1. **La Comisión Nacional del Mercado de Valores (en adelante, CNMV) tiene competencias de supervisión sobre las siguientes entidades:**
    A. Las Sociedades y Agencias de Valores.
    B. Las instituciones de inversión colectiva.
    C. Las empresas de asesoramiento financiero.
    D. Todas las respuestas anteriores son correctas.

2. **¿Cuáles de los siguientes NO es un Órgano rector de la CNMV?**
    A. El Comité Ejecutivo.
    B. El Departamento de Control Interno.
    C. El Presidente.
    D. El Consejo.

3. **Según el Reglamento (UE) 2016/679 (RGPD), ¿qué se entiende por datos personales?**
    A. Toda información relativa a personas jurídicas identificadas.
    B. Toda información relativa a personas físicas identificadas o identificables.
    C. Solo datos relativos a actividades financieras.
    D. Únicamente datos obtenidos a través de medios digitales.

4. **¿Cuál de los siguientes NO es un principio del RGPD?**
    A. Limitación de la finalidad.
    B. Minimización de datos.
    C. Máxima rentabilidad económica.
    D. Exactitud.

5. **El derecho de acceso recogido en el RGPD implica que una persona puede:**
    A. Modificar libremente los datos almacenados por cualquier entidad.
    B. Solicitar una copia de sus datos personales tratados por un responsable.
    C. Eliminar los datos de terceros.
    D. Prohibir el uso comercial de sus datos.

6. **Según la Ley Orgánica 3/2018 (LOPDGDD), ¿qué organismo vela por el cumplimiento de la normativa de protección de datos en España?**
    A. Tribunal Supremo.
    B. Agencia Española de Protección de Datos.
    C. Ministerio del Interior.
    D. Consejo General del Poder Judicial.

7. **La base jurídica más habitual para el tratamiento de datos personales según el RGPD es:**
    A. El consentimiento del interesado.
    B. La recomendación de terceros.
    C. La publicidad general.
    D. La rentabilidad comercial.

8. **La Ley Orgánica 3/2018 (LOPDGDD) garantiza los derechos digitales. ¿Cuál de los siguientes se considera un derecho digital contemplado en dicha ley?**
    A. Derecho al dividendo digital.
    B. Derecho a la desconexión digital.
    C. Derecho al acceso gratuito a internet.
    D. Derecho a la reparación tecnológica gratuita.

9. **Según el RGPD, ¿cuándo debe nombrarse obligatoriamente un Delegado de Protección de Datos (DPD o DPO)?**
    A. En todas las empresas con más de 10 trabajadores.
    B. Siempre que el tratamiento se lleve a cabo en el ámbito sanitario, pero nunca en el educativo.
    C. Solo cuando la empresa maneja exclusivamente datos financieros.
    D. Cuando las actividades principales del responsable impliquen operaciones que requieran una observación habitual y sistemática de personas a gran escala.

10. **Si una empresa ubicada en España utiliza servicios en la nube de un proveedor con servidores fuera de la Unión Europea, ¿qué debe garantizar principalmente según el RGPD?**
    A. Que los precios del servicio sean competitivos.
    B. Que el país receptor haya ratificado el Convenio Europeo de Derechos Humanos.
    C. Que existan garantías adecuadas como cláusulas contractuales tipo o decisiones de actuación aprobadas por la Comisión Europea.
    D. Que los servidores cuenten con certificaciones ISO independientes de la ubicación.

11. ¿Qué representa el concepto de "riesgo residual"?

A. El riesgo inicial antes de aplicar cualquier control.
B. El riesgo que permanece tras aplicar controles o medidas de mitigación.
C. El riesgo exclusivamente asociado a errores humanos.
D. El riesgo financiero derivado de una inversión tecnológica.

12. Según ISO/IEC 27005, ¿qué proceso se sigue para gestionar riesgos relacionados con la seguridad de la información?

A. Identificación, evaluación, tratamiento, aceptación y revisión periódica del riesgo.
B. Identificación y eliminación inmediata del riesgo.
C. Exclusivamente la prevención mediante auditorías externas.
D. Solo registro y documentación de riesgos sin tratamiento activo.

13. ¿Qué enfoque caracteriza la metodología OCTAVE para la evaluación de riesgos?

A. Enfoque exclusivo en herramientas automatizadas.
B. Enfoque centrado principalmente en controles tecnológicos avanzados.
C. Evaluación basada en escenarios predefinidos sin interacción humana.
D. Evaluación participativa centrada en la organización, activos y escenarios de amenazas.

