¿A qué nos referimos con seguridad de la información?

¿Qué es la seguridad de la información?

La seguridad de la información (InfoSec) es la protección de la información importante contra el acceso, la divulgación, el uso, la alteración o la interrupción no autorizados. Ayuda a garantizar que los datos confidenciales de la organización estén disponibles para los usuarios autorizados, permanezcan confidenciales y mantengan su integridad.

La seguridad de la información en este contexto representa una rama de la ciberseguridad cuyos objetivos principales son tres: Mantener la confidencialidad, integridad y disponibilidad de los datos de un individuo u organización.

Los términos **seguridad de la información**, **seguridad informática**, **ciberseguridad** y **la seguridad de los datos** se usan a menudo (y erróneamente) indistintamente. Si bien estos campos se superponen y se informan entre sí, difieren principalmente en su alcance.

- **La seguridad de la** información es un término general que engloba los procesos de una organización por proteger la información. Incluye seguridad física de activos de TI, seguridad de endpoints, cifrado de datos, seguridad de red y más.
- **La seguridad de TI** también se ocupa de proteger los activos de TI físicos y digitales y los centros de datos, pero no incluye la protección para el almacenamiento de archivos en papel y otros medios. Se centra en los activos tecnológicos más que en la información en sí.
- **La ciberseguridad** se centra en proteger los sistemas de información digital. El objetivo es ayudar a proteger los datos y activos digitales de las amenazas cibernéticas. Si bien es una tarea enorme, la ciberseguridad tiene un alcance limitado, ya que no se preocupa por proteger los datos en papel o analógicos.
- **La seguridad de los datos** es la práctica de proteger la información digital del acceso no autorizado, la corrupción o el robo a lo largo de todo su ciclo de vida. Incluye la seguridad física del hardware y los dispositivos de almacenamiento, junto con controles administrativos y de acceso. También cubre la seguridad lógica de las aplicaciones de software y las políticas y procedimientos organizacionales.

¿Cuáles son las principales amenazas a nuestros datos?

La exposición a la red es una de los principales factores que afectan la seguridad de la información. Esto principalmente debido a que las características del ciberespacio lo han convertido en el lugar ideal para ejecutar ataques de todo tipo.

La tríada CIA

Sugerida por primera vez por el Instituto Nacional de Estándares y Tecnología (NIST) de EE.UU. en 1977, la tríada CIA tiene como objetivo guiar a las organizaciones en la elección de tecnologías, políticas y prácticas para proteger sus sistemas de información. Los elementos de la tríada de la CIA incluyen:

- **Confidencialidad**
- **Integridad**
- **Disponibilidad**

1 | Objetivos de la seguridad informática: Confidencialidad

El primer pilar de los **objetivos de la seguridad informática** es la confidencialidad. Este se encarga de que los datos ingresados a un sistema no se divulguen públicamente. Con esto en mente, utilizan distintas estrategias que garantizan que ninguna persona sin autorización pueda acceder a ellos. Algunos de estos métodos pueden ser

- **Encriptación**: Esta metodología transforma la información mediante un algoritmo. Cuenta con dos claves. Una de cifrado y otra de descifrado. Solo aquellos **usuarios autorizados** que cuentan con la última clave pueden acceder al mismo.
- **Control de Acceso**: Estos controles forman parte de una **política de seguridad** para el acceso al sistema. A aquellos **usuarios autorizados** se les otorga una credencial intransferible. Es importante destacar que no todos poseen los mismos privilegios o libertades para circular por las redes de un sistema.
- **Autentificación**: El proceso de autentificación confirma la identidad de una persona para que este ingrese a las TI de una organización. Entre las formas más empleadas están las credenciales, las huellas dactilares, o claves.
- **Autorización**: Esta estrategia de los **objetivos de la seguridad informática** acepta o deniega el permiso a un usuario para hacer o tener algo. Esto se decide mediante una política de control de acceso y la autentificación de la identidad.

