Universidad Autónoma de Madrid

PRUEBAS SELECTIVAS PARA EL INGRESO EN LA ESCALA ESPECIAL SUPERIOR DE SISTEMAS Y TECNOLOGIAS DE LA INFORMACION DE LA UNIVERSIDAD AUTONOMA DE MADRID, POR EL SISTEMA GENERAL DE OPOSICION LIBRE – TECNICO ANALISTA DE CIBERSEGURIDAD, CONVOCADO POR RESOLUCIÓN DE 28 DE OCTUBRE DE 2024 (BOE DE 7 DE NOVIEMBRE) (BOCM DE 8 DE NOVIEMBRE).

SEGUNDO EJERCICIO DE LA FASE DE OPOSICIÓN

2 de abril de 2025

No pasar esta página hasta que lo indique el tribunal

1) Qué características hacen que la información sea inútil en una organización?

a) Que sea relevante u oportuna.
b) Que sea precisa.
c) Que sea clara y comprensible.
d) Que sea toda la información posible.

2) ¿Qué elementos no están relacionados con el uso de la información en la Administración?

a) Planificación estratégica.
b) Control y evaluación.
c) Toma de decisiones informadas.
d) Ninguna de las anteriores.

3) ¿Qué organismo coordina la estrategia TIC en la Administración General del Estado?

a) La Secretaría General de Administración Digital (SGAD).
b) El Ministerio de Administraciones Públicas.
c) El Ministerio para la Transformación Digital y de la Función Pública.
d) El Centro Criptológico Nacional (CCN).

4) ¿Qué enfoque se utiliza comúnmente en la gestión de sistemas para garantizar su disponibilidad y rendimiento?

a) Gestión reactiva con planificación previa.
b) Implementación de un marco de trabajo como ITIL.
c) Uso exclusivo de herramientas de monitoreo manual.
d) Externalización completa de los sistemas sin supervisión.

5) ¿Qué herramienta se utiliza comúnmente para la planificación estratégica de TIC?

a) Balanced Scorecard.
b) Benchmarking.
c) Diagramas de flujo.
d) Herramientas de CRM.

6) ¿Qué concepto mide el retorno financiero de las inversiones en TIC?

a) TCO.
b) ROI.
c) KPI.
d) SLA.

7) ¿Qué tipo de mensaje utiliza un cliente para solicitar una dirección IP al servidor DHCP?

a) DHCPREQUEST.
b) DHCPACK.
c) DHCPNAK.
d) DHCPDISCOVER.

8) ¿Qué estándar Wi-Fi ofrece la mayor velocidad y menor latencia en dispositivos personales actuales?

a) Wi-Fi 4 (802.11n).
b) Wi-Fi 5 (802.11ac).
c) Wi-Fi 6 (802.11ax).
d) Wi-Fi 3 (802.11g).

9) ¿Cuál es la principal diferencia entre las redes Wi-Fi de 2.4 GHz y 5 GHz en cuanto a conectividad?

a) La red de 2.4 GHz tiene mayor velocidad y menor alcance.
b) La red de 5 GHz tiene mayor velocidad y menor alcance.
c) La red de 2.4 GHz tiene menor velocidad y menor alcance.
d) La red de 5 GHz tiene mayor velocidad y mayor alcance.

10) ¿Qué tipo de protección jurídica se aplica a los programas de ordenador bajo la legislación internacional?

a) Protección mediante patentes.
b) Protección mediante derechos de autor, sin necesidad de registro.
c) Protección a través de licencias de uso.
d) Protección a través de acuerdos de confidencialidad.

11) ¿Cuál de las siguientes técnicas se utiliza para calcular la ruta crítica en un proyecto?

a) Método PERT.
b) Análisis DAFO.
c) Técnica de Monte Carlo.
d) Diagrama de Pareto.

12) En la matriz de riesgos, ¿cómo se clasifica un riesgo con alta probabilidad y bajo impacto?

a) Riesgo crítico.
b) Riesgo secundario.
c) Riesgo tolerable.
d) Riesgo residual.

13) ¿Cuál es la principal desventaja del almacenamiento directo (DAS) frente a NAS o SAN?

a) Alta latencia.
b) Complejidad de configuración.
c) Falta de escalabilidad y uso compartido.
d) Costos elevados.

14) ¿Qué opción de systemctl permite habilitar un servicio para que se inicie automáticamente al arrancar el sistema?

a) systemctl restart servicio.
b) systemctl start servicio.
c) systemctl reload servicio.
d) Ninguna de las anteriores.

15) ¿Qué versión de Windows introdujo el requisito de TPM 2.0 para su instalación?

a) Windows 7.
b) Windows 8.
c) Windows 10.
d) Windows 11.

16) ¿Qué sistema de archivos usa macOS desde High Sierra en adelante?

a) NTFS.
b) HFS+.
c) APFS.
d) ext4.

17) ¿Qué tipo de firma electrónica tiene el mismo valor legal que una firma manuscrita?

a) Firma electrónica simple.
b) Firma digitalizada.
c) Firma electrónica cualificada.
d) Ninguna de las anteriores.

