LABORATORIO 2

CIBERSEGURIDAD

FABIAN ANDRES BENJUMEA

UNIVERSIDAD POPULAR DEL CESAR

VALLEDUPAR

2025

¿Qué es confidencialidad, integridad y disponibilidad?

Confidencialidad

Es proteger la información de accesos no autorizados. Solo las personas, sistemas o entidades que tengan permiso pueden acceder a los datos.

- Ejemplo: Una contraseña que protege tu correo electrónico.
- Técnicas comunes: cifrado, control de accesos, autenticación.

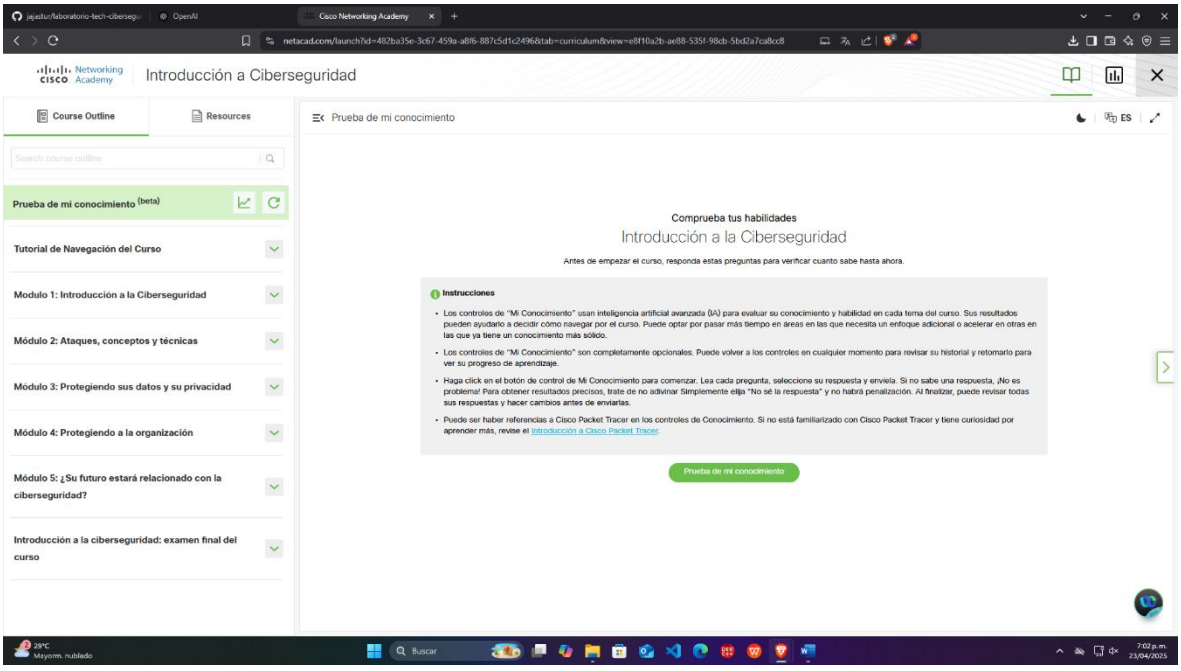
Integridad

Significa asegurarse de que la información no ha sido alterada de forma no autorizada. La información debe ser precisa y completa.

- Ejemplo: Un archivo que no ha sido modificado desde que fue enviado.
- Técnicas comunes: firmas digitales, hash (como SHA-256), control de versiones.

Disponibilidad

La información debe estar accesible cuando se necesita. Esto incluye prevenir fallos de sistema, ataques (como DDoS) y garantizar respaldo (back



ups).

- Ejemplo: Poder entrar al sistema de tu banco en línea a cualquier hora.

- Técnicas comunes: redundancia, copias de seguridad, mantenimiento continuo.

Pregunta 1: ¿Qué concepto considera mas critico en una empresa de salud? ¿y en una empresa de comercio electrónico?

Empresa de salud

Confidencialidad es el concepto más crítico.

- **¿Por qué?** En salud se maneja información extremadamente sensible: historiales clínicos, diagnósticos, tratamientos, resultados de pruebas. Si esta información se filtra, puede causar daño a los pacientes, violar leyes como la **HIPAA** (en EE. UU.) o la **Ley de Protección de Datos** (en otros países), y arruinar la reputación del centro médico.