2 | Objetivos de la seguridad informática: Integridad

El segundo pilar de los **objetivos de la seguridad informática** es la integridad. Esta es necesaria para **garantizar que los datos** sean reales, precisos y correctos. Su objetivo es impedir que la información sea vulnerada de manera no autorizada.

- **Copias de seguridad**: Estas copias, o también backups, se encargan de generar un respaldo periódico de todos los datos de una organización en caso de que estos se pierdan, se destruyan o los modifiquen sin autorización previa por una fuente no legítima.
- **Sumas de comprobación**: Mediante este código se le otorga un valor numérico al contenido de un archivo mediante el cálculo de una función. Esto sirve para asegurar que dos conjuntos de datos sean iguales
- **Códigos de corrección de datos**: Con esta estrategia se pueden identificar hasta los mínimos cambios en un bloque de datos.

3 | Objetivos de la Seguridad Informática: Disponibilidad

El tercer, y último pilar de los o**bjetivos de la seguridad informática**, es la disponibilidad. Ella nos asegura que nuestros datos están disponibles en el momento oportuno para que podamos hacer uso de ella. Siempre y cuando, seas una de las **personas autorizadas a acceder**, claro.

- Protecciones físicas: Con esto nos aseguramos que la información crítica esté resguardada en lugares seguros.
- Redundancias computacionales. Esta estrategia nos protege contra fallas involuntarias o accidentales. Deja a buen resguardo los dispositivos de almacenamiento de respaldo.

Parte 1: Estudio guiado por temas

Unidad Temática 1: Conceptos Generales

1. **Definición de Seguridad de la Información**:
    - Es la protección de la información importante contra el **acceso, la divulgación, el uso, la alteración o la interrupción** no autorizados. Ayuda a garantizar que los datos confidenciales de la organización estén **disponibles** para los usuarios autorizados, permanezcan **confidenciales** y mantengan su **integridad.**
2. **Objetivos de la Seguridad de la Información** (Tríada CIA):
    - **Confidencialidad**: solo usuarios autorizados acceden a la información.
        - **Encriptación.**
        - **Control de Acceso.**
        - **Autentificación**.
        - **Autorización.**
    - **Integridad**: la información no ha sido modificada sin autorización.
        - **Copias de seguridad.**
        - **Sumas de comprobación.**
        - **Códigos de corrección de datos.**
    - **Disponibilidad**: los usuarios autorizados pueden acceder cuando lo necesiten.
        - **Protecciones físicas.**
        - **Redundancias computacionales.**
3. **Importancia**:
    - Evita pérdidas económicas, daño reputacional.
    - Protege activos críticos.
    - Favorece el cumplimiento legal.
4. **Mejores prácticas**:
    - VPN.
    - Limitar el número de usuarios conectados.
    - Asignar perfiles de usuarios.
    - Firewalls.

- Políticas en el manejo de contraseñas.
- Políticas de seguridad deben estar respaldadas y divulgadas.
- Uso de contraseñas robustas.
- Mantenimiento actualizado del software.
- Copias de seguridad frecuentes.
- Formación del personal.

Unidad Temática 2: Análisis, Evaluación y Gestión de Riesgos

1. **¿Qué es un riesgo en seguridad informática?**
    - Es la probabilidad de que una amenaza aproveche una vulnerabilidad para causar daño.
2. **Evaluación de riesgos**:
    - **Identificar** activos y su valor.
    - **Detectar** amenazas y vulnerabilidades.
    - **Evaluar** probabilidad e impacto.
    - **Gestión**: mitigación, transferencia, aceptación o evitación.
3. **Guía práctica**:
    - Crear inventario de activos.
    - Evaluar amenazas (hackers, errores humanos, fallos técnicos).
    - Determinar el impacto de un incidente.
4. **Importancia:**

- Permite asignar recursos eficientemente.
- Anticipa incidentes y prepara respuestas.
- Es base para implementar normas como ISO 27001.

