SESION 2 DESARROLLO

🔹 **Paso 1: Definir los Términos (20 min)**

1. **Leer y comprender** los conceptos de:
    - Confidencialidad
    - Integridad
    - Disponibilidad
2. **Estudiar los conceptos relacionados** (cifrado, autenticación, redundancia, etc.).
3. **Anotar ejemplos breves** de cada uno para uso personal o compartir con el grupo.

📌 *Resultado esperado:* Comprensión clara de los tres conceptos.

Desarrollo del paso 1

Confidencialidad

Es algo que garantiza que nuestra información personal es totalmente sensible para el publico o para un usuario común solo personas que tu autorices pueden saber tu información clasificada ya que es algo restringido que no se puede tocar por terceros ni nadie más. Se relaciona con:

1.Cifrados de extremo a extremo lo que significa que nadie puede ver tu información solo personas autorizadas pueden ver.

2.Controles de acceso y autenticación: están pensados para otorgar permisos aquellos que puedan ver esa información pero bajo una series de permisos que tu le asignes para que puedan procesarla y la autenticación para comprobar si cuentas con medios de seguridad para mas protección.

Ejemplo: Si yo tengo que entregar un documento confidencial que tiene mis datos y se lo voy a dar a una agencia de empleo o de industria debo ponerle permiso a la persona para que pueda manipular mis datos que estén en ese documento siempre y cuando yo lo autorice con anticipación para que no puedan ser alterados ni tampoco hacer plagio.

Integridad

garantía de que los datos y los sistemas permanecen precisos, consistentes e inalterados durante todo su ciclo de vida es decir ósea nunca serán modificados ni alterados sin tu consentimiento.

Ejemplo: Si guardare algo de valor en una caja fuerte y nunca lo sacare lo que nadie puede hacerlo sin mi permiso solo yo tengo la decisión de sacar a guardar lo que sea de valor.

Disponibilidad

capacidad de acceder a la información y los sistemas cuando se necesitan. Es uno de los tres pilares fundamentales de la seguridad de la información, junto con la confidencialidad y la integridad. La disponibilidad garantiza que los usuarios autorizados puedan acceder a los datos y servicios de manera oportuna y confiable.

El concepto de disponibilidad en ciberseguridad:

- **Acceso oportuno y fiable:** La información y los sistemas deben estar accesibles cuando se necesitan, sin interrupciones innecesarias.
- **Usuarios autorizados:** Solo los usuarios con permisos deben poder acceder a los recursos.
- **Recuperación de datos:** En caso de interrupción o pérdida de datos, debe haber mecanismos para recuperar la información.

Ejemplo:

- **Atacante:**

Un atacante utiliza software malicioso para bloquear el acceso a un servidor web, impidiendo que los usuarios puedan acceder a la página web.

- **Acción:**

El propietario del sitio web debe restaurar el acceso al servidor para que la página web esté nuevamente disponible para los usuarios.

- **Prevención:**

La implementación de medidas de seguridad como sistemas de detección de intrusiones, software antivirus y copias de seguridad regulares puede ayudar a prevenir este tipo de ataques

🔹 **Paso 2: Analizar Ejemplos Prácticos (25 min)**

4. **Revisar los tres ejemplos prácticos** dados (empresa de salud, software, banco).
5. **Participar en la discusión** (si es en clase o foro) y responder a preguntas como:
    - ¿Qué otros métodos mejorarían la confidencialidad?
    - ¿Qué pasa si no se mantiene la integridad?
    - ¿Consecuencias de no tener disponibilidad?

Escribir tus propias respuestas a estas preguntas (puedes incluirlas en el documento final).

📌 *Resultado esperado:* Relación de los conceptos con situaciones reales.

4.Empresa de salud

Pues como son datos sensible pues tienen que usar un sistema de cifrado fuerte y que este en monitorea constante de quien entra y sale en la base de datos para prevenir personas no autorizadas.

