Ayuntamiento de Alcorcón

ACTA Nº 2

ACTA DE LA SESION DEL PRIMER EJERCICIO DE LA CONVOCATORIA PARA LA COBERTURA DE 1 PLAZA DE TÉCNICO SUPERIOR, PUESTO DE TRABAJO TÉCNICO/A DE SEGURIDAD INFORMÁTICA, MEDIANTE EL SISTEMA DE CONCURSO-OPOSICIÓN LIBRE PARA EL AYUNTAMIENTO DE ALCORCÓN.

En Alcorcón, siendo las 13:00 horas del día 12 de febrero de 2025, en la sala de reuniones de informática, calle Iglesia 7 de Alcorcón se reúnen los miembros asistentes del Órgano de Selección "DE 1 PLAZA DE TÉCNICO/A DE SEGURIDAD INFORMÁTICA, MEDIANTE EL SISTEMA DE CONCURSO-OPOSICIÓN LIBRE PARA EL AYUNTAMIENTO DE ALCORCÓN:

PRESIDENTA: Dña. Estela Fernández López

VOCALES: 1.- Dña. Silvia Jáñez Cordero
2.- Dña. Eva María Domínguez Jiménez
3.- Dña. Leonor Torres Moreno

SECRETARIO: D. Carlos Andrés Guerrero Fernández

ASESORES: D. Emilio González González
D. Fernando Menéndez Crespo

Es el objeto de esta sesión, la celebración del primer ejercicio del proceso de oposición, examen tipo test de 80 preguntas más 5 preguntas de reserva con 4 respuestas alternativas, siendo sólo una de ellas correcta, sobre la totalidad del temario indicado en el Anexo I (temario general y temario específico).

El acierto puntúa 0,25 y el error resta 0,08.

A tal efecto se procede a preparar el ejercicio entre todos los miembros del Tribunal, poniendo en común el trabajo realizado por cada uno de ellos en función de su especialización profesional.

Impresos tales ejercicios en presencia de todos los miembros asistentes en las oficinas del Departamento de Informática, se procede a su clasificado, grapado y ensobrado, de tal forma que, ultimadas tales cuestiones, se realiza un desplazamiento al lugar del examen (IMEPE), para un reconocimiento del aula y se realizan pequeñas adaptaciones en pupitres y ventilación de la sala para asegurar la máxima comodidad y seguridad de los aspirantes.

De conformidad con las determinaciones de la convocatoria (acta anterior), y dando por finalizada la preparación del ejercicio, la Presidenta da orden de comenzar con el llamamiento de los aspirantes en el entorno de las 16:00 horas, concurriendo los siguientes que se dirán, debidamente identificados, que conforme van entrando van recibiendo instrucciones sobre el modo en que se haya de proceder para la realización del ejercicio, así como hoja de datos personales, sobres para introducir los diversos documentos y hojas para desarrollar los ejercicios propuestos:

APELLIDO 1	***APELLIDO 2***	***NOMBRE***
ANDRÉS	ESPINAL	LIDIA
DIAZ DEL CAMPO	HORTIGÜELA	ALBERTO
LOPEZ	MOLLO	JESUS
MARTINEZ DE MUNIAIN	IRIGOYEN	PEDRO
MIGUEL	MERINO	JOSE LUIS
MONGE	GALLEGO	ADRIAN
QUINTANA	VAQUERO	RUTH
SERRANO	MAYOR	EUGENIO

Admitidos los aspirantes del cuadro previa puntual comprobación de su identidad, da comienzo el ejercicio, no produciéndose durante su desarrollo incidencia alguna.

Terminado el examen en el entorno de las 17:40 horas tras 90 minutos conferidos, se informa sobre el modo en el que se va a proceder a recoger el sobre que contiene los ejercicios realizados y el sobre cerrado con datos identificativos de cada aspirante, documentos que son introducidos por cada uno de ellos, que proceden a su cierre de manera ordenada y diligente.

Uno de los opositores centraliza la recogida de todos los sobres y procede a su mezcla aleatoria y numeración, previamente a que sean custodiados hasta el momento en que se vaya a producir la corrección de los ejercicios, que será absolutamente anónima, pues los sobres que contienen la identificación del aspirante no serán abiertos hasta que hayan sido corregidos todos los ejercicios. Comienza la corrección sin solución de continuidad.

Resultado de la corrección, se tiene

Sobre	Nombre de Opositor	Acertadas + 0,25	Falladas – 0,08	No contestadas	Puntuación
1	RUTH QUINTANA VAQUERO	61	9	10	14,53
2	PEDRO MARTINEZ DE MUNIAIN IRIGOYEN	53	6	21	12,77
3	EUGENIO SERRANO MAYOR	64	8	8	15,36
4	ALBERTO DIAZ DEL CAMPO	71	7	2	17,19
5	LIDIA ANDRÉS ESPINAL	72	8	0	17,36
6	JOSE LUIS MIGUEL MERINO	73	7	0	17,69
7	JESÚS LÓPEZ MOLLO	75	1	4	18,67
8	ADRIAN MONGE GALLEGO	62	13	5	14,46

Estableciendo las bases de la convocatoria que al segundo ejercicio tan solo pueden optar aquellos aspirantes que hayan superado el primero por haber obtenido una puntuación de 10 o más puntos, se convoca a todo los opositores que han obtenido al menos esa puntuación para la realización del **SUPUESTO PRÁCTICO** relacionado con el programa que figura como temario específico dentro del Anexo I de las bases (que será propuesto por el Órgano de Selección en el momento de realización de la prueba) **EL DÍA 25 DE MARZO DE 2025** en el Centro de Formación del Instituto Municipal para el Empleo y la Promoción Económica de ALCORCÓN (IMEPE), Calle Industrias, 73 de esta Localidad, **a las 10:30 horas**.

