MANUAL DEL PARTICIPANTE

BUENAS PRÁCTICAS EN SEGURIDAD DE LA INFORMACIÓN

CON LA FAMILIA DE NORMAS ISO/IEC 27000

Este manual te guía en la comprensión y aplicación de las mejores prácticas de la familia de normas ISO/IEC 27000, ofreciendo herramientas prácticas para implementar un Sistema de Gestión de Seguridad de la Información.

TALENTO

CONTENIDO

MÓDULO 1

INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

LA CIBERSEGURIDAD Y LA SEGURIDAD DE LA INFORMACIÓN SON CONCEPTOS RELACIONADOS QUE CON FRECUENCIA SE CONFUNDEN ENTRE SÍ.

SIN EMBARGO, AUNQUE LA CIBERSEGURIDAD Y LA SEGURIDAD DE LA INFORMACIÓN ESTÁN RELACIONADAS, NO SON LO MISMO.

SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información se centra en proteger la información o los datos que están bajo el cuidado de una organización. Las empresas recopilan datos de los clientes y los generan internamente. Una violación o destrucción de estos datos podría causar un daño grave a los clientes de una compañía y podría perjudicar su capacidad para permanecer en el negocio y competir en el mercado.

Las amenazas a la seguridad de la información corporativa incluyen riesgos para los datos digitales y no digitales. Una estrategia de seguridad de la información debe considerar todos los riesgos potenciales para los datos de una empresa

INCLUYENDO:

- AMENAZAS HUMANAS Y NO HUMANAS
- A LOS DATOS
- UN ATAQUE DE RANSOMWARE, ATAQUE DE DDOS, DENEGACIÓN DE SERVICIO, PHISING, ETC.

¿QUÉ ES LA CIBERSEGURIDAD?

"LA CIBERSEGURIDAD SE REFIERE A TODOS LOS ASPECTOS DE LA PROTECCIÓN DE UNA ORGANIZACIÓN, SUS EMPLEADOS Y ACTIVOS CONTRA LAS AMENAZAS CIBERNÉTICAS. A MEDIDA QUE LOS CIBERATAQUES SE VUELVEN MÁS COMUNES Y SOFISTICADOS Y LOS PROBLEMAS DE SEGURIDAD EN LA EMPRESA SE VUELVEN MÁS COMPLEJOS, SE REQUIERE UNA VARIEDAD DE SOLUCIONES DE CIBERSEGURIDAD PARA MITIGAR EL RIESGO CIBERNÉTICO EMPRESARIAL."

Es importante desarrollar una estructura de gobernanza de TI en una Empresa, negocio o Institución que se alinee con los objetivos institucionales y garantice que todos los integrantes dentro de la organización sean conscientes de sus responsabilidades en lo que respecta a la ciberseguridad.

GOBERNANZA DE SEGURIDAD TI

La gobernanza de la seguridad de TI no debe confundirse con la administración de la seguridad de TI, la cual define e implementar los controles que una organización necesita para mitigar los riesgos.

Una organización debe establecer políticas de seguridad claras y detalladas que todos los empleados conozcan.

LAS ORGANIZACIONES GRANDES Y PEQUEÑAS RECONOCEN EL VALOR DE RECOPILAR Y ANALIZAR DATOS Y, COMO RESULTADO, RECOPILAN UNA CANTIDAD CADA VEZ MAYOR DE INFORMACIÓN PERSONAL SOBRE SUS CLIENTES.

Los ciberdelincuentes siempre están buscando formas de obtener acceso a estos datos valiosos y aprovecharlos para su propio beneficio personal. Por lo tanto, todas las organizaciones que recopilan datos confidenciales deben ser buenos guardianes de estos datos.

Como profesional de la ciberseguridad, su trabajo consiste en poder proteger la información de principio a fin dentro de una organización. Esta no es una tarea fácil y no es razonable esperar que una sola persona tenga todos los conocimientos necesarios para poder hacerlo.

La Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) desarrollaron un marco integral para guiar la administración de la seguridad de la información.

LA FAMILIA DE NORMAS ISO/IEC 27000 EN LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

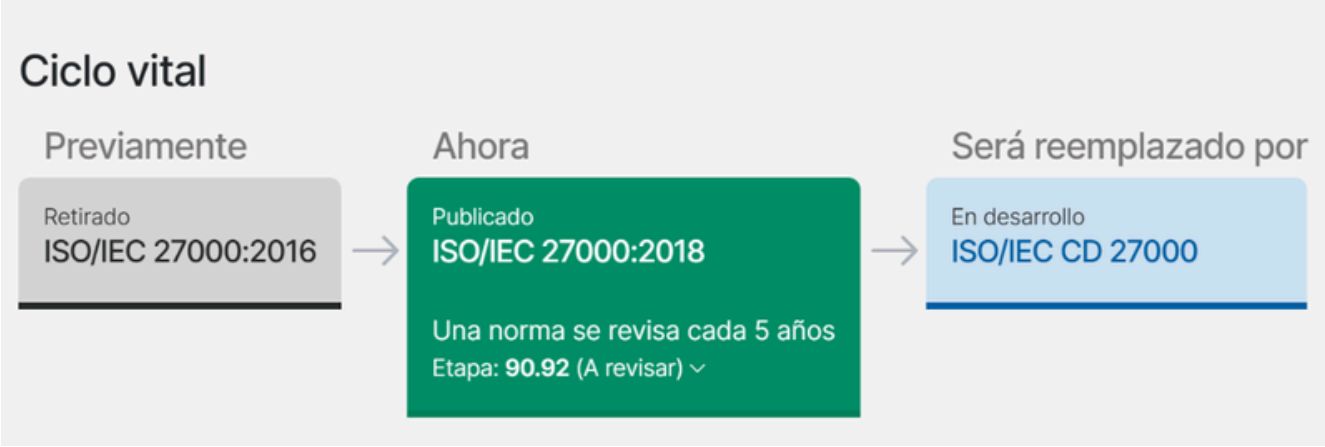
LA SEGURIDAD INFORMÁTICA, LA CIBERSEGURIDAD Y LA PROTECCIÓN DE LA PRIVACIDAD SON FUNDAMENTALES PARA LAS EMPRESAS Y ORGANIZACIONES DE LA ACTUALIDAD. LA FAMILIA DE NORMAS ISO/IEC 27000 LAS PROTEGE.

La norma ISO/IEC 27000 es una serie de estándares de seguridad de la información o mejores prácticas para ayudar a las organizaciones a mejorar la seguridad de la información. Las normas ISO 27000, publicadas por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), establecen los requisitos integrales del sistema de administración de seguridad de la información (SGSI).

Un SGSI incluye todos los controles administrativos, técnicos y operacionales para mantener la información segura dentro de una organización.

La ISO/IEC 27001 es la norma más conocida del mundo para sistemas de gestión de seguridad de la información (SGSI) y sus requisitos.

Más de una docena de normas de la familia ISO/IEC 27000 cubren otras prácticas recomendadas en materia de protección de datos y ciberresiliencia. En conjunto, permiten a las organizaciones de todos los sectores y tamaños gestionar la seguridad de activos como la información financiera, la propiedad intelectual, los datos de los empleados y la información confiada por terceros.



FAMILIA DE NORMAS ISO/IEC 27000.

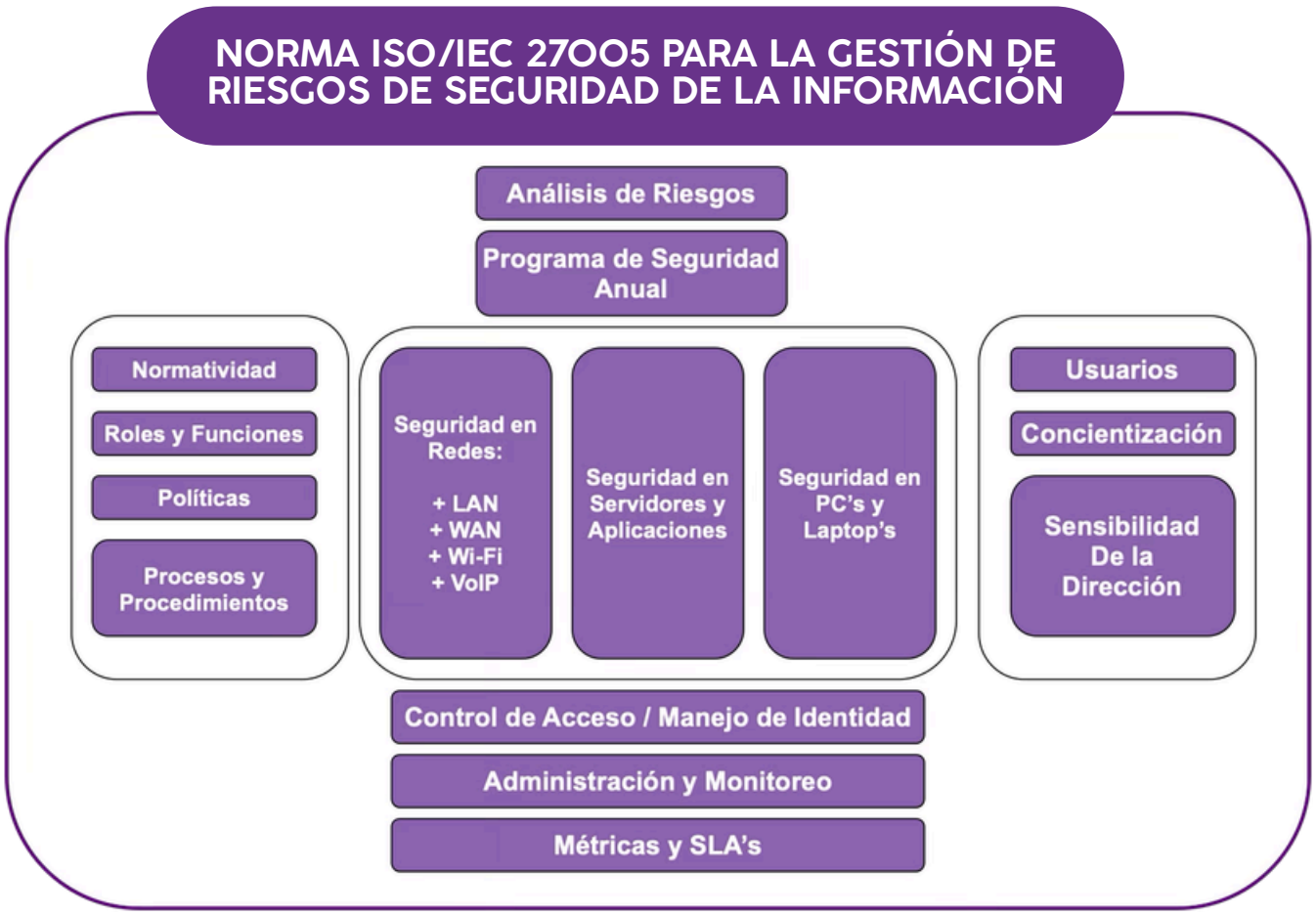
- Requisitos del Sistemas de gestión de la seguridad de la información SGSI (ISO/IEC 27001:2022).
- Controles de seguridad de la información (ISO/IEC 27002:2022)
- Gestión de los riesgos de seguridad de la información (ISO/IEC 27005)

NOTAS:

MÓDULO 2

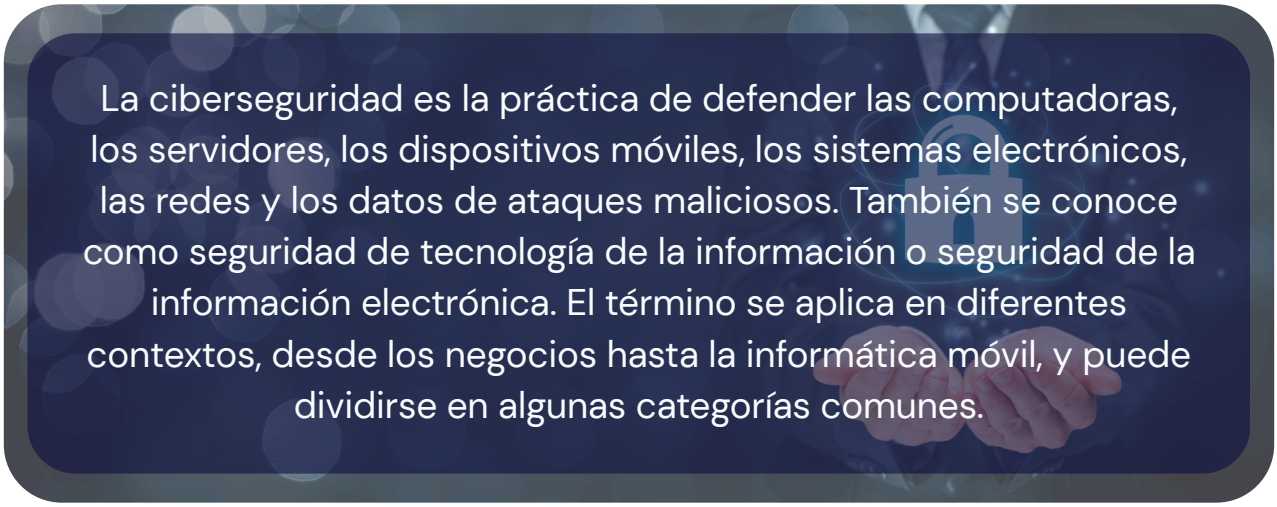
VISIÓN GLOBAL DE LA SEGURIDAD DE LA INFORMACIÓN

VISIÓN GLOBAL DE LA SEGURIDAD



El objetivo de la ciberseguridad es garantizar la confidencialidad, integridad y disponibilidad de la información en el entorno digital.

CIBERSEGURIDAD



Evaluar las vulnerabilidades de redes, servidores, aplicaciones, equipos de cómputo y dispositivos móviles para crear un plan de gestión de riesgos.

Seleccionar los controles de seguridad (norma ISO/IEC 27002) basados en los resultados de la evaluación de riesgos.

CATEGORÍAS COMUNES:

- La **seguridad de red** es la práctica de proteger una red informática de los intrusos, ya sean atacantes dirigidos o malware oportunista.
- La **seguridad de las aplicaciones** se enfoca en mantener el software y los dispositivos libres de amenazas. Una aplicación afectada podría brindar acceso a los datos que está destinada a proteger.
- La **seguridad eficaz** comienza en la etapa de diseño, mucho antes de la implementación de un programa o dispositivo. La seguridad de la información protege la integridad y la privacidad de los datos, tanto en el almacenamiento como en el tránsito.
- La **seguridad operativa** incluye los procesos y decisiones para manejar y proteger los recursos de datos. Los permisos que tienen los usuarios para acceder a una red y los procedimientos que determinan cómo y dónde pueden almacenarse o compartirse los datos se incluyen en esta categoría.

- La **recuperación ante desastres y la continuidad del negocio** definen la forma en que una organización responde a un incidente de ciberseguridad o a cualquier otro evento que cause que se detengan sus operaciones o se pierdan datos. Las políticas de recuperación ante desastres dictan la forma en que la organización restaura sus operaciones e información para volver a la misma capacidad operativa que antes del evento.
- La **capacitación del usuario final** aborda el factor de ciberseguridad más impredecible: las personas. Si se incumplen las buenas prácticas de seguridad, cualquier persona puede introducir accidentalmente un virus en un sistema que de otro modo sería seguro. Enseñarles a los usuarios a eliminar los archivos adjuntos de correos electrónicos sospechosos, a no conectar unidades USB no identificadas y otras lecciones importantes es fundamental para la seguridad de cualquier organización.

NOTAS:

MÓDULO 3

GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN (NORMA ISO/IEC 27005)

ACTIVO

Es cualquier cosa que tenga valor para la organización.

En el contexto de la seguridad de la información, pueden distinguirse dos tipos de activos:

1. Los activos primarios:
- La información
- Los procesos de negocio y las actividades
2. Los activos de apoyo (de los que dependen los activos primarios) de todo tipo
- Hardware
- Software
- Redes
- Personal
- Infraestructura (Centros de datos)

Este es un esquema de inventario y clasificación de los activos de información dentro de una organización.

AMENAZAS Y VULNERABILIDADES EN EL ENTORNO DIGITAL

En el contexto de riesgos digitales, los conceptos de amenazas y vulnerabilidades son clave para comprender cómo se compromete la seguridad de la información y la ciberseguridad.

¿QUÉ ES UNA AMENAZA?

Una amenaza es cualquier evento, acción o circunstancia que puede explotar una vulnerabilidad y causar daño a un sistema, servicio o información.

Ejemplo simple:
Imagina que tienes una casa con una puerta sin cerradura.
Amenaza: Un ladrón que quiere entrar.
Vulnerabilidad: La puerta sin cerradura.

Ejemplos de riesgos digitales:

- Ataques de malware (virus, ransomware, spyware).
- Phishing (engaño para robar credenciales).
- Ataques de denegación de servicio (DDoS) (saturación de un sistema).
- Robo de identidad (uso fraudulento de datos personales).
- Explotación de fallos en software (ataques a vulnerabilidades no corregidas).

¿QUÉ ES UNA VULNERABILIDAD?

Una vulnerabilidad es una debilidad o falla en un sistema, aplicación o proceso que puede ser explotado por una amenaza.

Ejemplo simple: Siguiendo el ejemplo de la pandemia:
1. Vulnerabilidad: no ponerte la vacuna
2. Amenaza: COVID

Ejemplos de riesgos digitales:

- Contraseñas débiles (ejemplo: "123456" o "contraseña").
- Falta de actualizaciones en software (explotación de vulnerabilidades conocidas).

- Ausencia de cifrado en la transmisión de datos (intercepción por atacantes).
- Falta de segmentación en redes (un ataque a un equipo puede comprometer toda la red).
- Permisos excesivos en usuarios (un empleado con acceso innecesario a información crítica)

DIFERENCIA CLAVE ENTRE AMENAZA Y VULNERABILIDAD

Concepto	Definición	Ejemplo de seguridad digital
Amenaza	Evento que puede causar daño	Un hacker intenta robar credenciales de usuarios
Vulnerabilidad	Debilidad que puede ser explotada	Uso de contraseñas débiles en una empresa

Una vulnerabilidad no representa un riesgo por sí sola, pero cuando una amenaza es explotada, se convierte en un incidente de seguridad.

EJEMPLOS DE AMENAZAS Y VULNERABILIDADES

AMENAZAS (Acción para explotar la vulnerabilidad)	**VULNERABILIDADES** (Debilidad, falla)
Empleados malintencionados	Uso de contraseñas predeterminadas, débiles o comunes
Malware (phishing, virus ramsomware)	Software desactualizado (sin parches)
Desastre natural	Falta de validación de campos
Ataques de vulneración de correos electrónicos	Configuración predeterminada en dispositivos
Ataques de vulneración de correos electrónicos	Configuración predeterminada en dispositivos

Reflexiona: ¿Cómo podemos reducir las vulnerabilidades para minimizar el impacto de las amenazas digitales?

GESTIÓN DE LOS RIESGOS

Los problemas de ciberseguridad rara vez saltan a la vista como lo hacen los problemas informáticos normales. Esto se debe a que los atacantes cibernéticos crean amenazas cibernéticas a propósito para evitar ser detectados.

¿Cómo sabe una organización cuánto esfuerzo y recursos requiere para mantener la red y los datos seguros?

Estas preguntas pueden responderse mediante la evaluación del riesgo y la vulnerabilidad. Las organizaciones aplican técnicas de gestión de riesgos para seleccionar y especificar sus controles de seguridad. Las organizaciones utilizan un Sistema de Gestión de Seguridad de la Información (SGSI) para identificar, analizar y abordar los riesgos de seguridad de la información.

Promover la conciencia del riesgo dentro de la organización ayuda a los empleados a desarrollar una comprensión de los riesgos que existen, su impacto potencial y cómo la organización puede gestionar esos riesgos.

La administración de riesgos es un proceso formal que mide el impacto de una amenaza y el costo de implementar controles o contramedidas para mitigar esa amenaza.

Gestión del riesgo:

- Identificación el riesgo
- Análisis del riesgo
- Evaluación del riesgo
- Tratamiento del riesgo

Los analistas evalúan el riesgo que representan las vulnerabilidades para una organización. Incluye la evaluación de la probabilidad de ataques, identifica los tipos de posibles amenazas y evalúa el impacto de las explotaciones exitosas en la organización.

IDENTIFICACIÓN EL RIESGO

Identificar los tipos de posibles amenazas tomando como referencia los activos primarios y de apoyo ya inventariados en la organización y considerados como críticos.

ANÁLISIS DEL RIESGO

Examina los peligros que plantean los eventos provocados por la naturaleza y los humanos a los activos de la organización.

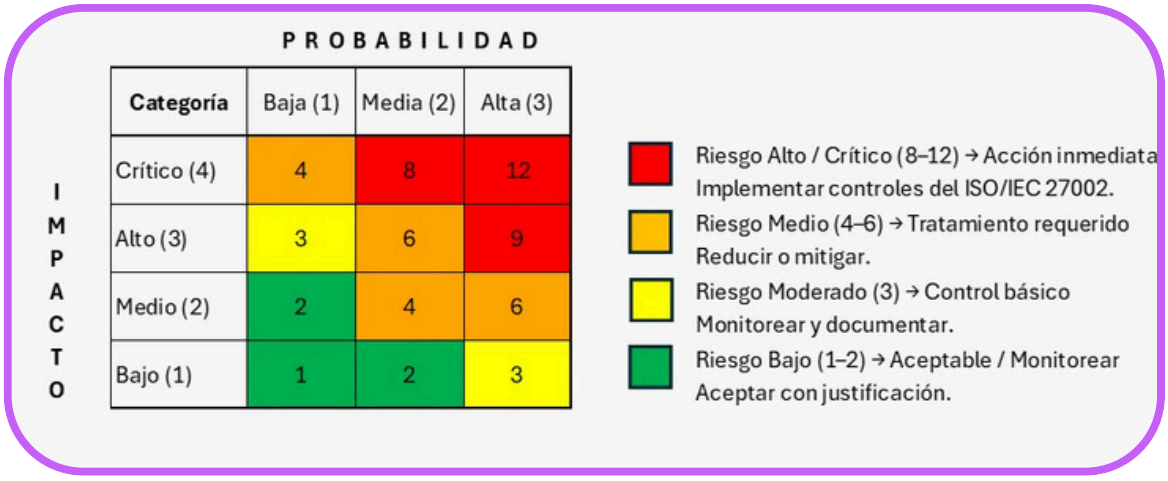
El análisis de riesgos tiene 3 objetivos:

1. Identificar los activos y su valor.
2. Identificar las vulnerabilidades y amenazas.
3. Cuantificar la probabilidad y el impacto de las amenazas identificadas.

