CONVOCATORIA	CL2024M
PLAZA/PUESTO	Técnico/a informático de gestión, encuadrada en la escala de Administración especial, subescala técnica, clase auxiliares
TIPO	Tercer ejercicio – Caso práctico
FECHA	09/04/2025

Supuesto práctico:

Como personal perteneciente al equipo técnico de TI en una administración pública que dispone de *3 sedes geográficas, 500 usuarios y sistemas críticos sujetos al* ENS (Nivel Alto), debe usted resolver las siguientes cuestiones técnicas críticas derivadas de una auditoría reciente.

1. Tras analizar un ataque de "ARP spoofing" en su red, se requiere implementar una solución que mitigue este riesgo cumpliendo con el ENS. ¿Qué combinación de medidas técnicas sería válida para Nivel Alto?: (2 puntos)

a) Configuración de port-security en switches + DHCP snooping.

b) Segmentación VLAN + desactivación de IPv6.

c) Implementación de 802.1X + IPsec en todos los segmentos.

d) Migración a IPv6 + filtrado MAC estático.

2. En el contexto del ENS (Nivel Alto), se detecta que un atacante está suplantando identidades mediante email spoofing en su dominio corporativo. ¿Qué conjunto de medidas técnicas implementaría para mitigar este riesgo de forma permanente y cumplir con la normativa?: (2 puntos)

a) Configuración de SPF + DMARC en modo "reject" + DKIM con claves RSA-2048.

b) Filtrado de correo basado en listas negras (RBL) + formación a usuarios.

c) Migración a OAuth 2.0 para autenticación + firma S/MIME en todos los correos.

d) Habilitar STARTTLS en el servidor MTA + cuarentena para correos sospechosos.

3. Según el ENS, ¿qué requisito es obligatorio para los certificados digitales utilizados en firma electrónica avanzada en un sistema de Nivel Alto?: (1 punto)

a) Emitidos por cualquier Prestador de Servicios de Certificación (PSC).

b) Algoritmos RSA-2048 y SHA-256 como mínimo.

c) Validez máxima de 5 años con renovación automática.

d) Almacenamiento exclusivo en HSM certificados FIPS 140-2 Nivel 3.

4. Describa un diseño simplificado para una arquitectura de confianza cero (Zero Trust), aplicable a la administración pública descrita en el enunciado principal, donde se incluya: (hasta 5 puntos)

- El modelo de autenticación y autorización (IAM). (1,5 punto)
- Un sistema de segmentación de red adaptable (microsegmentación). (1,5 punto)
- El sistema de protección de endpoints y monitorización proactiva. (1 punto)
- La integración con normativas (ENS, ISO 27001). (1 punto)