18) ¿Qué desafío se presenta en la integración de datos provenientes de dispositivos IoT en un sistema SIEM?

a) La falta de normalización en los formatos de los logs generados por los dispositivos IoT, que dificultan la correlación y el análisis de eventos.
b) La escasa cantidad de logs generados por los dispositivos IoT, lo que hace difícil identificar patrones de comportamiento anómalo.
c) La necesidad de incorporar inteligencia artificial para filtrar datos irrelevantes de IoT sin afectar la detección de amenazas.
d) La incapacidad de los dispositivos IoT para generar eventos significativos que puedan ser aprovechados por el sistema SIEM para realizar análisis de seguridad.

19) En un sistema de autenticación, si se utiliza un "sal" (salt) aleatorio para cada usuario, ¿qué factor adicional debe ser considerado para garantizar una seguridad robusta en el almacenamiento de contraseñas?

a) La longitud de la contraseña debe ser mayor a 12 caracteres.
b) El "sal" debe ser almacenado en un lugar separado del valor hash.
c) El "sal" debe ser reutilizado para cada usuario para facilitar su recuperación.
d) La función hash debe ser resistente a colisiones y debe aplicar múltiples iteraciones.

20) ¿Cómo se relaciona un sistema SIEM con el cumplimiento de la normativa de seguridad en la protección de datos, como el GDPR (Reglamento General de Protección de Datos)?

a) El SIEM asegura la encriptación de los datos personales para cumplir con el GDPR.
b) El SIEM permite la monitorización continua de los accesos y actividades en sistemas que contienen datos personales.
c) El SIEM se utiliza para realizar auditorías de las políticas de privacidad de la organización.
d) El SIEM garantiza que los datos personales se eliminen automáticamente después de un período de tiempo predefinido para cumplir con la normativa de retención de datos.

21) ¿Qué protocolo es utilizado para hacer más seguras la transmisión de audio o video en un sistema de video conferencias?

a) H.264.
b) H.323.
c) SRTP.
d) TLSv1.3.

22) ¿Cuál de las siguientes opciones sobre los generadores en Python ES CORRECTA?

a) Los generadores no pueden contener estructuras de control como if o while.
b) Los generadores son más rápidos que las listas en todos los casos.
c) Los generadores utilizan yield en lugar de return.
d) Una vez agotado un generador, se puede volver a iterar sobre él sin reiniciarlo.

23) ¿Cuál de las siguientes afirmaciones sobre asyncio en Python ES CORRECTA?

a) asyncio se usa para paralelismo en múltiples núcleos de CPU.
b) Permite ejecutar funciones síncronas sin bloquear el hilo principal utilizando async y await.
c) asyncio solo es compatible con Python 3.4 o superior.
d) No permite manejar excepciones dentro de funciones asíncronas.

24) ¿Cuál es la diferencia principal entre new y malloc() en C++?

a) malloc() inicializa la memoria asignada, mientras que new no.
b) new llama al constructor del objeto, mientras que malloc() no.
c) malloc() es más seguro que new.
d) new devuelve NULL en caso de error, mientras que malloc() lanza una excepción.

25) ¿Cuál de las siguientes características es exclusiva de C++ y no está presente en C?

a) Punteros y aritmética de punteros.
b) Sobrecarga de operadores.
c) Estructuras (struct).
d) Uso de la función printf para salida estándar.

26) ¿Qué significa la propiedad position: absolute; en CSS?

a) Posiciona un elemento con respecto al documento.
b) Posiciona un elemento en relación con su contenedor más cercano que tiene position.
c) Posiciona un elemento con respecto a la pantalla completa.
d) Posiciona el elemento en relación con su posición original.

27) ¿Qué formato de datos utiliza el protocolo SOAP para intercambiar información entre servicios web?

a) JSON.
b) YAML.
c) XML.
d) BSON.

28) En Web Services, ¿qué rol desempeña UDDI?

a) Define el formato de mensajes XML para Web Services SOAP.
b) Proporciona un directorio de servicios web para su descubrimiento y registro.
c) Gestiona la seguridad de los Web Services a través de autenticación y cifrado.
d) Permite convertir servicios REST en servicios SOAP automáticamente.

29) En Git, ¿qué comando permite deshacer un git add antes de hacer commit?

a) git revert <archivo> **.**
b) git reset HEAD <archivo>.
c) git stash pop.
d) git checkout HEAD <archivo>.

30) ¿Qué significa realizar un "rebase interactivo" en Git?

a) Modificar múltiples commits anteriores cambiando su orden, combinándolos o editándolos.
b) Resolver conflictos entre ramas de forma automática.
c) Fusionar múltiples ramas simultáneamente.
d) Sincronizar el repositorio local con múltiples repositorios remotos.

31) ¿Qué comando de Git se utilizaría para ver el historial de cambios de un archivo específico?

a) git diff filename.
b) git blame filename.
c) git log --follow filename.
d) git history filename.

32) ¿Qué reglamento europeo regula la identificación y firma electrónica en la UE?

a) RGPD.
b) Reglamento (UE) 2024/1689.
c) ENS.
d) eIDAS.

33) ¿Cuál de los siguientes algoritmos se usa comúnmente para la sincronización de relojes en sistemas distribuidos?

a) Algoritmo de Huffman.
b) Algoritmo de Dijkstra.
c) Algoritmo de Prim.
d) Algoritmo de Cristian.