Se puede analizar de manera cuantitativa y cualitativa, en este curso nos enfocaremos en el análisis de riesgo cualitativo.

Una matriz de riesgos es una herramienta que ayuda a priorizar los riesgos para determinar para cuales de ellos debe la organización desarrollar una respuesta. Los resultados se pueden clasificar y utilizar como guía para determinar si la organización toma alguna medida.

Cuando la matriz de riesgo está codificada por colores, como se muestra aquí, se el denominado mapa de calor de riesgo.



MITIGACIÓN DEL RIESGO

La mitigación implica reducir la probabilidad o la gravedad de una pérdida por amenazas. Muchos controles técnicos mitigan el riesgo incluidos sistemas de autenticación, permisos de archivos y los firewalls.

La organización debe comprender que la mitigación de riesgos puede tener tanto un impacto positivo como negativo en la organización. La buena mitigación de riesgos encuentra un equilibrio entre el impacto negativo de las contramedidas, los controles y el beneficio de la reducción del riesgo.

Aceptar el riesgo y reevaluarlo periódicamente

Una estrategia a corto plazo es aceptar el riesgo necesitando la creación de planes de contingencia para dicho riesgo. Las personas y las organizaciones deben aceptar el riesgo diariamente.

Reducir el riesgo mediante la implementación de controles

Las modernas metodologías reducen el riesgo mediante el desarrollo incremental de software, y la provisión de parches y actualizaciones periódicas para abordar las vulnerabilidades y los errores de configuración.

Evitar el riesgo modificando completamente el enfoque

Un buen plan de mitigación de riesgos puede incluir dos o más estrategias.

Transferir el riesgo a terceros

Subcontratar servicios, la adquisición de seguros y la adquisición de contratos de mantenimiento son ejemplos de transferencia del riesgo. Contratar especialistas para realizar las tareas fundamentales a fin de preducir el riesgo puede ser una buena opción y producir mejores resultados con una menor inversión a largo plazo.

TRATAMIENTO DEL RIESGO

Los controles de seguridad son salvaguardas o contramedidas que una organización implementa para evitar, detectar, contrarrestar o minimizar los riesgos de seguridad de los activos de la organización.

- **Controles administrativos**

Los controles administrativos consisten en procedimientos y políticas que una organización implementa cuando se trata con información confidencial. Estos controles determinan cómo actúan las personas.

- **Controles técnicos**

Los controles técnicos implican hardware o software implementado para administrar el riesgo y proporcionar protección.

- **Controles físicos**

Los controles físicos son mecanismos como cercas y cerraduras implementados para proteger sistemas, instalaciones, personal y recursos. Los controles físicos separan físicamente a las personas u otras amenazas de los sistemas.

- **Controles de seguridad funcional (Preventivos, detectivos y correctivos)**

Los controles de seguridad preventivos evitan que se produzcan actividades no deseadas o no autorizadas y/o aplican restricciones a los usuarios autorizados.

Por ejemplo, asignar privilegios específicos de usuario en un sistema es un control preventivo, ya que establece límites para evitar que ciertos usuarios accedan y realicen acciones no autorizadas.
Un firewall que bloquea el acceso a un puerto o servicio que los delincuentes cibernéticos puedan atacar es también un control preventivo.

Los **controles de detección** de acceso identifican diferentes tipos de actividad no autorizada. Los controles de detección no son una medida preventiva, sino que se centran en el descubrimiento de una infracción a la seguridad una vez que ha ocurrido.

Todos los sistemas de detección tienen varias cosas en común. Buscan actividades inusuales o prohibidas y pueden ser muy simples, como un detector de movimiento o un guardia de seguridad, o complejas, como un sistema de detección de intrusiones. Los controles de detección también proporcionan métodos para grabar o alertar a los operadores del sistema sobre un posible acceso no autorizado.

Los **controles correctivos** contrarrestan algo indeseable al restaurar el sistema a un estado de confidencialidad, integridad y disponibilidad.
También pueden restaurar los sistemas a la normalidad luego de que se reduzca una actividad no autorizada.

Las organizaciones establecen controles de acceso correctivos después de que un sistema experimente una amenaza. Los ejemplos incluyen políticas de seguridad, alarmas, programas antivirus, sistemas de detección de intrusiones, puertas trampa y planificación de la continuidad de los negocios.

CONTEXTO DEL CASO:

La empresa TechSecure Inc., una firma de tecnología que brinda servicios en la nube a clientes corporativos, ha sido víctima de un ataque cibernético.
Un empleado recibió un correo electrónico de phishing que parecía provenir del departamento de TI interno, solicitando la actualización de credenciales en un enlace externo.
Al ingresar sus credenciales en la página falsa, los atacantes lograron acceso no autorizado al entorno interno de TechSecure Inc., extrayendo información confidencial de clientes y modificando configuraciones críticas de seguridad.

Impacto del Ataque:

- Pérdida de datos de clientes, incluyendo información financiera y registros de proyectos.
- Modificación de configuraciones en servidores de producción.
- Daño reputacional al ser expuesto en medios de comunicación.
- Potencial incumplimiento de normativas de seguridad de datos (ISO 27001, GDPR, etc.).

1. **Análisis de Riesgos:**

Los participantes deben analizar el caso y responder a las siguientes preguntas:

- ¿Cuáles son los activos afectados en este caso?
- ¿Cuáles son las amenazas cibernéticas identificadas?
- ¿Cuáles son las vulnerabilidades explotadas?
- ¿Cuál es el impacto del ataque en la organización?
- ¿Cómo se pudo haber prevenido este incidente?

2. **Evaluación del Riesgo:**

Utilizando una tabla de evaluación de riesgos, los alumnos deben clasificar la probabilidad e impacto del ataque en una escala de:

- Probabilidad: Alta, Media, Baja.
- Impacto: Crítico, Alto, Medio, Bajo.

3. **Propuesta de Mitigación:**

Los participantes deben sugerir al menos tres medidas de seguridad para reducir la exposición a este tipo de amenaza en el futuro. Ejemplos:

- Implementación de autenticación multifactor (MFA).
- Monitoreo de tráfico en la red con IDS/IPS.
- Programas de concienciación en ciberseguridad para empleados.

¿Cuáles son los activos afectados en este caso?
¿Cuáles son las amenazas cibernéticas identificadas?
¿Cuáles son las vulnerabilidades explotadas?
¿Cuál es el impacto del ataque en la organización?
¿Cómo se pudo haber prevenido este incidente?

DESCRIBE TU PROPUESTA DE MITIGACIÓN DE LOS RIESGOS:

NOTAS:

MÓDULO 4

PILARES DE LA SEGURIDAD DE LA INFORMACIÓN (TRIADA CID)

¿PORQUE UNA CULTURA DE LA SEGURIDAD?

En cualquier organización, la seguridad de la información es estratégica. La información de la organización **es uno de los activos más valiosos.**

Por ello, es necesario que todos los que forman parte de dicha organización se sensibilicen acerca de la necesidad de proteger la información **durante su creación, procesamiento, almacenamiento, difusión y destrucción.**

- **Disponibilidad:** Se refiere a que exista acceso a tiempo a los datos y a los sistemas de información para los usuarios autorizados. Es decir, a la accesibilidad de la información y los recursos de la red.

- **Integridad:** Se refiere a salvaguardar la exactitud y consistencia de la información. Es decir, a su confiabilidad y autenticidad.

- **Confidencialidad:** Se refiere a que la información solo pueda ser accedida por los usuarios autorizados. Es decir, a la limitación del acceso.

SE TIENE LA IDEA ERRÓNEA DE QUE ÚNICAMENTE LA TECNOLOGÍA NOS PROTEGERÁ.
SE PIENSA QUE CON SOLO PONER UN FIREWALL, UN TECLADO BIOMÉTRICO, ETC. ES SUFICIENTE. PERO AL FINAL, DESCUBRIMOS QUE NO ES ASÍ.

Para que una estrategia de seguridad sea efectiva, se deben involucrar los cuatro aspectos de la seguridad: **Organización, personas, Instalaciones físicas y Tecnología.**

Por más sofisticados que sean los sistemas de seguridad, si falta alguno de estos elementos, el modelo fracasará.

Pero antes de implementar las estrategias de seguridad debemos conocer ¿Qué? vamos a proteger.

TIPOS DE DATOS DE LA ORGANIZACIÓN

Los datos tradicionales suelen ser generados y mantenidos por todas las organizaciones, grandes y pequeñas. Incluye lo siguiente:

Datos transaccionales, como detalles relacionados con la compra y venta, actividades de producción y operaciones organizativas básicas, como cualquier información utilizada para tomar decisiones de empleo.

La propiedad intelectual, como patentes, marcas registradas y planes de nuevos productos, permite a una empresa obtener una ventaja económica sobre sus competidores. Esta información a menudo se considera un secreto comercial y perderla puede resultar desastroso para el futuro de una empresa.

Los datos financieros, como las declaraciones de ingresos, los balances y las declaraciones de flujo de caja brindan información sobre el estado de la empresa.

PILARES DE LA SEGURIDAD DE LA INFORMACIÓN

El McCumber Cube es un marco modelo creado por John McCumber en 1991 para ayudar a las organizaciones a establecer y evaluar iniciativas de seguridad de la información al considerar todos los factores relacionados que las afectan.

ESTE MODELO DE SEGURIDAD TIENE TRES DIMENSIONES:

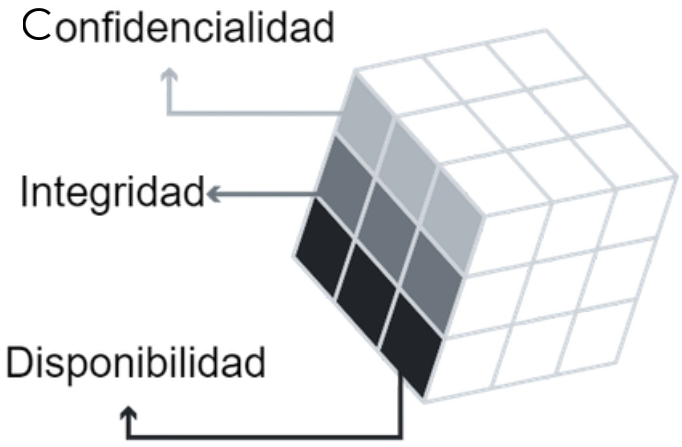
1. LOS PRINCIPIOS FUNDAMENTALES PARA PROTEGER LOS SISTEMAS DE INFORMACIÓN.
2. LA PROTECCIÓN DE LA INFORMACIÓN EN CADA UNO DE SUS ESTADOS POSIBLES.
3. LAS MEDIDAS DE SEGURIDAD UTILIZADAS PARA PROTEGER LOS DATOS.

1. LOS PRINCIPIOS FUNDAMENTALES PARA PROTEGER LOS SISTEMAS DE INFORMACIÓN

- **La confidencialidad** es un conjunto de reglas que evita que la información sensible sea revelada a personas no autorizadas, espacio de recursos y procesos. Los métodos utilizados para garantizar la confidencialidad incluyen **el cifrado** de datos, **la autenticación y el control de** acceso.