14. Según ISO 31000, ¿cuál es la definición más precisa de riesgo?

A. Posibilidad de sufrir pérdidas financieras únicamente.
B. Incertidumbre sobre los objetivos, considerando tanto impactos negativos como positivos.
C. Probabilidad exclusiva de incidentes tecnológicos.
D. Consecuencia negativa inevitable de cualquier proyecto.

15. ¿Qué efecto genera un ransomware en el sistema infectado?

A. Cifra archivos para impedir el acceso a ellos.
B. Aumenta el rendimiento del equipo.
C. Realiza copias de seguridad automáticas.
D. Borra inmediatamente todos los archivos.

16. ¿Cuál de los siguientes perfiles NO debería formar parte del Comité de Riesgos de una empresa?

A. El director de cumplimiento normativo (compliance).
B. El responsable de seguridad de la información (CISO).
C. Un auditor contratado puntualmente.
D. El director financiero (CFO).

17. ¿Cuál es la fórmula correcta para calcular el Riesgo Residual (RR)?

A. RR = PI × I
B. RR = RI + EC
C. RR = RI – EC
D. RR = VA × FE

- **RR**: Riesgo Residual
- **RI**: Riesgo Inherente (riesgo antes de aplicar controles)
- **EC**: Eficacia de los Controles (o reducción del riesgo debido a los controles aplicados)
- **PI**: Probabilidad × Impacto (forma común de expresar el riesgo)
- **VA**: Valor del Activo
- **FE**: Factor de Exposición

18. ¿Cuál de los siguientes controles se encuentra definido específicamente en la norma ISO/IEC 27005?

A. Control de acceso basado en roles (RBAC).
B. Cifrado de la información en tránsito.
C. Registro y monitoreo de eventos de seguridad.
D. Ninguno; la norma ISO/IEC 27005 no define controles específicos, sino que proporciona un marco para la gestión del riesgo.

19. ¿Cuál es el objetivo principal de la norma ISO/IEC 27001?

A. Establecer buenas prácticas para la gestión de servicios TI.
B. Establecer un sistema de gestión ambiental.
C. Establecer, implementar, mantener y mejorar un SGSI.
D. Evaluar el cumplimiento legal de una organización.

20. ¿Qué tecnología permite detectar comportamientos anómalos o maliciosos en una red TIC?

A. IPS (Intrusion Prevention System).
B. SIEM (Security Information and Event Management).
C. VPN (Virtual Private Network).
D. ERP (Enterprise Resource Planning).

21. ¿Cuál de las siguientes técnicas permite detectar amenazas persistentes avanzadas (APT) en un entorno empresarial?

A. Escaneo de puertos periódicos.
B. Análisis de tráfico mediante Deep Packet Inspection (DPI).
C. Uso de antivirus tradicionales con firmas actualizadas.
D. Cifrado de datos en reposo.

22. ¿Qué ventaja clave aporta el uso de un sistema EDR (Endpoint Detection and Response) frente a un antivirus convencional?

A. Requiere menos recursos de CPU.
B. Permite análisis en tiempo real y respuesta ante incidentes.
C. No necesita conexión a internet.
D. Detecta únicamente malware basado en firmas.

23. ¿Cómo puede utilizarse Mitre ATT&CK para mejorar las capacidades defensivas de una organización?

A. Proporciona únicamente soluciones técnicas automáticas.
B. Documenta cómo se ejecutan los ataques para desarrollar controles defensivos específicos.
C. Elimina automáticamente el malware detectado.
D. Previene la ejecución de ataques DDoS.

24. ¿Qué característica es fundamental en un sistema de respaldo eficaz?

A. Que almacene los datos cifrados y en una ubicación distinta al entorno de producción.
B. Que dependa del equipo del usuario.
C. Que se actualice solo cuando existan errores.
D. Que use formatos de compresión antiguos.

25. ¿Cuál es una ventaja de utilizar políticas de “mínimos privilegios”?

A. Todos los usuarios pueden hacer todo desde el inicio.

B. Se mejora la experiencia de usuario.
C. Se reduce el riesgo de accesos indebidos o acciones no autorizadas.
D. Se requiere menos hardware.

26. ¿Qué medida técnica permite la recuperación granular de datos tras un incidente sin restaurar completamente la infraestructura?

A. Snapshot de disco a nivel de hipervisor.
B. Replicación basada en bloques.
C. Backup diferencial sobre almacenamiento definido por software.
D. Restauración granular desde backup por objetos (Object-Level Recovery).

27. ¿Cuál es una desventaja crítica de depender únicamente de backups incrementales diarios en entornos con datos críticos en tiempo real?

A. Ocupan más espacio que los backups completos.
B. No permiten la restauración a un punto preciso en el tiempo inmediato previo al incidente.
C. No pueden usarse en sistemas virtualizados.
D. Inhabilitan el versionado de archivos.

