SEGURIDAD DE LA INFORMACIÓN

CAROLINA MATOS
AGOSTO, 2023

AGENDA

- ¿Qué es seguridad de la información?
- Elementos Claves de la seguridad de la información.
- Dimensiones de Seguridad de la información.
- Amenazas o ataques más comunes.
- Importancia de Ciberseguridad.
- Medidas de protección y concientización.
- Preguntas y respuestas.

¿Qué es seguridad de la información?

Es la protección de la información confidencial, valiosa y sensible de una organización o individuo contra amenazas y ataques cibernéticos.
Esto implica implementar medidas y controles para garantizar la **confidencialidad**, **integridad** y **disponibilidad** de la información.

Ciberseguridad

La ciberseguridad es la práctica de proteger equipos, redes, aplicaciones de software, sistemas críticos y datos de posibles amenazas digitales.

Elementos Claves de Seguridad

La seguridad de la información se basa en una combinación de procesos, personas y tecnología para garantizar la protección de los activos digitales de una organización.

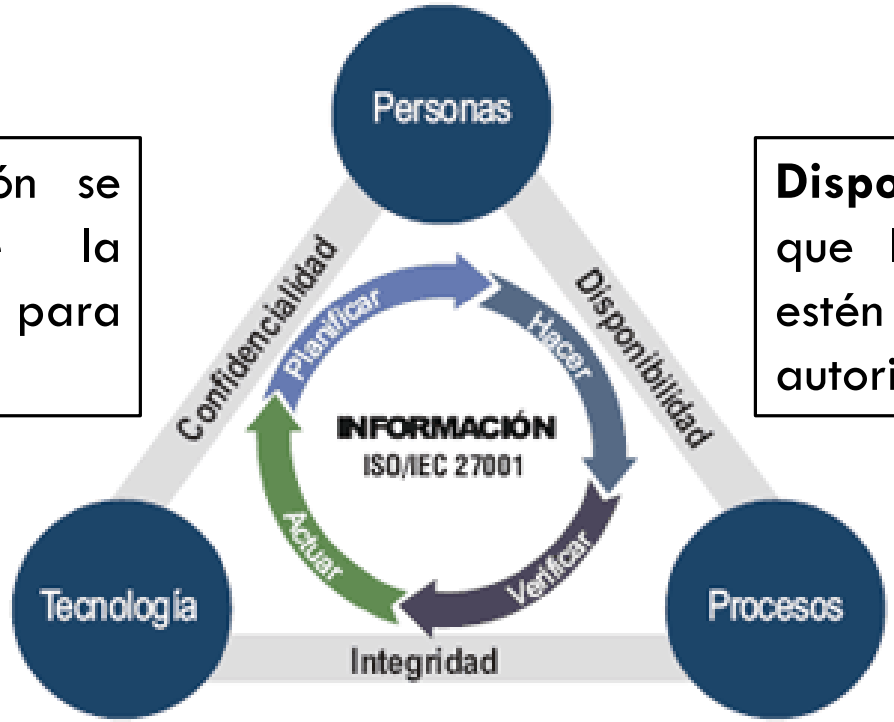
- Firewalls y Sistemas de Detección.
- Antivirus y Antimalware.
- Cifrado de Datos.
- Autenticación Multifactor (AMF)

- Responsables de Seguridad
- Usuarios Finales
- Equipo de Respuesta a Incidentes

- Políticas de Seguridad.
- Gestión de Riesgos.
- Gestión de Incidentes.
- Auditorías y Evaluaciones.
- Formación, Concienciación.

Dimensiones de Seguridad de la información.

Confidencialidad: Esta dimensión se enfoca en garantizar que la información solo esté disponible para personas autorizadas.



Disponibilidad: Refiere a garantizar que la información y los sistemas estén disponibles para las personas autorizadas cuando sea necesario.

Integridad: Se refiere a mantener la exactitud de los datos. Implica prevenir modificaciones no autorizadas o no deseadas en la información.

Amenazas o ataques más comunes

Phishing

Es un método en el cual los ciberdelincuentes intentan engañar a los usuarios para que revelen información confidencial. Esto se hace a través correos o sitios web falsos que parecen legítimos.

Malware

Es un software malicioso, diseñado para dañar, robar información o tomar el control de los sistemas informáticos. Puede ingresar a través de descargas, archivos adjuntos de correo electrónico, sitios web infectados o dispositivos USB infectados.

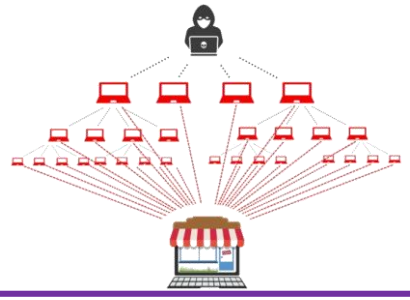
Ransomware

Es un tipo de malware que cifra los archivos o bloquea el acceso al sistema de una organización y exige un rescate para desbloquearlos. Se utilizan tácticas de intimidación y extorsión para obtener dinero de las organizaciones afectadas.

Amenazas o ataques más comunes

Ataques de denegación de servicio (DDoS)

Tienen como objetivo saturar los recursos de una red o sitio web, lo que resulta en la interrupción del servicio para usuarios legítimos.



Ataques de ingeniería social

Aprovechan la manipulación psicológica y la confianza para obtener información confidencial. Esto puede implicar llamadas telefónicas fraudulentas, correos electrónicos engañosos o incluso la suplantación de identidad.

Fuga de información

Puede ocurrir debido a errores humanos, descuidos o actividades maliciosas. La filtración de datos confidenciales puede dañar la reputación de la organización y causar problemas legales y financieros significativos.

Importancia de la Seguridad de la Información

Protección de datos confidenciales: Las organizaciones manejan y almacenan una gran cantidad de datos sensibles.

Cumplimiento normativo y legal: Muchos sectores industriales están sujetos a regulaciones y leyes que exigen el cumplimiento de medidas de seguridad de la información.

Mantenimiento de la confianza del cliente: La seguridad de la información es fundamental para generar confianza en los clientes y socios comerciales.

Continuidad del negocio: Las brechas de seguridad pueden interrumpir las operaciones comerciales y dañar la reputación de la organización.

Prevención de pérdida de datos y fraude: Las organizaciones pueden sufrir pérdidas financieras y de reputación debido al robo de datos o al fraude cibernético.

Medidas de protección y Concientización

- Simulacros, formación y campañas sobre ingeniería social y cómo reconocer intentos de phishing.
- La importancia de formar a los empleados y usuarios en prácticas seguras.
- Promoción de una cultura de seguridad en la organización.
- Uso de contraseñas seguras y autenticación de dos factores.
- Actualización regular de software y sistemas.
- Uso de firewall y software antivirus/antimalware.
- Respaldo de datos. Monitoreo y detección.

¡ GRACIAS !