Laboratorio # 2

Confidencialidad

Definición: La confidencialidad se refiere a la protección de la información para asegurar que solo las personas autorizadas puedan acceder a ella. Es uno de los pilares fundamentales de la seguridad de la información.

Ejemplo: Una empresa maneja los historiales médicos de sus empleados. Para proteger esta información, implementa un sistema de gestión que requiere que cada usuario se autentique con una contraseña segura y utiliza cifrado de datos para que, aunque alguien intercepte la información, no pueda leerla sin la clave.

Resultado: Solo los médicos autorizados y el personal de RR.HH. pueden ver los historiales médicos, manteniendo la confidencialidad.

Integridad

Definición: La integridad implica proteger los datos contra modificaciones no autorizadas, asegurando que la información se mantenga exacta, coherente y confiable a lo largo del tiempo.

Ejemplo: Una organización financiera transmite datos sobre transacciones bancarias entre sucursales. Para asegurarse de que no se alteren durante el envío, cada mensaje incluye una suma de verificación (hash). Si el valor hash recibido no coincide con el original, se sabe que los datos fueron modificados y se descarta la transacción.

Resultado: Los datos permanecen íntegros, y cualquier alteración maliciosa o accidental se detecta rápidamente.

Disponibilidad

Definición: La disponibilidad garantiza que los sistemas, aplicaciones y datos estén accesibles para los usuarios autorizados en el momento en que los necesiten, incluso ante fallos o ataques.

Ejemplo: Una tienda en línea tiene servidores replicados en diferentes ubicaciones geográficas. Si un servidor falla por mantenimiento o un ataque (por ejemplo, DDoS), otro entra en funcionamiento automáticamente, permitiendo que los clientes sigan comprando sin interrupciones.

Resultado: El servicio sigue disponible 24/7 para los usuarios, incluso en caso de problemas técnicos.

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

En una empresa de salud: Aunque la confidencialidad es prioritaria, la disponibilidad también es crítica. Imagina que:

Un sistema de emergencias no está disponible cuando llega un paciente en estado crítico.

La historia clínica no se puede consultar durante una operación.

Consecuencia: El personal médico no puede tomar decisiones informadas rápidamente = impacto directo en la salud del paciente.

En una empresa de comercio electrónico: La disponibilidad es prácticamente sinónimo de ventas. Si el sitio web, app o sistema de pagos se cae:

El cliente no puede comprar.

Se pierden transacciones.

Se daña la reputación de la marca.

Ejemplo clásico: Amazon en Prime Day tiene arquitecturas distribuidas y servidores redundantes precisamente para garantizar disponibilidad continua ante millones de usuarios simultáneos.

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

Paso 1: Analizar el contexto de la organización

Antes de priorizar, es importante preguntarse:

¿Qué tipo de datos manejamos? (médicos, financieros, usuarios, internos)

¿Qué pasaría si la información se filtra, se altera o se pierde temporalmente?

¿Qué activos son más críticos para el funcionamiento diario?

Paso 2: Priorización basada en el riesgo

Una estrategia eficaz es usar un enfoque basado en riesgos:

Pilar	¿Cuándo priorizarlo primero?	Ejemplos
Confidencialidad	Si manejas datos sensibles y regulados (salud, finanzas, datos personales)	Hospital, banco, empresa con datos de clientes

Pilar	¿Cuándo priorizarlo primero?	Ejemplos
Integridad	Si la veracidad de los datos es clave para las decisiones o el funcionamiento	Sistemas financieros, laboratorios, control de calidad
Disponibilidad	Si el acceso continuo es crítico para el negocio	E-commerce, servicios 24/7, atención de emergencias

Definir los Tipos de Malware

Virus: es un software malicioso que se adjuntan a archivos legítimos y se propagan con la ejecución de los archivos y estos pueden dañar, eliminar o modificar los archivos.

Ejemplo: ILOVEYOU (2000) — Se propagaba por correo electrónico con un archivo adjunto llamado *LOVE-LETTER-FOR-YOU.txt.vbs*. Al abrirlo, sobrescribía archivos y se reenviaba automáticamente a los contactos del usuario.

Gusano: es un tipo de malware que se replica automáticamente y se propaga por redes sin necesidad de que el usuario lo ejecute. Suelen saturar redes y consumir recursos del sistema.