28. ¿Qué funcionalidad del protocolo Kerberos puede ser explotada si no se limita adecuadamente en entornos IAM?

A. Delegación no restringida que permite movimiento lateral tras comprometer una cuenta privilegiada.
B. Bloqueo automático de cuentas tras 3 intentos.
C. Expiración de sesión tras 8 horas.
D. Cifrado TLS en tránsito.

29. ¿Por qué se deben realizar pruebas regulares de restauración en una estrategia de recuperación?

A. Para comprobar que el backup ocupa poco espacio.
B. Para validar que los procedimientos funcionan y los datos son recuperables en el tiempo definido por el RTO.
C. Para evitar tener que realizar backups completos.
D. Porque es obligatorio en todos los países.

30. ¿Qué protocolo se utiliza para navegación web cifrada?

A. HTTP.
B. FTP.
C. SSH.
D. HTTPS.

31. ¿Qué garantiza el cifrado de datos "en reposo"?

A. Que los datos estén disponibles más rápido.
B. Que los datos almacenados estén protegidos frente a accesos no autorizados.
C. Que los datos se repliquen automáticamente.
D. Que los datos estén firmados.

32. ¿Cuál de los siguientes se considera un algoritmo de cifrado simétrico ampliamente utilizado?

A. RSA.
B. ECC.
C. SHA-256.
D. AES.

33. ¿Cuál de los siguientes protocolos garantiza cifrado extremo a extremo en comunicaciones?

A. FTP.
B. Telnet.
C. SSH.
D. SMTP sin TLS.

34. ¿Cuál es una buena práctica para evitar el uso de certificados caducados o comprometidos?

A. Habilitar OSCP stapling y automatizar la renovación mediante ACME (como Let's Encrypt).
B. Usar certificados autofirmados con validez indefinida.
C. No establecer fechas de expiración.
D. Reutilizar certificados antiguos.

35. ¿Cuál es la finalidad de la firma electrónica cualificada según eIDAS?

A. Firmar en papel y luego escanear.
B. Sustituir cualquier autenticación web.

C. Tener el mismo efecto legal que una firma manuscrita, con garantías técnicas reforzadas.
D. Solo para documentos administrativos menores.

36. En un clúster activo-activo con balanceo de carga, ¿qué sucede si un nodo falla?

A. Todos los servicios se interrumpen hasta que el nodo se reinicie.
B. El balanceador redirige automáticamente el tráfico a los nodos restantes.
C. El sistema entra en modo de mantenimiento.
D. Se pierden todos los datos procesados por ese nodo.

37. ¿Qué factor hace especialmente difícil la detección de ataques tipo Living off the Land (LotL)?

A. Utilizan tráfico cifrado exclusivamente.
B. Se basan en archivos adjuntos PDF maliciosos.
C. Emplean herramientas legítimas del sistema para ejecutar acciones maliciosas.
D. Necesitan vulnerabilidades zero-day para ejecutarse.

38. ¿Qué tipo de amenaza es más común en entornos cloud con configuraciones incorrectas de control de acceso?

A. Ataque DDoS.
B. Exposición accidental de datos.
C. Cross-Site Scripting (XSS).
D. Inyección de comandos.

39. ¿Cuál es una característica distintiva de una APT (Amenaza Persistente Avanzada)?

A. Utiliza malware de acceso masivo con ataques automatizados.
B. Se basa exclusivamente en ransomware para obtener beneficios económicos.
C. Permanece oculta durante largos periodos y emplea técnicas avanzadas de evasión.
D. Siempre requiere la explotación de vulnerabilidades en sistemas SCADA.

40. ¿Cuál es el principal beneficio de integrar inteligencia de amenazas en una solución SIEM?

A. Incrementar el rendimiento de los servidores.
B. Correlacionar eventos locales con indicadores de compromiso (IOCs) conocidos.
C. Detectar ataques físicos a servidores.
D. Optimizar el tráfico de red entre sedes remotas.

PREGUNTAS DE RESERVA:

41. ¿Cuál es uno de los principales desafíos técnicos para detectar campañas de smishing a nivel corporativo?

A. Los SMS están cifrados punto a punto.
B. El canal SMS no pasa por los sistemas de filtrado de correo ni firewalls convencionales.
C. Todos los SMS se almacenan en servidores del proveedor.
D. Los SMS no permiten incluir enlaces.

42. ¿Qué medida técnica es más eficaz para detectar un ataque DDoS en curso en una red empresarial?

A. Uso de firewall perimetral sin logs.
B. Monitoreo de volumen de tráfico inusual y patrones de paquetes en el IDS/IPS.
C. Revisión manual de tráfico en Wireshark.
D. Análisis del tiempo de carga de páginas web.