1. La confidencialidad es el principio que protege la información para que solo las personas autorizadas puedan verla o usarla. Su objetivo es evitar que usuarios no autorizados accedan, copien o filtren datos sensibles. Protege la privacidad de personas y empresas. Evita robos de información como contraseñas, datos bancarios o secretos comerciales. Cumple con leyes y normas de protección de datos (como GDPR, HIPAA, etc.).
2. La integridad es el principio que protege los datos contra cambios no autorizados.

Su propósito es asegurar que la información sea confiable, es decir, que no ha sido alterada, manipulada o dañada sin permiso. Garantiza que los datos se mantengan correctos y exactos. Permite confiar en la información para tomar decisiones. Evita errores, fraudes o sabotajes causados por datos alterados.

1. La disponibilidad significa que la información y los recursos deben estar accesibles para los usuarios autorizados cuando los necesiten. No basta con que los datos existan: tienen que estar disponibles en el momento correcto. Permite que las personas puedan trabajar, acceder a servicios y tomar decisiones en el momento oportuno. Asegura la continuidad del negocio y evita interrupciones. Protege contra fallos técnicos y ataques que busquen dejar fuera de servicio un sistema (como ataques DDoS).
2. Una empresa de salud maneja registros médicos de pacientes, que contienen información sensible como: Diagnósticos médicos, Tratamientos, Información personal (nombre, dirección, número de seguro, etc.). Proteger estos datos es crítico para cumplir con leyes de privacidad y mantener la confianza de los pacientes. La empresa utiliza cifrado de datos para proteger los registros médicos.

Esto significa que los archivos están codificados de forma que, si alguien no autorizado intenta verlos, no puede entender la información. Solo el personal médico autorizado (doctores, enfermeras) tiene llaves de acceso o credenciales especiales para descifrar y leer los datos. Además, el sistema controla quién puede ver, editar o eliminar los registros. Incluso si los datos son robados o interceptados, seguirán siendo ilegibles para los atacantes porque están cifrados.

Así se asegura la confidencialidad: solo las personas autorizadas pueden acceder a la información médica.

1. Para proteger la integridad de los archivos, la empresa genera una suma de verificación (hash) —por ejemplo, utilizando algoritmos como SHA-256— para cada archivo de instalación. Este hash se publica en su sitio web oficial junto con el archivo descargable. Cuando un cliente descarga el instalador, puede calcular el hash del archivo en su propia computadora y compararlo con el hash publicado. Si ambos hashes coinciden, significa que el archivo no fue modificado ni dañado durante la descarga. Si los hashes no coinciden, es señal de que el archivo podría haber sido alterado (por corrupción de datos o por un ataque malicioso).
2. El banco implementa servidores redundantes y sistemas de respaldo. Esto significa:

* Servidores redundantes: Hay múltiples servidores que realizan las mismas funciones. Si uno falla (por ejemplo, por un problema de hardware), otro servidor automáticamente asume su lugar sin que el usuario final lo note.
* Sistemas de respaldo (backups): Toda la información importante (datos de clientes, transacciones, configuraciones de los sistemas) se copia regularmente en ubicaciones seguras. En caso de que ocurra una falla grave o pérdida de datos, el banco puede restaurar rápidamente la información desde estos respaldos.
* Además, algunos bancos utilizan centros de datos en diferentes ciudades (redundancia geográfica) para protegerse incluso contra desastres naturales.

1. -- ¿Qué concepto consideras más crítico en el contexto de una empresa de salud ¿Y en una empresa de comercio electrónico ¿Cómo podrías priorizar la implementación de estos conceptos en una organización con recursos limitados

Confidencialidad es el concepto más crítico.

Las organizaciones de salud manejan información sensible de los pacientes (historias clínicas, diagnósticos, tratamientos).

Si esta información se filtra o es robada, puede tener consecuencias legales y éticas graves, además de dañar la confianza de los pacientes.

Empresa de Comercio Electrónico:

Disponibilidad es lo más crítico.

Los usuarios esperan poder acceder a la tienda en línea en cualquier momento.

Si el sitio cae o funciona mal, las ventas se pierden al instante, y los clientes pueden irse a la competencia.

Aunque la confidencialidad (por ejemplo, de los datos de pago) también es muy importante, si no hay disponibilidad, no hay negocio.

8)

La Confidencialidad, Integridad y Disponibilidad son los tres pilares esenciales de la ciberseguridad. Cada uno protege un aspecto clave de la información y los sistemas, y juntos garantizan que los datos estén seguros, confiables y accesibles cuando se necesiten:

Confidencialidad asegura que solo las personas autorizadas puedan acceder a la información. Protege los datos sensibles contra accesos no autorizados, como filtraciones o espionaje.

Integridad garantiza que la información no sea alterada de manera indebida, ya sea por errores accidentales o por ataques maliciosos. Se asegura que los datos sean exactos y confiables.

Disponibilidad garantiza que los sistemas y la información estén accesibles para los usuarios autorizados cuando los necesiten, incluso en caso de fallos técnicos o ciberataques.

Trabajando juntos:

Si uno de estos elementos falla, los otros también se ven afectados. Por ejemplo:

Si la disponibilidad falla (el sistema cae), aunque la confidencialidad e integridad estén intactas, los usuarios no podrán acceder a los datos.

Si la integridad se compromete (datos alterados), no importa que los datos estén confidenciales o disponibles: ya no se puede confiar en ellos.

Si la confidencialidad se pierde (datos filtrados), los usuarios no autorizados podrían acceder y manipular o explotar los datos.