sala de servidores. Se identificó que un individuo había obtenido, mediante métodos fraudulentos, una tarjeta RFID perteneciente a un empleado de mantenimiento. Con la tarjeta en mano, el atacante logró ingresar a la planta, pero al

intentar acceder a áreas de alta seguridad, los lectores biométricos impidieron el paso. Paralelamente, se registraron intentos de acceso remoto a la plataforma SCADA utilizando credenciales certificadas. Gracias a las alertas automáticas del sistema, el incidente fue contenido y se inició una investigación para determinar la brecha en la seguridad.

Preguntas para el análisis:

- ¿Qué vulnerabilidades en el control de acceso físico y digital permitieron que el atacante intentara ingresar a áreas restringidas?
- ¿Cómo contribuyó la combinación de métodos (tarjeta RFID y autenticación biométrica) a minimizar el impacto del incidente?
- ¿Qué medidas adicionales podrían implementarse para prevenir el uso fraudulento de tarjetas RFID en el futuro?
- ¿De qué manera puede el monitoreo en tiempo real y la auditoría de eventos mejorar la detección de accesos inusuales tanto en el entorno físico como en el digital?

CASO DE ESTUDIO 2: CONTROL DE ACCESO EN EL CENTRO DE INNOVACIÓN "TECHINNOVATE ECUADOR"

Contexto:

"TechInnovate Ecuador" es un centro de innovación tecnológica ubicado en Guayaquil, especializado en el desarrollo de software y proyectos de investigación de alto valor. La empresa maneja información sensible y propiedad intelectual en sus laboratorios, oficinas y servidores. Para proteger estos activos, se han implementado controles de acceso integrados.

Acceso físico: Empleo de sistemas de reconocimiento facial en la entrada principal y lectores de huellas en áreas de alta seguridad, como los laboratorios y salas de servidores.

Acceso digital: Sistema de autenticación multifactor que requiere una combinación de identificador y contraseña, token OTP enviado a dispositivos móviles y verificación biométrica a través de cámaras o sensores.

Incidente:

Durante una auditoría interna rutinaria, el sistema de control de acceso físico detectó un intento de entrada fuera del horario laboral. Se registró que una persona, utilizando una imagen manipulada, trató de pasar el control de reconocimiento facial en la entrada principal. Simultáneamente, se supervisa un acceso inusual a los servidores donde se alojan

los repositorios de proyectos, con múltiples intentos fallidos de autenticación digital. La integración de alertas del sistema tanto en el aspecto físico como digital permitió bloquear de inmediato el acceso del usuario y activar protocolos de investigación para identificar la fuente del intento fraudulento.

Preguntas para el análisis:

- ¿Qué mecanismos de control de acceso (físico y digital) demostraron ser efectivos para detectar y bloquear el intento de acceso no autorizado?
- ¿Qué debilidades o puntos de mejora se pueden identificar en el proceso de verificación de identidad, considerando el uso de imágenes manipuladas?
- ¿Cómo puede la autenticación multifactor contribuir a la protección de sistemas sensibles ante intentos de acceso anómalos?
- ¿Qué protocolos de respuesta y auditoría se podrían fortalecer para mejorar la detección temprana y la gestión de incidentes similares?

capítulo tres

CIBERSEGURIDAD

3 / CIBERSEGURIDAD

En la era digital actual, la ciberseguridad se ha convertido en un componente esencial para la protección de la información y los sistemas tecnológicos. La ciberseguridad se define como una capa de protección para los archivos de información, abarcando la seguridad de las tecnologías de la información en diversos contextos, desde aplicaciones móviles hasta grandes negocios. Este capítulo tiene como objetivo proporcionar una comprensión clara de lo que implica la ciberseguridad, destacando su importancia y las diferentes áreas que abarca, como la seguridad de red, la seguridad de la información, la seguridad operativa y la continuidad del negocio.

A lo largo de este capítulo, se explorarán los procedimientos y herramientas implementados para proteger la información generada y procesada a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos. Además, se discutirán los diferentes tipos de ciberseguridad y las fases clave para mantener un entorno seguro, desde la prevención hasta la reacción ante ciberataques. Esta introducción sentará las bases para una comprensión integral de la ciberseguridad y su papel crucial en la protección de los activos digitales

3.1 / DEFINICIÓN DE CIBERSEGURIDAD

La ciberseguridad es "una capa de protección para los archivos de información". En definitiva, se trata de la seguridad de las tecnologías de la información y se aplica en contextos muy diversos, desde aplicaciones móviles hasta negocios. De esta forma, hablamos de seguridad de red, de la información, operativa y de la continuidad del negocio, entre otras. (Solano Rodriguez & Riascos Erazo, 2021)

Ciberseguridad puede definirse como:

Conjunto de procedimientos y herramientas implementados para proteger la información generada y procesada a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos.

Ilustración 10. Ciberseguridad (Generado en Copilot)

3.2 / TIPOS DE CIBERSEGURIDAD

La ciberseguridad es un campo muy amplio, ya que la información que se necesita proteger depende de controlar diferentes elementos que intervienen en su procesamiento. Por ello, se pueden citar los siguientes tipos de ciberseguridad:

- **De hardware:** Protege la integridad de los equipos físicos de un sistema informático.
- **De software:** Protege la integridad del soporte operacional de un sistema informático.
- **De redes:** Tiene como objetivo proteger la información durante los procesos de emisión y recepción entre diferentes sistemas informáticos, impidiendo que sea interceptada y descifrada por terceros.
- **Personal:** Se aplica sobre usuarios individuales en un entorno privado.
- **Física:** Se relaciona con la seguridad de hardware, pero basado en la protección analógica del sistema.
- **Lógica:** Seguridad que no se realiza de forma analógica, ya que involucra tareas de ciberseguridad activa y pasiva.

3.3 / FASES DE CIBERSEGURIDAD

Prevención

Para proteger un sistema de información es según Mata (2024) “es importante identificar las posibles amenazas, riesgos o peligros, esto involucra” realizar un análisis de riesgos que analice a detalle las situaciones de peligro a las que nos enfrentamos y cuáles serían las posibles consecuencias sobre los datos, información y activos afectados.

Localización

Al detectar un problema, la organización debe ser capaz de gestionar estos riesgos, esto involucra realizar una valoración de diferentes medidas de protección y decidir en cada caso cuál es la mejor solución, analizando siempre el posible riesgo de la decisión tomada. En este proceso, es importante identificar el origen de la amenaza y ajustar las medidas para asegurar que el riesgo no vuelva a suceder.

Reacción

La organización debe establecer un plan emergente que contenga las acciones a tomar ante una futura alarma del mismo tipo. Actualizar antivirus y contraseñas pueden ser medidas sencillas que ayudan mucho y evaluar constantemente los efectos de las medidas adoptadas.

3.3.1 / CIBERATAQUES

Un ciberataque es cualquier esfuerzo intencional para robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos a través del acceso no autorizado a una red, sistema informático o dispositivo digital. (Vega, 2020)

Los ciberataques, en su forma más general, pueden pertenecer a una de estas tres categorías:

- Ciberguerra
- Ciberterrorismo
- Cibercrimen

Ciberguerra: Estos ataques a sistemas informáticos tienen fines políticos. Su objetivo es obtener información clasificada y confidencial que, debido a su contenido sensible, podría desprestigiar a un partido político o gobierno si se utiliza de manera inapropiada. Además, esta información podría ser empleada con fines de chantaje

Ciberterrorismo: Es una forma de terrorismo que utiliza medios digitales para atacar sistemas informáticos, redes de telecomunicaciones e información privada con el objetivo de intimidar o coaccionar a gobiernos o poblaciones.

Cibercrimen: El cibercrimen se refiere a cualquier actividad delictiva que involucra el uso de computadoras, redes informáticas o dispositivos electrónicos, estos engaños son muy comunes en la red. Los hackers pueden utilizar diferentes métodos para obtener información que les permita ganar dinero, ya sea a través de una estafa o suplantación de identidad.

3.3.2 / CIBERATACANTES

Los atacantes son individuos o grupos que buscan explotar vulnerabilidades para obtener beneficios personales o financieros. Su interés abarca todo aquello que pueda generar provecho, desde tarjetas de crédito hasta diseños de productos. (Álvarez Marañón, 2020)

3.3.3 / TIPOS DE CIBERATACANTES

Aficionados: Se trata de individuos sin experiencia que emplean herramientas o guías accesibles en Internet para llevar a cabo ataques. Algunos lo hacen por simple curiosidad, mientras que otros desean mostrar sus habilidades y causar perjuicio. Aunque estos atacantes de sombrero blanco pueden utilizar herramientas sencillas, sus acciones aún pueden tener efectos devastadores.

Piratas Informáticos: Según José Roa (2013), el término “hacker” se utiliza de manera genérica para referirse a un individuo que evade las protecciones de un sistema.. Este tipo de atacantes accede a sistemas informáticos o redes para obtener acceso. Según la intención detrás de su intrusión, pueden ser clasificados como hackers de sombrero blanco, gris o negro.

Atacantes de Sombrero Blanco: Acceden a redes o sistemas informáticos con el propósito de identificar vulnerabilidades y fortalecer la seguridad de estos. Estas intrusiones se llevan a cabo con autorización previa y los resultados se comunican al propietario. Este proceso no solo ayuda a mejorar la protección contra posibles amenazas, sino que también permite a los propietarios de los sistemas comprender mejor sus puntos débiles y tomar medidas proactivas para mitigarlos. Además, estas evaluaciones de seguridad pueden incluir recomendaciones detalladas y planes de acción para abordar las vulnerabilidades encontradas, asegurando así una defensa más robusta y efectiva contra futuros ataques.

Ilustración 11. Piratas Informáticos (Generado en Copilot)

Atacantes de Sombrero Gris: Pueden buscar vulnerabilidades en un sistema, pero solo informarán de sus hallazgos a los propietarios si coincide con su agenda. Incluso podrían publicar detalles sobre la vulnerabilidad en Internet para que otros atacantes puedan aprovecharla.

Hackers de Sombrero Negro: Explotan las vulnerabilidades para obtener beneficios personales, financieros o políticos de manera ilegal.

3.3.4 / HACKERS ORGANIZADOS

Estos atacantes abarcan desde organizaciones de ciberdelincuentes y hacktivistas hasta terroristas y piratas informáticos respaldados por el estado. Generalmente, son altamente organizados, lo que les permite llevar a cabo ataques complejos y coordinados. Además,

algunos de estos grupos ofrecen servicios de ciberdelito a otros delincuentes, actuando como proveedores en un mercado negro digital. Esta oferta de servicios puede incluir desde ataques de ransomware y robo de datos hasta espionaje cibernético y sabotaje, aumentando así el alcance y el impacto potencial de sus actividades delictivas. (Joyanes Aguilar, 2023)

Los hacktivistas llevan a cabo acciones con el objetivo de hacer declaraciones políticas y sensibilizar al público sobre temas que consideran importantes. Utilizan sus habilidades para promover causas sociales o políticas, a menudo mediante la exposición de información confidencial o la interrupción de servicios en línea.

Por otro lado, los atacantes patrocinados por el estado se dedican a recopilar inteligencia o realizar actos de sabotaje en nombre de su gobierno. Estos individuos suelen estar altamente capacitados y contar con un financiamiento significativo, lo que les permite ejecutar ataques sofisticados y bien planificados. Sus objetivos suelen ser específicos y estratégicos, buscando obtener ventajas políticas, económicas o militares para su país. Estos ataques pueden incluir el espionaje cibernético, la infiltración en infraestructuras críticas y la manipulación de información para influir en eventos internacionales.

3.3.5 / MODALIDADES DE CIBERATAQUES

Hoy en día, es común escuchar sobre la creciente variedad de amenazas en Internet. A medida que más personas se conectan en línea, también aumenta el número de cibercriminales que buscan aprovecharse de quienes tienen menos conocimiento sobre seguridad. “Algunas amenazas están dirigidas a empresas, pero también existe una variedad de engaños diseñados para obtener información relevante con la cual pueden causar daño, principalmente económico, a los usuarios de Internet”. (Vega, 2020)

El cibercrimen se ha transformado en una industria lucrativa. Los criminales intentan sustraer información como datos financieros, detalles de tarjetas de crédito, información personal u otros datos que puedan vender o intercambiar. Estos delincuentes se vuelven cada vez más sofisticados y utilizan una variedad de métodos para atacar las redes informáticas de las empresas.

Cualquier intento deliberado de acceder sin autorización a sistemas informáticos, redes o dispositivos digitales con el objetivo de robar, exponer, alterar, deshabilitar o destruir datos y aplicaciones.

3.4 / MALWARE

3.4.1 / DEFINICIÓN

La palabra “malware” proviene del inglés y es la combinación de las palabras “malicious software” o “software malicioso”. Se refiere a cualquier código que puede ser utilizado para robar datos, eludir controles de acceso, causar daño o comprometer un sistema. A diferencia del software legítimo, que está diseñado para realizar tareas útiles o productivas, el malware tiene intenciones dañinas. (Guerra Soto, 2018)

Es cualquier tipo de software malicioso diseñado para dañar, explotar o deshabilitar dispositivos, servicios o redes programable

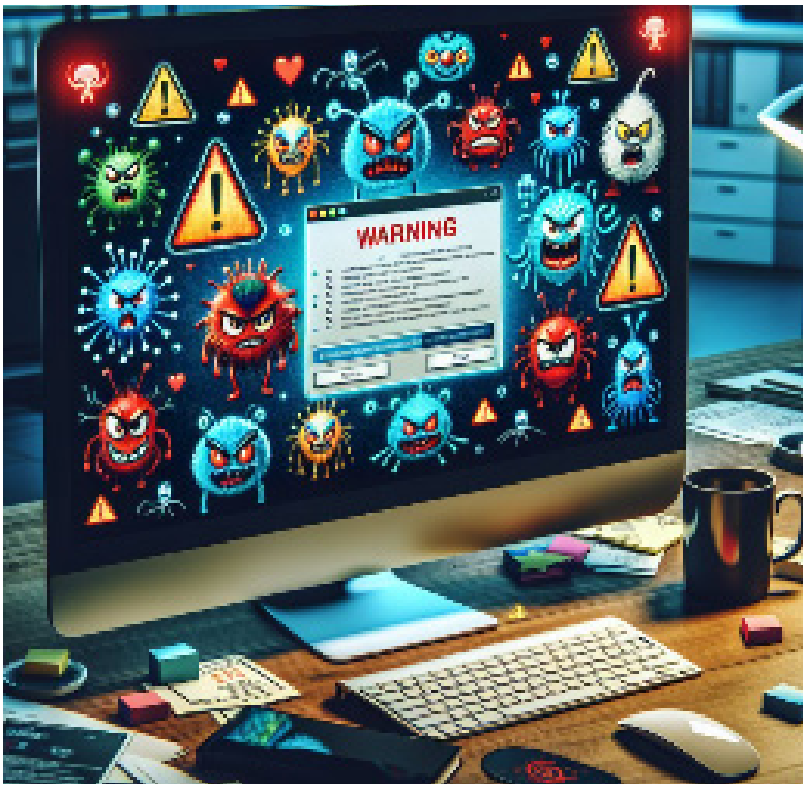


Ilustración 12. Malware (Generado en Copilot)

3.4.2 / TIPOS DE MALWARE

Malware, una abreviatura de “malicious software” o “software malicioso”. se refiere a cualquier programa o código diseñado con intenciones dañinas para perjudicar, explotar o infiltrarse en dispositivos, sistemas informáticos, redes y otros recursos digitales sin el conocimiento o consentimiento del usuario.