Unidad Temática 3: ISO/IEC 27001

1. **¿Qué es?**
    - Estándar Internacional certificable que establece los **requisitos formales** para implementar un **Sistema de Gestión de Seguridad de la Información (SGSI)**.
2. **Objetivo:**

    Lograr un nivel adecuado de seguridad para garantizar continuidad de la organización, minimizando el riesgo.
3. **Características clave**:
    - Basada en análisis de riesgos.
    - Mejora continua con enfoque PDCA (Plan-Do-Check-Act).
    - Requiere políticas, controles, auditoría interna, y correctivas.
4. **Implementación**:
    - Establecer políticas.
    - Evaluar riesgos.
    - Diseñar controles.
    - Monitorear y mejorar.
    - Roles y responsabilidades claras.

Unidad Temática 4: ISO/IEC 27002

1. **¿Qué es?**
    - Complemento de ISO/IEC 27001: Es una **guía no certificable** que **describe cómo implementar** los controles de seguridad sugeridos en la ISO 27001.
2. **Diferencias con ISO/IEC 27001**:
    - 27001 = define requisitos.
    - 27002 = proporciona la **guía práctica** para implementar controles.
3. **Dominios** (algunos ejemplos):
    - Política de seguridad.

- Seguridad física.
- Control de accesos.
- Gestión de incidentes.
- Continuidad del negocio.

4. **Enfoque:**

- Centrado en proteger los activos y datos de forma integral.
- Adaptable a organizaciones de cualquier tipo o tamaño.

Unidad Temática 5: Implantación de SGSI

1. **¿Qué es un SGSI?**
   - Conjunto de políticas, procesos, auditorías y prácticas que permiten proteger la información y responder ante incidentes.
2. **Objetivo**:
   No busca **máxima seguridad**, sino **el nivel de seguridad adecuado** según el apetito de riesgo y los recursos de la organización.
3. **Componentes clave**:
   - Política SGSI.
   - Clasificación de activos.
   - Controles, procesos, KPIs.
   - Revisión por la alta dirección.
4. **Beneficios**
   - Protección de datos confidenciales.
   - Cumplimiento normativo.
   - Reducción de costos.
   - Cultura organizacional proactiva.
   - Continuidad del negocio.
   - Adaptación a nuevas amenazas.
   - Proteger activos.
   - Ganar confianza de clientes.

5. **Pasos de implementación** de un **SGSI**
    1. **Crear la política SGSI**
        - Define por qué la empresa necesita un SGSI, sus objetivos, alcance y quién lo liderará.
    2. **Identificar y clasificar los activos**
        - ¿Qué datos se deben proteger? Por ejemplo: datos financieros, información de clientes, reportes internos.
    3. **Evaluar riesgos**
        - ¿Qué amenazas y vulnerabilidades existen? ¿Cuál sería su impacto?
    4. **Diseñar controles de seguridad**
        - Por ejemplo: cifrado de datos, firewalls, capacitación del personal, autenticación en dos pasos.
    5. **Implementar y operar el SGSI**
        - Poner en práctica los procesos y controles. Documentar todo.
    6. **Medir resultados con KPIs**
        - ¿Está funcionando el SGSI? ¿Se han reducido incidentes?
    7. **Corregir y mejorar continuamente**
        - Realizar ajustes con base en auditorías e incidentes ocurridos.
    8. **Revisión por la gerencia**
        - La alta dirección debe evaluar si se están cumpliendo los objetivos.
6. **Factores de éxito:**
    1. **Compromiso de la gerencia**: si los líderes no apoyan, el sistema fracasa.
    2. **Competencia del equipo implementador**: deben conocer ISO 27001 y gestión de riesgos.
    3. **Capacitación y cultura de seguridad** en todos los empleados.