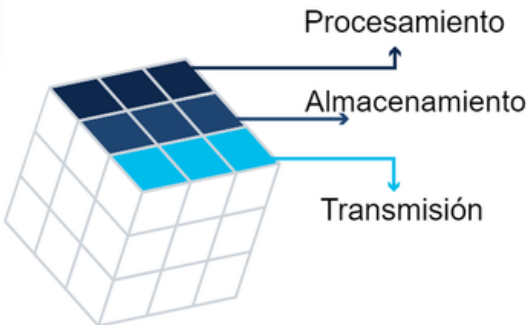
- **La integridad** garantiza que la información o los procesos del sistema estén protegidos contra modificaciones intencionales o accidentales. Una forma de garantizar la integridad es utilizar una función **hash o suma** de comprobación.

- **La disponibilidad** significa que los usuarios autorizados pueden acceder a los sistemas y datos cuando y donde sea necesario y aquellos que no cumplen con las condiciones establecidas, no lo son. Esto se puede lograr **mediante el manteniendo el equipo, realizando reparaciones de hardware, manteniendo los sistemas operativos y el software actualizados, y creando copias de seguridad.**



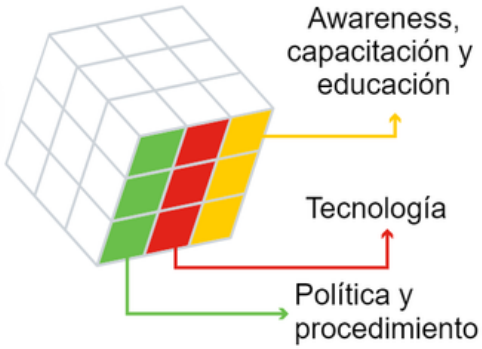
2. LA PROTECCIÓN DE LA INFORMACIÓN EN CADA UNO DE SUS ESTADOS POSIBLES

- **El procesamiento** se refiere a los datos que se utilizan para realizar una operación como la actualización de un registro de base de datos (datos en proceso).
- **El almacenamiento** se refiere a los datos almacenados en la memoria o en un dispositivo de almacenamiento permanente, como un disco duro, una unidad de estado sólido o una unidad USB (datos en reposo).
- **La transmisión** se refiere a los datos que viajan entre sistemas de información (datos en tránsito).



3. LAS MEDIDAS DE SEGURIDAD UTILIZADAS PARA PROTEGER LOS DATOS

- **La concientización,** la capacitación y la educación son las medidas implementadas por una organización para garantizar que los usuarios estén informados sobre las posibles amenazas a la seguridad y las acciones que pueden tomar para proteger los sistemas de información.
- **La tecnología** se refiere a las soluciones basadas en software (y hardware) diseñadas para proteger los sistemas de información como los firewalls, que monitorean continuamente su red en busca de posibles incidentes maliciosos.
- **La política y el procedimiento** se refieren a los controles administrativos que proporcionan una base para la forma en que una organización implementa el aseguramiento de la información, como los planes de respuesta a incidentes y las pautas de mejores prácticas.



A pesar de las mejores intenciones y de todas las salvaguardas que puede implementar, proteger a las organizaciones de todos los ciberataques no es factible.

Los ciberdelincuentes están constantemente encontrando nuevas formas de atacar y, eventualmente, tendrán éxito.

Cuando lo hagan, corresponderá a los profesionales de la ciberseguridad, responder rápidamente para minimizar su impacto.

FUENTE: CISCO

CIBERSEGURIDAD

La ciberseguridad es el esfuerzo constante por proteger los sistemas de red y todos los datos contra el uso no autorizado o los daños.

A nivel personal, debe proteger su identidad, sus datos y sus dispositivos informáticos.

A nivel corporativo, es responsabilidad de todos proteger la reputación, los datos y los clientes de la organización.

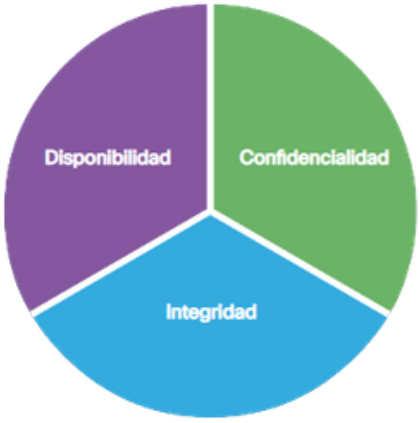
TRIADA CID

Es una guía para la seguridad informática de una organización.

La confidencialidad garantiza la privacidad de los datos mediante la restricción del acceso con el cifrado de la autenticación.

La integridad garantiza que la información sea precisa y confiable.

La disponibilidad garantiza que la información esté disponible a las personas autorizadas.



La confidencialidad

Entre los métodos para garantizar la confidencialidad se incluyen:
El cifrado de datos, nombre de usuario y contraseña, la autenticación de dos factores y la minimización de la exposición de la información confidencial.

La integridad

Garantiza que la información sea precisa, consistente y confiabledurante su ciclo de vida.
Las sumas de comprobación se calculan con funciones de hash. Algunas de las sumas de comprobación comunes son MD5, SHA-1, SHA-256 y SHA-512.

La disponibilidad

Garantiza que la información esté disponible a las personas autorizadas.
Mantener los equipos, realizar reparaciones de hardware, mantener los sistemas operativos y el software actualizados, así como crear respaldos, garantiza la disponibilidad de la red y los datos a los usuarios autorizados.

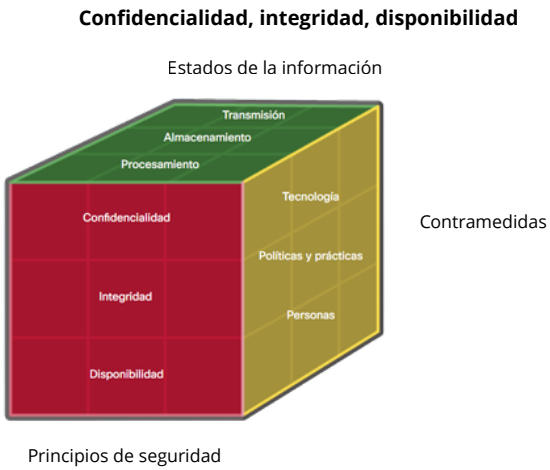
CUBO DE MCCUMBER

- **La confidencialidad** previene la divulgación de información a las personas los recursos o los procesos no autorizados.

- **La integridad** hace referencia a la precisión, la uniformidad y la confiabilidad de datos.

- **La disponibilidad** garantiza que los usuarios pueden tener acceso a la información cuando sea necesario.

IMPORTANTE: Utilice el acrónimo CID para recordar los 3 principios.



CONFIDENCIALIDAD

La confidencialidad previene la divulgación de información a las personas los recursos y los procesos no autorizados.
Otro término para la confidencialidad es el de privacidad.

Las organizaciones restringen el acceso para asegurar que solo los operadores autorizados pueden usar los datos u otros recursos de red.

Las organizaciones necesitan capacitar a los empleados sobre las mejores prácticas en la protección de la información confidencial para protegerse a sí mismos y a la organización de los ataques.

Los métodos utilizados para garantizar la confidencialidad incluyen:

- El cifrado de datos
- La autenticación
- El control de acceso.

INTEGRIDAD

La integridad es la precisión, uniformidad y confiabilidad de los datos durante su ciclo de vida.
Otro término para la integridad es el de calidad.

Los datos experimentan varias operaciones como captura, almacenamiento, recuperación, actualización y transferencia. Las entidades no autorizadas deben mantener inalteradas los datos durante todas estas operaciones.

Los métodos utilizados para garantizar la integridad de los datos incluyen:

- La función de hash
- Las comprobaciones de validación de datos
- Las comprobaciones de consistencia de los datos
- Los controles de acceso.

Los sistemas de integridad de datos pueden incluir uno o más de los métodos mencionados anteriormente.

DISPONIBILIDAD

Mantener la disponibilidad de los sistemas y servicios de información en todo momento.

Los ataques cibernéticos y las fallas en el sistema pueden impedir el acceso a los sistemas y servicios de información.

Los ataques de denegación de servicio (DoS) amenazan la disponibilidad del sistema y evitan que los usuarios legítimos tengan acceso y usen sistemas de información cuando sea necesario.

Los métodos utilizados para garantizar la disponibilidad incluyen:

- La redundancia del sistema
- Las copias de seguridad del sistema
- Mayor recuperabilidad del sistema
- Mantenimiento del equipo
- Sistemas operativos y software actualizados
- Planes para recuperarse rápidamente de desastres no planificados.

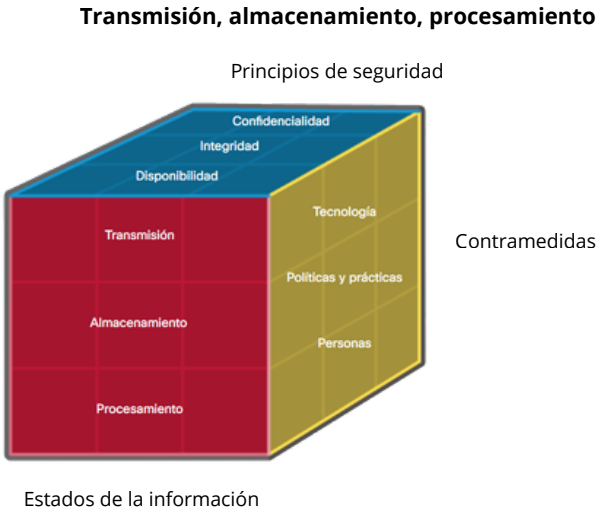
CUBO DE MCCUMBER

El mundo cibernético es un mundo de datos; los especialistas se centran en la protección de los datos.

La segunda dimensión del cubo de destrezas de ciberseguridad se concentra en los problemas de proteger todos los estados de los datos en el mundo cibernético.

Los datos tienen tres estados posibles:

- Datos en tránsito
- Datos almacenados
- Datos en proceso



TRANSMISIÓN DE DATOS

La transmisión de datos implica el envío de la información de un dispositivo a otro.

Métodos para transmitir información entre dispositivos, se incluyen los siguientes:

- Red de transferencia: utiliza medios extraíbles para mover físicamente los datos de una computadora a otra
- Redes cableadas: utilizan cables para transmitir datos

Redes inalámbricas: utilizan ondas de radio para transmitir datos.

DESAFÍOS EN LA PROTECCIÓN DE DATOS EN TRÁNSITO

La protección de los datos transmitidos es uno de los trabajos más desafiantes.

Con el crecimiento de los dispositivos móviles e inalámbricos, los profesionales de ciberseguridad son responsables de proteger cantidades masivas de datos que cruzan la red a diario.

Desafíos al proteger estos datos:

- Protección de la confidencialidad de los datos: los delincuentes pueden capturar, guardar y robar datos en tránsito.
- Protección de la integridad de los datos: los delincuentes pueden interceptar y alterar los datos en tránsito.
- Protección de la disponibilidad de los datos: los delincuentes pueden usar dispositivos falsos o no autorizados para interrumpir la disponibilidad de los datos.