El malware puede tener diversos objetivos, como robar información personal, interrumpir el funcionamiento normal de un sistema, espiar la actividad del usuario o incluso extorsionar a las víctimas. Entre los tipos más comunes de malware se encuentran los virus, ransomware, spyware, gusanos y adware

Tabla 4, Tipos de malware

MALWARE	DESCRIPCIÓN
Virus	Los virus informáticos son códigos de software diseñados para propagarse de un equipo a otro. Estos programas pueden copiarse a sí mismos e infectar un ordenador sin el permiso o conocimiento del usuario. Un virus puede dañar o eliminar datos guardados. Frecuentemente, utilizan programas de correo electrónico para propagarse a través de la red hacia otros ordenadores, e incluso pueden borrar todo el contenido del disco duro. “Programa con código malicioso que infecta la computadora con el objetivo de alterar su normal funcionamiento”. (Cicariello, 2022)

Caballos de Troya- Virus Troyano	Metafóricamente, un “caballo de Troya” describe la táctica de engañar a alguien para que permita la entrada de un atacante en una zona segura. En el ámbito de la informática, un caballo de Troya, o “Troyano”, es un software malicioso que se disfraza de programa legítimo para engañar a los usuarios y hacer que lo ejecuten voluntariamente. La forma más común de propagación es por medio de correo electrónico; pueden aparecer como un mensaje de alguien conocido. Al hacer clic en el correo electrónico y el archivo adjunto, se descarga malware en la computadora. Los troyanos también se propagan al hacer clic en anuncios falsos.
Adware	El adware es un software creado para rastrear datos sobre los hábitos de navegación de los usuarios, con esa información, activa anuncios y ventanas emergentes de forma automática. Los usuarios suelen dar consentimiento a recibir este tipo de información al instalar aplicaciones al aceptar los acuerdos de usuarios sin leer cuidadosamente su contenido, por ello no son formas ilegítimas de ingresos para las empresas que permiten a los usuarios probar su software de forma gratuita, mostrando anuncios mientras se usa el software.
Spyware	A diferencia de un adware , este malware se instala en la computadora sin la autorización del usuario. Suelen ser peligrosos porque pueden capturar información personal, incluidas direcciones de correo electrónico, contraseñas e incluso números de tarjetas de crédito, lo que lo hace peligroso debido al alto riesgo de robo de identidad.
Ransomware	Cuando alguien es víctima de un ataque de ransomware, toda la información de su computadora o dispositivo queda “atrapada” o cifrada. La víctima debe pagar una suma de dinero al hacker para recuperar sus datos.
Spam	Popularmente conocido como correo basura, el spam es el envío masivo de correos electrónicos no solicitados. Aunque no es peligroso en sí mismo, además de quitarte mucho tiempo, es posible que contenga código malicioso escondido entre tanta basura.
Botnets	Una botnet es una red de computadoras que trabajan en conjunto para fines de dudosa moralidad. Cuanto más grande es la red, más peligrosa se vuelve, pudiendo inundar a miles de personas con spam o derribar un sitio web mediante un ataque DDoS.
Denegación de servicio (Denial-of-service)	Este tipo de ataque, también conocido como DoS, impide o dificulta el uso autorizado de redes, sistemas y aplicaciones debido al agotamiento de los recursos. Por lo general, estos ataques están dirigidos a los servidores de una compañía con el fin de imposibilitar el acceso de los usuarios.
Bomba lógica (Logic bomb)	Este tipo de ataque se lleva a cabo insertando intencionalmente un fragmento de código dañino dentro del código fuente de un software. El objetivo es ejecutar una función maliciosa cuando se cumplan ciertas condiciones determinadas.
Worm (gusano)	Es un programa malicioso que utiliza mecanismos de red para propagarse. A diferencia de los virus informáticos, los gusanos no requieren intervención humana para expandirse.

3.4.3 / FORMAS DE PROPAGACIÓN DE UN MALWARE

Los programas maliciosos o malware llegan a un ordenador principalmente por las siguientes razones:

- Explotando una vulnerabilidad
- A través de un archivo malicioso
- Al utilizar dispositivos extraíbles

3.4.4 / FORMAS DE PROTEGERSE DE UN MALWARE

Proteger los dispositivos y la información contra los efectos negativos del malware requiere que los usuarios apliquen buenas prácticas de seguridad. Esto implica ser responsables al utilizar dispositivos, compartir información y descargar archivos de Internet. A continuación, se presentan algunas prácticas recomendadas:

- Mantener actualizado el sistema operativo con todos los parches más recientes y activar las actualizaciones automáticas si es posible.
- Instalar periódicamente todas las actualizaciones del navegador.
- Ser muy cuidadoso al hacer clic en un enlace o descargar un archivo.
- Desconfiar de cualquier elemento de un correo electrónico que parezca sospechoso.
- No abrir archivos si se desconoce su extensión o si se reciben advertencias o mensajes del navegador web que no resulten familiares.
- Tener en cuenta que algunos programas incluyen malware u otro software engañoso como parte de su proceso de instalación.
- Tener mucha precaución con las unidades USB.

3.5 / INGENIERIA SOCIAL

3.5.1 / DEFINICIÓN DE INGENIERÍA SOCIAL

La ingeniería social es un conjunto de técnicas psicológicas y habilidades sociales, como la influencia, la persuasión y la sugestión. Su objetivo es que un usuario revele información sensible, sin ser consciente de los riesgos que esto implica. Se trata de la manipulación de personas, influenciándolas para que ejecuten determinadas acciones, lo que las convierte en víctimas de delitos informáticos. A diferencia de los ataques técnicos que explotan vulnerabilidades en software o hardware, la ingeniería social se basa en explotar la confianza, el comportamiento humano y las interacciones sociales. (Arboledas Brihuega, 2013)

La Ingeniería Social consiste en persuadir a una persona para influir en sus acciones.

3.5.2 / LA INGENIERÍA SOCIAL APROVECHA CIERTAS CARACTERÍSTICAS DE LA NATURALEZA HUMANA COMO:

- Todos queremos ayudar.
- El primer movimiento hacia el otro siempre es de confianza.
- Evitamos decir “NO”
- A todos nos gusta que nos alaben.

Convencer a una persona para que realice una tarea es generalmente más sencillo que intentar hackear un sistema utilizando códigos y algoritmos. Esto se debe a que no es necesario eludir sistemas de detección de intrusos o firewalls. La ingeniería social, que se basa en manipular a las personas para obtener información o acceso, puede ser una herramienta poderosa y efectiva. Además, las herramientas para utilizar son gratuitas o de muy bajo costo, y finalmente, porque las personas son la mayor vulnerabilidad en cualquier empresa.

Ilustración 13. Ingeniería social (Generado en Copilot)

3.5.3 / CATEGORÍAS DE ATAQUES DE INGENIERÍA SOCIAL

Ataques Técnicos: Combina técnicas de manipulación psicológica con métodos técnicos para engañar a las víctimas y obtener acceso no autorizado o información confidencial. Estos ataques no se basan únicamente en la explotación de vulnerabilidades humanas, sino que integran aspectos técnicos para hacer el ataque más eficaz y cómodo (Gutiérrez Salazar, 2019). Algunas de sus características son:

- No hay interacción directa con las víctimas.
- El atacante emplea correos electrónicos, sitios web y boletines.
- El atacante se hace pasar por una entidad conocida y confiable.
- Su objetivo es obtener información sensible de los usuarios.
- Tiene un alto índice de éxito.

Ataques al Ego: En el ámbito de la ingeniería social, esta técnica se aprovecha de la vanidad, el orgullo o el deseo de reconocimiento de una persona para manipularla y obtener información confidencial o acceso no autorizado. Se fundamenta en la necesidad de la víctima de sentirse importante, admirada o superior, utilizando ese deseo para influir en sus acciones. El atacante apela a la vanidad y el ego de la víctima.

- La víctima intenta demostrar su inteligencia y eficacia.

- Se busca que la víctima sienta que está contribuyendo en un asunto significativo (y que posiblemente recibirá reconocimiento por ello).
- Generalmente, la víctima no se percata del ataque.

Este tipo de ataque es particularmente efectivo porque explota las emociones y la psicología humana, haciendo que las personas bajen la guardia y actúen de manera que normalmente no lo harían. Al sentirse valoradas y reconocidas, las víctimas pueden ser más propensas a compartir información sensible o realizar acciones que comprometan la seguridad, sin darse cuenta de que están siendo manipuladas.

Ataques de Simpatía: Este tipo de ataque se basa en el principio de que las personas son más propensas a cooperar con alguien que perciben como necesitado o en una situación difícil. Explota la empatía, la compasión o el deseo de ayudar a una persona para manipularla y obtener información confidencial o acceso no autorizado.

- Se crea una situación en la que es imperativo finalizar una tarea o actividad de manera urgente.
- Se apela a la empatía de la persona.
- El atacante solicita ayuda repetidamente hasta encontrar a alguien que le brinde la información o el acceso necesario.
- El atacante se muestra bastante desesperado, indicando que su trabajo está en juego si no completa su tarea.

Ataques de Intimidación: El atacante busca provocar una respuesta emocional de miedo o ansiedad en la víctima para que actúe de manera que normalmente no lo haría. Utiliza tácticas de miedo, amenaza o coerción para manipular a una persona y obtener acceso a información confidencial o realizar acciones que comprometan la seguridad.

- El atacante se hace pasar por una figura de autoridad dentro de la organización.
- Intenta usar su posición para obligar a la víctima a colaborar.
- Si encuentra resistencia, recurre a la intimidación y amenazas, como la pérdida de empleo, multas o acciones legales.

3.5.4 / TÉCNICAS DE INGENIERÍA SOCIAL

Tabla 5, Tabla 6, Técnicas de Ingeniería Social

TÉCNICA	DESCRIPCIÓN
Vishing	Ataque de phishing realizado por teléfono o a través de un sistema de comunicación por voz. El cibercriminal se pone en contacto con la víctima a través de una llamada.
Pretextos	Los ciberdelincuentes elaboran situaciones para persuadir a sus víctimas de que revelen información privada o accedan a sus recursos en la red. Generalmente, el atacante crea una historia o pretexto convincente, haciéndose pasar por una figura de autoridad legítima para engañar a la víctima..
Phishing	El ciberdelincuente utiliza un cebo fraudulento y espera a que algún usuario caiga en la trampa, para así obtener credenciales u otro tipo de información sensible.
Scareware	Es un ataque cibernético que busca asustar y engañar a las personas, haciéndoles creer que su computadora o dispositivo está infectado con malware. El estafador convence al usuario de que compre un software de seguridad falso, que en realidad es malware. Este tipo de ataque utiliza ventanas emergentes y varias tácticas de ingeniería social para lograr su objetivo
Baiting	Es una técnica parecida al phishing, pero se basa en falsas promesas o recompensas para despertar la curiosidad y mantener el interés de la víctima, aprovechándose de su codicia
Shoulder Surfing	Es una técnica en la que el atacante observa por encima del hombro de la víctima mientras esta introduce información confidencial, como contraseñas o números de tarjetas de crédito, para obtener estos datos sin su conocimiento.
SPAM	Cualquier correo electrónico o mensaje recibido que no es deseado y/o solicitado. Su envío se produce de forma masiva a un gran número de direcciones. No siempre es malicioso, aunque constituye una pérdida de tiempo y un gasto de recursos innecesario.

3.5.5 / PRECAUCIONES PARA EVITAR SER VÍCTIMAS DE INGENIERÍA SOCIAL

Para evitar ser víctima de un ataque de ingeniería social, toma en cuenta las siguientes sugerencias:

- No revelar información personal ni datos confidenciales (credenciales, números de tarjetas de crédito, cuentas bancarias, etc.) por teléfono, email o servicios de mensajería instantánea.
- Tener cuidado al compartir información y evitar exponerse en internet y en redes sociales publicando información personal (número de teléfono, dirección, hábitos, etc.). Estos datos facilitan el trabajo a los ciberdelincuentes.
- Verificar los archivos adjuntos y no descargarlos si se desconoce su contenido, aunque provengan de un contacto conocido.
- Instalar y mantener siempre actualizado un antivirus en todos los dispositivos.
- Sentido común y precaución son los mejores aliados en la defensa contra la ingeniería social.

3.6 / CASOS DE ESTUDIO CONTROL DE ACCESO CIBERSEGURIDAD

Caso de Estudio 1: Ataque Ransomware en EcoTours Ecuador SA

Contexto:

EcoTours Ecuador SA es una empresa dedicada a la promoción y gestión de paquetes de ecoturismo y viajes de aventura. Su plataforma digital integra sistemas de reservas, gestión de itinerarios y almacenamiento en la nube de información sensible de clientes (datos personales, historiales de reservas y detalles financieros). La compañía, en su afán de modernizar sus procesos, implementó controles de ciberseguridad básicos en sus redes y sistemas; sin embargo, la actualización y el monitoreo constante de dichos mecanismos no se han reforzado en el tiempo, lo que dejaba expuestas algunas vulnerabilidades en su infraestructura.

Incidente:

Una mañana, el departamento de TI de EcoTours Ecuador SA detectó múltiples alertas inusuales en la red. En cuestión de minutos, varios servidores críticos dejaron de responder y apareció en pantalla un mensaje exigiendo el pago de un rescate en criptomonedas, informando que la totalidad de los datos había sido cifrada. Se procedimientos que el ataque se había iniciado a través de una vulnerabilidad en un software de gestión de reservas, que permitió la instalación de un ransomware. La propagación del malware comprometió no solo el acceso a la información de clientes y reservas, sino también la continuidad operativa de la empresa, afectando la capacidad de procesar nuevas solicitudes y de mantener la comunicación con sus clientes.

Preguntas para el análisis:

- ¿Cuáles fueron los fallos en los controles de ciberseguridad (tanto en la prevención como en la localización) que permitieron que el ransomware se infiltrara en la red de EcoTours Ecuador SA?
- ¿De qué manera afecta un ataque de ransomware la continuidad operativa de una empresa que depende de sistemas digitales para gestionar información crítica?
- ¿Qué protocolos de reacción ante incidentes se deben implementar para minimizar el impacto y facilitar una recuperación rápida de la información?
- ¿Qué importancia tienen las actualizaciones periódicas del software y la capacitación constante en ciberseguridad para prevenir este tipo de ataques?