34) En el modelo de computación en la nube, ¿qué capa de servicio proporciona entornos de desarrollo y herramientas sin gestionar la infraestructura subyacente?

a) PaaS.
b) IaaS.
c) SaaS.
d) Serverless Computing.

35) ¿Qué técnica permite reducir significativamente los tiempos de recuperación (RTO) en caso de desastre en un sistema crítico?

a) Restauración de snapshots de almacenamiento.
b) Backup diferencial con restauración en caliente.
c) Replicación continua con conmutación por error automática.
d) Almacenamiento y recuperación desde la nube.

36) En un sistema de almacenamiento WORM, ¿qué propiedad fundamental tiene el sistema de almacenamiento?

a) Aplica deduplicación en el almacenamiento por lo que resulta muy eficiente.
b) Mantiene historico de cambios y la modificación de los datos almacenados es accesible y reversible.
c) Utiliza RAID 10 para garantizar una alta tolerancia a fallos.
d) No permite modificaciones ni eliminaciones de datos una vez almacenados.

37) ¿Cuál es una ventaja clave de implementar canary deployments dentro de un pipeline de CI/CD?

a) Permite liberar nuevas versiones a un subconjunto de usuarios antes de un despliegue completo.
b) Reduce el tiempo de ejecución de las pruebas unitarias y de integración tras cada commit.
c) Elimina la necesidad de pruebas en entornos de staging.
d) Asegura que todas las instancias reciban la nueva versión de forma consistente.

38) Según el Esquema Nacional de Interoperabilidad (ENI), ¿cuál de los siguientes elementos es obligatorio en un documento electrónico?

a) Metadatos mínimos obligatorios para garantizar su interoperabilidad.
b) Firma electrónica interoperable en todos los documentos.
c) Un formato interoperable de acuerdo con los estándares internaciones.
d) Certificación de la autenticidad del documento mediante notario digital.

39) ¿Cuál de las siguientes afirmaciones sobre la gestión de expedientes electrónicos conforme al ENI, ES CORRECTA?

a) Un expediente electrónico debe contener solo documentos en formato PDF.
b) Los expedientes electrónicos contienen copias de los documentos en papel en formatos interoperables.
c) Solo los documentos firmados digitalmente pueden formar parte de un expediente electrónico.
d) Un expediente debe estar estructurado mediante índices, metadatos y relaciones entre documentos.

40) En el contexto de la documentación electrónica, ¿qué función cumple el CSV?

a) Permite verificar la autenticidad e integridad de un documento sin necesidad de firma electrónica.
b) Es un identificador único asignado a la dupla documento/usuario en la Administración.
c) Se utiliza para verificar la validad de la firma en los documentos electrónicos.
d) Es un código utilizado para validar la integridad de los expedientes electrónicos antes de su archivo.

41) En una API REST, ¿qué código de estado HTTP indica que la solicitud se ha procesado correctamente pero no devuelve contenido?

a) 204.
b) 201.
c) 200.
d) 206.

42) ¿Qué estándar de seguridad se recomienda para la autenticación y autorización en APIs RESTful?

a) WS-Security.
b) OAuth 2.0 con tokens JWT.
c) XML Encryption.
d) SAML con canal SSL.

43) ¿Cuál de los siguientes protocolos de VPN proporciona el mejor equilibrio entre seguridad y rendimiento en la actualidad?

a) PPTP.
b) WireGuard.
c) L2TP/IPsec.
d) SSTP.

44) En una VPN basada en IPsec, ¿cuál es la función del protocolo IKE?

a) Negociar y gestionar dinámicamente las claves de cifrado.
b) Cifra y autentica el tráfico de red para garantizar la confidencialidad e integridad de los datos.
c) Proporcionar autenticación extremo a extremo mediante certificados digitales.
d) Proporcionar autenticación multifactor basada en TOTP.

45) ¿Cuál de las siguientes afirmaciones sobre el protocolo HTTP/3 es correcta?

a) Usa el protocolo TCP para la transmisión de datos.
b) Está basado en QUIC desarrollado por Google.
c) Requiere que los servidores web utilicen certificados reconocidos.
d) No admite la multiplexación de conexiones.

46) ¿Cuál de los siguientes tipos de fibra óptica es más adecuado para largas distancias en redes de telecomunicaciones?

a) Fibra óptica plástica (POF).
b) Multimodo (MMF – Multi Mode Fiber).
c) Monomodo (SMF – Single Mode Fiber).
d) Fibra óptica de banda ancha (BBF).

47) En una comunicación que sigue el modelo OSI, ¿qué capa es responsable de la cifrado y compresión de datos?

a) Capa de sesión.
b) Capa de presentación.
c) Capa de aplicación.
d) Capa de red.

48) ¿Cuál de los siguientes algoritmos de cifrado se considera seguro para proteger las redes Wi-Fi bajo WPA3?

a) AES-GCMP.
b) RC4.
c) CCMP.
d) AES-CBC.

49) En un entorno Wi-Fi, ¿qué técnica permite dirigir la señal de un punto de acceso hacia un cliente específico para mejorar la cobertura y el rendimiento?

a) Frequency Hopping.
b) BSSID Hopping.
c) SSID Cloaking.
d) Beamforming.

