Confidencialidad:

En el contexto de la **ciberseguridad**, se refiere a la propiedad de que **la información solo sea accesible por las personas autorizadas**.

Su objetivo principal es **proteger los datos sensibles o privados** de accesos no autorizados.

Ejemplos:

- Cifrado de datos.
- Uso de contraseñas seguras.
- Control de accesos y permisos.
- Autenticación de usuarios.

Integridad:

En el contexto de la **seguridad de la información**, significa que **los datos no han sido alterados, modificados o eliminados de forma no autorizada**. Es decir, que la información se mantiene **exacta, completa y confiable** desde su origen hasta su destino.

Ejemplos:

- **Firmas digitales**: aseguran que el contenido no ha sido modificado.
- **Hashing** (funciones hash): permite verificar si los datos han sido alterados.
- **Controles de acceso**: evitan que usuarios no autorizados cambien información.
- **Sistemas de respaldo (backups)**: permiten restaurar datos si se corrompen.

Disponibilidad:

En ciberseguridad, significa que **la información y los sistemas están accesibles y funcionando correctamente cuando los usuarios autorizados los necesitan**.

- **Sistemas redundantes** (por ejemplo, servidores de respaldo).
- **Copias de seguridad** (backups) regulares.
- **Protección contra ataques DDoS** (que buscan colapsar los servicios).
- **Mantenimiento preventivo** de hardware y software.

Pregunta 1: ¿Qué concepto consideras más crítico en el contexto de una empresa de salud ¿Y en una empresa de comercio electrónico?

En la empresa de salud sería confidencialidad debido a la información tan sensible que manejan estas empresas como historiales médicos, diagnósticos, etc.

Para una empresa de comercio electrónico Disponibilidad debido a que dependen de que sus plataformas estén constantemente online.

Pregunta 2: ¿Cómo podrías priorizar la implementación de estos conceptos en una organización con recursos limitados?

Evaluando el riesgo e impacto:
Habría que preguntarse cosas como: ¿Qué tipo de información maneja?
¿Qué sucede si esta información no está disponible o se pierde?
Para saber que se debe priorizar.

Usando los controles básicos de cada una de las implementaciones.
Intentar crecer de forma modular, donde, dependiendo del presupuesto y de como esté creciendo usar mejores materiales.

Parte 2:

Defina y ejemplos:
Virus: Es un tipo de malware diseñado para infectar archivos o sistemas y propagarse a otros equipos, causando daño por cada equipo que pasa, corrompiendo datos o borrando archivos, bloqueando o ralentizando el sistema, etc.

Gusano: Es un tipo de malware el cual está diseñado para infectar redes, replicando y enviándose por las mismas sin necesidad de un intermediario o un archivo por el cual propagarse pudiendo, por ejemplo, Puede abrir puertas traseras (backdoors) para que atacantes tomen el control.

Troyano: Es un malware el cual infecta el dispositivo mediante hacerse pasar por un programa legitimo el cual se activa al momento de ejecutar el archivo, sirviendo para robar datos, instalar otros malwares, formar parte de una botnet o red de computadoras zombies, etc

Ransomware: Este malware “Secuestra” tus archivos o dispositivo, bloqueándolos mediante cifrado, donde se generalmente se pide una suma de dinero para poder recuperarlos

Malware: Es cualquier tipo de programa o código que ha sido creado con el propósito de dañar, infiltrarse, robar o alterar un sistema informático sin consentimiento del usuario.

Spyware: Es un malware el cual se instala en tu dispositivo sin tu conocimiento y se dedica a espiarte, recopilando datos personales, de navegación, contraseñas, correos, conversaciones, etc. Registrando lo que se dice y capturando lo que escribes.

Parte 3