Caso de Estudio 2: Ingeniería Social y Propagación de Malware en AgroDigital Ecuador SA

Contexto:

AgroDigital Ecuador SA es una empresa que integra tecnología en la cadena de suministro agrícola, facilitando la coordinación entre productores, distribuidores y puntos de venta a través de un sistema digital de gestión de inventarios, logística y transacciones financieras. La organización maneja datos sensibles relacionados con clientes, empleados y operaciones comerciales. Aunque cuenta con sistemas de protección para redes y hardware, el factor humano representa un eslabón crítico en su estrategia de ciberseguridad.

Incidente:

Durante un día laboral rutinario, un empleado del área administrativa recibió un correo electrónico que parecía provenir de un proveedor habitual. El mensaje solicitaba, de manera urgente, actualizar las credenciales de acceso mediante un enlace incluido en el correo. Confiando en la veracidad del mensaje, el empleado hizo clic y procedió a ingresar sus datos en un formulario en línea. Poco después, se descubrió que se trataba de un ataque de phishing basado en técnicas de ingeniería social. Los datos comprometidos permitieron a los atacantes instalar un troyano en la red interna, el cual se propagó silenciosamente a través de otros sistemas, accediendo a información confidencial y alterando ciertos procesos operativos. La fuga de datos y la interrupción temporal de la operación obligaron a la empresa a activar su protocolo de respuesta a incidentes, afectando tanto la reputación como la operatividad del negocio.

Preguntas para el análisis:

- ¿Qué elementos del ataque (por ejemplo, el diseño del correo y la urgencia del mensaje) fueron determinantes para que el empleado cayera en la trampa?
- ¿Qué medidas de ciberseguridad y formación en concienciación para empleados se podrían implementar en AgroDigital Ecuador SA para prevenir ataques de phishing y reducir el riesgo de ingeniería social?
- ¿Cómo debería optimizarse el proceso de localización y reacción ante incidentes para identificar y aislar rápidamente la propagación del malware una vez que se ha producido una brecha?
- ¿Qué consecuencias puede tener la pérdida o alteraciones de datos sensibles en la operación y reputación de una empresa que depende fuertemente de sus sistemas digitales para la gestión de su suministro?

capítulo cuatro

GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

En el ámbito de la seguridad de la información, es crucial comprender los conceptos fundamentales relacionados con la gestión de riesgos. Un riesgo se define como la posibilidad de que ocurra un evento no deseado que tenga consecuencias negativas para la seguridad de los recursos de información. En el contexto informático, un riesgo puede representar una dificultad en el cumplimiento de una meta o una amenaza a la pérdida de documentos, y puede clasificarse en términos de ganancia o pérdida.

Este capítulo se dedica a explicar términos esenciales que son clave para la gestión de riesgos. Entre estos términos se encuentran la probabilidad de materialización de un riesgo, las amenazas que pueden afectar a una organización, las vulnerabilidades que pueden ser explotadas, y los activos que necesitan protección. Además, se analizará el impacto que un incidente de seguridad puede tener sobre estos activos y las salvaguardas que se pueden implementar para mitigar dichos riesgos.

Comprender estos conceptos es fundamental para poder identificar, evaluar y gestionar los riesgos de manera efectiva, permitiendo a las organizaciones proteger sus recursos de información y tomar decisiones informadas sobre cómo abordar los riesgos potenciales.

4.1 / DEFINICIONES IMPORTANTES

Un riesgo es esencialmente la posibilidad de ocurrencia de un evento no deseado, de consecuencias negativas, en nuestro contexto, sobre la seguridad de los recursos de información, riesgo informático se define como una dificultad que interviene en el cumplimiento de una meta o así mismo una amenaza a la pérdida de documentos. Este riesgo puede estar clasificado en ganancia o pérdida. Algunos términos relacionados a la gestión de riesgos son:

4.1.1 / PROBABILIDAD:

Posibilidad de materialización de un riesgo, se refiere a la posibilidad o frecuencia con la que una amenaza puede explotar una vulnerabilidad en un sistema, red o aplicación, causando un impacto negativo en la confidencialidad, integridad o disponibilidad de la información. Es un factor clave en la evaluación del riesgo, ya que ayuda a estimar la frecuencia esperada de ocurrencia de un incidente de seguridad basado en la existencia de vulnerabilidades y amenazas (Pfleeger, Sahri, & Margulies, 2020).

4.1.2 / AMENAZAS:

Son acciones que se presentan en una empresa ocasionando resultados negativos y

pueden ser de carácter físico o lógico. Una amenaza es una acción que podría resultar en la violación, interrupción o corrupción de un sistema mediante la explotación de vulnerabilidades conocidas o desconocidas (Samaniego Mena & Ponce Ordoñez, 2021)

4.1.3 / VULNERABILIDADES:

Son debilidades o defectos en un sistema, software, red o proceso que puede ser explotado por atacantes para comprometer la integridad, confidencialidad o disponibilidad de los datos o los recursos del sistema. Estas debilidades pueden ser causadas por errores de programación, configuraciones incorrectas, políticas de seguridad inadecuadas o fallos en los mecanismos de protección (Stallings, 2017) .

4.1.4 / ACTIVOS:

Componente, elemento o funcionalidad de un sistema de información que puede de ser atacado accidentalmente deliberada o con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos (Caballero & Cilleros, 2019)

4.1.5 / IMPACTO:

Consecuencias o efectos negativos que un incidente de seguridad tiene sobre los activos de información cuando una amenaza explota una vulnerabilidad. Este impacto puede manifestarse en términos de pérdida de confidencialidad, integridad o disponibilidad de los datos, y su severidad puede variar dependiendo del tipo de información afectada y el alcance del incidente.

Una organización se ve afectada cuando se produce una situación que atenta contra su funcionamiento normal, alcance producido o daño causado en caso de que una amenaza se materialice (Samaniego Mena & Ponce Ordoñez, 2021)

4.1.6 / SALVAGUARDAS:

También conocidas como controles de seguridad son medidas, mecanismos, o estrategias implementadas para proteger los activos de información contra amenazas, vulnerabilidades o incidentes que puedan comprometer la confidencialidad, integridad o disponibilidad de los datos. Estas salvaguardas pueden ser de carácter técnico, administrativo o físico y se diseñan para reducir el riesgo y mitigar el impacto de posibles ataques o fallos de seguridad.

4.2 / GESTIÓN DE RIESGOS

La gestión de riesgos es un proceso que permite identificar, analizar, evaluar y categorizar los

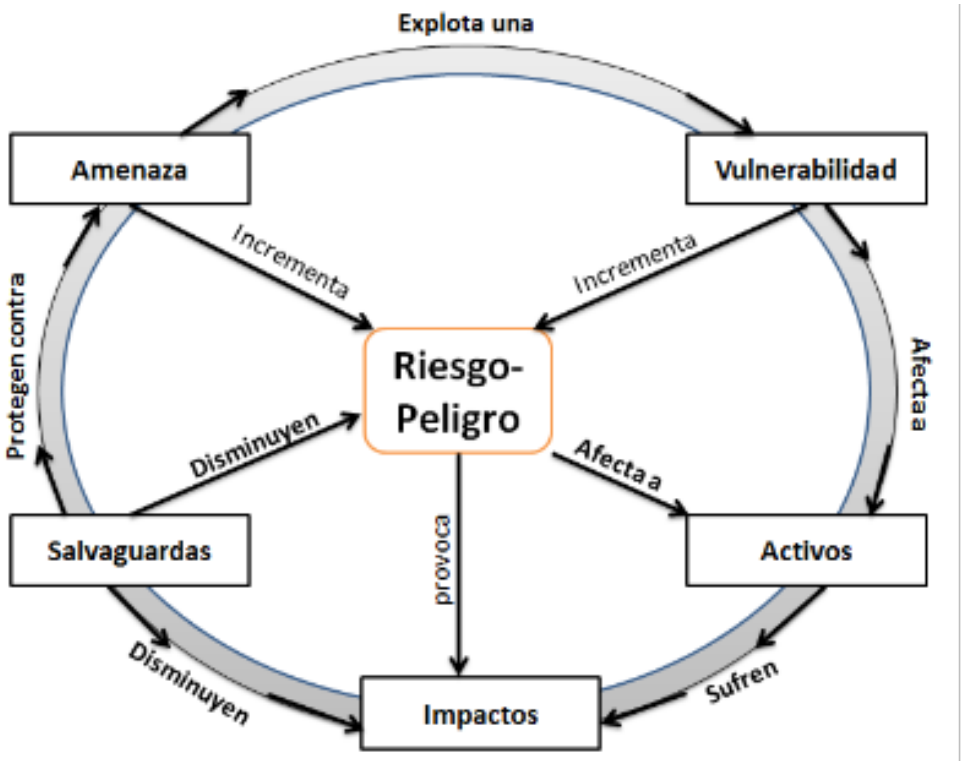


Ilustración 14. Ciclo de la Gestión de riesgos.

riesgos, para luego implementar mecanismos que faciliten su control.. Proceso mediante el cual se identifican, evalúan y gestionan los riesgos relacionados con la seguridad de la información dentro de una para tomar las decisiones sobre su asunción, mitigación o transferencia (Valencia Duque, Marulamnda Echeverry, & López Trujillo, 2024).

La gestión de riesgos permite a las organizaciones tomar decisiones informadas sobre la asunción, mitigación o transferencia de riesgos. La asunción de riesgos implica aceptar el riesgo y sus posibles consecuencias, la mitigación de riesgos se refiere a la implementación de medidas para reducir la probabilidad o el impacto del riesgo, y la transferencia de riesgos consiste en trasladar el riesgo a un tercero, como en el caso de contratar un seguro.

Ilustración 15. Gestión de riesgos (Generado en Copilot)

4.2.1 / FASES DE LA GESTIÓN DE RIESGOS

Las fases comunes para gestionar riesgos son:

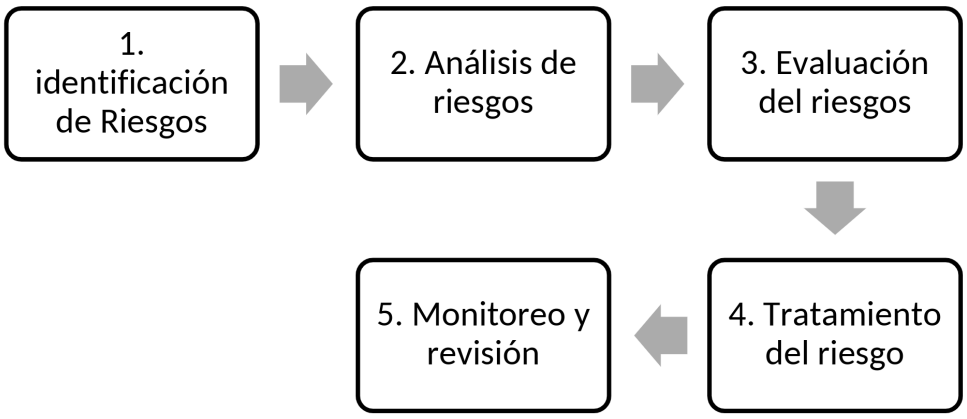


Ilustración 16. Ciclo de la Gestión de riesgos.

4.2.2 / IDENTIFICACIÓN DE RIESGOS:

Consiste en determinar los posibles riesgos a los cuales están expuestos los activos de información, se trata de descubrir y listar todas las posibles amenazas, vulnerabilidades y riesgos que pueden comprometer los sistemas de información, se debe considerar que para activo son diferentes los riesgos que pueden afectar por ejemplo un computador puede ser afectado por un agentes físicos como humedad, temperatura, robos, incendios mientras que los datos pueden ser dañados por malware.

4.2.3 / ANÁLISIS:

Consiste en Identificar los elementos de un sistema que necesitan protección, sus vulnerabilidades que lo hacen más débil y las amenazas que lo ponen en riesgo, con el objetivo de determinar su nivel de riesgo. Puede incluir actividades como:

- Identificar activos
- Valorar Activos
- Identificar Riesgos
- Valorar Riesgos

4.2.4 / EVALUACIÓN DE RIESGOS:

Consiste en analizar los riesgos identificados, evaluando su probabilidad de ocurrencia y el impacto que tendrían si se concretan. Es importante considerar que no todos los riesgos

tienen el mismo nivel de gravedad, dependiendo de la organización se debe realizar un análisis de cada uno y dependiendo de los efectos negativos que ocasionen pueden ser:

4.2.4.1 / RIESGOS CATASTRÓFICOS

Estos riesgos tienen el potencial de causar daños extremadamente severos a la organización, incluyendo la pérdida total de datos críticos, interrupciones prolongadas de los servicios y daños irreparables a la infraestructura. Ejemplos incluyen:

- **Ataques de ransomware** que cifran todos los datos de la empresa y exigen un rescate.
- **Desastres naturales** que destruyen centros de datos sin posibilidad de recuperación.
- **Brechas de seguridad masivas** que resultan en la exposición de información sensible de millones de usuarios

4.2.8.2 / RIESGOS GRAVES

Estos riesgos pueden causar daños significativos, pero generalmente son manejables con una respuesta adecuada. Pueden incluir:

- **Intrusiones de malware** que comprometen sistemas importantes pero no críticos.
- **Fallas en la infraestructura** que causan interrupciones temporales en los servicios.
- **Errores humanos** que resultan en la pérdida de datos importantes pero recuperables

4.2.4.3 / RIESGOS LEVES

Estos riesgos tienen un impacto menor y son más fáciles de mitigar. Suelen incluir:

- **Pequeñas vulnerabilidades** en el software que pueden ser parcheadas rápidamente.
- **Errores de configuración** que no afectan significativamente las operaciones.
- **Incidentes de phishing** que son detectados y neutralizados antes de causar daño

4.2.5 / TRATAMIENTO DE RIESGOS:

Una vez seleccionada la estrategia de tratamiento de riesgos, se deben definir e implementar las medidas de protección adecuadas. Esto incluye:

- **Desarrollo de Políticas y Procedimientos:** Crear políticas claras y procedimientos detallados para guiar la implementación de medidas de seguridad.
- **Tecnologías de Seguridad:** Implementar tecnologías como antivirus, sistemas de detección de intrusos, y cifrado de datos.
- **Monitoreo y Auditoría:** Establecer sistemas de monitoreo continuo y auditorías regulares

para asegurar que las medidas de protección sean efectivas.