50) ¿Cuál es la principal diferencia entre RIP y OSPF en cuanto al encaminamiento?

a) OSPF no requiere convergencia de rutas, a diferencia de RIP.
b) OSPF usa un mecanismo de conteo de saltos, mientras que RIP usa métricas de costo.
c) RIP es adecuado para redes grandes, mientras que OSPF solo se usa en redes pequeñas.
d) RIP es un protocolo de vector-distancia, mientras que OSPF es de estado de enlace.

51) ¿Qué algoritmo de encaminamiento utiliza OSPF para calcular la mejor ruta en una red IP?

a) Dijkstra.
b) Bellman-Ford.
c) Floyd-Warshall.
d) Distance Vector.

52) ¿Qué función tiene el protocolo Diameter en redes de servicios convergentes IMS?

a) Gestión de la calidad de servicio en redes basadas en NGN.
b) Transporte de datos multimedia en sesiones de videollamada.
c) Autenticación, autorización y control de acceso de usuarios.
d) Sustituir a SIP en la señalización de llamadas.

53) ¿Cuál de los siguientes protocolos es más seguro y se usa comúnmente en 802.1X para la autenticación de usuarios en redes cableadas e inalámbricas?

a) PAP.
b) EAP.
c) EAPol.
d) CHAP.

54) ¿Qué protocolo se usa en redes LAN inalámbricas para gestionar el acceso al medio y minimizar colisiones?

a) CSMA/CB.
b) CSMA/CD.
c) CSMA/CP.
d) CSMA/CA.

55) ¿Qué protocolo es comúnmente utilizado en redes LAN cableadas para evitar bucles de conmutación?

a) STP.
b) EIGRP.
c) DDP.
d) DCCP.

56) En un entorno de red donde se implementa VTP (VLAN Trunking Protocol) en modo transparente, ¿qué impacto tiene la adición de una nueva VLAN en un switch en este modo sobre los demás switches de la red?

a) La nueva VLAN se propaga a todos los switches de la red.
b) La nueva VLAN solo se configura localmente en el switch donde se creó.
c) Los demás switches actualizan sus bases de datos de VLANs, pero no la propagan.
d) Se produce un error de versión de VTP en los demás switches.

57) ¿Qué servicio de la Red SARA permite a las universidades verificar datos de identidad de los estudiantes?

a) Servicio de Notificaciones Electrónicas.
b) Servicio de Intercambio de Registros.
c) Servicio de Verificación de Datos.
d) Servicio de Firma Electrónica.

58) ¿Cuál de los siguientes NO es uno de los principios básicos del ENS establecidos en el Real Decreto 311/2022?

a) Seguridad por defecto.
b) Gestión de amenazas.
c) Seguridad integral.
d) Líneas de defensa.

59) De acuerdo con la Guía CCN-STIC 804: ENS. Guía de implantación. Indica cuál de las siguientes afirmaciones sobre la medida op.pl.2 Arquitectura de seguridad <u>ES CORRECTA</u>.

a) La arquitectura de seguridad es elaborada bajo la dirección del Responsable del Sistema, y es aprobada por el Responsable de la Seguridad.
b) La arquitectura de seguridad es elaborada bajo la dirección del Responsable del Seguridad, y es aprobada por el Responsable de la Sistema.
c) La arquitectura de seguridad es elaborada bajo la dirección del Responsable del Sistema, y es aprobada por el Comité de Seguridad de la Información.
d) La arquitectura de seguridad es elaborada bajo la dirección del Responsable del Seguridad, y es aprobada por el Comité de Seguridad de la Información.

60) De acuerdo con la Guía CCN-STIC 881: Guía de Adecuación al ENS para Universidades. ¿A quién se propone para ostentar la presidencia del Comité de Seguridad TIC de una universidad?

a) El Responsable de Seguridad de la Información.
b) El Director o Jefe de servicio TIC de la Universidad.
c) El Secretario General de la Universidad o vicesecretario delegado.
d) El Rector o su delegado.

61) De acuerdo con la Guía CCN-STIC 817: Guía de gestión de ciberincidentes. Un incidente que afecta a más del 50% de los sistemas de la organización, será considerado de nivel:

a) MEDIO.
b) ALTO.
c) MUY ALTO.
d) CRITICO.

62) De acuerdo con la Guía CCN-STIC 817: Guía de gestión de ciberincidentes.¿Qué herramienta del CCN es recomendada para la gestión de incidentes de seguridad?

a) ANA.
b) LUCIA.
c) GLORIA.
d) REYES.

63) ¿Qué nivel de impacto potencial de un incidente se considera significativo para que sea obligatoria su notificación al CCN?.

a) MEDIO, ALTO, MUY ALTO y CRÍTICO.
b) ALTO, MUY ALTO y CRÍTICO.
c) MUY ALTO y CRÍTICO.
d) CRÍTICO.

64) ¿Cuál de las siguientes herramientas del CCN es una solución desarrollada con el objetivo de identificar el compromiso de la red de una organización por parte de amenazas persistentes avanzadas (APT)?

a) CLAUDIA.
b) LORETO.
c) ELENA.
d) CARMEN.

