Laboratorio 2 Cursos CiberSeguridad

Jesús Rodrigo Toro Navarro

Seguridad informática

Universidad Popular del Cesar

Valledupar, Cesar

PARTE 1

1)Definición Confidencialidad, Integridad y Disponibilidad

Confidencialidad: Es la seguridad y certeza de que tus datos no serán visto por tercero sin autorización

Integridad: Asegura que la información no ha sido alterada de manera no autorizada, ya sea accidental o maliciosamente.

Disponibilidad: Garantiza que los sistemas, servicios y datos estén accesibles cuando se necesiten.

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

En una empresa de salud considero que es mas critico el de confidencialidad porque manejan datos personales muy sensibles: historiales médicos, diagnósticos, tratamientos, información genética, etc., están sujetos a regulaciones estrictas, como la HIPAA en EE. UU. o la LOPD/GDPR en Europa, una brecha de confidencialidad puede poner en riesgo la privacidad del paciente y la reputación de la institución.

Y en una de comercio electrónico seria la de disponibilidad porque si la tienda **no está disponible**, los clientes no pueden comprar lo que es igual pérdida directa de ingresos, también afecta también la experiencia del usuario y la percepción de fiabilidad.

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

1. **Confidencialidad** es la prioridad número uno si se manejan datos sensibles o regulados.
2. **Disponibilidad** es clave si se depende de sistemas en línea o si la empresa no puede permitirse tiempos de inactividad.
3. **Integridad** es crucial, pero a menudo puede esperar una vez que las medidas para confidencialidad y disponibilidad estén en marcha.

En cada caso, se deben maximizar las soluciones de **bajo costo** y **fácil implementación** mientras se va escalando conforme aumentan los recursos.

PARTE 2

Virus: Un **virus** es un tipo de malware diseñado para **infectar** y **modificar** archivos o programas en una computadora o sistema, y puede **auto-replicarse**. Se adhiere a archivos legítimos o programas y se ejecuta cuando el archivo infectado es abierto o ejecutado.

Un ejemplo sería CIH (Chernobyl) un virus que infectaba archivos ejecutables y, en algunos casos, borraba archivos importantes del sistema, además de dañar la BIOS de la computadora, volviendo la máquina inutilizable.

Gusano: A diferencia del virus, un **gusano** es un tipo de malware que **se replica** y se propaga por sí mismo, sin necesidad de un programa huésped. Se propaga generalmente a través de redes y sistemas, aprovechando vulnerabilidades en el software para infectar otras máquinas.

Un ejemplo sería ILOVEYOU un gusano que se propagó en mayo de 2000 a través del correo electrónico, infectando millones de computadoras y causando pérdidas económicas significativas. Se ocultaba en un correo con el asunto "I Love You" e infectaba a los contactos en la libreta de direcciones.

Troyano: El **troyano** es un tipo de malware que se presenta como un programa legítimo o útil, pero que **oculta** un comportamiento malicioso en su interior. El nombre proviene de la famosa historia del **Caballo de Troya**, ya que engaña a los usuarios para que lo instalen.

Un ejemplo sería Zeus un troyano bancario que se instala en computadoras con el propósito de robar credenciales bancarias. Se infiltra mediante phishing y es capaz de capturar información sensible del usuario.

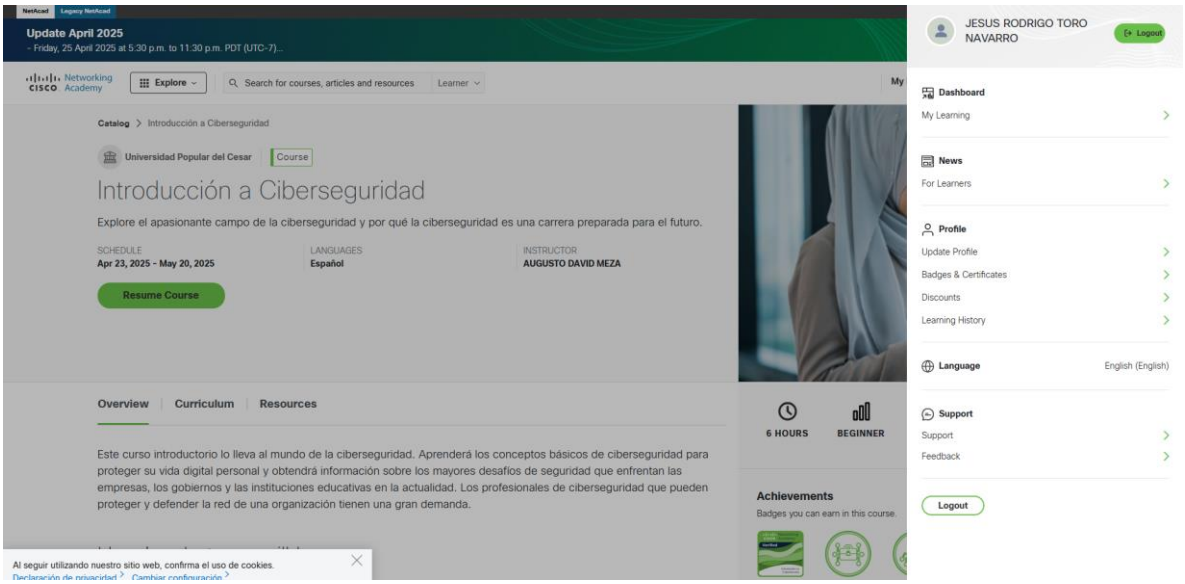
Ransomware: El ransomware es un tipo de malware que bloquea o cifra los archivos de la víctima y luego exige un rescate para devolver el acceso a los datos. Los ataques de ransomware son conocidos por su alta rentabilidad para los atacantes, ya que suelen involucrar pagos de rescates en criptomonedas.

