Robert Alberto Pertuz Palacio

Guía de Laboratorio – Sesión 2

Paso 1: Definir los Términos Clave

Confidencialidad
La confidencialidad implica la protección de la información para asegurar que solo las personas autorizadas puedan acceder a ella. Es esencial para prevenir fugas de información o accesos indebidos. Se logra mediante el uso de cifrado, autenticación (como contraseñas y biometría) y controles de acceso.

Integridad
La integridad consiste en garantizar que los datos no sean modificados sin autorización. Esto asegura que la información sea confiable. Se utilizan mecanismos como funciones hash, firmas digitales y control de versiones.

Disponibilidad
La disponibilidad garantiza que la información y los recursos estén accesibles para los usuarios autorizados cuando los necesiten. Se implementa mediante servidores redundantes, respaldos y planes de recuperación ante desastres.

Paso 2:

¿Qué concepto considero más crítico en una empresa de salud y en una de comercio electrónico?

creo que en una empresa de salud el más importante es la **confidencialidad**. Esto lo pienso porque los datos de salud de las personas son súper privados, o sea, no cualquiera debería poder verlos. Si alguien no autorizado accede a esos datos, puede ser muy grave, tanto por temas personales como legales. Me imagino que si un hacker roba la historia clínica de alguien, eso podría afectar muchísimo su vida. Por eso, proteger esa información para que solo el personal médico pueda verla me parece lo más clave.

En cambio, en una empresa de **comercio electrónico**, creo que lo más importante es la **disponibilidad**. Porque si la página se cae o no se puede usar, los clientes no pueden comprar nada, se pierde plata, y además puede quedar mal la empresa.

¿Como podrias priorizar la implementacion en una empresa con recursos limitados?

Bueno, si una organización no tiene muchos recursos (como pasa en muchas empresas pequeñas o que están empezando), yo creo que lo más lógico sería priorizar dependiendo de los riesgos más grandes que puedan tener. O sea, si manejan datos muy sensibles como en una clínica o consultorio, yo empezaría por la confidencialidad, usando contraseñas fuertes, cifrado, y asegurándome de que solo ciertas personas puedan acceder a la información.

Después, pensaría en la disponibilidad, porque no sirve de nada tener todo protegido si luego los empleados o clientes no pueden entrar al sistema cuando lo necesitan. Podría buscar soluciones que no sean tan costosas, como respaldos en la nube o servicios con buena reputación.

Y por último, pero no menos importante, la integridad, para asegurarme de que los datos no cambien por error o por culpa de alguien con malas intenciones. A veces eso se puede hacer con software gratuito o incluso con procesos manuales de revisión, si no hay mucho presupuesto.

DEFINA Y EJEMPLO:

¿Qué es un virus?
Es un programa que se mete en tu dispositivo sin permiso y puede dañar archivos o robar datos. Se copia solo y se esconde en otros archivos.

Ejemplo:
Descargué un plugin de sonidos para editar música y venía con un virus que espía mis grabaciones sin que yo lo supiera.

¿Qué es un gusano?
Es un tipo de malware que se copia a sí mismo y se propaga por redes sin que uno haga nada. No necesita esconderse en archivos.

Ejemplo:
Conecté mi USB en una red pública y el gusano se copió a otras computadoras automáticamente, sin que nadie lo abriera.

¿Qué es un troyano?
Es un malware que se hace pasar por un programa útil o inofensivo, pero en realidad abre una puerta para que otros ataquen tu equipo.