65) ¿Cuál es la función principal de las Instrucciones Técnicas de Seguridad (ITS) emitidas por el CCN-CERT?

a) Establecer directrices técnicas de obligado cumplimiento para la aplicación del Esquema Nacional de Seguridad.
b) Establecer directrices técnicas recomendadas para la aplicación del Esquema Nacional de Seguridad.
c) Establecer directrices técnicas opcionales para la aplicación del Esquema Nacional de Seguridad.
d) Definir estándares de seguridad aplicables a cualquier tipo de Administración Pública.

66) ¿Cuál de las siguientes afirmaciones sobre las sanciones establecidas en la LOPDGDD y el RGPD <u>ES CORRECTA</u>?

a) Las sanciones pueden llegar hasta 10 millones de euros o el 2% del volumen de negocio anual global, según el RGPD.
b) Las sanciones pueden llegar hasta 10 millones de euros o el 4% del volumen de negocio anual global, según el RGPD.
c) Las sanciones pueden llegar hasta 20 millones de euros o el 4% del volumen de negocio anual global, según el RGPD.
d) Las sanciones pueden llegar hasta 20 millones de euros o el 2% del volumen de negocio anual global, según el RGPD.

67) Según la LOPDGDD, ¿cuál es el plazo máximo para notificar una violación de seguridad de datos personales a la Agencia Española de Protección de Datos?

a) 24 horas.
b) 72 horas.
c) 48 horas.
d) 7 días naturales.

68) ¿Cuál de los siguientes principios del RGPD hace referencia a la necesidad de justificar y documentar todas las actividades de tratamiento de datos personales?

a) Principio de seguridad y confidencialidad.
b) Principio de proporcionalidad en el almacenamiento.
c) Principio de licitud, lealtad y transparencia.
d) Principio de responsabilidad proactiva.

69) En el marco del RGPD, el interés legítimo puede ser una base jurídica válida para el tratamiento de datos personales cuando…

a) El responsable del tratamiento ha realizado una evaluación de impacto en la que se concluye que los riesgos para los interesados son bajos, permitiendo el uso del interés legítimo.
b) El tratamiento tiene una finalidad comercial clara y directa, siempre que el interesado no haya manifestado oposición expresa.
c) Se aplican medidas de minimización de datos y anonimización, lo que exime al responsable de justificar la base legal utilizada.
d) Se ha realizado una evaluación de intereses en la que se determina que los derechos y libertades del interesado no prevalecen sobre el interés del responsable o de un tercero.

70) ¿Qué sectores se consideran "entidades esenciales" bajo la Directiva NIS2?

a) Telecomunicaciones, defensa, investigación y comercio.
b) Defensa, energía, banca y transporte.
c) Energía, transporte, banca y salud.
d) Energía, banca, telecomunicaciones y defensa.

71) Según la Estrategia Nacional de Ciberseguridad 2019, el Consejo Nacional de Ciberseguridad tiene como una de sus funciones:

a) Asesorar al Consejo de Seguridad Nacional en materia de ciberseguridad.
b) Coordinar la respuesta ante incidentes de ciberseguridad a nivel nacional.
c) Elaborar y difundir normas, instrucciones, guías y recomendaciones de ciberseguridad.
d) Organizar la contribución de recursos a la ciberseguridad nacional conforme a lo establecido por la ley.

72) En la norma ISO/IEC 27001:2013, el documento que justifica la selección de los controles de seguridad a aplicar en una organización se denomina:

a) Declaración de Aplicabilidad.
b) Plan de Gestión de Riesgos.
c) Plan de Reducción del Perfil de Amenazas.
d) Declaración de Control de Amenazas.

73) ¿Cuál de las siguientes es una documentación que no se requiere para la certificación ISO 22301?

a) El Plan de Continuidad de Negocio.
b) El Análisis de Impacto en el Negocio.
c) El informe de auditoría externa.
d) El registro de pruebas.

74) ¿Cuál de las siguientes NO es una de las cuatro dimensiones de la gestión de servicios en ITIL v4?

a) Organizaciones y personas.
b) Información y tecnología.
c) Socios y proveedores.
d) Gestión financiera.

75) ¿Cuál de los siguientes factores NO es clave en la gestión de una auditoría informática?

a) Selección de un equipo auditor con las competencias adecuadas.
b) Realización formal del informe de análisis de impacto.
c) Establecimiento de un calendario detallado con hitos de auditoría.
d) Aplicación de metodologías reconocidas de evaluación y control.

76) ¿Qué se busca al realizar una auditoría operativa en TI?

a) Optimizar los procesos tecnológicos asegurando su alineación con los objetivos del negocio.
b) Evaluar la eficiencia de los sistemas a partir del tiempo de respuesta ante solicitudes de los usuarios.
c) Identificar posibles mejoras en el rendimiento de los sistemas para prolongar su vida útil.
d) Ajustar las políticas de TI para garantizar que se cumplan las normativas del sector.

77) ¿Qué tipo de análisis de riesgos se realiza en la metodología Magerit v3?

a) Análisis cuantitativo y de impacto.
b) Análisis cualitativo y de recuperación.
c) Análisis cuantitativo y cualitativo.
d) Análisis de impacto financiero y de negocio.