- **Sensibilización y Capacitación de Usuarios:** Es fundamental sensibilizar y capacitar a los usuarios sobre las medidas de seguridad implementadas. Esto puede incluir:
- **Programas de Capacitación:** Realizar talleres y cursos sobre buenas prácticas de seguridad informática.
- **Campañas de Concienciación:** Utilizar campañas de comunicación para informar a los empleados sobre las políticas de seguridad y su importancia.
- **Simulacros y Ejercicios:** Realizar simulacros de incidentes de seguridad para preparar a los empleados y evaluar la efectividad de las medidas de respuesta.

Estas acciones no solo ayudan a proteger la información y los sistemas, sino que también fomentan una cultura de seguridad dentro de la organización.

4.2.6 / MONITOREO Y REVISIÓN:

El monitoreo y la revisión son componentes esenciales en la gestión de riesgos, ya que aseguran que las medidas de seguridad implementadas sigan siendo efectivas y adecuadas a lo largo del tiempo. Este proceso implica varias actividades clave:

- Monitoreo Continuo
- Auditorías y Revisiones Periódicas
- Revisión y Ajuste
- Actualización de Estrategias
- Comunicación y Reportes

El monitoreo es importante porque permite a la organización adaptarse rápidamente a nuevos riesgos y cambios en el entorno.

- **Mejora Continua:** Fomenta una cultura de mejora continua en la gestión de riesgos.
- **Prevención de Incidentes:** Ayuda a identificar y mitigar riesgos antes de que se conviertan en incidentes graves.
- **Cumplimiento Normativo:** Asegura que la organización cumpla con las normativas y estándares de seguridad aplicables.

El monitoreo y la revisión son procesos dinámicos y continuos que requieren atención constante y recursos dedicados. Implementar un sistema eficaz de monitoreo y revisión no solo protege a la organización contra riesgos potenciales, sino que también la posiciona para un crecimiento sostenible y exitoso en un entorno empresarial en constante cambio.

4.3 / METODOLOGÍAS PARA ANALIZAR RIESGOS

Gestionar riesgos es fundamental en el proceso de gestión de seguridad de la información de una organización, ya que permite identificar, evaluar y reducir los peligros identificados hasta un nivel aceptable y enmarcarlos en un modelo de mejora continua. Las metodologías de evaluación de riesgos permiten identificación de vulnerabilidades, amenazas y el impacto de las mismas sobre la confidencialidad, integridad y disponibilidad de los activos de la organización.

Las actividades comunes de las metodologías para analizar riesgos son:

- Identificación de activos de información críticos.
- Identificación de vulnerabilidades.
- Identificación de amenazas.
- Identificación de impacto y probabilidad de ocurrencia.
- Cálculo de riesgos identificados.
- Definición de opciones de tratamiento de riesgos.

4.3.1 / IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN CRÍTICOS

Un activo es cualquier recurso de la empresa necesario para desempeñar las actividades diarias y cuya no disponibilidad o deterioro supone un agravio o coste. Dependiendo de la organización, su tamaño, estructura y tipo de servicio que brinda los activos de información pueden ser diferentes, así como la importancia que tenga cada uno y los efectos negativos que podrían provocar en el funcionamiento de la empresa en caso de sufrir algún daño.

4.3.1.1 / CATEGORÍAS DE ACTIVOS DE INFORMACIÓN

Se pude tomar como referencia la siguiente categorización de activos

Tabla 7 Categorías de Activos

CATEGORÍA DE ACTIVOS DE INFORMACIÓN	EJEMPLO DE ACTIVOS
Activos esenciales	Información que se maneja Servicios prestados
Equipamiento Informático	Aplicaciones (software) Equipos informáticos (hardware) Comunicaciones Dispositivos de información como discos, Memorias, cintas, etc.

Entorno-Infraestructura	Equipos y suministros: mobiliario energía, climatización, etc.
Personal	Usuarios Operadores y administradores Desarrolladores

En la organización existen Activos relevantes que podrían ser:

- Datos que materializan la información.
- Toda aplicación informática, herramienta de software que se utilice para manejar datos.
- Todo equipo informático que se utilice para almacenar datos y aplicaciones
- Dispositivos y o unidades de almacenamiento de datos.
- Otros equipos auxiliares que complementan un sistema informático.
- Redes y equipos de comunicaciones que se utilizan para intercambiar datos.
- Instalaciones e infraestructura donde se ubican equipos informáticos y de comunicaciones.
- Personal que operan todos los elementos informáticos

4.3.2 / VALORACIÓN DE ACTIVOS

La valoración corresponde a un análisis de la necesidad de proteger un bien, considerando que mientras más valioso es, más protección necesita; se puede hacer dicho análisis considerando los principios de seguridad

Tabla 8 Valoración de activos

PRINCIPIO	ANÁLISIS
Confidencialidad	¿Qué efecto negativo causaría si tuviera acceso quien no debe? Esta valoración es exclusiva de datos
Integridad	¿Qué daño causaría si fuera dañado o alterado? Esta valoración está relacionada con los datos, que pueden estar manipulados, alterados, de forma total o parcialmente
Disponibilidad	¿Qué daño ocasionaría el no poder utilizarlo en el momento requerido? Esta valoración está relacionada con equipos y servicios

La valoración de un activo corresponde a establecer el costo que involucraría recuperarse de un evento que dañe, afecte o inutilice el activo. Se pueden tomar en consideración algunas situaciones como las siguientes:

- Costo de reposición, adquisición e instalación
- Costo de mano de obra necesaria para recuperar el activo
- Pérdida de ingresos ocasionada por paralización de servicios que deriva en pérdida de confianza y de clientes
- Posibles sanciones por incumplimiento contratos, o infracciones legales
- Daño a terceros
- Daños medioambientales

4.3.2.1 / VALORACIÓN CUALITATIVA VS VALORACIÓN CUALITATIVA

Valoración Cualitativa

Las escalas cualitativas permiten calificar a cada activo en un orden relativo con relación a los demás, puede considerarse como ordenes de magnitud de riesgos. La dificultad radica en que no se permiten comparaciones de valores más allá de lo relativo, impidiendo realizar cálculos matemáticos limitando el análisis. Las escalas se definen a criterio del evaluador: Muy valioso, Valioso, Poco Valioso

Valoración Cuantitativa

Corresponden a asignaciones numéricas en función del análisis del evaluador; al trabajar con números permite realizar operaciones matemáticas. La interpretación numérica permite un análisis que no admite discusión ni controversia

Tabla 9 Valoración de activos Cualitativa-Cuantitativa

VALORACIÓN DE ACTIVOS

VALORACIÓN CUALITATIVA	VALORACIÓN CUANTITATIVA	IMPORTANCIA DEL ACTIVO
Muy Valioso	4-5	Cualquier daño en el activo paraliza las actividades de la empresa, pone en riego la continuidad de operaciones de forma prolongada

Valioso	2-3	Cualquier daño en el activo paraliza las actividades de la empresa de forma temporal
Poco valioso	1-2	Cualquier daño en el activo no representa mayor problema para el normal funcionamiento de la organización

4.3.3 / DEFINIR AMENAZAS

Considerando cada activo es necesario identificar a qué peligros es susceptible cada uno, así por ejemplo un servidor podría sufrir un robo, daño, robo de información, hackeo.

4.3.3.1 / CATEGORÍAS DE AMENAZAS

De origen natural: Todos aquellos considerados como accidentes o desastres (terremotos, inundaciones, deslaves, maremotos, etc.). Incidentes ante los cuales un sistema de información es víctima pasiva, sin embargo puede sufrir sus efectos negativos.

Del entorno de origen industrial: Los desastres industriales como contaminación, fallos eléctricos, también pueden afectar al sistema de información por lo tanto es necesario considerar protegerse ante posibles eventos de este tipo.

Defectos de las aplicaciones: Algunos problemas están directamente relacionados con errores en el mismo diseño de los sistemas, en otros casos errores al momento de implementar o problemas de incompatibilidad con los equipos en los que se ejecutan, en consecuencia derivan en las denominadas vulnerabilidades técnicas.

Provocadas por personas de forma accidental: El personal que tiene acceso a un sistema, en ciertas ocasiones por desconocimiento, falta de entrenamiento o error involuntario puede realizar acciones indebidas que comprometan al sistema.

Provocadas por personas de forma deliberada: En ciertos casos, el personal que tiene acceso al sistema, puede ejecutar acciones en el sistema con la intención de causar un daño, puede ser con intención de obtener algún beneficio o simplemente con el propósito de afectar al sistema.

4.3.4 / VALORACIÓN DE AMENAZAS

Una vez que se ha identificado que una amenaza puede perjudicar a un activo, hay que valorar y analizar su afectación en el valor del activo, para ello se debe considerar dos elementos que influyen, la probabilidad de ocurrencia del riesgo y el impacto que puede tener sobre el activo y/o funcionamiento de la empresa. Para obtener el valor de la amenaza de forma cuantitativa se utiliza la fórmula:

VALOR DEL RIESGO=PROBABILIDAD*IMPACTO

La **PROBABILIDAD** de que ocurra un riesgo se calcula evaluando los controles implementados para prevenirlo. Es decir, a mayor número de controles que protegen el activo, menor es la probabilidad de que el riesgo se materialice. Este valor se obtiene mediante la aplicación de un checklist, en el cual se verifican los controles y medidas implementadas para evitar el riesgo. Por lo tanto, a mayor número de controles aplicados, menor será la probabilidad de ocurrencia del riesgo.

Tabla 10 Escala para cálculo de probabilidad de ocurrencia de una amenaza

PORCENTAJE DE CONTROLES APLICADOS	VALOR DE PROBABILIDAD (CUANTITATIVO)	VALOR DE PROBABILIDAD (CUALITATIVO)
76%-100%	1	Muy Baja-Muy raro
41%-75%	2	Baja – poco probable
21%-40%	3	Media-posible
11%-20%	4	Alta- muy alto
0%-10%	5	Muy alta- casi seguro

El impacto se refiere a la magnitud del daño que un activo experimenta cuando una amenaza se materializa. Esto se determina conociendo el valor de los activos en diversas dimensiones y la degradación que las amenazas provocan, se puede derivar directamente el impacto que estas tendrían sobre el sistema. Para calcular el impacto, es necesario analizar las dimensiones de seguridad de la información y asignar un valor de gravedad. Se puede utilizar una escala con las siguientes consideraciones:

Tabla 11 Escala para valoración de Impacto de una amenaza o riesgo

Valor del impacto	Consecuencias	Tipo de impacto
1	• Pérdida económica mínima • La cobertura de los medios locales se resuelve rápidamente • Incidente que no requiere ser reportado a las autoridades reguladoras • Sin lesiones para empleados o terceros, como clientes o proveedores • Descontento del personal	Impacto Incidental
2	• Pérdida económica entre un valor mínimo y un valor máximo • Daño a la reputación a nivel local • Incidente que debe ser reportado al regulador, pero sin necesidad de seguimiento • Sin lesiones menores para empleados o terceros, como clientes o proveedores • Problemas generales en la moral del personal y aumento en la rotación de empleados	Impacto Menor
3	• Impacto negativo en los medios de comunicación a nivel nacional a corto plazo • Requisito de informar a las entidades reguladoras sobre incidentes • Necesidad de tratamiento médico ambulatorio para empleados o terceros, como clientes o proveedores • Problemas generales en la moral del personal y alta rotación	Impacto Moderado
4	• Pérdida financiera entre un valor considerable • Impacto negativo en los medios de comunicación a nivel nacional a largo plazo • Pérdida considerable de cuota de mercado • Obligación de informar a las entidades reguladoras sobre incidentes • Necesidad de atención hospitalaria limitada para empleados o terceros, como clientes o proveedores • Alta rotación de personal con experiencia	Impacto Importante
5	• Pérdida económica insostenible para el negocio • Cobertura negativa en medios internacionales a largo plazo; pérdida completa de la cuota de mercado • Enfrentamiento de juicios con riesgo de encarcelamiento para los directivos • Multas significativas • Litigios que incluyen demandas colectivas • Lesiones graves o muertes de empleados o terceros, como clientes o proveedores • Fuga de talentos con consecuencias perjudiciales para el negocio	Impacto Extremo

Con base al análisis de la tabla de impacto se puede calcular el valor de impacto de un riesgo en particular de la siguiente manera

Tabla 12 Cálculo de Impacto de un riesgo (valores de ejemplo)

RIESGO	NOMBRE DEL RIESGO
Impacto a la integridad	4
Impacto a la confidencialidad	3
Impacto a la disponibilidad	5
Valor del impacto	(4+3+5)/3=4
Tipo de impacto	Impacto Importante

4.3.4.1 / MATRIZ DE RIESGOS

Una matriz de riesgos es una herramienta visual utilizada en la gestión de riesgos para evaluar y priorizar los riesgos potenciales que pueden afectar a una organización o proyecto. Esta matriz permite identificar y analizar los riesgos en función de dos factores principales: la probabilidad de que ocurra el riesgo y el impacto que tendría si se materializara. Finalmente es posible calcular el valor del riesgo o amenaza aplicado la fórmula antes mencionada

VALOR DEL RIESGO=PROBABILIDAD*IMPACTO

Tabla 13 Ejemplo de cálculo del valor de un riesgo

RIESGO	VALOR PROBABILIDAD	VALOR IMPACTO	VALOR DEL RIESGO	TIPO DE RIESGO
Riesgo 1	2	3	6	Riesgo apreciable
Riesgo 2	3	4	12	Riesgo Importante
Riesgo 3	5	5	25	Riesgo Muy grave
Riesgo 4	4	4	16	Riesgo Muy grave

Tabla 14 Escala para valorar riesgos

VALOR DE RIESGO	TIPO DE RIESGO	
1-2	Riesgo Marginal	Se debe revisar, no requiere de medidas preventivas
3-8	Riesgo Apreciable	Analizar la posibilidad de implementar medidas preventivas para reducir el nivel del riesgo
9-12	Riesgo Importante	Requiere medidas preventivas obligatorias
13-25	Riesgo muy grave	Requiere medidas preventivas urgentes

Tabla 15 Escala de Color –matriz de riesgos

			IMPACTO				
			IMPACTO INCIDENTAL	IMPACTO MENOR	IMPACTO MODERADO	IMPACTO IMPORTANTE	IMPACTO EXTREMO
			1	2	3	4	5
PROBABILIDAD	MUY ALTA	5	5	10	15	20	25
	ALTA	4	4	8	12	16	20
	MEDIA	3	3	6	9	12	15
	BAJA	2	2	4	6	8	10
	MUY BAJA	1	1	2	3	4	5

4.3.5 / PLAN DE TRATAMIENTO DE RIESGOS

Una vez identificados los riesgos a los que están expuestos los activos de información y la gravedad de cada uno de ellos, corresponde dependiendo del caso establecer un plan para prevenir, mitigar o trasladar los mismos. Este plan puede incluir diferentes tipos de medidas:

Medidas Físicas y técnicas

- Construcción de Infraestructura
- Controles de acceso
- Instalación de sistemas de video vigilancia
- Instalación de una planta eléctrica
- Sistemas biométricos

Medidas Personales

- Contratación de personal
- Capacitaciones
- Socialización

Medidas Organizacionales

- Normas
- Reglamentos
- Políticas de seguridad
- Auditorías

4.3.6 / SELECCIÓN DE CONTROLES Y DECLARACIÓN DE APLICABILIDAD

De todas las medidas o salvaguardas identificadas es necesario realizar un análisis Costo-Beneficio, para determinar cuáles son factibles de aplicar o implementar; para ello se puede considerar los siguientes criterios:

- Tipo de activos a proteger, considerando que existen formas particulares para proteger cada tipo de activo
- Dimensión de seguridad a proteger, en el caso de datos se protege privacidad, integridad mientras que en el caso de equipos o servicios disponibilidad
- Amenazas o riesgos contra los cuales se debe proteger el activo
- Si existen salvaguardas alternativas

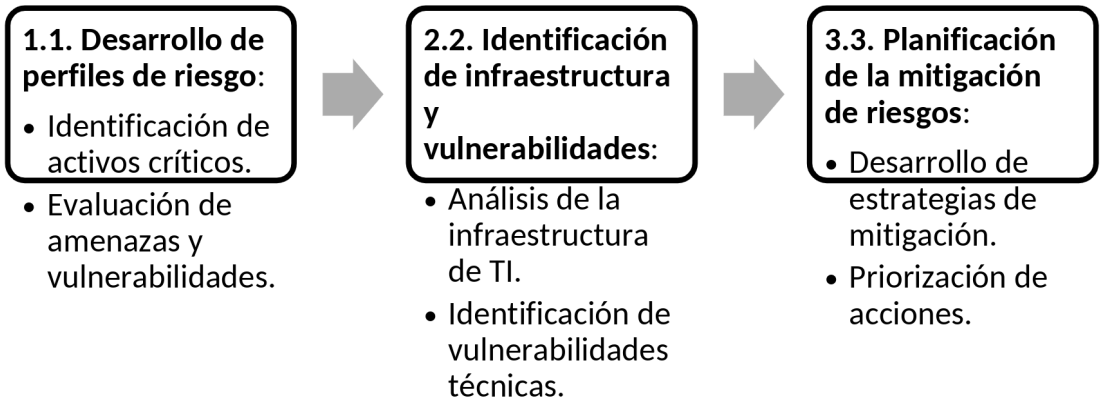
4.4 / METODOLOGÍAS PARA ANALIZAR RIESGOS

Existen varias metodologías para analizar riesgos de seguridad informática, ofrecen diferentes enfoques y herramientas para la gestión de riesgos de seguridad informática, permitiendo a las organizaciones elegir la que mejor se adapte a sus necesidades y contexto. A continuación se citan algunas:

4.4.1 / OCTAVE (OPERATIONALLY CRITICAL THREAT, ASSET, AND VULNERABILITY EVALUATION):

Es una metodología de evaluación de riesgos que se centra en la identificación de activos críticos, amenazas y vulnerabilidades. Se utiliza para desarrollar un perfil de riesgo organizacional y priorizar las acciones de mitigación. Su enfoque es participativo, involucrando a diferentes niveles de la organización para obtener una visión completa de los riesgos.

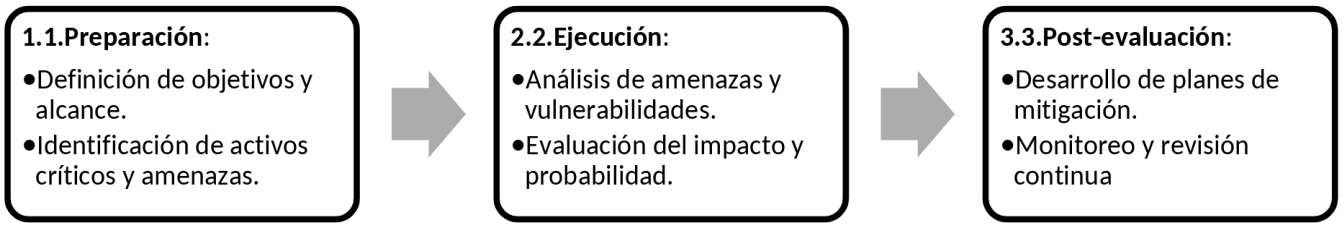
Ilustración 17: Fases de OCTAVE



4.4.2 / NIST SP 800-30 (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY SPECIAL PUBLICATION 800-30):

Esta guía proporciona un marco para la gestión de riesgos de TI, incluyendo la identificación, evaluación y mitigación de riesgos. Es ampliamente utilizada en el sector público y privado en los Estados Unidos. Su enfoque es estructurado y basado en estándares, con un fuerte énfasis en la documentación y el seguimiento continuo.

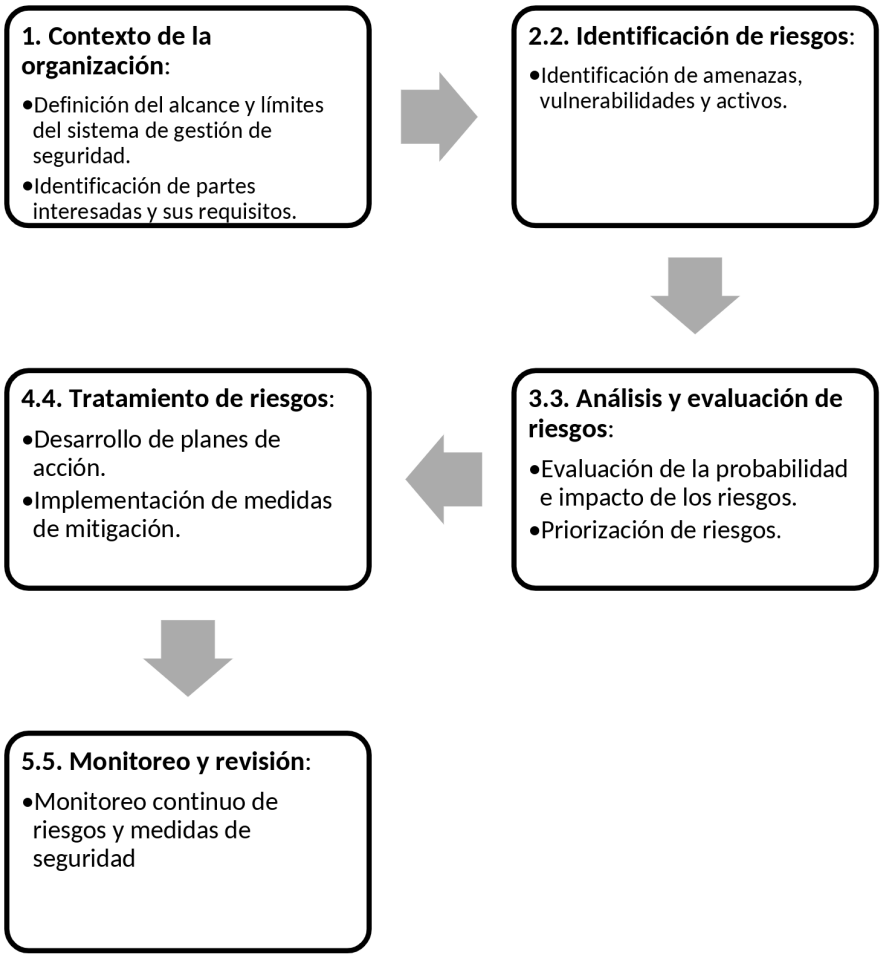
Ilustración 18. Fases de NIST SP 800-30



4.4.3 / ISO/IEC 27005:

Parte de la familia de estándares ISO/IEC 27000, esta norma proporciona directrices para gestionar riesgos de seguridad e información. Es compatible con ISO/IEC 27001 y se centra en la identificación, evaluación y tratamiento de riesgos. Basada en estándares internacionales, adecuado para organizaciones que buscan cumplir con requisitos de certificación.

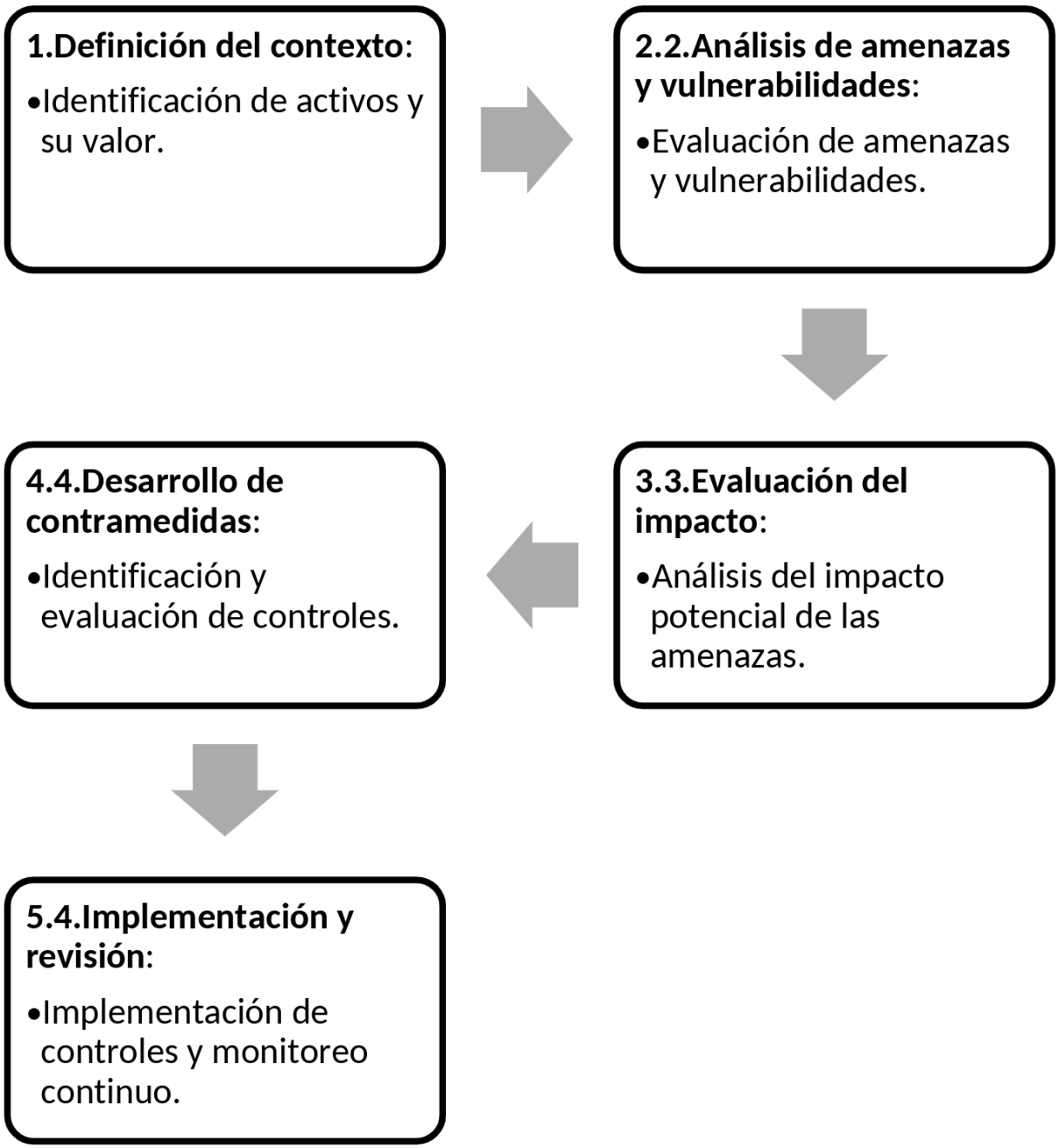
Ilustración 19. Fases de ISO/IEC 27005



4.4.4 / CRAMM (CCTA RISK ANALYSIS AND MANAGEMENT METHOD):

CRAMM es una metodología desarrollada por el gobierno del Reino Unido para la evaluación y gestión de riesgos de TI. Incluye herramientas para la identificación de activos, amenazas y vulnerabilidades, así como para la evaluación del impacto y la probabilidad. Detallado y estructurado, con un fuerte énfasis en la documentación y el análisis exhaustivo.

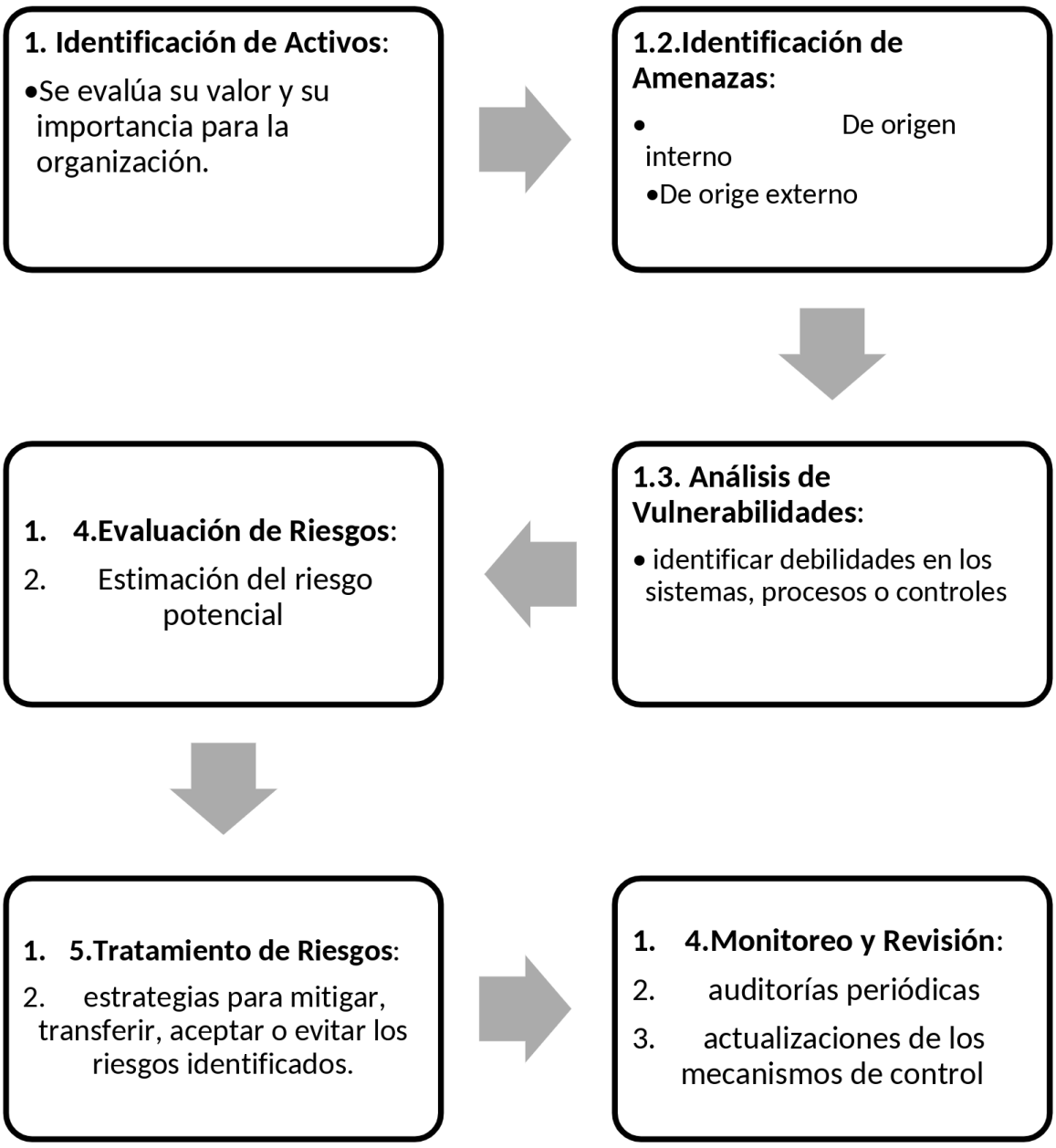
Ilustración 20. Fases de CRAMM



4.4.5 / MAGERIT (METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN):

Desarrollada por el gobierno español, MAGERIT proporciona un marco para la gestión de riesgos de TI, incluyendo la identificación, análisis y tratamiento de riesgos. Es especialmente útil para organizaciones del sector público. Enfoque estructurado y adaptado a las necesidades del sector público, con un fuerte énfasis en la documentación y la transparencia.