Contramedidas para los DATOS EN TRÁNSITO

ALMACENAMIENTO – DATOS GUARDADOS

Los datos almacenados significan que un tipo de dispositivo de almacenamiento conserva los datos cuando ningún usuario o proceso los utiliza. Un dispositivo de almacenamiento puede ser local (en un dispositivo informático) o centralizado (en la red).

Existen varias opciones para almacenar datos.

- Almacenamiento de conexión directa (DAS). DD o USB
- La Matriz redundante de discos independientes (RAID). Proporciona un mejor rendimiento y una mejor tolerancia a fallas.
- Un dispositivo de almacenamiento conectado a la red (NAS)
- Una aruitectura de red de área de almacenamiento (SAN)
- El almacenamiento en la nube

Los datos almacenados significan que un tipo de dispositivo de almacenamiento conserva los datos cuando ningún usuario o proceso los utiliza. Un dispositivo de almacenamiento puede ser local (en un dispositivo informático) o centralizado (en la red).

Existen varias opciones para almacenar datos.

- Almacenamiento de conexión directa (DAS). DD o USB
- La Matriz redundante de discos independientes (RAID). Proporciona un mejor rendimiento y una mejor tolerancia a fallas.
- Un dispositivo de almacenamiento conectado a la red (NAS)
- Una arquitectura de red de área de almacenamiento (SAN)
- El almacenamiento en la nube

Los datos almacenados significan que un tipo de dispositivo de almacenamiento conserva los datos cuando ningún usuario o proceso los utiliza. Un dispositivo de almacenamiento puede ser local (en un dispositivo informático) o centralizado (en la red).

Existen varias opciones para almacenar datos.

- Almacenamiento de conexión directa (DAS). DD o USB
- La Matriz redundante de discos independientes (RAID). Proporciona un mejor rendimiento y una mejor tolerancia a fallas.
- Un dispositivo de almacenamiento conectado a la red (NAS)
- Una aruitectura de red de área de almacenamiento (SAN)
- El almacenamiento en la nube

DESAFÍOS DE LOS DATOS ALMACENADOS

Para mejorar el almacenamiento de datos:

- Las empresas pueden automatizar y centralizar las copias de respaldo de datos.
- El almacenamiento de conexión directa es más difícil de administrar y controlar.
- Las copias de respaldo pueden ser manuales o automáticas.
- Las organizaciones deben limitar los tipos de datos almacenados de conexión directa.
- No almacenar los datos críticos en dispositivos de conexión directa.
- Los sistemas de almacenamiento en red ofrecen una alternativa más segura.
- Los sistemas de almacenamiento en red incluidos RAID, SAN y NAS proporcionan mayor rendimiento y redundancia. Aunque son más complicados para configurar y administrar.
- Manejan más datos.
- Mayor riesgo para la organización si falla el dispositivo.

Los desafíos particulares de almacenamiento en red: configuración, la prueba y la supervisión del sistema.

FORMAS DE PROCESAMIENTO Y CÓMPUTO DE DATOS

Se refiere a los datos durante la entrada, la modificación, el cómputo o el resultado.

La protección de la integridad de los datos comienza con la entrada inicial de datos.
Las organizaciones utilizan varios métodos para recopilar datos, como ingreso

manual de datos, formularios de análisis, cargas de archivos y datos recopilados de los sensores.

Los procesos como la codificación y decodificación, compresión y descompresión y cifrado y descifrado son ejemplos de la modificación de los datos.

La salida de datos se refiere a los datos que salen de impresoras, pantallas electrónicas o directamente a otros dispositivos. La precisión de los datos de salida es fundamental ya que el resultado proporciona información y afecta la toma de decisiones.

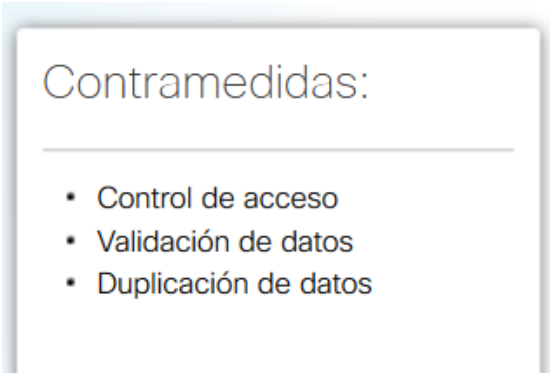
DESAFÍOS EN LA PROTECCIÓN DE DATOS EN PROCESO

La protección contra la modificación de los datos no válidos durante el proceso puede tener un efecto adverso.

Los errores de software son el motivo de muchas desgracias y desastres.

La protección de los datos durante el proceso requiere sistemas bien diseñados.

Los profesionales de ciberseguridad diseñan políticas y procedimientos que requieren pruebas, mantenimientos y actualización de sistemas para mantenerlos en funcionamiento con la menor cantidad de errores.



CUBO DE MCCUMBER

Los profesionales en ciberseguridad deben utilizar todos los poderes disponibles a su disposición para proteger los datos del mundo cibernético.

1.El primer tipo de poder incluye tecnologías, dispositivos y productos disponibles para proteger los SI.

2.Crear una defensa sólida al establecer las políticas, los procedimientos y seguir las prácticas adecuadas.

3.Los profesionales deben esforzarse por obtener conocimientos en seguridad y amenazas. Establecer una cultura de aprendizaje y conciencia.

MEDIDAS DE PROTECCIÓN TECNOLÓGICA (SOFTWARE)

Las medidas de protección de software

Incluyen programas y servicios que protegen los sistemas operativos, las bases de datos y otros servicios que operan en las estaciones de trabajo, los dispositivos portátiles y los servidores.

Los administradores instalan las contramedidas o las protecciones basadas en software en los hosts o los servidores individuales.

Existen varias tecnologías basadas en software utilizadas para proteger los activos de la organización:

- Firewall
- Escáneres de redes y puertos
- Analizadores de protocolos o de firmas
- Escáneres de vulnerabilidades
- Sistemas de detección de intrusos

MEDIDAS DE PROTECCIÓN TECNOLÓGICA (HARDWARE)

Las medidas de protección de hardware

Existen varias tecnologías basadas en hardware utilizadas para proteger los activos de la organización:

- Los dispositivos de firewall bloquean el tráfico no deseado. Los firewalls contienen reglas que definen el tráfico permitido dentro y fuera de la red.

- Los sistemas de detección de intrusiones (IDS) exclusivos detectan signos de ataques o de tráfico inusual en una red y envía una alerta.

- Los sistemas de prevención de intrusiones (IPS) detectan signos de ataques o de tráfico inusual en una red, generan una alerta y toman medidas correctivas.

- Los servicios de filtrado de contenido controlan el acceso y la transmisión de contenido inaceptable u ofensivo.

MEDIDAS DE PROTECCIÓN TECNOLÓGICAS (RED)

Existen varias tecnologías basadas en red que se utilizan
para proteger los activos de la organización:

La red privada virtual (VPN) es una red virtual segura que utiliza la red pública (es decir, Internet). La seguridad de una VPN reside en el cifrado del contenido de paquetes entre los terminales que definen la VPN.

MEDIDAS DE PROTECCIÓN TECNOLÓGICA (HARDWARE)

- Los sistemas de prevención de intrusiones (IPS) detectan signos de ataques o de tráfico inusual en una red, generan una alerta y toman medidas correctivas.

- Los servicios de filtrado de contenido controlan el acceso y la transmisión de contenido inaceptable u ofensivo.

POLÍTICAS Y PROCEDIMIENTOS

Establecimiento de una cultura de conocimiento de la ciberseguridad

Los miembros de una organización deben tener en cuenta
las políticas de seguridad y tener el conocimiento para hacer
de la seguridad una parte de sus actividades diarias.

Un programa de reconocimiento de seguridad depende de:

- El entorno de la organización
- El nivel de amenaza

La creación de una cultura de seguridad es un esfuerzo continuo de la administración superior y el compromiso de todos los usuarios y empleados.

Ejemplos:
Establecimiento de políticas y procedimientos por parte de la administración.
Días de concientización sobre la ciberseguridad.
Publicación de mensajes y señalizaciones sobre ciberseguridad.
Creación de talleres y seminarios para aumentar la conciencia.

Una política de seguridad es un conjunto de objetivos de seguridad para una empresa que incluye las reglas de comportamiento de usuarios y administradores y especifica los requisitos del sistema.

Estos objetivos, estas reglas y estos requisitos en conjunto garantizan la seguridad de una red, de los datos y de los sistemas informáticos de una organización.

Una política de seguridad completa logra varias tareas:

- Demuestra el compromiso de una organización con la seguridad.
- Establece las reglas para el comportamiento esperado.
- Garantiza la uniformidad en las operaciones del sistema, el software y la adquisición y uso de hardware, y el mantenimiento.
- Define las consecuencias legales de violaciones.
- Brinda al personal de seguridad el respaldo de la administración.

Las políticas de seguridad informan a los usuarios, al personal y a los gerentes los requisitos de una organización para proteger la tecnología y los activos de información.

ESTÁNDARES

Los estándares ayudan al personal de TI a mantener la uniformidad en el funcionamiento de la red.

Los documentos sobre estándares proporcionan las tecnologías que los usuarios o los programas específicos necesitan, además de los requisitos o criterios del programa que una organización debe seguir. Esto permite al personal de TI mejorar la eficiencia y simplicidad en el diseño, el mantenimiento y la resolución de problemas.

Uno de los principios de seguridad más importantes es el de uniformidad.

Por este motivo, es necesario que las organizaciones establezcan estándares.

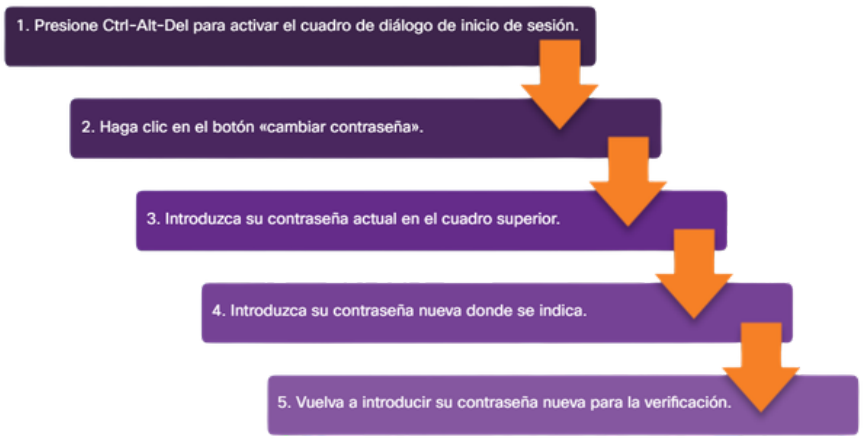
Cada organización desarrolla estándares para admitir el entorno operativo único.

PROCEDIMIENTOS

Los documentos de procedimiento son más detallados que los estándares.

Los documentos de procedimiento incluyen detalles de implementación que contienen generalmente instrucciones paso a paso y gráficos.

Las grandes organizaciones deben usar documentos de procedimientos para mantener la uniformidad de la implementación que se necesita para un entorno seguro.



Ejemplo:
Procedimiento para cambiar
Una contraseña.

CÓMO IMPLEMENTAR LA CAPACITACIÓN Y FORMACIÓN EN CIBERSEGURIDAD (PERSONAS)

Invertir mucho dinero en tecnología no variará si las personas dentro de la organización son el eslabón más débil en el área de ciberseguridad.