78) ¿Cuál de los siguientes desafíos es más crítico en la implementación y gestión de un SIEM en entornos empresariales complejos?

a) La integración con sistemas heredados y protocolos propietarios, lo que limita la correlación de eventos y dificulta la visibilidad de amenazas en infraestructuras antiguas.
b) La ingesta y procesamiento de volúmenes masivos de eventos en tiempo real sin comprometer el rendimiento ni generar una cantidad incontrolable de falsos positivos.
c) La imposibilidad de detectar técnicas de evasión avanzadas, como ataques basados en *living-off-the-land* (LotL), debido a la dependencia exclusiva de reglas de correlación predefinidas.
d) La falta de sincronización y estandarización de formatos en fuentes de logs distribuidas entre múltiples regiones geográficas, nubes públicas y privadas, lo que afecta la correlación y detección de amenazas en arquitecturas híbridas y de microservicios.

79) ¿Cuál es una de las diferencias clave entre EDR y XDR en la detección de amenazas?

a) EDR correlaciona eventos del endpoint mientras que XDR se enfoca más en una sola capa de seguridad.
b) EDR correlaciona eventos de múltiples capas de seguridad mientras que XDR se enfoca más en el endpoint.
c) XDR correlaciona eventos de una sola capa mientras que EDR se enfoca en múltiples capas de seguridad.
d) XDR correlaciona eventos de múltiples capas de seguridad mientras que EDR se enfoca en el endpoint.

80) ¿Cuáles de las siguientes son técnicas que los atacantes usan para evadir la detección de un sistema EDR?

a) Usando técnicas de inyección de código en procesos legítimos y ataques de tipo fileless.
b) Usando técnicas de tipo Living off the land (LotL), ataques de tipo fileless y Cryptojacking.
c) Realizando ataques de tipo fileless, XSS y ataques de replay.
d) Realizando ataques de tipo adversario en el medio (AitM), Spear phishing y uso de Controladores Vulnerables (BYOVD).

81) ¿Qué aspecto diferencia a un Red Team de un equipo de pentesting convencional?

a) Los Red Teams trabajan en estrecha colaboración con el Blue Team para corregir vulnerabilidades en tiempo real.
b) Los Red Teams realizan auditorías de cumplimiento sin explotar vulnerabilidades.
c) Los Red Teams operan con un enfoque más amplio, simulando ataques avanzados y persistentes (APT) con objetivos específicos.
d) Los equipos de pentesting utilizan técnicas más agresivas y sin limitaciones dentro de los entornos empresariales.

82) ¿Cuál de las siguientes herramientas sería más útil para un Blue Team en la detección de amenazas dentro de una infraestructura?

a) Metasploit.
b) Nmap.
c) Mimikatz.
d) Wireshark.

83) ¿Cómo se puede evitar la contaminación de la evidencia en el proceso de adquisición forense?

a) Accediendo a los archivos originales con permisos de solo lectura y copiándolos manualmente a otro dispositivo.
b) Asegurando que el investigador tenga privilegios administrativos en el sistema para acceder a toda la información sin restricciones.
c) Realizando la adquisición en un entorno desconectado de la red.
d) Utilizando bloqueadores de escritura que impidan cualquier modificación en el medio original.

84) ¿Cómo se puede evitar la contaminación de la evidencia en el proceso de adquisición forense?

a) Asegurando que el investigador tenga privilegios administrativos en el sistema para acceder a toda la información sin restricciones.
b) Accediendo a los archivos originales con permisos de solo lectura y copiándolos manualmente a otro dispositivo.
c) Realizando la adquisición en un entorno desconectado de la red.
d) Utilizando bloqueadores de escritura que impidan cualquier modificación en el medio original.

85) ¿Cuál de las siguientes afirmaciones sobre herramientas forenses <u>ES CORRECTA</u>?

a) Autopsy proporciona una interfaz gráfica para analizar discos, archivos y metadatos de manera forense.
b) FTK Imager permite la adquisición de imágenes forenses y su análisis profundo basado en sus módulos de análisis integrados.
c) Sleuth Kit es un conjunto de herramientas gráficas diseñado para el análisis de imágenes forenses.
d) EnCase es una herramienta de código abierto utilizada principalmente como estándar por las fuerzas y cuerpo de seguridad de muchos países.

86) ¿Cuál de los siguientes ataques está relacionado con la explotación de protocolos de autenticación en redes?

a) Ataque Pass-the-Hash (PtH), que permite autenticarse sin conocer la contraseña en sistemas Windows que usan NTLM.
b) Ataque "Evil Twin", que explota servidores DNS vulnerables para redirigir tráfico a sitios maliciosos.
c) Ataque Man-in-the-Browser (MitB), que intercepta comunicaciones cifradas sin necesidad de modificar credenciales.
d) Ataque Slowloris, que explota la gestión de sesiones en servidores web saturando sus conexiones.

