Cyber Security Introduction

Reactivos

Pregunta 1

¿Cuál es la definición de una amenaza de ciberseguridad?

Opciones:

a. La magnitud del daño causado por un ciberataque.
b. Un control de seguridad informática.
c. Un evento que genera incertidumbre en la ejecución de un objetivo.
d. Un acto malicioso que busca dañar datos o interrumpir la vida digital.

Pregunta 2

¿Qué es una vulnerabilidad en ciberseguridad?

Opciones:

a. Un evento inesperado durante la ejecución de una acción.
b. Una medida de seguridad que reduce el riesgo de ciberataques.
c. Una debilidad que los ciberdelincuentes pueden explotar para obtener acceso no autorizado.
d. La magnitud del daño causado por un ciberataque.

Pregunta 3

¿Cuál de las siguientes amenazas de ciberseguridad se caracteriza por bloquear el acceso a un sistema informático hasta que se pague un rescate?

Opciones:

a. Malware
b. Ransomware
c. Spyware
d. Ataques tipo *phishing*

Pregunta 4

¿Qué tipo de ataque tiene como objetivo cerrar una máquina o red, haciéndola inaccesible para los usuarios previstos?

Opciones:

a. Ataque de Denegación de Servicio (DoS)
b. Malware
c. Ransomware
d. Ataques de día cero

Pregunta 5

¿Cuál es el propósito de los controles de seguridad de la información en ciberseguridad?

Opciones:

a. Realizar ataques cibernéticos.
b. Reducir el riesgo de ciberataques y mejorar la seguridad de una organización.
c. Obtener acceso no autorizado a un sistema informático.
d. Bloquear el acceso a un sistema informático hasta que se pague un rescate.

Pregunta 6

¿Cuál es la definición de ciberseguridad?

Opciones:

a. Implementar procesos y herramientas de seguridad.
b. Aplicar tecnologías para proteger sistemas y datos.
c. Proteger la información comercial confidencial.
d. Salvaguardar recursos tangibles y no físicos.

Pregunta 7

Qué representa la tríada CIA en el contexto de la seguridad de la información?

Opciones:

a. Tres objetivos principales de la ciberseguridad.
b. Un modelo de seguridad basado en criptografía.
c. Un modelo de seguridad que se centra en la autenticidad.
d. La garantía de no repudio en la ciberseguridad.

Pregunta 8

¿Cuál es el propósito principal de un plan de seguridad de la información (ISP)?

Opciones:

a. Blindar el código de software contra intrusiones.
b. Garantizar la autenticidad de la información.
c. Maximizar las inversiones y oportunidades comerciales.
d. Proteger la información y los recursos críticos.

Pregunta 9

¿Cuál fue uno de los principales métodos de propagación del *ransomware*?

Opciones:

a. Ataques dirigidos a la tríada CIA.
b. Explotación de vulnerabilidades en servidores web.
c. Envío de correos electrónicos maliciosos.
d. Intrusión física en los sistemas de la organización.

Pregunta 10

¿Qué se debe cuidar en la seguridad de la información según el último párrafo?

Opciones:

a. El ciberespacio de la organización.
b. Los recursos físicos de la organización.
c. Los activos informáticos de la organización.
d. Toda la información dentro de la organización.

Pregunta 11

¿Cuál es el propósito principal de la familia de estándares ISO/IEC 27000?

Opciones:

a. Mejorar la seguridad de la información en las organizaciones.
b. Establecer un marco de referencia para mejorar la productividad.
c. Reducir el fraude con tarjetas de crédito.
d. Regular la privacidad y seguridad en la Unión Europea.

Pregunta 12

¿Qué se busca lograr con el estándar PCI DSS?

Opciones:

a. Mejorar la seguridad de la información en la Unión Europea.
b. Establecer un marco de referencia para mejorar la productividad.
c. Reducir la vulnerabilidad de la información del titular de la tarjeta.
d. Gestionar el riesgo en la prestación de servicios de TI.

Pregunta 13

¿Cuál de los estándares se enfoca en el cumplimiento normativo, la gestión de riesgos y la alineación de la estrategia de TI con los objetivos organizacionales?