Un programa de reconocimiento de seguridad es sumamente importante, se puede implementar capacitación formal:

Este proceso debe ser continúo dado que las nuevas amenazas y técnicas están siempre.

NOTAS:

MÓDULO 5

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) – ISO/IEC 27001

¿QUÉ ES ISO/IEC 27001?

La norma ISO/IEC 27001 es la norma más conocida del mundo para sistemas de gestión de seguridad de la información (SGSI) . Define los requisitos que debe cumplir un SGSI.

La norma ISO/IEC 27001 proporciona a las empresas de cualquier tamaño y de todos los sectores de actividad orientación para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información.

¿POR QUÉ ES IMPORTANTE LA NORMA ISO/IEC 27001?

En vista del aumento de los delitos cibernéticos y la aparición constante de nuevas amenazas, puede resultar difícil o incluso imposible gestionar los riesgos cibernéticos. La norma ISO/IEC 27001 ayuda a las organizaciones a tomar conciencia de los riesgos y a identificar y abordar de forma proactiva las debilidades.

La norma ISO/IEC 27001 promueve un enfoque holístico de la seguridad de la información: examina a las personas, las políticas y la tecnología. Un sistema de gestión de la seguridad de la información implementado de acuerdo con esta norma es una herramienta para la gestión de riesgos, la ciberresiliencia y la excelencia operativa.

Beneficios

- Resiliencia ante los ciberataques
- Preparación para nuevas amenazas
- Integridad, confidencialidad y disponibilidad de los datos
- Seguridad en todos los soportes
- Protección de toda la organización
- Ahorro de costes

Este estándar se centra en orientar a las PYMES en el desarrollo e implementación de un sistema de gestión de seguridad de la información (SGSI) de acuerdo con la norma ISO/IEC 27001, con el fin de ayudarles a protegerse de los riesgos cibernéticos.

¿POR QUÉ ES IMPORTANTE EL CUMPLIMIENTO DE LA NORMA ISO 27001?

El cumplimiento de la norma ISO 27001 no es obligatorio para ninguna organización, las empresas pueden optar por lograr y mantener el cumplimiento de la norma ISO 27001 para demostrar que han implementado los controles y procesos de seguridad necesarios para proteger sus sistemas y los datos confidenciales en su posesión.

Cumplir con la norma ISO 27001 es importante como elemento diferenciador en el mercado y como base para cumplir con otros requisitos y normas obligatorios. Una organización que cumple con la norma ISO 27001 probablemente sea más segura que una que no la cumple, y la norma proporciona un marco sólido para desarrollar muchos de los controles de seguridad que exigen otras normativas.

El objetivo principal de la norma ISO 27001 es orientar a las organizaciones en la creación, implementación y aplicación de un SGSI. Este SGSI describe los controles, procesos y procedimientos que la empresa ha puesto en marcha para garantizar la confidencialidad, integridad y disponibilidad de los datos que posee.

Para cumplir con la norma ISO 27001, una organización debe tener una visibilidad profunda de su infraestructura de TI y de sus operaciones de seguridad. La empresa debe poder demostrar su capacidad para mapear y monitorear los flujos de datos dentro de su entorno y que cuenta con los controles de seguridad adecuados para proteger sus datos.

Para lograr el cumplimiento de la norma ISO 27001, una organización también debe documentar los pasos que se tomaron en el proceso de desarrollo del SGSI.

La documentación clave incluye:

- Alcance del SGSI
- Política de seguridad de la información
- Proceso y plan de evaluación de riesgos de seguridad de la información
- Objetivos de la seguridad de la información
- Evidencia de la competencia de las personas que trabajan en seguridad de la información
- Resultados de la evaluación y tratamiento de riesgos de seguridad de la información
- Programa de Auditoría Interna del SGSI y Resultados de las Auditorías Realizadas
- Evidencia de revisiones de liderazgo del SGSI
- Evidencia de no conformidades identificadas y resultados de acciones correctivas

¿CÓMO OBTENER LA CERTIFICACIÓN ISO 27001?

La certificación ISO 27001 requiere auditorías anuales por parte de un organismo de certificación ISO 27001 acreditado. Antes de someterse a una auditoría de terceros, una organización debe realizar una auditoría interna para medir su cumplimiento con las normas ISO 27001 y desarrollar un SGSI de acuerdo con la norma. Una vez que se ha generado la documentación necesaria y se han implementado los controles de seguridad requeridos, la empresa está preparada para contratar a un auditor externo.

La norma ISO 27001 define un conjunto de controles de auditoría que deben incluirse en un SGSI conforme.
Ejemplo de algunos controles que se deben incluir:

1. **Políticas de seguridad de la información:** Este control describe cómo se deben documentar y revisar las políticas de seguridad como parte del SGSI.
2. **Organización de la seguridad de la información:** Las responsabilidades de los roles son una parte importante de un SGSI. Este control desglosa las responsabilidades de seguridad en toda la organización, lo que garantiza que exista una responsabilidad clara para cada tarea.
3. **Seguridad de recursos humanos:** Este control aborda cómo se capacita a los empleados en ciberseguridad al iniciar y finalizar funciones dentro de una organización, incluida la incorporación, la salida y los cambios de puestos.
4. **Gestión de activos:** La seguridad de los datos es una preocupación principal de la norma ISO 27001. Este control se centra en la gestión del acceso y la seguridad de los activos que afectan la seguridad de los datos, incluidos el hardware, el software y las bases de datos.
5. **Control de acceso:** Este control analiza cómo una organización gestiona el acceso a los datos para protegerse contra el acceso no autorizado a datos confidenciales o valiosos.
6. **Criptografía:** El cifrado es una de las herramientas más poderosas para la protección de datos. Las empresas deberían implementar el cifrado de datos siempre que sea posible utilizando algoritmos criptográficos sólidos.
7. **Seguridad física y ambiental:** El acceso físico a los sistemas puede socavar los controles de seguridad digital. Este control se centra en proteger los edificios y equipos dentro de una organización.
8. **Seguridad de las operaciones:** La seguridad de las operaciones se centra en la forma en que la organización procesa y gestiona los datos. La organización debe tener visibilidad y control sobre los flujos de datos dentro de su entorno de TI.
9. **Seguridad de las comunicaciones:** Los sistemas de comunicación utilizados por una organización (correo electrónico, videoconferencia, etc.) deben cifrar los datos en tránsito y contar con fuertes controles de acceso.
10. **Adquisición, desarrollo y mantenimiento de sistemas:** Este control se centra en garantizar que los nuevos sistemas introducidos en el entorno de una organización no pongan en peligro la seguridad de la empresa y que los sistemas existentes se mantengan en un estado seguro.
11. **Relaciones con proveedores:** Las relaciones con terceros generan la posibilidad de ataques a la cadena de suministro. Un SGSI debe incluir controles para realizar un seguimiento de las relaciones y gestionar el riesgo de terceros.

12. **Gestión de incidentes de seguridad de la información:** La empresa debe tener procesos establecidos para detectar y gestionar incidentes de seguridad.
13. **Aspectos de seguridad de la información en la gestión de la continuidad del negocio:** Además de los incidentes de seguridad, la empresa debe estar preparada para gestionar otros eventos (como incendios, cortes de energía, etc.) que podrían afectar negativamente la seguridad.
14. **Cumplimiento:** Como parte del cumplimiento de la norma ISO 27001, la organización debe poder demostrar el pleno cumplimiento de otras regulaciones obligatorias a las que está sujeta la organización.

NOTAS:

MÓDULO 6

CONTROLES DE SEGURIDAD EFECTIVOS (ISO/IEC 27002)

¿QUÉ ES ISO/IEC 27002?

La norma ISO/IEC 27002 es una norma internacional que proporciona orientación a las organizaciones que buscan establecer, implementar y mejorar un sistema de gestión de seguridad de la información (SGSI) centrado en la ciberseguridad.

Mientras que la norma ISO/IEC 27001 describe los requisitos para un SGSI, la norma ISO/IEC 27002 ofrece las mejores prácticas y objetivos de control relacionados con aspectos clave de la ciberseguridad, incluidos el control de acceso, la criptografía, la seguridad de los recursos humanos y la respuesta a incidentes.

La norma sirve como modelo práctico para las organizaciones que buscan salvaguardar eficazmente sus activos de información contra las amenazas cibernéticas. Al seguir las pautas de la norma ISO/IEC 27002, las empresas pueden adoptar un enfoque proactivo para la gestión de riesgos de ciberseguridad y proteger la información crítica del acceso no autorizado y la pérdida.

¿POR QUÉ ES IMPORTANTE LA NORMA ISO/IEC 27002?

El panorama digital en rápida evolución ha traído consigo oportunidades sin precedentes para las empresas, pero también ha introducido una gran cantidad de vulnerabilidades y amenazas.

La norma ISO/IEC 27002 surge como una herramienta crucial en este contexto, ayudando a las organizaciones a navegar por la intrincada red de desafíos de seguridad de la información. Equipa a las empresas con un marco probado y comprobado de mejores prácticas, asegurando que no solo protejan sus datos confidenciales, sino que también fomenten la confianza entre las partes interesadas, los clientes y los socios.

BENEFICIOS:

- **Marco de seguridad integral:** proporciona un conjunto detallado de pautas y mejores prácticas que cubren diversas dimensiones de la seguridad de la información.
- **Gestión de riesgos:** permite a las organizaciones identificar, evaluar y gestionar eficazmente los riesgos de seguridad de la información.
- **Mayor confianza de las partes interesadas:** demuestra un compromiso con la protección de datos confidenciales, lo que refuerza la credibilidad de la organización.
- **Cumplimiento normativo:** ayuda a cumplir con diversos mandatos legales, contractuales y reglamentarios de protección de datos.
- **Resiliencia operativa:** reduce la probabilidad de incidentes de seguridad que puedan interrumpir las operaciones comerciales.
- **Ventaja competitiva:** en un mercado impulsado por datos, tener una postura sólida en materia de seguridad de la información puede diferenciar a una organización de sus competidores.

¿QUIÉN DEBERÍA ADOPTAR LA NORMA ISO/IEC 27002?

Cualquier organización, independientemente de su tamaño o industria, que busque reforzar su marco de seguridad de la información, particularmente aquellas que tienen o están buscando la certificación ISO/IEC 27001.

¿CÓMO SE RELACIONA LA NORMA ISO/IEC 27002 CON LA NORMA ISO/IEC 27001?

Cualquier organización, independientemente de su tamaño o industria, que busque reforzar su marco de seguridad de la información, particularmente aquellas que tienen o están buscando la certificación ISO/IEC 27001.

¿LA NORMA ISO/IEC 27002 CONDUCE A LA CERTIFICACIÓN?

No , la norma ISO/IEC 27002 ofrece recomendaciones de mejores prácticas y no se puede certificar según ella. Sin embargo, las organizaciones pueden obtener la certificación según la norma ISO/IEC 27001, que hace referencia a las directrices de la norma ISO/IEC 27002.

¿LA NORMA ISO/IEC 27002 CONDUCE A LA CERTIFICACIÓN?

Sí , la norma abarca una amplia gama de temas de seguridad de la información, incluidos aquellos relacionados con las amenazas y vulnerabilidades de la ciberseguridad.