87) En un escenario de defensa avanzada, ¿qué técnica puede ser empleada para detectar la presencia de un rootkit en un sistema Windows comprometido?

a) La inspección de los archivos de sistema críticos en busca de cambios inusuales en sus permisos y atributos, ya que los rootkits suelen ocultar su presencia en estos archivos.
b) La revisión de las configuraciones de red, ya que los rootkits modifican principalmente el tráfico y las configuraciones de red del sistema.
c) La utilización de herramientas de detección de rootkits chkrootkit y rkhunter.
d) El análisis de los controladores de dispositivos utilizando herramientas de hashing como sigcheck para comparar los hashes de los controladores contra bases de datos de firmas conocidas.

88) En la fase de exfiltración de datos en un ataque de APT, ¿qué técnica es más utilizada para evitar la detección por parte de sistemas de monitorización de red?

a) El uso de protocolos de red comúnmente permitidos como HTTPS para encapsular datos exfiltrados, evadiendo así sistemas de detección que no analizan el contenido del tráfico cifrado.
b) La creación de un túnel VPN utilizando credenciales válidas de la víctima, permitiendo que el tráfico de exfiltración sea enmascarado dentro de una conexión legítima.
c) La exfiltración de datos mediante archivos comprimidos y cifrados, los cuales son enviados en pequeños fragmentos a diferentes servidores de comando y control (C2).
d) El uso de técnicas de esteganografía para esconder los datos en archivos de imágenes o audio, evitando la inspección superficial de los contenidos transmitidos.

89) ¿Qué configuración en sysctl.conf ayuda a mitigar ataques de spoofing y escaneo de redes en un sistema Linux?

a) net.ipv4.conf.all.accept_redirects = 1.
b) net.ipv4.conf.all.log_martians = 1.
c) net.ipv4.conf.all.accept_source_route = 1.
d) net.ipv4.ip_forward = 1.

90) En el contexto de DevSecOps, ¿cuál de las siguientes prácticas es más efectiva para garantizar que la seguridad se integre de manera continua y fluida a lo largo del ciclo de vida del desarrollo de software, minimizando los riesgos de vulnerabilidades en producción?

a) Realizar auditorías de seguridad al final del proceso de desarrollo, asegurando que el código cumpla con los estándares de seguridad antes de ser lanzado a producción.
b) Incorporar pruebas de seguridad automatizadas dentro del pipeline.
c) Implementar parches de seguridad en las fases posteriores a la entrega del software, considerando que las vulnerabilidades en las fases iniciales son menos críticas para el ciclo de vida.
d) Utilizar herramientas de análisis de vulnerabilidades de infraestructura (como escaneos de seguridad en contenedores y configuraciones de infraestructura como código) durante el ciclo de vida de desarrollo.

91) En el contexto de orquestación de seguridad dentro de un entorno DevSecOps, ¿cuál de las siguientes herramientas es más utilizada para coordinar y automatizar la respuesta ante incidentes de seguridad a través de un flujo de trabajo automatizado?

a) TheHive.
b) Jenkins.
c) Trellix.
d) OWASP ZAP.

92) ¿Cuál es una ventaja clave de un IPS de nueva generación (NGIPS) frente a un IPS tradicional?

a) Reducción de la cantidad de eventos generados sin afectar la seguridad.
b) Inspección profunda de paquetes con capacidad de descifrado de tráfico cifrado.
c) Eliminación de la necesidad de actualizar las firmas de amenazas.
d) Operación exclusiva en la capa 2 del modelo OSI para reducir latencia.

93) En un archivo docker-compose.yml, ¿qué define la opción depends_on?

a) La opción depends_on especifica el orden en que se deben iniciar los contenedores en función de sus dependencias.
b) depends_on garantiza que los contenedores dependientes estén listos y disponibles antes de iniciar el contenedor principal.
c) depends_on asegura que los contenedores además de arrancar en un orden se detengan en el orden inverso al que fueron iniciados.
d) depends_on asegura que todas las dependencias entre contendores se tienen en cuenta y son resueltas antes de arrancar cada contenedor.

94) ¿Qué hace la directiva EXPOSE en un Dockerfile?

a) EXPOSE permite al contenedor compartir puertos con contenedores en otras redes Docker, facilitando la conectividad entre diferentes contenedores.
b) EXPOSE abre un puerto en el contenedor para que cualquier servicio externo pueda acceder a él, incluyendo tráfico de red externo al contenedor.
c) EXPOSE expone un puerto solo para que el sistema operativo host pueda acceder al contenedor.
d) EXPOSE documenta el puerto que la aplicación dentro del contenedor utilizará para la comunicación con otros contenedores o el host.

95) ¿Cuál de las siguientes técnicas criptográficas garantiza la integridad y la autenticidad de un mensaje, permitiendo verificar que no ha sido alterado durante su transmisión?

a) Cifrado simétrico.
b) Función de hash y firmas digitales.
c) Criptografía asimétrica.
d) Autenticación de mensajes (MAC).

96) ¿Qué protocolos pueden ser usados por los atacantes para lanzar ataques DoS de reflexión y amplificación?

a) LDAP.
b) NTP.
c) Memcached.
d) Todas las anteriores son correctas.

97) ¿Cuál es la función principal del registro DMARC?

a) Cifrar las comunicaciones entre servidores de correo electrónico.
b) Proteger contra ataques de denegación de servicio (DoS).
c) Definir cómo deben ser tratados los mensajes que fallan las verificaciones SPF y DKIM.
d) Filtrar el correo electrónico no deseado (spam).