Opciones:

a. GDPR
b. ISO 27000
c. COBIT
d. ITIL

Pregunta 14

¿Qué estándar de seguridad cibernética está diseñado para reducir la vulnerabilidad de la información del titular de la tarjeta en organizaciones que manejan datos de tarjetas de crédito?

Opciones:

a. GDPR
b. ITIL
c. ISO 27000
d. PCI DSS

Pregunta 15

¿Cuál de las siguientes normativas se aplica a la privacidad y seguridad de datos en la Unión Europea y puede resultar en fuertes multas por violación?

Opciones:

a. ISO 27000
b. GDPR
c. ITIL
d. COBIT

Pregunta 16

¿Por qué es importante para las organizaciones cumplir con las regulaciones de ciberseguridad?

Opciones:

a. Para garantizar la integridad de los datos.
b. Para evitar sanciones económicas.
c. Para reducir la necesidad de controles físicos.
d. Para mejorar la calidad de los productos y servicios.

Pregunta 17

¿Cuál es el propósito de una política de seguridad cibernética en una organización?

Opciones:

a. Definir procedimientos técnicos detallados.
b. Documentar la declaración de intenciones y enfoques para la gestión de riesgos.
c. Establecer controles físicos para prevenir amenazas.
d. Definir roles y responsabilidades del departamento de TI.

Pregunta 18

¿Cuál de los siguientes NO es un tipo de control de ciberseguridad?

Opciones:

a. Guardias de seguridad
b. Autenticación multifactorial
c. Cortafuegos
d. Política de seguridad cibernética

Pregunta 19

¿Cuál es el propósito principal de un plan de contingencia de ciberseguridad?

Opciones:

a. Identificar y gestionar las amenazas futuras de la organización.
b. Establecer políticas de seguridad cibernética.
c. Recuperar servicios y datos de TI después de una brecha de seguridad o desastre.
d. Proteger los datos y activos antes de que ocurra una brecha de seguridad.

Pregunta 20

¿Cuál de los siguientes estándares se centra en la planificación de la continuidad del negocio en caso de incidentes disruptivos?

Opciones:

a. ISO 22301.
b. ISO 27001.
c. ISO 9001.
d. ISO 14001.

Pregunta 21

¿Qué fase de la metodología PTES se enfoca en la recopilación de información del objetivo y la planificación de los ataques de ingeniería social?

Opciones:

a. Threat modelling
b. Pre-Engagement
c. Vulnerably analysis
d. Post-Exploitation

Pregunta 22

¿Cuál de las siguientes metodologías se centra en la identificación de vulnerabilidades de seguridad en aplicaciones web?

Opciones:

a. PTES

b. OWASP
c. OSSTMM
d. OWASP

Pregunta 23

¿Qué etapa de la metodología NIST se enfoca en la implementación de políticas de ciberseguridad y la preparación de un plan de respuesta ante amenazas?

Opciones:

a. Proteger
b. Detectar
c. Identificar
d. Responder

Pregunta 24

¿Qué tipo de información se considera como "abierta" en la metodología OSINT?

Opciones:

a. Información accesible al público
b. Información hackeada
c. Información robada
d. Información confidencial

Pregunta 25

¿Qué metodología se utiliza para realizar pruebas de penetración y pruebas de seguridad?

Opciones:

a. NIST
b. OSSTMM
c. OWASP
d. PTES

Pregunta 26

¿Cuál es el rol del CISO (Chief Information Security Officer) en una organización de ciberseguridad?

Opciones:

a. Auditar las prácticas de manejo de datos.
b. Gestionar la ciberseguridad de nivel operativo.
c. Proteger los activos de información de la empresa.
d. Supervisar que los recursos de la organización se empleen adecuadamente.

Pregunta 27

¿Cuál es la función principal del oficial de riesgos en ciberseguridad?

Opciones:

a. Probar la efectividad de los programas de seguridad.
b. Coordinar la respuesta y recuperación de incidentes de seguridad.
c. Desarrollar planes para mitigar los riesgos.
d. Capacitar a los empleados sobre buenas prácticas de seguridad.

Pregunta 28

¿Cuál es el objetivo principal del equipo *Red Team* en ciberseguridad?