EXPLICACIÓN DEL ISO/IEC 27002:2013

El estándar ISO 27000 está representado por dominios independientes. Los cuales proporcionan la base para desarrollar estándares de seguridad y prácticas efectivas de administración de la seguridad dentro de las organizaciones, además de ayudar a facilitar la comunicación entre las organizaciones.

Los dominios están formados por objetivos de control (ISO 27001) y controles (ISO 27002).

Por ejemplo...

Los objetivos de control definen los requisitos de alto nivel para implementar un sistema integral de administración de seguridad de la información dentro de una organización, y generalmente proporcionan una lista de verificación para usar durante una auditoría de SGSI.

Pasar esta auditoría indica que una organización cumple con la norma ISO 27001 y les brinda a los socios confianza en la seguridad de los datos y en las operaciones de la organización.

Por ejemplo...

Los controles establecen cómo lograr los objetivos de control de una organización. Establecen pautas para implementar, mantener y mejorar la administración de la seguridad de la información en una organización.

Un ejemplo de la combinación y cumplimiento de las normas ISO 27001 e ISO 27002

Un objetivo de control de una organización es controlar el acceso a las redes usando mecanismos de autenticación adecuados para los usuarios y los equipos. (27001)

Un control relevante, por lo tanto, es utilizar contraseñas seguras que consten de al menos ocho caracteres y una combinación de letras mayúsculas y minúsculas, números y símbolos. (27002)

El estándar en la actualidad cuenta con 93 controles (ISO/IEC 27002:2022)

EJEMPLOS DE 4 OBJETIVOS DE CONTROL CON SU RESPECTIVO CONTROL DEL ISO 27OO2

Para evitar el acceso no autorizado a los sistemas y aplicaciones
El acceso estará restringido de acuerdo con una política de control de acceso.
Para evitar la explotación de vulnerabilidades del software
Se establecerán e implementarán reglas sobre la instalación de software por parte de los empleados.
Para garantizar un enfoque coherente y eficaz para la administración de incidentes de seguridad de la información
Los empleados deberán informar cualquier debilidad de seguridad de la información observada o sospechada.
Para evitar la pérdida, el daño, el robo o el compromiso de datos confidenciales
Se implementará una política de escritorio limpio

NOTAS:

MÓDULO 7

ASPECTO ORGANIZACIONAL PARA GESTIONAR LA SEGURIDAD (GOBERNANZA)

ASPECTO ORGANIZACIONAL PARA GESTIONAR LA SEGURIDAD DE LA INFORMACIÓN (GOBERNANZA)

La gobernanza es un tema importante en la ciberseguridad, ya que describe las políticas y los procesos vigentes dentro de una organización que definen las responsabilidades por la aplicación y la rendición de cuentas para mitigar el riesgo cibernético. Estos deben alinearse con las regulaciones clave como el ISO/IEC 27001 e ISO/IEC 27002.

Como profesionales de la ciberseguridad, deben tener conocimiento de las diferentes leyes que regulan la seguridad de la información, la ciberseguridad y la privacidad para garantizar el cumplimiento de la organización. Y no olvidemos su obligación ética de hacer siempre lo correcto.

Una política de ciberseguridad es un documento de alto nivel que describe la visión de una organización para la ciberseguridad, incluidos sus objetivos, necesidades, alcance y responsabilidades.

Se puede tomar como referencia el ISO 27001 (SGSI) y debe incluir:

- El compromiso de una organización con la seguridad.
- Establecer los estándares de comportamiento y requisitos de seguridad para llevar a cabo actividades, procesos y operaciones, y proteger los activos de tecnología e información dentro de una organización.
- Garantizar que la adquisición, el uso, el mantenimiento de la operación del sistema, software y hardware sean consistentes dentro de la organización.
- Definir las consecuencias legales de las violaciones a las políticas.
- Brindar al equipo de seguridad el soporte que necesitan de la alta gerencia.

Una organización debe establecer políticas de seguridad claras y detalladas que todos los empleados conozcan.

Por ejemplo:

Política de identificación y autenticación

Especifica quién debe tener acceso a los recursos de red y qué procedimientos de verificación existen para facilitar esto.

Política de contraseñas

Definir los requisitos mínimos de contraseña, como la cantidad y el tipo de caracteres utilizados y la frecuencia con la que deben cambiarse.

Política de uso aceptable

Destaca un conjunto de reglas que determinan el acceso y el uso de los recursos de red. También puede definir las consecuencias de infringir las políticas.

Política de acceso remoto

Establece cómo conectarse de forma remota a la red interna de una organización y explica qué información es accesible de forma remota.

Política de mantenimiento de la red

Describir los procedimientos para actualizar los sistemas operativos y las aplicaciones de usuario final de una organización.

Política de manejo de incidentes

Proporciona orientación sobre cómo reportar y responder a incidentes relacionados con la seguridad dentro de una organización.

Política de datos

Establece reglas mensurables para procesar datos dentro de una organización, como especificar dónde se almacenan los datos, cómo se clasifican los datos (alto, medio, bajo, confidencial, público o privado) y cómo se manejan y eliminan los datos.

Política de contraseñas

Aplique las reglas para crear credenciales, como la longitud mínima y máxima de una contraseña, 1 mayúscula, un símbolo y 1 número.

NOTAS:

MÓDULO 8

ASPECTO PERSONAL DE CONCIENTIZACIÓN EN SEGURIDAD

¿ERES EL ESLABÓN MÁS DEBIL O MÁS FUERTE EN TU EMPRESA?, DEPENDE DE TI

MALWARE

Se refiere al software malicioso. Es una de las ciberamenazas más comunes, que un cibercriminal o un hacker ha creado para interrumpir o dañar el equipo de un usuario. Con frecuencia el malware se propaga a través de un archivo adjunto de correo electrónico no solicitado o de una descarga de apariencia legítima y el objetivo de un malware es ganar dinero o realizar ciberataques que dañen a las empresas o personas en beneficio de los cibercriminales o hackers.

Hay diferentes tipos de malware, entre los que se incluyen los siguientes:

- **Virus:** un programa capaz de reproducirse, que se incrusta un archivo limpio y se extiende por todo el sistema informático e infecta a los archivos con código malicioso.
- **Spyware:** un programa que registra en secreto lo que hace un usuario para que los cibercriminales puedan hacer uso de esta información. Por ejemplo, el spyware podría capturar los detalles de las tarjetas de crédito.
- **Ransomware:** malware que bloquea los archivos y datos de un usuario, con la amenaza de borrarlos, a menos que se pague un rescate.
- **Adware:** software de publicidad que puede utilizarse para difundir malware.
- **Botnets:** redes de computadoras con infección de malware que los cibercriminales utilizan para realizar tareas en línea sin el permiso del usuario.

INGENIERÍA SOCIAL

Los ataques utilizan trucos, coerción y otras formas de manipulación psicológica para lograr que el objetivo haga lo que el atacante quiere. Algunos ejemplos de tácticas comunes de ingeniería social incluyen:

- **Phishing:** Los ataques de phishing utilizan técnicas de ingeniería social para intentar engañar al destinatario para que realice una acción que beneficie al atacante. Los mensajes de phishing (enviados por correo electrónico, redes sociales, aplicaciones de comunicaciones corporativas u otras plataformas de mensajería) generalmente están diseñados para engañar a un objetivo para que haga clic en un enlace malicioso, abra un archivo adjunto malicioso o entregue información confidencial, como credenciales de inicio de sesión, sus datos de tarjetas de crédito y otra información personal.
- **Vishing:** Los ataques de vishing utilizan muchas de las mismas técnicas que el phishing, pero se realizan por teléfono. El atacante intenta que el objetivo realice alguna acción o entregue datos confidenciales, como la información de la tarjeta de pago o las credenciales de inicio de sesión.

La determinación de los controles depende de las decisiones de la organización tras una evaluación de los riesgos enfocado en el aspecto de las personas o el personal en caso de ser una Empresa, con un alcance claramente definido. Las decisiones relacionadas con los riesgos identificados deberían basarse en los criterios de aceptación de los riesgos, las opciones de tratamiento de riesgos y el enfoque de gestión de riesgos aplicado por la organización.

Algunos elementos en los que se pueden implementar controles del ISO/IEC 27002

- Términos y condiciones de contratación
- Concienciación, educación y formación en SI
- Acuerdos de confidencialidad o no divulgación
- Teletrabajo
- Notificación de eventos de SI

Concienciación, Educación y Formación en SI

EJEMPLO

- Amenaza: Ataque de ingeniería social a los usuarios
- Vulnerabilidad: XSS en el sitio de registro de usuarios
- Riesgo: Ataque de ingeniería social a los usuarios mediante una explotación XSS en el sitio de registros de usuarios
- Ocurrencia e impacto: Poco probable, Impacto crítico
- Resultado: Es poco probable que nuestros usuarios sufran un ataque de ingeniería social mediante la explotación de la vulnerabilidad XSS que hay en el sitio de registros de usuarios, pero de ocurrir, sería un impacto crítico.

CONTROL A IMPLEMENTAR:

Todo el personal debe ser continuamente evaluado con ejercicios de conciencia de seguridad:

- Campañas de phishing
- Exámenes

De igual forma, se tienen que brindar cursos y pláticas de concientización para que los empleados entiendan los riesgos y cómo prevenirlos.

CONTROL A IMPLEMENTAR:

El personal de la organización y las partes interesadas pertinentes deberían recibir una adecuada concienciación, educación y formalización sobre la seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, y de las políticas y los procedimientos específicos, según corresponda a su puesto de trabajo.

NOTAS:

MÓDULO 9

ASPECTO DE INSTALACIONES FÍSICAS

ASPECTO DE INSTALACIONES FÍSICAS PARA SALVAGUARDAR ESPACIOS DE ACTIVOS DE INFORMACIÓN.

La determinación de los controles depende de las decisiones de la organización tras una evaluación de los riesgos enfocado en el aspecto de las instalaciones físicas, con un alcance claramente definido. Las decisiones relacionadas con los riesgos identificados deberían basarse en los criterios de aceptación de los riesgos, las opciones de tratamiento de riesgos y el enfoque de gestión de riesgos aplicado por la organización.

ALGUNOS ELEMENTOS EN LOS QUE SE PUEDEN IMPLEMENTAR CONTROLES DEL ISO/IEC 27002

- **Controles físicos de entrada**

Propósito: Garantizar que sólo se produce el acceso físico autorizado a la información de la organización y a otros activos asociados.
Control: Las áreas seguras deberían estar protegidas por controles de entrada y puntos de acceso adecuados.

- **Seguridad de oficinas y centro de datos**
- **Monitorización de la seguridad física**

Propósito: Detectar e impedir el acceso físico no autorizado.
Control: Las instalaciones deberían ser monitorizadas continuamente para detectar cualquier acceso físico no autorizado.

- **Seguridad del cableado**

Propósito: Evitar la pérdida, daño, robo o compromiso de información y otros activos asociados y la interrupción de las operaciones de la organización relacionadas con el cableado de energía y comunicaciones.

Control: Protección El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debería estar protegido frente a interceptaciones, interferencias o daños.

Se debe considerar lo siguiente:

SEPARAR LOS CABLES DE ENERGÍA DE LOS CABLES DE COMUNICACIONES PARA EVITAR INTERFERENCIAS.

- Accesos controlados a los paneles de conexión y a las salas de cableado (por ejemplo, con llaves mecánicas o claves PINs).