Empresa de comercio electrónico

Disponibilidad es probablemente el aspecto más crítico.

- **¿Por qué?** Si una tienda en línea no está disponible, no se pueden hacer ventas, los clientes se van con la competencia, y se pierden ingresos. A diferencia de un hospital, la confidencialidad sigue siendo importante (por datos bancarios y personales), pero si el sitio se cae en pleno Black Friday, el impacto económico es inmediato.

Pregunta 2: ¿cómo podrías priorizar la implementación a una empresa con recursos limitados?

1. Evaluar los riesgos específicos de la empresa

Lo primero es identificar los riesgos más importantes. Para esto, se puede hacer una evaluación de riesgos donde se determina:

2. Priorizar según impacto y probabilidad

Usando una matriz de riesgos (impacto vs. probabilidad), se puede priorizar las acciones de seguridad. Las amenazas de alto impacto y alta probabilidad deben ser tratadas de inmediato, mientras que las de bajo impacto o baja probabilidad pueden dejarse para más adelante.

3. Definir medidas mínimas necesarias para cada pilar (CIA)

Confidencialidad:

- **Protección de datos personales y sensibles**: Implementa cifrado de datos (al menos en la transmisión y almacenamiento) y autenticación segura (2FA, contraseñas fuertes).
- **Acceso restringido**: Asegúrate de que solo las personas necesarias tengan acceso a la información sensible, usando control de acceso.

Prioridad mínima: En un negocio pequeño, empezar con la protección de datos sensibles, como los números de tarjetas de crédito en comercio electrónico o historiales médicos en una empresa de salud.

Integridad:

- **Verificación de la integridad de los datos**: Usa hashing para asegurar que los datos no hayan sido modificados sin autorización.
- **Copias de seguridad**: Asegúrate de tener una copia de seguridad regular de los datos críticos, para poder recuperarlos en caso de error o ataque.

Difina y ejemplo:

Virus: Un virus es un tipo de malware que se adjunta a un archivo o programa legítimo y se propaga cuando el archivo o programa infectado es ejecutado. Puede modificar o destruir archivos, y propagarse a otros sistemas a través de medios como unidades USB, correos electrónicos o descargas de internet.

Ejemplo:
Un virus podría infectar un archivo de Microsoft Word. Cuando se abre el archivo, el virus se activa y comienza a replicarse, infectando otros documentos en el sistema y potencialmente enviándose a contactos en la lista de correo del usuario.

Gusano: es un tipo de malware que se propaga automáticamente a través de una red, replicándose y propagándose de forma autónoma sin necesidad de la interacción del usuario.

Ejemplo:

El gusano "ILOVEYOU" de 2000 se propagó rápidamente a través de correos electrónicos con el asunto "ILOVEYOU", infectando millones de computadoras en todo el mundo y causando daños significativos en empresas y gobiernos.

Troyano: es un tipo de malware que se disfraza de un programa legítimo para engañar a los usuarios.

Ejemplo:
Un archivo descargado que se presenta como una actualización de software o un archivo de juego, pero que en realidad es un troyano. Una vez instalado, el troyano permite que un atacante obtenga acceso remoto al dispositivo y robe información sensible, como contraseñas.

Ransomware: El ransomware es un tipo de malware que cifra los archivos de un usuario o una organización y luego exige un pago (rescate) para que los archivos vuelvan a ser accesibles.

Ejemplo:
El ransomware "WannaCry" de 2017 afectó a organizaciones en todo el mundo, incluyendo hospitales y empresas. Encriptó los archivos de los usuarios y exigió un rescate en Bitcoin para liberarlos. Muchos sistemas que no estaban actualizados con los últimos parches de seguridad fueron los más afectados.

Spyware: es un tipo de software malicioso que se instala en un dispositivo (como una computadora o teléfono) sin el conocimiento o consentimiento del usuario, con el objetivo de recopilar información personal y enviarla a terceros.

Ejemplo:
Un programa gratuito que, una vez instalado en un dispositivo, empieza a recopilar datos sobre los sitios web que visita el usuario, sus búsquedas y compras en línea, para luego enviar esa información a terceros con fines de marketing o para cometer fraudes.

Curso de CISCO