Opciones:

a. Emular ataques para probar la efectividad de las medidas de seguridad.
b. Defenderse de ataques reales.
c. Evaluar los riesgos de ciberseguridad de la organización.
d. Coordinar esfuerzos de respuesta y recuperación.

Pregunta 29

¿Qué tipo de atacante busca exponer secretos de gobiernos y empresas que considera malvados o contrarios a sus ideales?

Opciones:

a. Crimen organizado
b. Hacktivista
c. Interno
d. ScriptKiddie

Pregunta 30

¿Cuál es el papel de un auditor de ciberseguridad en una organización?

Opciones:

a. Proteger los activos de información de la empresa.
b. Gestionar con los gerentes y dueños del proceso de negocio.
c. Evaluar los riesgos de ciberseguridad y desarrollar planes para mitigarlos.
d. Coordinar esfuerzos de respuesta y recuperación de incidentes de seguridad.

Pregunta 31

¿Cuál es el propósito del *hacking* ético en ciberseguridad?

Opciones:

a. Infiltrarse en redes sin autorización.
b. Auditar las prácticas de manejo de datos.
c. Realizar actividades maliciosas en entornos controlados.
d. Proteger y blindar organizaciones mediante la corrección de sistemas de seguridad.

Pregunta 32

¿Cuáles son algunas herramientas destacadas utilizadas en el *hacking* ético?

Opciones:

a. Microsoft Word, Excel y PowerPoint.
b. Security Onion, Linux Kali y Metasploitable.
c. Photoshop, Adobe Illustrator y InDesign.
d. Google Chrome, Mozilla Firefox y Safari.

Pregunta 33

¿Por qué se sugiere realizar una configuración manual en lugar de dejar que la red se aprovisione mediante DHCP en el contexto de seguridad de red?

Opciones:

a. La configuración manual evita que ingresen dispositivos ajenos en la red.
b. La configuración manual es más rápida y eficiente que DHCP.
c. DHCP es inseguro y puede permitir el acceso no autorizado a la red.
d. La configuración manual es la única opción disponible para redes seguras.

Pregunta 34

¿Qué es “metasploitable” en el contexto de la ciberseguridad?

Opciones:

a. Un firewall de última generación.
b. Un antivirus de código abierto.
c. Una máquina virtual con vulnerabilidades preconfiguradas para prácticas de ciberseguridad.
d. Una aplicación de gestión de contraseñas.

Pregunta 35

¿Cuál es el propósito del escaneo de puertos en ciberseguridad?

Opciones:

a. Determinar qué puertos están abiertos en una red y podrían recibir o enviar datos.
b. Identificar vulnerabilidades en sistemas operativos.
c. Realizar ataques de inyección SQL.
d. Proteger sistemas contra ataques de Cross-Site Scripting.

Pregunta 36

¿Qué es *Cloud Computing*?

Opciones:

a. Un modelo de almacenamiento de información en *hardware* especializado.
b. La gestión de datos en servidores físicos de una empresa.
c. Un método para almacenar información en dispositivos locales.
d. La disponibilidad de servicios computacionales a través de internet.

Pregunta 37

¿Cuál de los siguientes no es un modelo de servicio en *Cloud Computing*?

Opciones:

a. Servicio como *software* (SaaS).
b. Plataforma como servicio (PaaS).
c. Infraestructura como *software* (Iaas).
d. Infraestructura como servicio (IaaS).

Pregunta 38

¿Cuál de los siguientes modelos de despliegue de *Cloud Computing* implica utilizar tanto una nube privada como una nube pública?

Opciones:

a. Nube pública
b. Nube híbrida
c. Nube privada
d. Nubes comunitarias

Pregunta 39

¿Cuál no es una característica esencial de *Cloud Computing*?

Opciones:

a. Escalado de infraestructuras
b. La dependencia de *hardware* específico
c. Almacenamiento de datos
d. Análisis de *Big Data*

Pregunta 40

¿Qué modelo de servicio en *Cloud Computing* proporciona una pila de aplicaciones completas como servicios, como correo, calendarios y herramientas ofimáticas?

Opciones:

a. *Software* como servicio (SaaS).
b. Infraestructura como servicio (IaaS).
c. Plataforma como servicio (PaaS).
d. Almacenamiento como servicio (StaaS).