98) ¿Cuál es la relación entre la clave privada DKIM, la clave pública DKIM y el registro DNS TXT en el proceso de autenticación de correo electrónico, y cómo se asegura la integridad del mensaje durante este proceso?

a) La clave privada se utiliza para cifrar el mensaje, la clave pública se utiliza para descifrarlo y el registro DNS TXT almacena la clave privada.
b) La clave pública se utiliza para firmar el mensaje, la clave privada se utiliza para verificar la firma y el registro DNS TXT almacena la clave pública.
c) La clave privada se utiliza para generar una firma digital que se incluye en la cabecera del mensaje, la clave pública se publica en el registro DNS TXT y se utiliza para verificar la firma.
d) La clave privada se utiliza para generar un hash del mensaje, la clave pública se utiliza para verificar el hash y el registro DNS TXT almacena el hash.

99) ¿Cuál es el propósito de las extensiones de cabecera en IPv6 y cómo contribuyen a la flexibilidad y extensibilidad del protocolo?

a) Las extensiones de cabecera se utilizan para la traducción de direcciones IPv4 a IPv6, manteniendo la compatibilidad.
b) Las extensiones de cabecera se utilizan para la gestión de la calidad del servicio (QoS), mejorando el rendimiento.
c) Las extensiones de cabecera se utilizan para añadir funcionalidades opcionales a la cabecera IPv6, permitiendo la evolución del protocolo sin modificar la cabecera base.
d) Las extensiones de cabecera se utilizan para la gestión de la seguridad, cifrando las comunicaciones IPv6.

100) ¿Cuál de los siguientes algoritmos es un ejemplo de cifrado asimétrico?

a) AES.
b) RSA.
c) 3DES.
d) DES.

PREGUNTAS DE RESERVA

101) ¿Qué permite hacer la licencia Creative Commons en relación con el uso de contenido?

a) Permite usar, modificar y distribuir el contenido sin restricciones.
b) Permite usar el contenido bajo ciertas condiciones, como atribución al autor y, en algunos casos, sin modificaciones.
c) Permite usar el contenido solo para fines no comerciales sin necesidad de atribuir al autor.
d) Permite que el contenido sea completamente público y se pueda compartir.

102) ¿Cuál de las siguientes topologías utiliza múltiples nodos para ofrecer almacenamiento redundante?

a) Almacenamiento distribuido.
b) Clúster de almacenamiento.
c) RAID 2.
d) Tiering.

103) ¿Qué combinación de teclas abre el Administrador de Tareas en Windows?

a) Ctrl + Alt + Supr.
b) Alt + F4.
c) Ctrl + Shift + Esc.
d) Windows + R.

104) ¿Cuál es el propósito principal del Protocolo OCSP (Online Certificate Status Protocol) en una PKI?

a) Valida la clave pública.
b) Verificar en tiempo real el estado de la CA.
c) Verificar en tiempo real el estado de un certificado digital.
d) Almacenar certificados en la nube.

105) ¿Por qué es importante el uso de mecanismos como RBAC en la seguridad de entornos corporativos?

a) Porque permite automatizar el acceso a todos los recursos de la red, garantizando una administración correcta.
b) Porque asegura que los usuarios solo accedan a los recursos necesarios según sus tareas y responsabilidades, limitando el riesgo de exposición de datos sensibles.
c) Porque permite el acceso de los usuarios a zonas seguras, validando previamente la seguridad de los dispositivos.
d) Porque obliga a que todos los usuarios utilicen distinto conjunto de credenciales, lo que aumenta la seguridad de los accesos.

106) ¿Qué salida genera el siguiente código en Python 3?

```
def func(val, lst=[]):
    lst.append(val)
    return lst

print(func(1))
print(func(2))
print(func(3))
```

a) [1] [2] [3].
b) [1] [1, 2] [1, 2, 3].
c) [1] [2] [3] [].
d) [1] [2] [3] [None].

107) ¿Qué hace el siguiente código en PHP?

```
<?php
$var = 10;
$var += "5";
echo $var;
?>
```

a) Imprime 15.
b) Imprime 5.
c) Imprime un error.
d) Imprime 105.

108) ¿Qué protocolo de Internet es responsable de intercambiar información sobre rutas entre sistemas autónomos (AS)?

a) OSPF.
b) BGP.
c) RIP.
d) IGMP.

109) ¿Qué función cumple un "pod" en Kubernetes y cómo afecta al despliegue de aplicaciones como microservicios?

a) Un pod es la unidad básica de despliegue en Kubernetes, que puede contener uno o más contenedores, y permite gestionar el ciclo de vida y la escalabilidad de los microservicios.
b) Un pod en kubernetes equivale a un contendor en docker.
c) Un pod una herramienta de monitoreo de contenedores que permite analizar el comportamiento de las aplicaciones microservicios en tiempo real.
d) Un pod es un servicio de almacenamiento en Kubernetes que permite compartir datos entre los contenedores de los microservicios.

110) ¿Qué tipo de dirección IPv6 se utiliza para la comunicación entre dispositivos en la misma red local?

a) Unicast global.
b) Multicast.
c) Link-local.
d) Anycast.