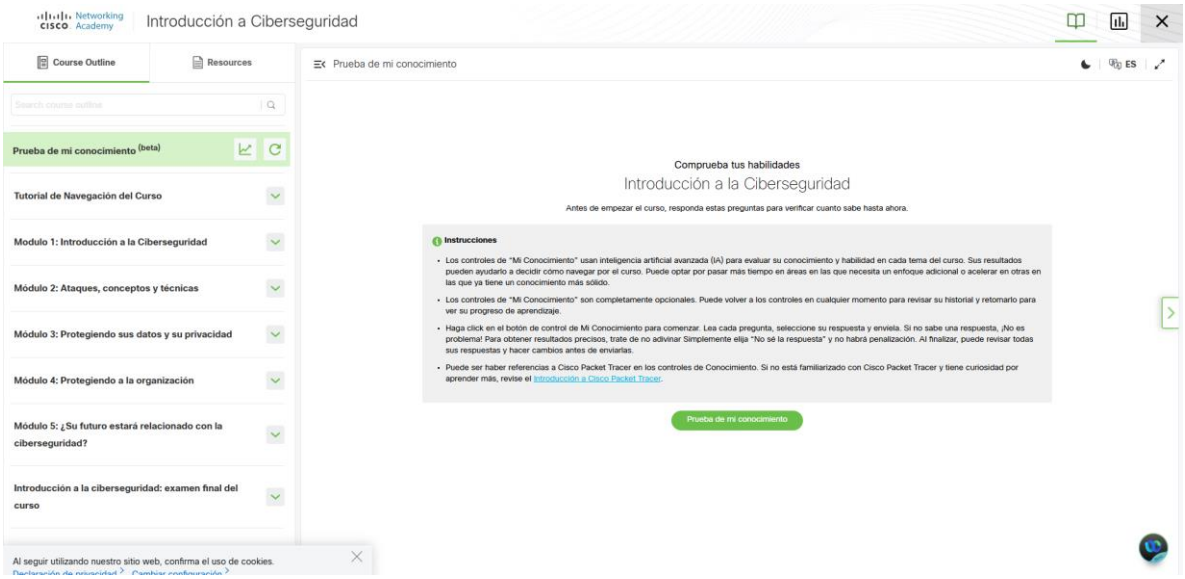
Un ejemplo sería WannaCry un ransomware masivo que afectó a cientos de miles de computadoras en 2017, explotando una vulnerabilidad en Microsoft Windows. Afectó a empresas, hospitales y organismos gubernamentales, y cifró archivos exigiendo pagos en Bitcoin.

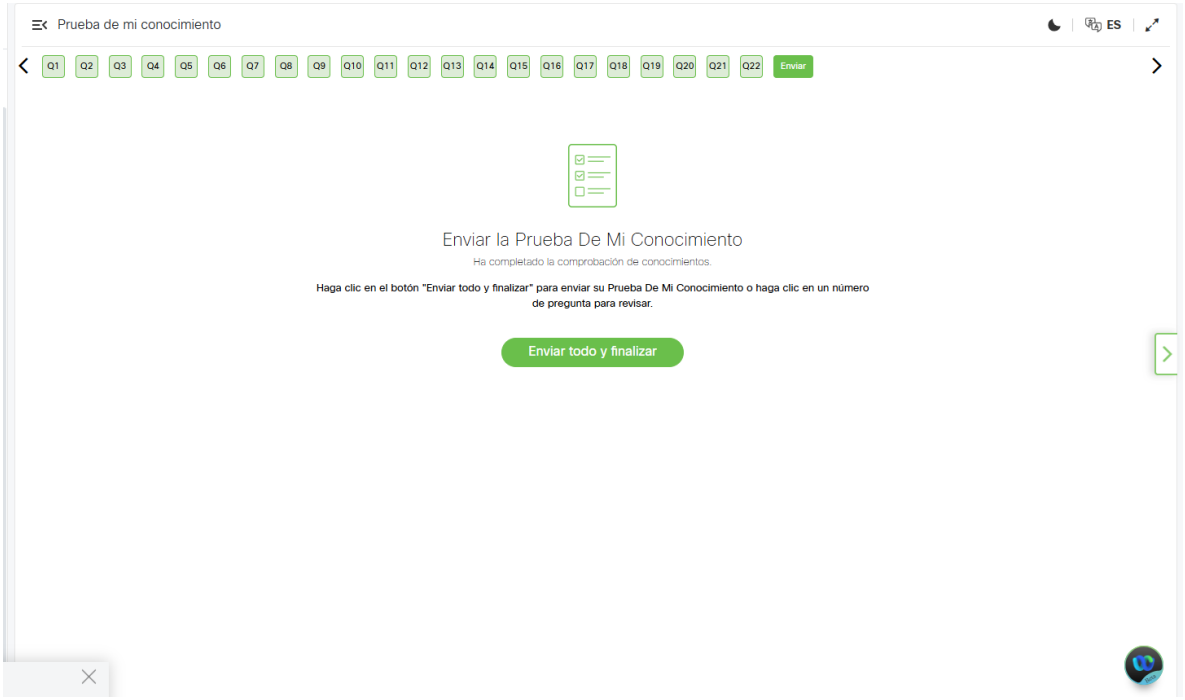
Spyware: El spyware es un tipo de malware que espía las actividades del usuario sin su conocimiento, con el fin de robar información sensible o para propósitos publicitarios. Generalmente, no causa daño directo al sistema, pero invade la privacidad del usuario.

