

Simulacro de Examen - Bastionado de Redes y Sistemas

**SIMULACRO DE EXAMEN: BASTIONADO DE REDES Y SISTEMAS**

**📌 Preguntas tipo test (24)**

1. **¿Cuál es el principal objetivo del análisis de riesgos en ciberseguridad?  
   A) Realizar copias de seguridad  
   B) Identificar vulnerabilidades  
   C) Proteger hardware únicamente  
   D) ✔ Prevenir incidentes de seguridad  
   *Tema 1***
2. **¿Qué norma se asocia con la gestión de seguridad de la información?  
   A) NIST 800-53  
   B) ✔ ISO 27001  
   C) CIS Controls  
   D) UNE 197010:2015  
   *Tema 2***
3. **¿Qué medida ayuda a mitigar errores humanos en seguridad?  
   A) ✔ Políticas de seguridad efectivas  
   B) Usar contraseñas débiles  
   C) Desactivar copias de seguridad  
   D) Permitir accesos sin restricciones  
   *Tema 1***
4. **¿Qué herramienta se utiliza para evaluar vulnerabilidades en sistemas operativos?  
   A) Firewall  
   B) Proxy  
   C) Antivirus  
   D) ✔ Análisis de vulnerabilidades  
   *Tema 1***
5. **¿Qué tipo de amenaza representa un ataque de tipo DDoS?  
   A) Desastre natural  
   B) Error humano  
   C) Falla del hardware  
   D) ✔ Ataque externo  
   *Tema 1***
6. **¿Qué es un estándar de securización?  
   A) Un antivirus avanzado  
   B) Una herramienta de cifrado  
   C) Un software de respaldo  
   D) ✔ Especificación técnica para minimizar riesgos  
   *Tema 2***
7. **¿Qué protocolo permite establecer conexiones seguras en redes?  
   A) Telnet  
   B) HTTP  
   C) FTP  
   D) ✔ VPN  
   *Tema 2***
8. **¿Qué técnica de autenticación se basa en algo que el usuario posee?  
   A) Ubicación geográfica  
   B) Contraseña  
   C) Huella dactilar  
   D) ✔ Token físico  
   *Tema 3***
9. **¿Qué componente es clave para el control de accesos físicos?  
   A) Software de respaldo  
   B) Antivirus  
   C) Firewall  
   D) ✔ Cámaras y alarmas  
   *Tema 2***
10. **¿Qué mecanismo permite autenticarse una sola vez para múltiples servicios?  
    A) Token de seguridad  
    B) Captcha  
    C) MFA  
    D) ✔ Single Sign-On (SSO)  
    *Tema 3***
11. **¿Qué tecnología utiliza ondas electromagnéticas para identificar dispositivos?  
    A) Bluetooth  
    B) NFC  
    C) Wi-Fi  
    D) ✔ RFID  
    *Tema 3***
12. **¿Qué tipo de cookie autentica al usuario en una sesión web?  
    A) Cookie publicitaria  
    B) Cookie de preferencia  
    C) Cookie de sesión  
    D) Cookie de seguridad  
    *Tema 3***
13. **¿Qué beneficio ofrece el uso de la firma electrónica?  
    A) Proteger archivos de virus  
    B) Mejorar el rendimiento de red  
    C) Aumentar memoria  
    D) ✔ Validez legal y agilidad en procesos  
    *Tema 4***
14. **¿Qué es una cuenta privilegiada?  
    A) Cuenta bloqueada  
    B) Cuenta temporal  
    C) Cuenta estándar  
    D) ✔ Cuenta con permisos avanzados  
    *Tema 5***
15. **¿Qué protocolo utiliza el servicio AAA para autenticar usuarios?  
    A) Telnet  
    B) ✔ RADIUS  
    C) FTP  
    D) SMTP  
    *Tema 5***
16. **¿Qué caracteriza al protocolo KERBEROS?  
    A) Permite acceso anónimo  
    B) Usa IPs dinámicas  
    C) No requiere credenciales  
    D) ✔ Autenticación segura en redes  
    *Tema 5***
17. **¿Cuál es el propósito de una Zona Desmilitarizada (DMZ)?  
    A) Compartir archivos sin seguridad  
    B) Aumentar velocidad de conexión  
    C) Eliminar malware  
    D) ✔ Aislar servicios accesibles desde internet  
    *Tema 6***
18. **¿Qué dispositivo se utiliza para crear una red VLAN?  
    A) Token físico  
    B) Firewall  
    C) Antivirus  
    D) ✔ Switch  
    *Tema 6***
19. **¿Qué solución protege el acceso a datos en la nube?  
    A) Red pública  
    B) Almacenamiento  
    C) Mejora de audio  
    D) ✔ CASB  
    *Tema 7***
20. **¿Qué tipo de ataque se enfoca en endpoints?  
    A) SQL Injection  
    B) Phishing  
    C) MITM  
    D) ✔ APT (Advanced Persistent Threat)  
    *Tema 7***
21. **¿Qué herramienta es fundamental para la seguridad del correo empresarial?  
    A) Reductor de ruido  
    B) Compresor de datos  
    C) Optimizador de archivos  
    D) ✔ Antimalware y antispam  
    *Tema 7***
22. **¿Qué diferencia hay entre IDS e IPS?  
    A) IDS bloquea y IPS detecta  
    B) Ninguno detecta amenazas  
    C) Ambos bloquean  
    D) ✔ IPS bloquea, IDS detecta  
    *Tema 8***
23. **¿Qué medida de seguridad se recomienda en la BIOS?  
    A) Desactivar funciones  
    B) Aumentar brillo  
    C) Acceso anónimo  
    D) ✔ Establecer contraseña de acceso  
    *Tema 9***
24. **¿Qué práctica recomendada existe para las copias de seguridad?  
    A) Evitar el cifrado  
    B) Hacerlas manualmente  
    C) Guardarlas en misma unidad  
    D) ✔ Realizarlas en entorno seguro y automatizado  
    *Tema 10***