¿Qué es un SGSI, cuál es su objetivo y por qué no busca alcanzar la máxima seguridad posible?

Un SGSI es un sistema estructurado que permite proteger los activos de información mediante políticas, procedimientos, auditorías y prácticas operativas. Su objetivo es minimizar riesgos, garantizar la continuidad del negocio y crear una cultura organizacional orientada a la seguridad. No busca la máxima seguridad, sino un nivel **adecuado y sostenible** de protección, de acuerdo con los riesgos que la organización esté dispuesta a asumir.

Explica cómo implementarías un SGSI paso a paso en una empresa mediana de servicios financieros. ¿Qué factores considerarías esenciales para su éxito?

Para implementar un SGSI en una empresa mediana de servicios financieros, comenzaría estableciendo una política clara que defina los objetivos y alcance del sistema. Luego, identificaría y clasificaría los activos de información sensibles, como los datos de clientes y transacciones. A partir de eso, evaluaría los riesgos y diseñaría controles adecuados, como autenticación de dos factores y cifrado.

Posteriormente, implementaría el SGSI, lo integraría en las operaciones diarias y mediría su efectividad mediante indicadores clave de desempeño. Haría ajustes necesarios y garantizaría revisiones periódicas por parte de la alta gerencia.

Los factores más importantes para el éxito del SGSI serían el compromiso de la dirección, un equipo capacitado en seguridad y la promoción de una cultura organizacional que valore la seguridad de la información.

¿Qué diferencias existen entre las normas ISO/IEC 27001 e ISO/IEC 27002? ¿Cómo se complementan en la práctica?

ISO/IEC 27001 es un estándar internacional que define los requisitos para establecer, implementar y mantener un SGSI. Es certificable y se enfoca en el "qué" se debe hacer.
En cambio, ISO/IEC 27002 es una guía de buenas prácticas que se enfoca en el "cómo" implementar esos controles de seguridad. No es certificable, pero es una herramienta muy útil para aplicar de forma efectiva la ISO 27001.
Ambas se complementan porque la 27002 brinda el soporte práctico para cumplir los requisitos formales exigidos por la 27001.

Durante una evaluación de riesgos en una pyme que almacena datos de clientes, ¿cómo identificarías los activos más críticos y qué acciones seguirías después?

En una evaluación de riesgos en una pyme que gestiona datos de clientes, primero identificaría todos los activos relacionados, como la base de datos de clientes, los

servidores, el sistema CRM y los empleados que acceden a esos datos. Luego clasificaría esos activos según su nivel de sensibilidad y el impacto que tendría su pérdida o exposición.

Después, evaluaría las amenazas y vulnerabilidades para cada activo. Por ejemplo, si un empleado puede acceder sin autenticación segura o si hay falta de copias de seguridad.

Con base en eso, propondría controles como cifrado de datos, autenticación multifactor, formación del personal y auditorías. Finalmente, todo esto se documenta y se revisa periódicamente para adaptarse a nuevas amenazas.

Imagina que eres la persona responsable de seguridad en una empresa de salud. ¿Qué buenas prácticas aplicarías según ISO 27001 e ISO 27002 para asegurar la confidencialidad de los pacientes?

En una empresa de salud, para proteger la confidencialidad de los datos de los pacientes aplicaría buenas prácticas basadas en las normas ISO 27001 e ISO 27002.

Primero establecería políticas claras de seguridad de la información, capacitando al personal sobre la confidencialidad médica. Clasificaría los datos según su nivel de sensibilidad.

En cuanto a los controles técnicos, implementaría autenticación multifactor, cifrado de datos en tránsito y en reposo, y limitaría los accesos solo al personal necesario.

También realizaría evaluaciones periódicas de riesgos y establecería un plan de respuesta ante incidentes, garantizando que, incluso ante una intrusión, los datos se mantengan protegidos.

Todo esto permitiría cumplir con los requisitos de seguridad y mantener la confianza de los pacientes.