Banco

Pues si un banco no tiene los servicios necesarios como los de seguridad o de comunicación con los cajeros automáticos por parte de ellos quedarían expuesto a vulnerabilidades como suplantaciones, clonaciones y grandes brechas de seguridad expuesta para así robar dinero sin que se den cuenta y perdida de usuarios.

Software

Si la integridad no se mantuviera, los sistemas informáticos y la información almacenada en ellos podrían quedar expuestos a graves riesgos con personas que son peligrosas.

5. □ **Métodos para mejorar la confidencialidad**: Se pueden utilizar técnicas como el cifrado de datos (AES, RSA), la autenticación multifactor (MFA), y el acceso basado en roles para limitar la exposición de información sensible. También es útil la implementación de redes privadas virtuales (VPN) y la seguridad en la capa de transporte (TLS) para proteger las comunicaciones.

- **Consecuencias de no mantener la integridad**: Como mencionamos antes, si la integridad no se mantiene, los datos pueden ser manipulados sin que los usuarios lo noten, lo que puede resultar en fraudes, pérdida de confianza en los sistemas o decisiones erróneas

basadas en información alterada. La verificación de integridad mediante hashes criptográficos y firmas digitales puede ayudar a prevenir este problema.

- **Impacto de no tener disponibilidad**: Sin disponibilidad, los sistemas y servicios críticos pueden volverse inaccesibles, lo que afecta directamente a negocios, instituciones y usuarios. Un ataque de denegación de servicio (DDoS) o un fallo en la infraestructura pueden impedir el acceso a información y recursos necesarios. La redundancia, el almacenamiento distribuido y la planificación ante desastres pueden mitigar estos riesgos.

6.Crear un segundo documento PDF que contenga:

- Definiciones de los tipos de malware.
- Ejemplos prácticos explicados.
- Análisis del impacto en los sistemas.

Definiciones y Características

🦠 **Virus**

Se adjunta a archivos legítimos. Se activa al ser ejecutado por el usuario.
Impacto: Daño a archivos, pérdida de información, propagación.

🪱 **Gusano**

Se replica automáticamente por redes sin intervención del usuario.
Impacto: Saturación de red, caída de sistemas, lentitud.

🐴 **Troyano**

Simula ser un software legítimo para engañar al usuario.
Impacto: Acceso remoto no autorizado, robo de datos, puerta a más malware.

🔐 **Ransomware**

Cifra archivos del sistema y exige un pago para recuperarlos.
Impacto: Pérdida de acceso, interrupción operativa, posible pérdida financiera.

👁️ **Spyware**

Espía las actividades del usuario sin consentimiento.
Impacto: Robo de información personal y financiera, pérdida de privacidad.

Ejemplos y Análisis de Impacto

Virus

Ejemplo: Un archivo infectado por correo electrónico ejecuta un virus que daña el sistema operativo.
Impacto: Pérdida de datos y propagación a otros usuarios.

Gusano

Ejemplo: Un gusano se propaga automáticamente por una red empresarial.
Impacto: Ralentiza la red, bloquea servicios, congestiona los sistemas.

Troyano

Ejemplo: Un empleado descarga una "herramienta gratuita" que resulta ser un troyano.
Impacto: El atacante accede a los archivos internos de la empresa.

Ransomware

Ejemplo: Una empresa abre un enlace malicioso y sus datos son cifrados.
Impacto: Suspensión de actividades, chantaje económico, riesgo reputacional.

Spyware

Ejemplo: El usuario instala una app con spyware que graba sus pulsaciones y roba credenciales bancarias.
Impacto: Fraude financiero, pérdida de privacidad, robo de identidad.

✅ Conclusión

Conocer los diferentes tipos de **malware** es esencial para desarrollar medidas de defensa eficaces. Cada uno tiene mecanismos únicos de infección y consecuencias distintas, pero todos representan riesgos serios para la seguridad informática.