**📂 Caso práctico: Seguridad en la red de una pequeña empresa**

**Enunciado:  
La empresa *RedSegura S.L.*, dedicada a servicios de consultoría digital, ha crecido y ahora dispone de 30 empleados. Recientemente ha sufrido un intento de acceso no autorizado a su servidor de correo y ha detectado dispositivos no registrados en su red. El departamento de TI está evaluando nuevas medidas de seguridad como la implementación de VLANs, la activación del Secure Boot en sus equipos, el despliegue de un SIEM y la auditoría de sus cuentas privilegiadas.**

**Preguntas del caso práctico (6)**

1. **¿Qué medida ayuda a aislar dispositivos por departamento en *RedSegura S.L.*?  
   A) Desactivar Wi-Fi  
   B) ✔ Crear VLANs en el switch  
   C) Utilizar Telnet  
   D) Usar cuentas compartidas  
   *Tema 6***
2. **¿Qué herramienta permite recolectar y analizar eventos de seguridad en la empresa?  
   A) Firewall  
   B) Antivirus  
   C) ✔ SIEM  
   D) DMZ  
   *Tema 8***
3. **¿Qué opción asegura el arranque confiable de los ordenadores?  
   A) Desactivar actualizaciones  
   B) Usar contraseñas débiles  
   C) ✔ Activar Secure Boot en BIOS  
   D) Compartir credenciales  
   *Tema 9***
4. **¿Qué riesgo representa no gestionar adecuadamente las cuentas con permisos avanzados?  
   A) Menor uso de recursos  
   B) Optimización del sistema  
   C) ✔ Acceso no autorizado a información sensible  
   D) Reducción del tráfico  
   *Tema 5***
5. **¿Qué método puede implementar la empresa para evitar compartir contraseñas en papel?  
   A) Base de datos sin cifrar  
   B) VPN abierta  
   C) ✔ Gestor de credenciales  
   D) Servidor FTP  
   *Tema 4***
6. **¿Qué protocolo podría reforzar las VPN en la empresa?  
   A) POP3  
   B) ✔ IPSec  
   C) SMTP  
   D) HTTP  
   *Tema 8***