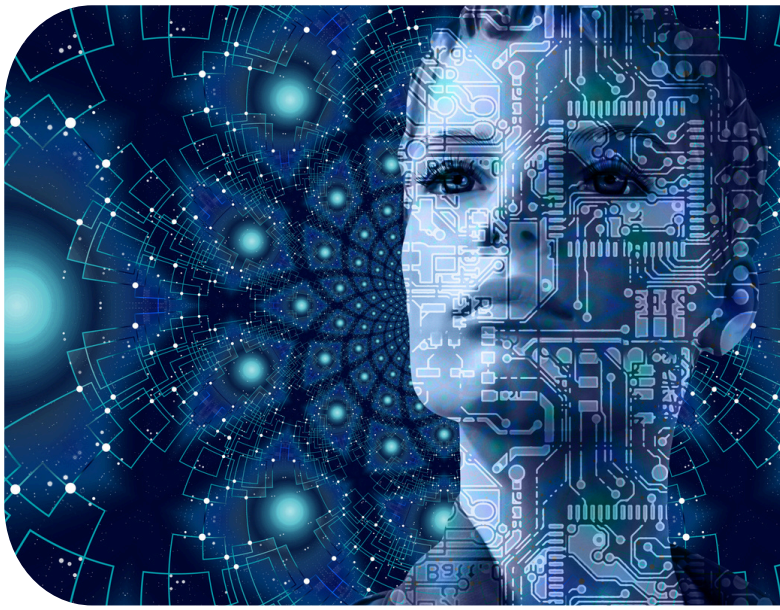
- Etiquetar los cables en cada extremo con suficientes indicaciones de origen y destino para permitir la identificación física y la inspección del cable.

- Mantenimiento de los equipos.

NOTAS:

MÓDULO 10

ASPECTO TECNOLÓGICO HERRAMIENTAS Y MEDIDAS TÉCNICAS



ASPECTO DE TECNOLOGÍAS (SISTEMAS, REDES, SOFTWARE Y HARDWARE UTILIZADOS PARA PROCESAR, ALMACENAR Y TRANSMITIR INFORMACIÓN).

La determinación de los controles depende de las decisiones de la organización tras una evaluación de los riesgos enfocado en el aspecto de las tecnologías, con un alcance claramente definido.
Las decisiones relacionadas con los riesgos identificados Deberían basarse en los criterios de aceptación de los riesgos, las opciones de tratamiento de riesgos y el enfoque de gestión de riesgos aplicado por la organización.

ALGUNOS ELEMENTOS EN LOS QUE SE PUEDEN IMPLEMENTAR CONTROLES DEL ISO/IEC 27002, AUNQUE EL ESTÁNDAR TIENE 34

- **Autenticación segura**

Control: Las tecnologías y procedimientos de autenticación segura deberían implementarse en función de las restricciones de acceso a la información y la política específica sobre control de acceso.
Propósito: Garantizar que un usuario o una entidad esté autenticado de forma segura cuando se le concede acceso a los sistemas, aplicaciones y servicios.
Guía:

- Debería elegirse una técnica de autenticación adecuada para justificar la identidad reivindicada de un usuario, software, mensajes y otras entidades.

- La solidez de la autenticación debería ser adecuada de acuerdo con la clasificación de la información a la que se va a acceder.

- Cuando se requiera una autenticación y verificación de identidad sólidas, deberían utilizarse métodos de autenticación alternativos a las contraseñas, tales como certificados digitales, tarjetas inteligentes, dispositivos o medios biométricos.

- La información de autenticación debería ir acompañada de factores de autenticación adicionales para acceder a los sistemas de información críticos (conocida también como autenticación multifactorial).

- El uso de una combinación de factores múltiples de autenticación, algo que sabes, algo que tienes y que eres, reduce las posibilidades de accesos no autorizados.

- La autenticación multifactorial se puede combinar con otras técnicas para requerir factores adicionales en circunstancias específicas, basadas en reglas y patrones predefinidos, como el acceso desde una ubicación inusual, a través de un dispositivo inusual o en un momento inusual.

- La información utilizada para la autenticación biométrica debería invalidarse si alguna vez se ve comprometida.

- La autenticación biométrica puede no estar disponible dependiendo de las condiciones de uso (por ejemplo, humedad o envejecimiento).

- Para anticiparse a estos problemas y estar preparados, la autenticación biométrica debería ir acompañada de, al menos, una técnica de autenticación alternativa.

- El procedimiento para iniciar sesión en un sistema o aplicación debería diseñarse para minimizar el riesgo de acceso no autorizado.

- Los procedimientos y tecnologías de inicio de sesión deberían implementarse teniendo en cuenta lo siguiente:

- Mostrar un aviso general advirtiendo que el acceso al sistema, a la aplicación o al servicio solo debería ser efectuado por aquellos usuarios autorizados;

- Validar la información de inicio de sesión sólo cuando estén completos todos los datos de entrada requeridos.

- **Controles contra el código malicioso**

Control: Se debería implementar una protección contra el código malicioso, respaldada por una concienciación adecuada al usuario.
Propósito: Garantizar que la información y otros activos asociados estén protegidos contra el código malicioso.

Guía:
La protección contra el código malicioso debería basarse en software de detección y reparación de código dañino, concienciación sobre la seguridad de la información, acceso adecuado al sistema y controles de gestión de cambios.

El uso de software de detección y reparación de código malicioso por sí solo no suele ser adecuado.

Deberían considerar las siguientes orientaciones:

a) implementar normas y controles que impidan o detecten el uso de programas informáticos no autorizados [por ejemplo, listas de aplicaciones permitidas (es decir, utilizando una lista que proporcione aplicaciones permitidas)]

b) implementar controles que impidan o detecten el uso de sitios web maliciosos conocidos o sospechosos (por ejemplo, listas de bloqueo);

c) reducir las vulnerabilidades que pueden ser explotadas por el código malicioso [por ejemplo, a través de la gestión de vulnerabilidades técnicas

- Eliminación de la información
- Copias de seguridad de la información
- Seguridad en redes

Control: Las redes y los dispositivos de red deberían ser securizados, gestionados y controlados para proteger la información en los sistemas y aplicaciones.

Propósito: Garantizar la seguridad en el uso de los servicios de red y de sus instalaciones de tratamiento de la información de apoyo frente a riesgos a través de la red.
Orientación: Deberían aplicarse controles para garantizar la seguridad de la información en las redes y proteger los servicios conectados del acceso no autorizado.

En particular, deberían tenerse en cuenta los siguientes puntos:
a) el tipo y nivel de clasificación de la información que la red puede soportar;

b) establecer responsabilidades y procedimientos para la gestión de equipos y dispositivos de red;

c) mantener la documentación actualizada, incluidos los diagramas de red y los archivos de configuración de los dispositivos (por ejemplo, enrutadores, conmutadores).

d) separar la responsabilidad operativa de las redes de las operaciones de los sistemas de TIC cuando proceda

e) establecer controles para salvaguardar la confidencialidad e integridad de los datos que pasan por redes públicas, redes de terceros o redes inalámbricas y para proteger las redes y aplicaciones conectadas. También pueden exigirse controles adicionales para mantener la disponibilidad de los servicios de red y los ordenadores conectados a la red;

f) el registro y el seguimiento adecuados para permitir el registro y la detección de acciones que puedan afectar o sean pertinentes a la seguridad de la información;

g) coordinar estrechamente las actividades de gestión de la red, tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de información.

h) autenticación de los sistemas en la red;

i) restringir y filtrar la conexión de los sistemas a la red (por ejemplo, utilizando firewalls); detectar, restringir y autenticar la conexión de equipos y dispositivos a la red.

j) bastionado de los dispositivos de red;

k) segregar los canales de administración de red de otros tráficos de red;

l) aislar temporalmente subredes críticas (por ejemplo, con puentes levadizos) si la red está bajo ataque;

m) desactivación de protocolos de red vulnerables.

ACTUALIZACIÓN FAMILIA ISO/IEC 27000

Cuando la Organización Internacional de Normalización (ISO) publicó una nueva versión de la norma ISO/IEC 27001 en 2022, los equipos de cumplimiento se preguntaron: **¿Cuál es la diferencia entre la norma ISO/IEC 27001:2013 y la ISO/IEC 27001:2022?**

Dado que la fecha límite para la transición se acerca rápidamente, las empresas deben asegurarse de que su certificación ISO 27001 esté actualizada.
Las organizaciones con certificación ISO 27001:2013 deben migrar a la versión 2022 antes del 31 de octubre de 2025.

La norma ISO 27001:2022 es una actualización moderada de la versión anterior de la norma: ISO 27001:2013. La mayor parte de los cambios se relacionan con los controles de los Anexos, ya que las actualizaciones se centraron en modernizarlos y alinearlos mejor con los estándares actuales de la industria.
Los controles de los Anexos se han agrupado de forma diferente, se han añadido nuevos controles de los Anexos y otros se han fusionado o renombrado.

Las empresas certificadas con la versión anterior, ISO 27001:2013, tienen como fecha límite el 31 de octubre de 2025 para completar su transición a la nueva versión.

La actualización más reciente de la familia ISO 27000 son las normas ISO/IEC 27001:2022 y ISO/IEC 27002:2022, publicadas en octubre y febrero de 2022, respectivamente.

¿CUÁL ES LA DIFERENCIA ENTRE ISO 27001:2022 E ISO 27001:2013?

CAMBIOS CLAVE EN ISO/IEC 27001:2022

- **Estructura y cláusulas:**

La estructura de la norma no ha cambiado, por lo que las cláusulas 4 a 10 siguen siendo la base para la auditoría de conformidad.

- **Enfoque en riesgos:**

Se mantiene el enfoque en la gestión de riesgos de seguridad de la información.

- **Controles:**

La norma ISO 27002:2022, la guía de implementación de los controles, ha sido actualizada. Esta versión agrupa los 93 controles en cuatro categorías: organizacionales, de personal, físicos y tecnológicos.

CAMBIOS CLAVE EN ISO/IEC 27001:2022

- **Ampliación del alcance:**

El alcance se ha ampliado para incluir la ciberseguridad y la protección de la privacidad, además de la seguridad de la información tradicional.

- **Nuevo nombre:**

El título de la norma ha cambiado de "Código de prácticas para controles de seguridad de la información" a "Seguridad de la información, ciberseguridad y protección de la privacidad – Controles de seguridad de la información".

- **Reorganización de controles:**

Anteriormente eran 14 dominios con 114 controles.
La norma de 2022 ha reorganizado y fusionado algunos controles de la versión anterior, introduciendo a su vez controles nuevos y otros modificados.

PLAZOS Y CONSIDERACIONES

- **Transición para organizaciones certificadas:**

Las organizaciones con certificación ISO 27001:2013 deben migrar a la versión 2022 antes del 31 de octubre de 2025.

- **Auditorías:**

Las auditorías de certificación y acreditación correspondientes a la edición 2022 comenzaron a realizarse desde el 1 de noviembre de 2023.

- **Nuevas certificaciones:**

Las organizaciones que soliciten la certificación por primera vez deben hacerlo con la versión 2022.

TALENTO

IMPULSAMOS LAS HABILIDADES DE TU EMPRESA

CONTÁCTANOS

mastalentoacademia.com

contacto@mastalentoacademia.com

Guadalajara, Jal.