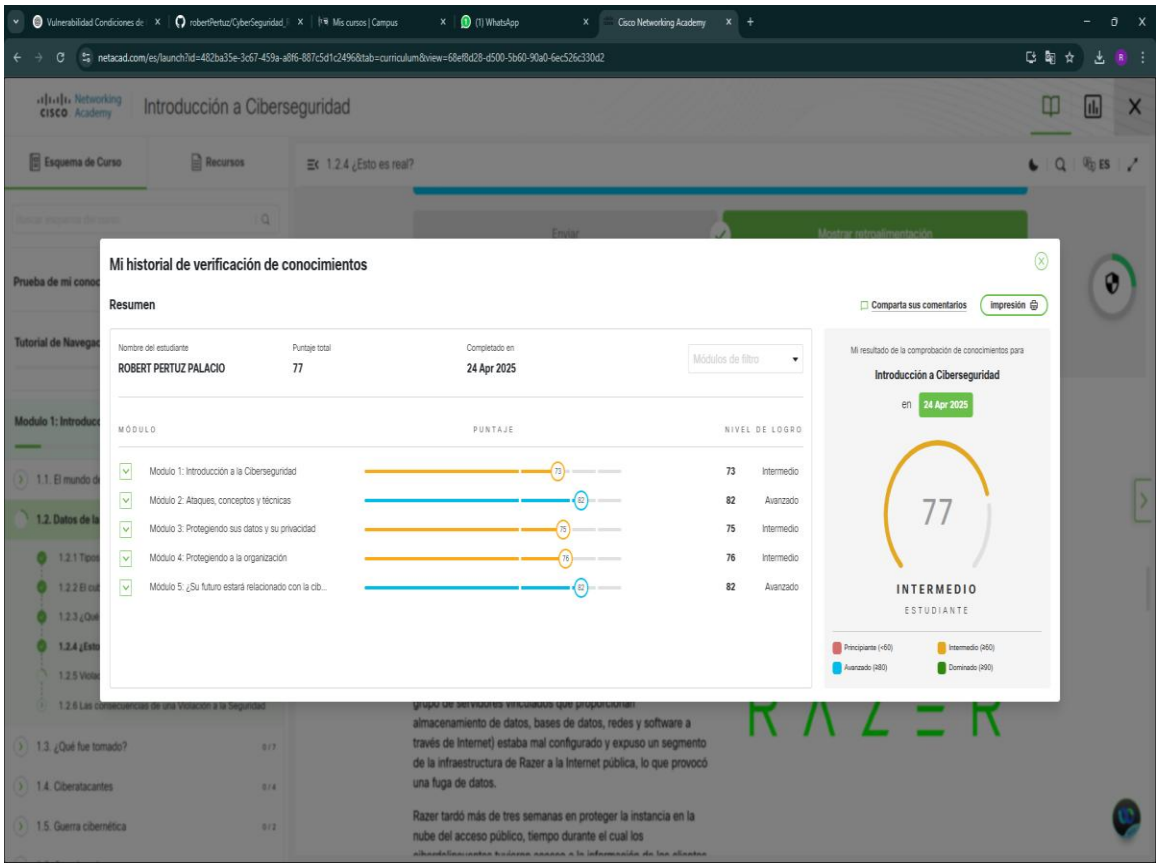
Ejemplo:
Bajé un juego de internet y funcionaba, pero también instaló un troyano que dejó entrar a un hacker sin que yo lo notara.

¿Qué es un ransomware?
Es un tipo de virus que bloquea tus archivos y te pide dinero (un "rescate") para recuperarlos.

Ejemplo:
Un compañero abrió un correo con una "factura" y el ransomware cifró todos sus documentos de la universidad. Le pedían pagar en bitcoins para devolverlos.

¿Qué es un spyware?
Es un programa que se instala sin permiso y espía lo que haces en tu computadora, como contraseñas o páginas que visitas.

Ejemplo:
Instalé una app para mejorar el rendimiento del PC y resultó tener spyware que grababa todo lo que escribía, incluso mis chats privados.


Introducción a Ciberseguridad
Esquema de Curso
Recursos
1.2.4 ¿Esto es real?
Mi historial de verificación de conocimientos
Resumen
Comparta sus comentarios
Impresión
Nombre del estudiante
ROBERT PERTUZ PALACIO
Puntaje total
77
Completado en
24 Apr 2025
Módulos de filtro
MÓDULO
PUNTAJE
NIVEL DE LOGRO
Módulo 1: Introducción a la Ciberseguridad
73
Intermedio
Módulo 2: Ataques, conceptos y técnicas
82
Avanzado
Módulo 3: Protegiendo sus datos y su privacidad
75
Intermedio
Módulo 4: Protegiendo a la organización
76
Intermedio
Módulo 5: ¿Su futuro estará relacionado con la cib...
82
Avanzado
Mi resultado de la comprobación de conocimientos para
Introducción a Ciberseguridad
en
24 Apr 2025
77
INTERMEDIO
ESTUDIANTE
Principiante (<60)
Intermedio (≥60)
Avanzado (≥80)
Dominado (≥90)
almacenamiento de datos, bases de datos, redes y software a través de Internet) estaba mal configurado y expuso un segmento de la infraestructura de Razer a la Internet pública, lo que provocó una fuga de datos.
Razer tardó más de tres semanas en proteger la instancia en la nube del acceso público, tiempo durante el cual los