Ilustración 21. Fases MAGERIT



4.5 / CASOS DE ESTUDIO CONTROL DE ACCESO CIBERSEGURIDAD

Caso de Estudio 1: Gestión de Riesgos en SaludConnect Ecuador SA

Contexto:

SaludConnect Ecuador SA es una empresa que ofrece servicios de telemedicina y administración historiales médicos electrónicos para hospitales y clínicas del país. La organización cuenta con una plataforma digital que integra datos sensibles de pacientes, información clínica, agendas médicas y resultados de solicitudes. Conscientes de la necesidad de proteger estos activos críticos, la empresa implementó un proceso de gestión de riesgos basado en metodologías internacionales (adaptadas a su realidad) que incluye la identificación de activos, evaluación de vulnerabilidades y amenazas, y la implementación de salvaguardas técnicas y administrativas. Sin embargo, debido a un rápido crecimiento y la constante evolución del entorno digital, algunos controles no se han actualizado conforme a las nuevas amenazas detectadas.

Incidente:

Durante una revisión de seguridad rutinaria, el equipo de TI detectó accesos anómalos en el módulo de autenticación de la plataforma. Se descubrió que un atacante había explotado una vulnerabilidad en el sistema de gestión de contraseñas (debido a una configuración obsoleta ya la falta de actualización de ciertos parches) para acceder de forma no autorizada a la base de datos de pacientes. Como consecuencia, datos clínicos y personales fueron comprometidos, generando una grave violación de la confidencialidad. La brecha impactó la integridad de la información y puso en riesgo la reputación de la empresa, a la vez que evidenció deficiencias en la identificación y tratamiento de ciertos riesgos críticos.

Preguntas para el análisis:

- ¿Cuáles son los activos críticos involucrados en la operación de SaludConnect (por ejemplo, bases de datos de pacientes, sistemas de gestión clínica, etc.) y cómo se valoraron en términos de confidencialidad, integridad y disponibilidad?
- ¿Qué vulnerabilidades específicas en el proceso de autenticación permitieron la explotación por parte del atacante y cómo se relacionan con los controles existentes?
- Utilizando la fórmula ***Valor del riesgo = Probabilidad × Impacto*** , ¿cómo se habría podido

cuantificar este riesgo antes del incidente?

- ¿Qué factores (por ejemplo, porcentaje de controles aplicados, vulnerabilidades detectadas) influyeron en la alta probabilidad y el elevado impacto del riesgo en este caso?
- ¿Qué medidas de tratamiento (mitigación, transferencia o asunción) se podrían haber implementado para reducir la probabilidad de materialización de este riesgo o su impacto?
- ¿Cómo podría haber mejorado el plan de actualización y revisión de salvaguardas técnicas y administrativas para prevenir incidentes similares?
- ¿Qué papel juega el monitoreo y la auditoría periódica en la detección temprana de vulnerabilidades, y cómo se podría integrar de forma más efectiva en el ciclo de gestión de riesgos de SaludConnect?

Caso de Estudio 2: Gestión de Riesgos en EduOnline Ecuador SA

Contexto:

EduOnline Ecuador SA es una plataforma de educación virtual que ofrece cursos, certificaciones y recursos digitales a estudiantes y profesionales a nivel nacional. Su infraestructura incluye un centro de datos propio, aplicaciones de gestión de aprendizaje y un repositorio digital con contenidos educativos de alto valor. La organización realizó un análisis de riesgos centrado en amenazas cibernéticas y vulnerabilidades del software, pero no había actualizado de forma integral su plan de continuidad ante riesgos catastróficos de origen natural o industrial, pese a operar en zonas de alta actividad sísmica y con infraestructura física sensible.

Incidente:

Una noche, un sismo moderado acompañado de fuertes lluvias provocaron inundaciones en la zona donde se ubicaba el centro de datos de EduOnline. Debido a que las salvaguardas físicas (como sistemas de climatización, protección contra inundaciones y fuentes de energía ininterrumpida) estaban insuficientemente dimensionadas, se registró la pérdida parcial de datos críticos y la interrupción prolongada de los servicios de la plataforma. La falta de un plan de tratamiento de riesgos que contemplara desastres naturales evidencia un grave descubierto en la evaluación y mitigación de riesgos que afectarán la disponibilidad de la información y la continuidad del negocio.

Preguntas para el análisis:

- ¿Qué activos de información y recursos (por ejemplo, centros de datos, sistemas de respaldo, equipos de climatización) se vieron comprometidos y cómo se valoraron en el análisis previo de riesgos físicos?
- ¿En qué medida el impacto (en términos de disponibilidad y continuidad) de la pérdida de estos activos fue subestimado durante la fase de evaluación?
- ¿Cómo se evaluó la probabilidad de ocurrencia de desastres naturales (como sismos o inundaciones) en la matriz de riesgos de EduOnline, y qué factores contribuyeron a una evaluación posiblemente sesgada o incompleta?
- ¿Qué deficiencias metodológicas (en la identificación de amenazas o en la revisión de controles) se pueden detectar en el proceso de gestión de riesgos de la organización?
- ¿Qué estrategias de tratamiento (mitigación, transferencia o aceptación) habrían sido apropiadas para abordar el riesgo de desastres naturales, y qué controles adicionales (técnicos, físicos y organizacionales) podrían implementarse?
- ¿Cómo se podrían integrar medidas de redundancia, sistemas de respaldo externos y protocolos de emergencia en el plan de tratamiento de riesgos para mejorar la resiliencia ante incidentes similares?
- ¿Qué mecanismos de monitoreo continuo y revisión periódica se deben establecer para asegurar que el plan de gestión de riesgos se actualice conforme a cambios en el entorno físico y tecnológico?
- ¿Cómo pueden los simulacros y ejercicios de contingencia contribuir a mejorar la respuesta de la organización ante riesgos catastróficos y garantizar la continuidad del negocio?

capítulo cinco

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

En el entorno empresarial actual, la seguridad de la información es un aspecto fundamental para cualquier organización. Un Sistema de Gestión de Seguridad de la Información (SGSI) es una herramienta esencial para administrar y proteger la información de manera eficiente. Este sistema implica la creación de un plan integral que abarca el diseño, implementación y mantenimiento de procesos destinados a asegurar la integridad, confidencialidad y disponibilidad de la información.

Un SGSI puede entenderse como un sistema de gestión centralizado que protege la información dentro de la organización mediante un conjunto de políticas, procedimientos y controles técnicos y físicos. Este sistema no solo se enfoca en los controles técnicos, sino que también incluye evaluaciones de riesgos relacionados con empleados, activos, recursos y procesos. Además, un SGSI requiere la participación activa de todos los empleados, desde el personal con menos responsabilidad hasta el CEO de la empresa.

Según la norma ISO 27001, un SGSI se define como un conjunto de políticas, procedimientos y directrices, junto con los recursos y actividades asociados, que son administrados colectivamente por una organización para proteger sus activos de información esenciales. Este capítulo explorará en detalle los componentes y beneficios de un SGSI, así como las políticas de seguridad de la información, los estándares de seguridad y las directrices necesarias para mantener un entorno seguro y protegido

5.1 / DEFINICIÓN

Un SGSI es un elemento para administración relacionado con la seguridad de la información, aspecto fundamental de cualquier empresa; implica crear un plan de diseño, implementación, y mantenimiento de una serie de procesos que permitan gestionar de manera eficiente la información, para asegurar la integridad, confidencialidad y disponibilidad de la información.

Puede entenderse además como:

- Un sistema de gestión centralizado que asegura la protección de la información dentro de la organización.
- Un conjunto de políticas, procedimientos y controles técnicos y físicos diseñados para salvaguardar la confidencialidad, disponibilidad e integridad de la información.
- Un método para proteger los datos, ya sea que afecten a toda la organización o solo a una área específica.

- Un marco amplio de visión y gestión que es esencial para tomar decisiones informadas sobre los riesgos específicos del entorno empresarial
- Un SGSI no solo abarca controles técnicos, sino también evaluaciones adicionales de riesgos relacionados con empleados, activos, recursos y procesos.
- Un SGSI requiere la participación de todos los empleados de la organización, desde el personal con menos responsabilidad hasta el CEO de la empresa.

Según ISO 27001 un SGSI se define como: "conjunto de políticas, procedimientos y directrices junto a los recursos y actividades asociados que son administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información esenciales (ISO, 2022)

5.2 / POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Es la declaración de las normas que deben seguirse para acceder a la información y los recursos. Los documentos de una política de seguridad deben ser dinámicos, es decir, ajustarse y mejorarse continuamente según los cambios en los entornos donde fueron creados.

Las políticas de seguridad se crean para proteger la información y los sistemas de una empresa, asegurando la integridad, confidencialidad y disponibilidad de los datos. Estos documentos deben incluir procedimientos específicos para hacer cumplir las normas establecidas, así como definir claramente las responsabilidades en todos los niveles de la organización. Además, es crucial que estas políticas se actualicen y mejoren continuamente para adaptarse a los cambios en el entorno y las nuevas amenazas. Todos ellos deben tener el apoyo gerencial de la organización. Las políticas de seguridad deben ser conocidos por todo el personal de una organización.

5.3 / ESTÁNDARES DE SEGURIDAD

Especifican el uso de ciertas tecnologías o métodos de un modo uniforme. Son obligatorios y en ocasiones implican determinados compromisos con ciertos sistemas operativos o fabricantes de software, algunos ejemplos son:

- ISO/IEC 27001: Este estándar establece los requisitos para un sistema de gestión de seguridad de la información (SGSI). Ayuda a las organizaciones a proteger su información de manera sistemática y eficiente

- ISO/IEC 27002: Proporciona directrices para la implementación de controles de seguridad de la información basados en las mejores prácticas. Es complementario a la ISO/IEC 27001
- NIST SP 800-53: Desarrollado por el Instituto Nacional de Estándares y Tecnología de EE.UU., este estándar ofrece un catálogo de controles de seguridad para proteger los sistemas de información federales
- PCI DSS: El Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago es obligatorio para todas las organizaciones que procesan, almacenan o transmiten datos de tarjetas de crédito. Establece medidas de seguridad para proteger la información de los titulares de tarjetas
- ISO/IEC 27701: Este estándar se enfoca en la gestión de la privacidad de la información y es una extensión de la ISO/IEC 27001. Proporciona directrices para la protección de datos personales
- ISO/IEC 27017: Ofrece recomendaciones específicas para la seguridad de la información en servicios de computación en la nube

5.4 / DIRECTRICES

Las directrices son documentos que proporcionan recomendaciones y orientaciones sobre cómo llevar a cabo ciertas actividades o implementar tecnologías, pero a diferencia de los estándares, no son de cumplimiento, ofrecen un marco flexible que las organizaciones pueden seguir para mejorar sus prácticas o procesos. Aunque no son obligatorias, se consideran buenas prácticas y pueden ayudar a alcanzar niveles de calidad y seguridad similares a los estándares.

Las directrices a menudo sirven como base para el desarrollo de estándares. Pueden ser utilizadas para probar y refinar prácticas antes de que se conviertan en requisitos obligatorios. Ejemplos de directrices podrías ser:

- Política de Seguridad de la Información: Una empresa puede desarrollar una política de seguridad de la información basada en la ISO/IEC 27002. Esta política incluiría directrices sobre cómo proteger la confidencialidad, integridad y disponibilidad de la información. Por ejemplo, podría especificar que todos los empleados deben usar contraseñas seguras y cambiarlas regularmente
- Guía de Control de Acceso: Implementar directrices que definan quién tiene acceso a qué información dentro de la empresa. Esto puede incluir el uso de autenticación multifactor (MFA) para acceder a sistemas críticos y la revisión periódica de los permisos de acceso

- Directrices para el Uso de Dispositivos Móviles: Establecer recomendaciones sobre el uso seguro de dispositivos móviles, como teléfonos y tabletas, que se utilizan para acceder a la red de la empresa. Esto podría incluir la instalación de software de seguridad y la prohibición de descargar aplicaciones no autorizadas.
- Plan de Respuesta a Incidentes: Crear un plan basado en las directrices del NIST SP 800-61 para la gestión de incidentes de seguridad informática. Este plan detallaría los pasos a seguir en caso de una brecha de seguridad, incluyendo la identificación, contención, erradicación y recuperación del incidente.

PROCEDIMIENTOS DE SEGURIDAD

Son descripciones detalladas de los pasos necesarios para realizar una tarea específica, permitiendo a los usuarios ejecutarla sin dudas. Estos procedimientos ayudan a las organizaciones a proteger su información y sistemas de manera efectiva, asegurando que todos los empleados sigan prácticas de seguridad consistentes.

Algunos ejemplos de procedimientos de seguridad son:

Procedimiento de Gestión de Contraseñas: Establece los pasos para crear, cambiar y gestionar contraseñas seguras.

Pasos:
- Crear contraseñas con al menos 12 caracteres, incluyendo letras mayúsculas, minúsculas, números y símbolos.
- Cambiar las contraseñas cada 90 días.
- No reutilizar contraseñas antiguas.
- Utilizar un gestor de contraseñas para almacenar y generar contraseñas seguras

Procedimiento de Respuesta a Incidentes de Seguridad: Detalla los pasos a seguir en caso de un incidente de seguridad, como una brecha de datos.

