Preguntas de Reflexión:

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

Empresa de Salud – Concepto más crítico: Confidencialidad

- En el sector salud, el **activo más sensible** son los **datos personales y médicos** de los pacientes.
- **Confidencialidad** garantiza que esta información no sea accedida ni divulgada por personas no autorizadas.
- Regulado por normas como **HIPAA** (en EE.UU.) o **LOPD/GDPR** (en Europa y Latinoamérica), su violación puede conllevar **multas severas y pérdida de confianza**.

Empresa de Comercio Electrónico – Concepto más crítico: Integridad

- Aquí lo esencial es que las **transacciones, precios, datos de productos y pagos** no sean alterados de forma maliciosa.
- La **integridad** asegura que los datos mostrados y almacenados no han sido manipulados, lo cual es clave para evitar fraudes y errores de cobro.
- También se relaciona con la protección de datos financieros de clientes (como tarjetas de crédito).

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

1. Evaluar riesgos reales

- Identificar qué tipo de ataque o brecha sería más **devastador para la operación**.
- Ej: ¿Perder clientes por falta de confianza? ¿Ser multado por incumplir normativas?

2. Aplicar controles básicos pero efectivos

- **Autenticación fuerte** (como MFA)
- **Actualizaciones periódicas**
- **Segmentación de red**
- **Concientización del personal** (capacitaciones simples pero constantes)

3. Usar soluciones gratuitas o de código abierto

- Antivirus, firewalls, SIEMs básicos y herramientas de análisis tienen buenas versiones gratuitas o de bajo costo.

4. Documentar políticas mínimas de seguridad

- Aunque sea algo sencillo, tener **políticas claras** evita muchos errores humanos.

5. Buscar alianzas o apoyo gubernamental

- En muchos países hay programas para ayudar a pequeñas empresas a implementar seguridad básica.

Conclusión del Laboratorio:

Resuma cómo la confidencialidad, integridad y disponibilidad trabajan juntas para proteger la información y los sistemas.

1. Confidencialidad

- **Objetivo:** Garantizar que solo las personas autorizadas tengan acceso a la información.
- **Cómo contribuye:** Protege los datos sensibles (como información personal, financiera o médica) de accesos no autorizados. La implementación de medidas como la **encriptación**, **autenticación multifactorial (MFA)** y **controles de acceso** asegura que la información solo esté disponible para los usuarios correctos.

2. Integridad

- **Objetivo:** Asegurar que la información no sea alterada o manipulada de manera no autorizada.
- **Cómo contribuye:** Permite que los datos mantengan su precisión y consistencia a lo largo del tiempo. El uso de **firmas digitales**, **hashing** y **control de versiones** ayuda a evitar modificaciones indebidas o ataques como la **manipulación de datos** o **fraudes**.

3. Disponibilidad

- **Objetivo:** Garantizar que la información y los sistemas estén accesibles y operativos cuando sean necesarios.
- **Cómo contribuye:** Protege contra **ataques de denegación de servicio (DDoS)** y otros eventos que pueden interrumpir el acceso a sistemas y datos. Se implementan **copias de seguridad**, **planes de recuperación ante desastres** y **monitoreo constante** para asegurar que los sistemas estén disponibles y funcionando sin fallos.

Destaca la importancia de implementar medidas que aseguren los tres aspectos para una ciberseguridad efectiva.

Para lograr una **ciberseguridad sólida**, no se puede priorizar un solo aspecto de la tríada CIA, ya que todos son esenciales para proteger la información y los sistemas de manera integral:

- **Si descuidas la confidencialidad**, la información puede ser expuesta a personas no autorizadas, lo que compromete la privacidad y la seguridad de los datos.
- **Si no se asegura la integridad**, los datos pueden ser manipulados o corrompidos, lo que podría resultar en **fraudes**, **errores operativos** o incluso daños irreparables a la confianza del cliente.
- **Si no se garantiza la disponibilidad**, las organizaciones pueden enfrentar tiempos de inactividad prolongados, pérdida de acceso a datos vitales o incluso **pérdidas económicas** importantes debido a la **interrupción del servicio**.

Por lo tanto, **una estrategia de ciberseguridad efectiva debe abordar los tres elementos** simultáneamente, integrando medidas que protejan la confidencialidad, mantengan la integridad de los datos y aseguren que los sistemas estén siempre disponibles cuando se necesiten.