Ejemplo: WannaCry (2017) — Se propagaba por una vulnerabilidad de Windows. Infectó más de 200,000 computadoras en 150 países en cuestión de días, paralizando hospitales y empresas.

Troyano: Un troyano es un programa malicioso que se disfraza de software legítimo para engañar al usuario. Al instalarse, permite al atacante controlar el sistema o robar información.

Ejemplo: Emotet — Comenzó como un troyano bancario, oculto en correos falsos de bancos o facturas. Una vez instalado, robaba contraseñas y descargaba otros malware.

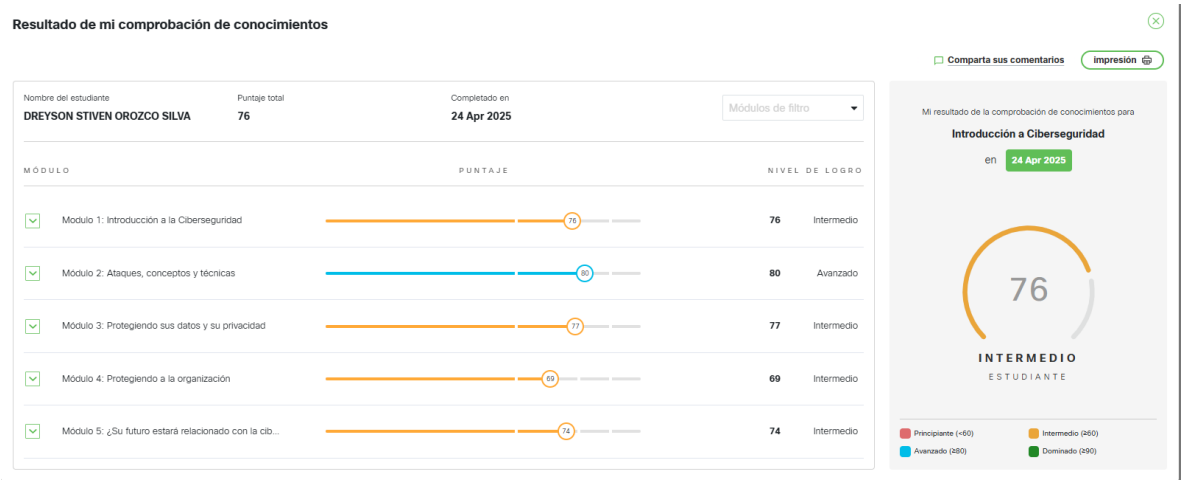
Ransomware: El ransomware cifra los archivos del sistema y exige un pago en criptomonedas para restaurar el acceso. Es muy usado para extorsión, especialmente a empresas y gobiernos.

Ejemplo: CryptoLocker (2013) — Infectó miles de PCs cifrando archivos importantes y solicitando pagos de entre $100 y $300 para desbloquearlos.

Spyware: El spyware se instala sin el conocimiento del usuario y monitorea su actividad, como contraseñas, navegación, mensajes o incluso el micrófono y la cámara.

Ejemplo: CoolWebSearch — Modificaba los resultados de búsqueda y redirigía al usuario a sitios web maliciosos mientras recolectaba información personal sin consentimiento.

Resultado de Prueba Cisco



Resultado de mi comprobación de conocimientos

Comparta sus comentarios | impresión

Nombre del estudiante	Puntaje total	Completado en
DREYSON STIVEN OROZCO SILVA	76	24 Apr 2025

Módulos de filtro

MÓDULO	PUNTAJE	NIVEL DE LOGRO	
Modulo 1: Introducción a la Ciberseguridad	76	76	Intermedio
Módulo 2: Ataques, conceptos y técnicas	80	80	Avanzado
Módulo 3: Protegiendo sus datos y su privacidad	77	77	Intermedio
Módulo 4: Protegiendo a la organización	69	69	Intermedio
Módulo 5: ¿Su futuro estará relacionado con la cib...	74	74	Intermedio

Mi resultado de la comprobación de conocimientos para

Introducción a Ciberseguridad

en 24 Apr 2025

76

INTERMEDIO

ESTUDIANTE

Principiante (<60) | Intermedio (≥60) | Avanzado (≥80) | Dominado (≥90)