

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

The image displays two screenshots of the Cisco Academy website. The top screenshot shows the course page for 'Introducción a Ciberseguridad' (Introduction to Cybersecurity) by Universidad Popular del Cesar. The page includes a 'Resume Course' button, a '6 HOURS' duration, and a 'BEGINNER' level. The bottom screenshot shows the 'Prueba de mi conocimiento' (Knowledge Check) interface, which includes a 'Comprueba tus habilidades' (Check your skills) section and a 'Prueba de mi conocimiento' button. The interface also features a sidebar with course outline and resources, and a bottom navigation bar.

Top Screenshot: Course Page

Update April 2025
- Friday, 25 April 2025 at 5:30 p.m. to 11:30 p.m. PDT (UTC-7) -

Networking
CISCO Academy

Explore Search for courses, articles and resources Learner

Catalog > Introducción a Ciberseguridad

Universidad Popular del Cesar Course

Introducción a Ciberseguridad

Explore el apasionante campo de la ciberseguridad y por qué la ciberseguridad es una carrera preparada para el futuro.

SCHEDULE Apr 23, 2025 - May 20, 2025 LANGUAGES Español INSTRUCTOR AUGUSTO DAVID MEZA

Resume Course

Overview Curriculum Resources

Este curso introductorio lo lleva al mundo de la ciberseguridad. Aprenderá los conceptos básicos de ciberseguridad para proteger su vida digital personal y obtendrá información sobre los mayores desafíos de seguridad que enfrentan las empresas, los gobiernos y las instituciones educativas en la actualidad. Los profesionales de ciberseguridad que pueden proteger y defender la red de una organización tienen una gran demanda.

6 HOURS BEGINNER

Achievements
Badges you can earn in this course

Dashboard My Learning News For Learners Profile Update Profile Badges & Certificates Discounts Learning History Language English (English) Support Support Feedback Logout

Al seguir utilizando nuestro sitio web, confirma el uso de cookies. [Participación de privacidad](#) [Cambiar configuración](#)

Bottom Screenshot: Knowledge Check Interface

Networking
CISCO Academy

Introducción a Ciberseguridad

Course Outline Resources

Search course outline

Prueba de mi conocimiento (beta)

Tutorial de Navegación del Curso

Módulo 1: Introducción a la Ciberseguridad

Módulo 2: Ataques, conceptos y técnicas

Módulo 3: Protegiendo sus datos y su privacidad

Módulo 4: Protegiendo a la organización

Módulo 5: ¿Su futuro estará relacionado con la ciberseguridad?

Introducción a la ciberseguridad: examen final del curso

Prueba de mi conocimiento

Comprueba tus habilidades
Introducción a la Ciberseguridad

Antes de empezar el curso, responde estas preguntas para verificar cuanto sabe hasta ahora.

Instrucciones

- Los controles de "Mi Conocimiento" usan inteligencia artificial avanzada (IA) para evaluar su conocimiento y habilidad en cada tema del curso. Sus resultados pueden ajustarlo a decidir cómo navegar por el curso. Puede optar por pasar más tiempo en áreas en las que necesita un enfoque adicional o acelerar en otras en las que ya tiene un conocimiento más sólido.
- Los controles de "Mi Conocimiento" son completamente opcionales. Puede volver a los controles en cualquier momento para revisar su historial y retomarlo para ver su progreso de aprendizaje.
- Haga click en el botón de control de Mi Conocimiento para comenzar. Lea cada pregunta, seleccione su respuesta y envíela. Si no sabe una respuesta, "No es problema! Para obtener resultados precisos, trate de no adivinar. Simplemente elija "No sé la respuesta" y no habrá penalización. Al finalizar, puede revisar todas sus respuestas y hacer cambios antes de enviarlas.
- Puede ser haber referencias a Cisco Packet Tracer en los controles de Conocimiento. Si no está familiarizado con Cisco Packet Tracer y tiene curiosidad por aprender más, revise el [Introducción a Cisco Packet Tracer](#).

Prueba de mi conocimiento

Al seguir utilizando nuestro sitio web, confirma el uso de cookies. [Participación de privacidad](#) [Cambiar configuración](#)

Prueba de mi conocimiento

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

