

LABORATORIO 2 TECH

JESUS DAVID DE LA HOZ PEÑA

UNIVERSIDAD POPULAR

VALLEDUPAR

2025

1) Definir lo siguiente:

Confidencialidad:

La confidencialidad se refiere a la propiedad de la información que garantiza que solo las personas autorizadas pueden acceder a ella. En otras palabras, es el deber de mantener la información en secreto y evitar su divulgación no autorizada, es decir que las personas no autorizadas no deben poder acceder a esa información.

Integridad

La integridad se refiere a la consistencia de la información, es decir personas no autorizadas no deben poder modificar a lo que no están autorizados, es decir la función de la integridad es garantizar que solo las personas autorizadas puedan cambiar sus datos

Disponibilidad

La disponibilidad es la capacidad de los sistemas y servicios para funcionar y ser accesibles cuando se necesitan, es decir deben estar disponible las 24 horas para que no se tenga problemas en caso de una urgencia

2) ¿ Que concepto considero más crítico en una empresa de salud y en una de comercio electrónico?

- En una empresa de salud lo mas importante es la confidencialidad debido a que la filtración de estos datos puede incluso afectar a los pacientes en su confianza, hay una confianza entre doctor-paciente y si la información es divulgada, la próxima vez el paciente puede terminar omitiendo datos esenciales.
- En una empresa de comercio electrónico lo mas importante es la integridad debido a que manejan bastantes transacciones entre el cliente-servidor, por tanto, si los datos no son correctos, el cliente puede terminar perdiendo esa confianza en la empresa terminando en menos ventas.

3) **¿Como podrías priorizar la implementación a una empresa con recursos limitados?**

Para priorizar la implementación de medidas de seguridad en una empresa con recursos limitados, es necesario identificar qué pilar del triángulo CIA (Confidencialidad, Integridad, Disponibilidad) es más importante según el tipo de negocio; por ejemplo, en salud suele ser la confidencialidad, mientras que en comercio electrónico puede ser la disponibilidad o la integridad. Luego, se deben clasificar los activos y riesgos, evaluando el impacto de una falla en cada pilar, y priorizar soluciones de bajo costo pero alto impacto, como controles de acceso, cifrado básico, respaldos frecuentes y capacitación al personal, enfocándose primero en los activos con mayor riesgo y en proteger aquello que, si se ve comprometido, causaría el mayor daño a la operación o reputación de la empresa, es decir teniendo en cuenta el enfoque de la empresa, se podría priorizar la implementación.

4) **Defina y de ejemplos:**

Virus

Es un programa que se adhiere a un archivo y cuando se ejecuta perjudica al usuario

Ejemplo: CIH (Chernobyl), que dañaba el BIOS del sistema.

Gusano

Se propaga solo a través de redes, sin necesidad de adjuntarse a archivos.

Ejemplo: WannaCry, que afectó miles de PCs en todo el mundo.

Troyano

Es un programa que imita a un programa legal o legítimo para engañar al usuario y robar su información

Ejemplo: Emotet, que aparentaba ser una factura o documento.

Ransomware

Es un programa que roba información cifrada y pide una recompensa para devolverlos

Ejemplo: LockBit, usado en ataques a empresas y hospitales.

Spyware

Es un espionaje que se le realiza al usuario sin permiso de él

Ejemplo: Pegasus, que accedía a cámaras, micrófonos y mensajes.

Taller Cisco

The screenshot displays the Cisco Academy interface for the 'Introducción a Ciberseguridad' course. On the left, a sidebar contains a 'Esquema de Curso' (Course Outline) with a search bar and a list of modules, each with a green checkmark indicating completion. The main content area is titled 'Prueba de mi conocimiento' (Test my knowledge) and shows 'Pregunta 4' (Question 4). The question asks: '¿Por qué las amenazas de seguridad internas pueden causar un daño mayor a una organización que las amenazas de seguridad externas?' (Why can internal security threats cause more damage to an organization than external security threats?). There are four radio button options: 'Los usuarios internos tienen mejores habilidades de hacking.' (Internal users have better hacking skills.), 'Los usuarios internos tienen acceso directo a los dispositivos de la infraestructura.' (Internal users have direct access to infrastructure devices.), 'Los usuarios internos pueden acceder a los datos de la organización sin autenticación' (Internal users can access organizational data without authentication), and 'Los usuarios internos pueden acceder a los dispositivos de la infraestructura a través de Internet' (Internal users can access infrastructure devices through the Internet). At the bottom, there is a checkbox for 'No se la respuesta' (No answer).

Resultado de mi comprobación de conocimientos



Comparta sus comentarios

Impresión

Nombre del estudiante		Puntaje total	Completado en		Módulos de filtro
JESUS DAVID DE LA HOZ PEÑA		66	24 Apr 2025		
MÓDULO	PUNTAJE			NIVEL DE LOGRO	
✓	Módulo 1: Introducción a la Ciberseguridad	<div><div></div></div> 67			67 Intermedio
✓	Módulo 2: Ataques, conceptos y técnicas	<div><div></div></div> 66			66 Intermedio
✓	Módulo 3: Protegiendo sus datos y su privacidad	<div><div></div></div> 68			68 Intermedio
✓	Módulo 4: Protegiendo a la organización	<div><div></div></div> 62			62 Intermedio
✓	Módulo 5: ¿Su futuro estará relacionado con la cib...	<div><div></div></div> 66			66 Intermedio

Mi resultado de la comprobación de conocimientos para

Introducción a Ciberseguridad

en **24 Apr 2025**

66

INTERMEDIO

ESTUDIANTE

Principiante (<60)

Intermedio (60)

Avanzado (80)

Dominado (90)