Pasos:
- Identificar y confirmar el incidente.
- Contener el incidente para evitar su propagación.
- Erradicar la causa del incidente.
- Recuperar los sistemas afectados.
- Realizar un análisis post-incidente y documentar las lecciones aprendidas

Procedimiento de Copias de Seguridad (Backups): Define cómo realizar y gestionar copias de seguridad de la información crítica.

Pasos:

- Realizar copias de seguridad diarias de todos los datos críticos.
- Almacenar las copias de seguridad en una ubicación segura y fuera del sitio principal.
- Probar regularmente la restauración de las copias de seguridad para asegurar su integridad.
- Mantener un registro de todas las copias de seguridad realizadas.

Procedimiento de Control de Acceso: Establece cómo gestionar y controlar el acceso a los sistemas y datos de la organización.

Pasos:

- Asignar permisos de acceso basados en el principio de mínimo privilegio.
- Revisar y actualizar regularmente los permisos de acceso.
- Utilizar autenticación multifactor (MFA) para acceder a sistemas críticos.
- Registrar y monitorear todos los accesos a los sistemas

Procedimiento de Seguridad en el Uso de Dispositivos Móviles: Proporciona directrices para el uso seguro de dispositivos móviles en la organización.

Pasos:

- Configurar dispositivos móviles con contraseñas seguras y cifrado de datos.
- Instalar software de seguridad y mantenerlo actualizado.
- Prohibir la descarga de aplicaciones no autorizadas.
- Establecer políticas de uso para dispositivos personales

5.6 / BENEFICIOS DE IMPLEMENTAR UN SGSI EN LA ORGANIZACIÓN

La implementación de un SGSI en una organización provee varias ventajas, algunas se listan a continuación:

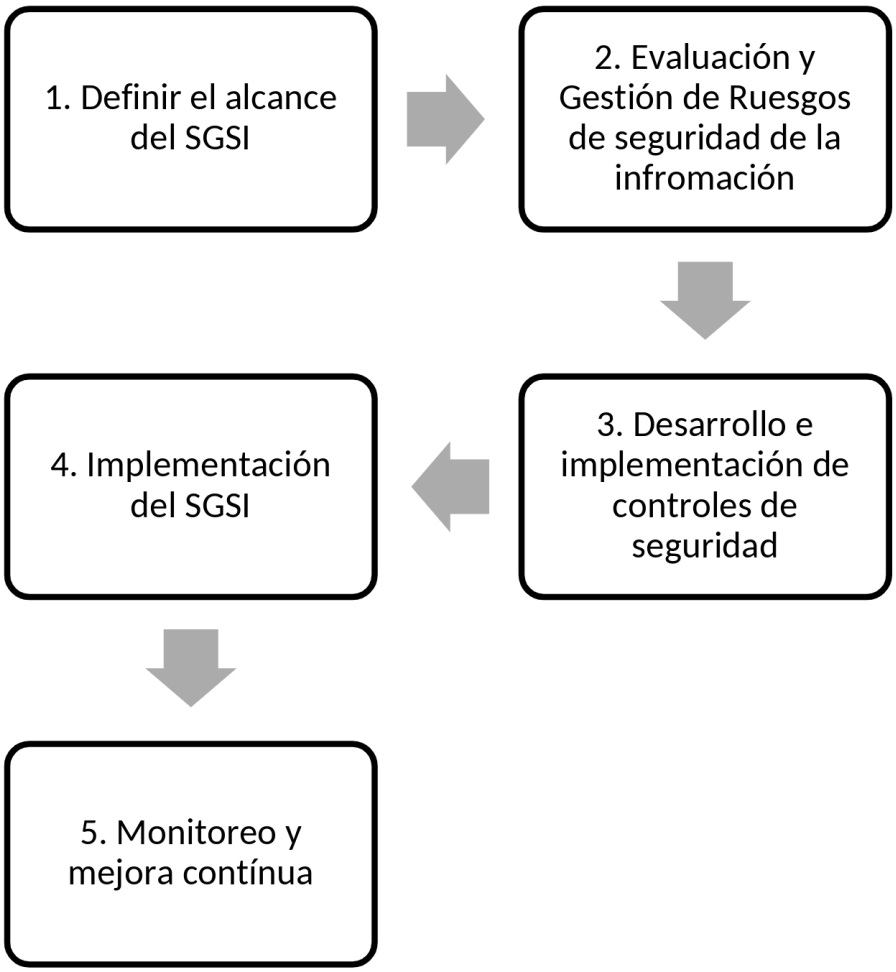
- Reduce el riesgo de que se produzcan pérdidas de información
- Define una metodología que permite gestionar la seguridad de la información de

manera clara y concisa, promoviendo la mejora continua en la organización

- Los clientes, socios estratégicos y proveedores cuentan con una garantía de la seguridad de sus datos
- Ofrece continuidad de operación y servicio
- Cumplimiento de la ley vigente
- Optimización de recursos y costes

5.7 / FASES DE UN SGSI

Ilustración 22. Fases de un SGSI



5.8 / ALCANCE DEL SGSI: DEFINIENDO LOS LÍMITES

Es esencial determinar los límites y la aplicabilidad del sistema, considerando factores como las ubicaciones, los departamentos, los activos de información y tecnología, así como

las partes interesadas relevantes. Este proceso implica evaluar cuidadosamente cada uno de estos elementos para asegurar que todos los aspectos críticos estén cubiertos. Definir un alcance preciso y claro es crucial para implementar un Sistema de Gestión de Seguridad de la Información (SGSI) que sea tanto efectivo como práctico. Un alcance bien definido garantiza que los esfuerzos de seguridad se dirijan adecuadamente, permitiendo una gestión eficiente de los riesgos y una protección robusta de la información. Además, facilita la alineación de los objetivos de seguridad con las necesidades y expectativas de todas las partes interesadas, promoviendo así una cultura de seguridad integral dentro de la organización.(Gómez Fernández & Fernández Rivero, 2018)

5.9 / EVALUACIÓN Y GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La gestión de riesgos de seguridad de la información es un proceso crucial que permite identificar, analizar y controlar las amenazas y vulnerabilidades a las que pueden estar expuestos los activos de información. A través de una evaluación exhaustiva, la empresa u organización puede determinar los riesgos y las debilidades del sistema, y aplicar medidas preventivas o correctivas para mitigarlos. Este enfoque no solo garantiza la seguridad y confiabilidad de la información, sino que también fortalece la resiliencia de la organización frente a posibles incidentes de seguridad. Además, la gestión de riesgos fomenta una cultura de seguridad proactiva, donde se promueve la continua revisión y mejora de las estrategias de protección, asegurando así una defensa robusta y adaptativa ante las amenazas emergentes.

5.10 / DESARROLLO E IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD

Una vez identificados los riesgos, es fundamental implementar controles de seguridad que contribuyan a su mitigación o gestión. La Norma ISO 27001, en su Anexo A, ofrece un conjunto de controles recomendados que sirven como guía para las organizaciones. Estas recomendaciones permiten a las empresas seleccionar los controles más adecuados y relevantes para sus circunstancias específicas. Al adoptar estos controles, las organizaciones pueden fortalecer su postura de seguridad, asegurando que los riesgos sean manejados de manera efectiva y que la protección de la información sea robusta y adaptada a sus necesidades particulares. Además, la implementación de estos controles fomenta una cultura de seguridad dentro de la organización, promoviendo la conciencia y el compromiso de todos los miembros en la protección de los activos de información.

5.11 / IMPLEMENTACIÓN DE SGSI: TRANSFORMANDO TEORÍA EN PRÁCTICA

Para implementar un SGSI se requiere de una planificación clara y detallada así como una ejecución meticulosa.

5.12 / ESTRATEGIAS DE IMPLEMENTACIÓN

Para una aplicación exitosa de un SGSI, debe estar centrado en los principios de seguridad de la información, confidencialidad, integridad y disponibilidad orientando la. Una buena estrategia de implementación debe considerar recursos necesarios, definir un cronograma y asignar responsabilidades.

5.13 / MONITOREO Y MEJORA CONTINUA

La seguridad de la información dentro de una organización es dinámica y está en constante evolución. Por ello, es crucial que SGSI sea evaluado y monitoreado de manera continua. Este proceso asegura que el SGSI permanezca efectivo frente a los cambios en los riesgos y el entorno operativo. La evaluación continua permite identificar nuevas amenazas y ajustar las estrategias de seguridad en consecuencia, garantizando así una protección adecuada y actualizada. Además, el monitoreo constante facilita la detección temprana de posibles vulnerabilidades y la implementación de medidas correctivas oportunas, fortaleciendo la resiliencia de la organización ante cualquier eventualidad..

5.14 / ELEMENTOS FUNDAMENTALES DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

5.14.1 / ANÁLISIS DEL CONTEXTO.

Es fundamental comprender la organización y todos los elementos que pueden influir en el Sistema de Seguridad de la Información.

5.14.2 / ANÁLISIS DE LAS PARTES INTERESADAS.

Este análisis podría incluirse en el punto anterior, ya que representa un factor interno o externo que también influye en el SGSI.

5.14.3 / RESPONSABILIDADES.

Definir las competencias y responsabilidades para cada uno de los activos designados, proporcionar formación en seguridad de la información, fomentar la interacción por parte de la Dirección y aumentar el compromiso.

5.14.4 / EVALUACIÓN DE RIESGOS.

Este punto es crucial para determinar el estado actual, definir estrategias y anticiparse a cualquier factor que pueda afectar a los activos de información.

- La prevención activa y detección de incidentes de seguridad de la información.
- Asegurar un enfoque integral de gestión de seguridad de la información.
- Un enfoque de mejora continua.

5.15 / CASOS DE ESTUDIO SGSI

Caso de Estudio 1: Gestión de Riesgos en SaludConnect Ecuador SA

Contexto:

SaludConnect Ecuador SA es una empresa que ofrece servicios de telemedicina y administración historiales médicos electrónicos para hospitales y clínicas del país. La organización cuenta con una plataforma digital que integra datos sensibles de pacientes, información clínica, agendas médicas y resultados de solicitudes. Conscientes de la necesidad de proteger estos activos críticos, la empresa implementó un proceso de gestión de riesgos basado en metodologías internacionales (adaptadas a su realidad) que incluye la identificación de activos, evaluación de vulnerabilidades y amenazas, y la implementación de salvaguardas técnicas y administrativas. Sin embargo, debido a un rápido crecimiento y la constante evolución del entorno digital, algunos controles no se han actualizado conforme a las nuevas amenazas detectadas.

Incidente:

Durante una revisión de seguridad rutinaria, el equipo de TI detectó accesos anómalos en el módulo de autenticación de la plataforma. Se descubrió que un atacante había explotado una vulnerabilidad en el sistema de gestión de contraseñas (debido a una configuración

obsoleta ya la falta de actualización de ciertos parches) para acceder de forma no autorizada a la base de datos de pacientes. Como consecuencia, datos clínicos y personales fueron comprometidos, generando una grave violación de la confidencialidad. La brecha impactó la integridad de la información y puso en riesgo la reputación de la empresa, a la vez que evidenció deficiencias en la identificación y tratamiento de ciertos riesgos críticos.

Preguntas para el análisis:

- ¿Cuáles son los activos críticos involucrados en la operación de SaludConnect (por ejemplo, bases de datos de pacientes, sistemas de gestión clínica, etc.) y cómo se valoraron en términos de confidencialidad, integridad y disponibilidad?
- ¿Qué vulnerabilidades específicas en el proceso de autenticación permitieron la explotación por parte del atacante y cómo se relacionan con los controles existentes?
- Utilizando la fórmula Valor del riesgo = Probabilidad × Impacto , ¿cómo se habría podido cuantificar este riesgo antes del incidente?
- ¿Qué factores (por ejemplo, porcentaje de controles aplicados, vulnerabilidades detectadas) influyeron en la alta probabilidad y el elevado impacto del riesgo en este caso?
- ¿Qué medidas de tratamiento (mitigación, transferencia o asunción) se podrían haber implementado para reducir la probabilidad de materialización de este riesgo o su impacto?
- ¿Cómo podría haber mejorado el plan de actualización y revisión de salvaguardas técnicas y administrativas para prevenir incidentes similares?
- ¿Qué papel juega el monitoreo y la auditoría periódica en la detección temprana de vulnerabilidades, y cómo se podría integrar de forma más efectiva en el ciclo de gestión de riesgos de SaludConnect?

Caso de Estudio 2: Gestión de Riesgos en EduOnline Ecuador SA

Contexto:

EduOnline Ecuador SA es una plataforma de educación virtual que ofrece cursos, certificaciones y recursos digitales a estudiantes y profesionales a nivel nacional. Su infraestructura incluye un centro de datos propio, aplicaciones de gestión de aprendizaje y un repositorio digital con contenidos educativos de alto valor. La organización realizó un análisis de riesgos centrado en amenazas cibernéticas y vulnerabilidades del software, pero no había actualizado de forma integral su plan de continuidad ante riesgos catastróficos de origen natural o industrial, pese a operar en zonas de alta actividad sísmica y con infraestructura física sensible.

Incidente:

Una noche, un sismo moderado acompañado de fuertes lluvias provocaron inundaciones en la zona donde se ubicaba el centro de datos de EduOnline. Debido a que las salvaguardas físicas (como sistemas de climatización, protección contra inundaciones y fuentes de energía ininterrumpida) estaban insuficientemente dimensionadas, se registró la pérdida parcial de datos críticos y la interrupción prolongada de los servicios de la plataforma. La falta de un plan de tratamiento de riesgos que contemplara desastres naturales evidencia un grave descubierto en la evaluación y mitigación de riesgos que afectarán la disponibilidad de la información y la continuidad del negocio.

