

Simulacro de Examen - Incidentes de Ciberseguridad

**Selecciona la opción correcta para cada una de las siguientes preguntas. Solo hay una respuesta válida por pregunta.**

1. **¿Qué es un incidente de ciberseguridad?**

A) Acceso no autorizado a sistemas

B) Uso normal del sistema

C) Mejora del rendimiento

D) Optimización de red

1. **¿Cuál es la primera fase en la gestión de incidentes de seguridad?**

A) Evaluación del daño

B) Notificación al equipo de TI

C) Detección del incidente

D) Restauración del sistema

1. **¿Qué herramienta se utiliza para el análisis forense digital?**

A) Norton Antivirus

B) EnCase

C) Microsoft Word

D) Google Chrome

1. **¿Qué significa el término 'phishing'?**

A) Creación de redes falsas

B) Suplantación de identidad

C) Optimización del tráfico

D) Mejora de la memoria

1. **¿Cuál es el objetivo principal de un plan de respuesta a incidentes?**

A) Mejorar el rendimiento del sistema

B) Maximizar la capacidad de almacenamiento

C) Minimizar el impacto en la organización

D) Reducir el uso de recursos

1. **¿Qué es un Plan de Concienciación en ciberseguridad?**

A) Proceso para cambiar hardware

B) Política de ventas

C) Software para diseño gráfico

D) Programa de educación en seguridad

1. **¿Qué fase es crucial en el ciclo de vida de un Plan de Concienciación?**

A) Preparación de backups

B) Monitorización y auditoría

C) Mejora de la red

D) Análisis financiero

1. **¿Qué técnica ayuda a evaluar la efectividad de un Plan de Concienciación?**

A) Cambio de contraseñas semanales

B) Instalación de software de diseño

C) Evaluaciones periódicas

D) Formateo de dispositivos

1. **¿Qué medida organizativa ayuda a proteger el puesto de trabajo?**

A) Política de uso de dispositivos externos

B) Uso libre de puertos USB

C) Desinstalar software crítico

D) Optimización de gráficos

1. **¿Qué medida técnica evita el uso no autorizado de dispositivos USB?**

A) Crear accesos directos

B) Restringir puertos USB

C) Cambiar la fuente del sistema

D) Aumentar el brillo de la pantalla

1. **¿Qué práctica ayuda a mantener la seguridad de la información en el puesto de trabajo?**

A) Dejar la sesión abierta

B) Compartir contraseñas

C) Bloquear la sesión al ausentarse

D) No actualizar el sistema operativo

1. **¿Qué técnica permite proteger la red de accesos no autorizados?**

A) Usar software sin licencia

B) Conectar cualquier dispositivo

C) Desactivar el antivirus

D) Implementar un sistema NAC

1. **¿Qué es OSINT en ciberseguridad?**

A) Sistema de cifrado

B) Análisis de malware

C) Herramienta de hacking

D) Inteligencia de fuentes abiertas

1. **¿Qué herramienta se usa para la investigación de identidades en OSINT?**

A) Shodan

B) Aircrack-ng

C) Maltego

D) Domaintools

1. **¿Qué significa SOC en ciberseguridad?**

A) Secure Online Connection

B) Security Operation Center

C) Server Operating Control

D) System Of Compliance

1. **¿Qué medida es fundamental en la fase de preparación para incidentes?**

A) Desarrollar políticas de seguridad

B) Instalar antivirus

C) Realizar backups

D) Bloquear puertos USB

1. **¿Qué herramienta permite realizar un volcado de memoria RAM?**

A) Maltego

B) Volatility

C) Shodan

D) Recon-ng

1. **¿Qué es una puerta trasera en ciberseguridad?**

A) Un tipo de firewall

B) Un método de encriptación

C) Un acceso no autorizado al sistema

D) Un software de autenticación

1. **¿Cuál es la principal función de un Plan de Recuperación ante Desastres (PRD)?**

A) Optimizar la velocidad

B) Eliminar malware

C) Restablecer servicios críticos

D) Configurar dispositivos móviles

1. **¿Qué técnica permite proteger discos duros ante fallos?**

A) RAID

B) Proxy

C) VPN

D) Firewall

1. **¿Qué es un 'Hot Site' en la recuperación de desastres?**

A) Copia de seguridad

B) CPD alternativo

C) Dispositivo de red

D) Sistema de monitorización

1. **¿Qué es el 'BIA' en el contexto del PCN?**

A) Base de Información Administrativa

B) Análisis de Impacto de Negocio

C) Barrera de Información Avanzada

D) Banco de Inversiones Activas

1. **¿Qué se debe hacer tras identificar un incidente en el sector público?**

A) Informar en redes sociales

B) Notificar al CCN-CERT

C) Eliminar registros

D) Auditar públicamente

1. **¿Qué organismo coordina la gestión de incidentes en administraciones públicas?**

A) INCIBE-CERT

B) RedIRIS

C) CCN-CERT

D) AEPD

# Caso Práctico: Ciberataque a una administración local

**Durante un lunes por la mañana, varios trabajadores de la administración local de un ayuntamiento español detectan fallos en el acceso a servicios internos como el correo y la gestión documental. El departamento de TI identifica que se ha producido un incidente de ciberseguridad tras una campaña de phishing exitosa contra varios empleados. Se ha desplegado malware y los sistemas críticos están comprometidos. El incidente es notificado y se activa el Plan de Respuesta a Incidentes. El equipo técnico trabaja en la contención, análisis, recuperación y comunicación del incidente a las autoridades competentes. Una vez restaurados los servicios, se ejecuta una auditoría técnica y se revisa el Plan de Continuidad del Negocio.**

1. **¿Cuál es la prioridad inmediata tras detectar el incidente?**

A) Informar por redes sociales

B) Apagar todos los equipos

C) Contener la amenaza y preservar evidencias

D) Actualizar los sistemas operativos

1. **¿Qué herramienta puede ayudar en el análisis de memoria del sistema afectado?**

A) Metasploit

B) Volatility

C) Aircrack-ng

D) BeEF

1. **¿Qué entidad debe recibir la notificación oficial del incidente?**

A) AEPD

B) INCIBE

C) CCN-CERT

D) RedIRIS

1. **¿Qué parte del PCN debe revisarse tras un incidente como este?**

A) Inventario de software

B) Plan de evacuación

C) Estrategias de recuperación y mantenimiento

D) Informe financiero

1. **¿Qué técnica forense digital se utilizaría para rastrear las actividades del malware?**

A) DLP

B) Sandboxing

C) Análisis de logs

D) Fuerza bruta

1. **¿Qué acción se recomienda tras restaurar el servicio?**

A) Auditoría técnica y documentación

B) Publicar el incidente en medios

C) Actualizar los perfiles en redes

D) Ignorar el evento si está resuelto