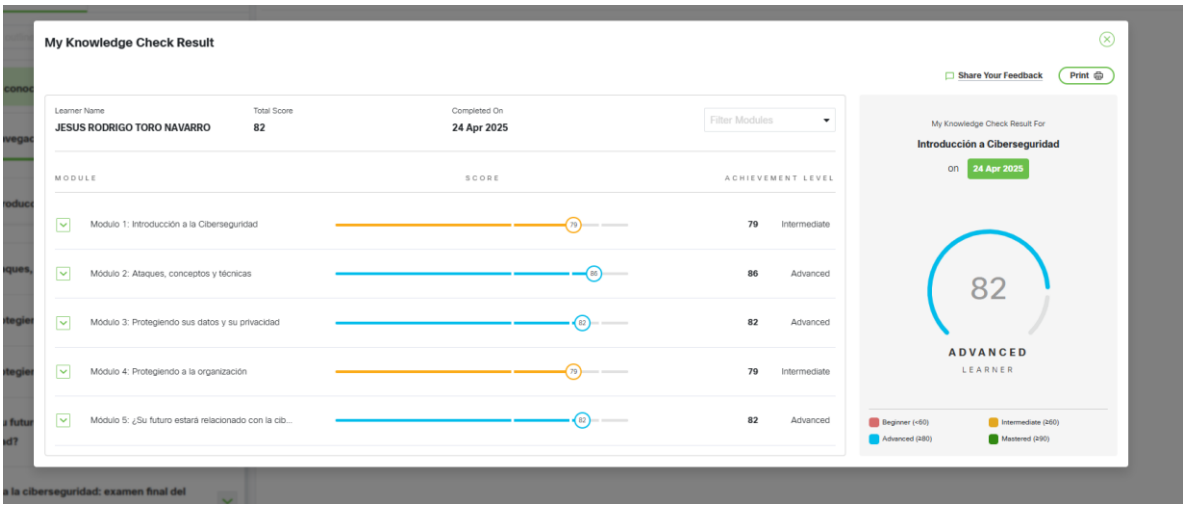
Un ejemplo sería CoolWebSearch un spyware que modificaba la configuración del navegador y redirigía las búsquedas a sitios web no deseados. Además, recopilaba información sobre las búsquedas de los usuarios para fines publicitarios.

CURSOS CISCO






Prueba de mi conocimiento
ES
Q1 Q2 Q3 Q4 Q5 Q6 Q7 Q8 Q9 Q10 Q11 Q12 Q13 Q14 Q15 Q16 Q17 Q18 Q19 Q20 Q21 Q22 Enviar
Enviar la Prueba De Mi Conocimiento
Ha completado la comprobación de conocimientos.
Haga clic en el botón "Enviar todo y finalizar" para enviar su Prueba De Mi Conocimiento o haga clic en un número de pregunta para revisar.
Enviar todo y finalizar


My Knowledge Check Result
Share Your Feedback
Print
Learner Name
JESUS RODRIGO TORO NAVARRO
Total Score
82
Completed On
24 Apr 2025
Filter Modules
MODULE
SCORE
ACHIEVEMENT LEVEL
Módulo 1: Introducción a la Ciberseguridad 79 Intermediate
Módulo 2: Ataques, conceptos y técnicas 86 Advanced
Módulo 3: Protegiendo sus datos y su privacidad 82 Advanced
Módulo 4: Protegiendo a la organización 79 Intermediate
Módulo 5: ¿Su futuro estará relacionado con la cib... 82 Advanced
My Knowledge Check Result For
Introducción a Ciberseguridad
on 24 Apr 2025
82
ADVANCED
LEARNER
Beginner (<60)
Intermediate (≥60)
Advanced (≥80)
Mastered (≥90)