Preguntas para el análisis:

- ¿Qué activos de información y recursos (por ejemplo, centros de datos, sistemas de respaldo, equipos de climatización) se vieron comprometidos y cómo se valoraron en el análisis previo de riesgos físicos?
- ¿En qué medida el impacto (en términos de disponibilidad y continuidad) de la pérdida de estos activos fue subestimado durante la fase de evaluación?
- ¿Cómo se evaluó la probabilidad de ocurrencia de desastres naturales (como sismos o inundaciones) en la matriz de riesgos de EduOnline, y qué factores contribuyeron a una evaluación posiblemente sesgada o incompleta?
- ¿Qué deficiencias metodológicas (en la identificación de amenazas o en la revisión de controles) se pueden detectar en el proceso de gestión de riesgos de la organización?
- ¿Qué estrategias de tratamiento (mitigación, transferencia o aceptación) habrían sido apropiadas para abordar el riesgo de desastres naturales, y qué controles adicionales (técnicos, físicos y organizacionales) podrían implementarse?
- ¿Cómo se podrían integrar medidas de redundancia, sistemas de respaldo externos y protocolos de emergencia en el plan de tratamiento de riesgos para mejorar la resiliencia ante incidentes similares?
- ¿Qué mecanismos de monitoreo continuo y revisión periódica se deben establecer para asegurar que el plan de gestión de riesgos se actualice conforme a cambios en el entorno físico y tecnológico?
- ¿Cómo pueden los simulacros y ejercicios de contingencia contribuir a mejorar la respuesta de la organización ante riesgos catastróficos y garantizar la continuidad del negocio?

capítulo seis

SGSI SEGÚN ISO 27001

ISO 227001 Es una norma internacional creada por la Organización Internacional de Normalización (ISO) para garantizar buenas prácticas de seguridad de la información, brinda herramientas que permiten a las empresas gestionar su información de manera segura. Este estándar internacional se creó, entre otras razones, para proporcionar a las organizaciones un modelo consistente que permita establecer, implementar, monitorear, revisar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI).

6.1 / QUÉ PERMITE LA NORMA ISO 27001

Permite Garantiza que la información proporcionada se mantenga confidencial, íntegra, accesible y cumpla con las normativas legales, con el fin de protegerla de posibles amenazas. Este enfoque integral no solo asegura que los datos sean accesibles únicamente por personas autorizadas, sino que también preserva su exactitud y consistencia a lo largo del tiempo. Además, al cumplir con las leyes y regulaciones pertinentes, se minimizan los riesgos legales y se promueve la confianza en la gestión de la información. Implementar estas medidas es crucial para salvaguardar los datos contra accesos no autorizados, alteraciones maliciosas y cualquier otro tipo de riesgo que pueda comprometer su seguridad, permite a las organizaciones entre otras cosas:

- Realizar un diagnóstico a través de entrevistas.
- Llevar a cabo un análisis detallado de todos los posibles riesgos.
- Desarrollar un plan de acción que se ajuste a las necesidades específicas de la empresa.
- Elaborar procedimientos.
- Comprender los requisitos de seguridad de la información y la necesidad de establecer una política y objetivos relacionados.
- Implementar y operar controles para gestionar los riesgos de seguridad de la información.
- Supervisar y evaluar el rendimiento y la efectividad del Sistema de Gestión de Seguridad de la Información (SGSI).
- Promover la mejora continua basada en la medición de los objetivos.

6.2 / ESTRUCTURA DE LA NORMA ISO 27001

Un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 está estructurado para asegurar la confidencialidad, integridad y disponibilidad de la información dentro de una organización

Ilustración 23. Estructura de SGSI-ISO 27001

6.2.1 / CONTEXTO DE LA ORGANIZACIÓN:

- **Comprensión de la organización y su contexto:** Identificar las cuestiones internas y externas que pueden afectar la capacidad de la organización para lograr los resultados esperados de su SGSI.
- **Comprensión de las necesidades y expectativas de las partes interesadas:** Determinar quiénes son las partes interesadas relevantes y cuáles son sus requisitos en relación con la seguridad de la información.
- **Determinación del alcance del SGSI:** Definir los límites y la aplicabilidad del SGSI para establecer su alcance

6.2.2 / LIDERAZGO:

- **Compromiso de la alta dirección:** Demostrar liderazgo y compromiso con el SGSI.
- **Política de seguridad de la información:** Establecer una política que sea adecuada al propósito de la organización.
- **Roles, responsabilidades y autoridades:** Asignar roles y responsabilidades claras para la gestión de la seguridad de la información

6.2.3 / PLANIFICACIÓN:

- **Acciones para abordar riesgos y oportunidades:** Planificar acciones para tratar los

riesgos y oportunidades relacionados con la seguridad de la información.

- **Objetivos de seguridad de la información y planificación para lograrlos:** Establecer objetivos medibles y planificar cómo alcanzarlos.
- **Planificación de cambios:** Considerar cómo los cambios pueden afectar el SGSI y planificar en consecuencia

6.2.4 / APOYO:

- **Recursos:** Proveer los recursos necesarios para establecer, implementar, mantener y mejorar el SGSI.
- **Competencia y concienciación:** Asegurar que el personal sea competente y esté consciente de sus responsabilidades.
- **Comunicación:** Establecer procesos de comunicación interna y externa.
- **Información documentada:** Controlar la creación, actualización y disposición de la documentación del SGSI

6.2.5 / OPERACIÓN:

- **Planificación y control operacional:** Implementar y controlar los procesos necesarios para cumplir con los requisitos del SGSI.
- **Evaluación de riesgos y tratamiento:** Realizar evaluaciones de riesgos y aplicar controles de seguridad adecuados.
- **Controles de seguridad:** Implementar controles basados en la ISO/IEC 27002 para gestionar los riesgos identificados

6.2.6 / EVALUACIÓN DEL DESEMPEÑO:

- **Monitoreo, medición, análisis y evaluación:** Monitorear y medir el desempeño del SGSI regularmente. Analizar y evaluar los resultados para identificar áreas de mejora. Asegurar que el sistema cumple con los objetivos de seguridad establecidos.
- **Auditoría interna:** Realizar auditorías internas periódicas para verificar el cumplimiento del SGSI con los requisitos de la norma. Identificar no conformidades y áreas de mejora. Asegurar la implementación de acciones correctivas necesarias.
- **Revisión por la dirección:** Revisar el SGSI a intervalos planificados para evaluar su adecuación, suficiencia y eficacia. Asegurar que el sistema sigue siendo relevante y efectivo. Tomar decisiones estratégicas para su mejora continua.

6.2.7 / MEJORA:

- **No conformidades y acciones correctivas:** Identificar y gestionar las no conformidades en el SGSI. Tomar acciones correctivas efectivas para prevenir su recurrencia y mantener la alineación con los objetivos de seguridad.
- **Mejora continua:** Identificar oportunidades de mejora en el SGSI. Implementar acciones para actualizar políticas, adoptar nuevas tecnologías y capacitar al personal, asegurando la evolución constante del sistema.

6.3 / CASOS DE ESTUDIO SGSI SEGÚN ISO 27001

Caso de Estudio 1: SGSI en AgroExport SA

Contexto:

AgroExport SA es una empresa dedicada a la exportación de productos agrícolas que cuenta con una amplia cadena de suministro y un sistema de información que gestiona datos críticos: registros de calidad, trazabilidad de productos, información financiera y logística. Consciente de la creciente exposición a riesgos cibernéticos y operacionales, la gerencia decidió implementar un SGSI basado en ISO/IEC 27001. El proyecto incluyó la elaboración de políticas de seguridad, procedimientos para el control de accesos a sistemas y equipos, directrices para la protección de información en la nube y un riguroso plan de capacitación para todos los empleados. Además, se realizaron auditorías internas periódicas y se actualizó el inventario de activos críticos para integrar todos los dispositivos y aplicaciones que forman parte del entorno digital.

Incidente:

Durante una revisión semestral del SGSI, el equipo de seguridad detectó que uno de los dispositivos de monitoreo de temperatura en los almacenes frigoríficos –utilizados para garantizar la calidad del producto durante el transporte– no había sido actualizado con las últimas configuraciones de seguridad. Este equipo, que debía estar integrado al SGSI mediante un procedimiento automatizado de registro de incidentes, presentó una vulnerabilidad en su firmware que permitió a un grupo de ciberdelincuentes acceder remotamente al sistema. Como consecuencia, se logró manipular los datos de temperatura, generando alertas falsas y retrasando la cadena de suministro, lo que puso en riesgo la calidad de los productos exportados y afectó la reputación de la empresa.

Preguntas para el análisis:

- ¿Qué fallos se pueden identificar en la definición del alcance del SGSI y en la actualización del inventario de activos, que permitieron que un dispositivo crítico quedara fuera de los controles de seguridad?
- ¿Cómo deben actualizarse los procedimientos de gestión y mantenimiento de equipos conectados para asegurar que todos los dispositivos, incluidos los que operan en ambientes críticos (como la cadena de frío), se integren de forma permanente al SGSI?
- ¿Qué estrategias de monitoreo y auditoría podrían implementarse para detectar de manera temprana vulnerabilidades en dispositivos del entorno industrial?
- ¿De qué forma se puede reforzar la capacitación del personal técnico para asegurar que todos comprendan la importancia de mantener actualizados los dispositivos integrados al SGSI?

Caso de Estudio 2: SGSI en MercadoDigital Ecuador SA

Contexto:

MercadoDigital Ecuador SA es una empresa de comercio electrónico que ofrece una plataforma para la compra y venta de productos en línea. Debido al manejo de información personal y financiera de miles de clientes, la compañía implementó un SGSI basado en ISO/IEC 27001, a divulgadas políticas de seguridad, estándares técnicos de protección (como encriptación de datos, autenticación multifactor y segmentación de red) y procedimientos de respuesta a incidentes. El SGSI también incluyó directrices para el uso seguro de dispositivos móviles y la integración de controles para terceros que colaboran en el mantenimiento y actualización del sistema.

Incidente:

Durante una auditoría interna, se detectó que uno de los servidores encargados de alojar información sensible no se encontraba debidamente registrado en el inventario del SGSI. Debido a un error en la actualización del alcance del sistema, este servidor carecía de los controles exigidos (como la aplicación de parches de seguridad y configuraciones recomendadas). Aprovechando esta omisión, un grupo de atacantes logró vulnerar la autenticación, accediendo de forma remota a datos de tarjetas de crédito y otra información personal de los clientes. El incidente provocó la interrupción temporal de la plataforma, afectó la confianza de los usuarios y generó una revisión forzada del SGSI.

Preguntas para el análisis:

- ¿Qué errores en la definición del alcance del SGSI y en el mantenimiento del inventario de activos permitieron que un servidor crítico quedara fuera de los controles de seguridad establecidos?
- ¿Cómo se podrían mejorar los procedimientos de actualización y verificación de la infraestructura tecnológica para asegurar que todos los elementos cumplan con los estándares y políticas de SGSI?
- ¿Qué medidas de respuesta a incidentes (técnicas y organizacionales) deben activarse de forma inmediata para mitigar el impacto de un acceso no autorizado en un entorno de comercio electrónico?
- ¿Qué mecanismos adicionales podrían implementarse para garantizar que los proveedores y colaboradores externos cumplan con los mismos estándares de seguridad que la organización?

REFERENCIAS

Álvarez Marañón, G. (2020). Cómo protegernos de los peligros de Internet. Los Libros de La Catarata.

Anderson, R. (2010). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.

Arboledas Brihuega, D. (2013). BackTrack 5. Hacking de redes inalámbricas. RA-MA S.A.

Areirio Bertolin, J. (2008). Seguridad de la información. Redes, informática y sistemas de información. Ediciones Paraninfo, S.A.

Avenía Delgado, C. A. (2017). Fundamentos de seguridad Informática. Colombia: Fundación Universitaria del Area Andina.

Baca Urbina, G. (2016). Introducción a la Seguridad Informática. México: PATRIA.

Caballero, M. d., & Cilleros, D. (2019). Ciberseguridad y transformación digital.

Cicariello, P. (2022). Malware, los más peligrosos y cómo enfrentarlos. RedUSERS.

Gallacher, L., & Morris, H. (2012). ITIL Foundation Exam Study Guide. Wiley.

Gómez Fernández, L., & Fernández Rivero, P. (2018). Cómo implantar un SGSI según ISO/IEC 27001 y su aplicación en el ESquema Nacional de SEguridad. MAdrid: AENOR.

Gómez Vieites, A. (2017). Enciclopedia de seguridad infomrática. Madrid: RA-MA.

Gómez, A. (2013). Auditoría de seguridad informática. Bogotá: StarBook.

Guerra Soto, M. (2018). Análisis de Malware para Sistemas Windows. RA-MA S.A.

Gutiérrez Salazar, P. (2019). El libro blanco del HACKER. RA-MA S.A.

ISO. (2022). Information securiy management system.

Joyanes Aguilar, L. (2023). Ciencias de datos. Marcombo. https://doi.org/ISBN:9788426737724, 8426737722

Mata, A. (2024). Ciberseguridad. Curso Práctico. RA-MA S.A.

Merkow, M., & Breithaupt, J. (2014). Information Security: Principles and Practices. Reino Unido: Pearson Education.

Pérez, J. (2015). Protección de datos y seguridad de la información: guía práctica para ciudadnos y empresas. MAdrid: RA-MA.

Pfleeger, C., Sahri, P., & Margulies, J. (2020). SEcurity in Computing. Prentice Hall.

Roa Buendía, J. F. (2013). Seguridad Informática. Madrid: McGraw Hill.

Samaniego Mena, E. A., & Ponce Ordoñez, J. A. (2021). Fundamentos de Seguridad Informática. Guayaquil: Grupo Compás.

Solano Rodriguez, O., & Riascos Erazo, S. (2021). Sistema de información contable en la era digital: Marco de referencia para su administración y control. Facultad de Ciencias de la Administración de la Universidad del Valle.

Stallings, W. (2017). Cryptography and Network Segurity: Principles and Practice. Pearson.

Tamilarasan, B., Srinivasan, R., Dhivya, S., Subramanian, E. K., & Govindasamy, C. (2023). CRYPTOGRAPHY AND NETWORK SECURITY: PRINCIPLES AND PRACTICE. SK Research

Group of Companies. https://doi.org/https://doi.org/10.1234/ISBN9788119980536
Terán, D. (2014). Administración Estratégica de la función informática. Alpha Editorial.
Turban, E., Sharda, R., & Delen, D. (2011). Decision Support and Business Intelligence Systems. Pearson.
Valencia Duque, F. J., Marulamnda Echeverry, C. E., & López Trujillo, M. (2024). Modelos y marcos de referencia de gestión de riesgos en entornos digitales. Bogotá: Universidad Nacional de Colombia.
Vega Briceño, E. (2021). Seguridad de la información. 3Ciencias.
Vega Briceño, E. (2021). Seguridad de la información. 3Ciencias.
Vega, E. (2020). Planificación y ejecución de evaluaciones de seguridad informática desde un enfoque de ethical hacking. 3Ciencias.

EDICIONES GESICAP

Fundamentos de Seguridad Informática y Ciberseguridad

En la era digital actual, la seguridad de la información y la ciberseguridad se han convertido en pilares fundamentales para la protección de datos y sistemas en todo el mundo. Este libro, "Fundamentos de Seguridad Informática y Ciberseguridad", está diseñado para proporcionar una comprensión integral de los conceptos clave y las mejores prácticas en esta área. A través de sus capítulos, se exploran definiciones generales, principios y dimensiones de la seguridad de la información, así como conceptos esenciales como riesgo, vulnerabilidad y amenaza.

ISBN: 978-9942-626-25-7