El Tribunal acuerda por unanimidad **NO** permitir a los opositores la entrada de ningún tipo de legislación o documentación de apoyo, ya sea en formato papel o digital. Exclusivamente se permitirá una calculadora, con exclusión expresa de otros dispositivos electrónicos con conexión a internet.

Para la lectura del ejercicio, que no podrá superar los 20 minutos, **se cursará pública convocatoria específica**, quedando los exámenes totalmente precintados y a disposición del Secretario hasta ese momento, **lo que se aprueba por unanimidad**.

El orden de lectura, en llamamiento único, será el resultante de del que en suerte ha tocado al número de sobre para cada opositor.

El Tribunal podrá hacer preguntas sobre lo expuesto con el objeto de precisar conceptos y valorar la calidad de la solución planteada.

Los parámetros de calificación de los ejercicios serán:

Los criterios de valoración del supuesto práctico serán los siguientes, sobre la puntuación máxima de cada ejercicio:

- 60%, conocimientos Técnicos (15 puntos) sobre la materia consultada, correcto manejo de conocimientos técnicos, la madurez y soltura en la aplicación de los conocimientos a la realidad de la profesión, en un nivel puramente práctico.

- 30 %, capacidad de análisis, justificación y orden (7,5 puntos): adecuada identificación y concreción del verdadero problema planteado y el planteamiento en su resolución.
- 10%, Capacidad de expresión escrita y oral (2,5 puntos): capacidad de comunicación del candidato, con un uso adecuado del lenguaje en su vertiente morfosintáctica,

respuesta a las preguntas del Tribunal fluida y acorde a las normativas y buenas prácticas profesionales.

Los aspirantes deberán venir debidamente identificados con su DNI.

Siendo las 18:20 horas, terminado el ejercicio tras agradecer a los aspirantes lo realizado, y corregido éste, por la Sra. Presidenta se levanta la sesión, extendiéndose la presente acta que será firmada en prueba de conformidad, de todo lo cual, como Secretario del Tribunal, doy fe.

EL SECRETARIO
Don Carlos Andrés Guerrero Fernández

Firmado por CARLOS ANDRES GUERRERO FERNANDEZ - ***5180** el día 06/03/2025 con un certificado emitido

VºBº LA PRESIDENTA
Dña. Estela Fernández López

Firmado por ESTELA FERNANDEZ LOPEZ - ***0622** el día 10/03/2025 con un certificado emitido por AC CAMERFIRMA FOR

VOCAL 1
Dña. Silvia Jáñez Cordero

Firmado por SILVIA JAÑEZ CORDERO - 71555132Q el día 06/03/2025 con un

VOCAL 2
Dña. Eva María Domínguez Jiménez

DOMINGUEZ JIMENEZ EVA MARIA - 50855116T

Firmado digitalmente por DOMINGUEZ JIMENEZ EVA MARIA - 50855116T
Fecha: 2025.03.06 16:27:18 +01'00'

VOCAL 3
D. Leonor Torres Moreno

Firmado por TORRES MORENO MARIA LEONOR - ***4678** el día 07/03/2025 con un

Los/las aspirantes dispondrán de un plazo de cinco días hábiles, contados a partir del siguiente al de la publicación, para presentar alegaciones, en su caso, a la presente acta, que serán resueltas por el propio Órgano de Selección.

ANEXO AL ACTA – PLANTILLA DE CORRECCIÓN

1. **El Rey prestará juramento de desempeñar fielmente sus funciones, guardar y hacer guardar la Constitución y sus leyes y respetar los derechos de los ciudadanos y de las Comunicades autónomas**
   - **a) Al ser proclamado por las Cortes Generales**
   - **b)** Al ser proclamado por el Congreso
   - **c)** Al ser proclamado por el Senado
   - **d)** Al ser proclamado por el presidente del Gobierno

2. **¿Podemos encontrar la fecha y hora oficial en las sedes electrónicas o sedes electrónicas asociadas de las Administraciones Públicas?**
   - **a)** No
   - **b) Si**
   - **c)** Solo en el caso de las Administraciones Locales
   - **d)** Solo en el caso de las Administración General del Estado

3. **¿Qué clase de sistema de identificación electrónica es Cl@ve?**
   - **a)** Un sistema basado en criptografía de clave pública para firma electrónica
   - **b) Un sistema de autenticación orientado a servicios públicos**
   - **c)** Un sistema de identificación de usuarios utilizando huella dactilar como factor único
   - **d)** Un sistema de verificación biométrica de acceso remoto a infraestructuras críticas

4. **¿Qué es la Dirección Electrónica Habilitada Única (DEHu)?**
   - **a)** Un buzón postal de notificaciones para facilitar a los ciudadanos el acceso y comparecencia a sus notificaciones y/o comunicaciones emitidas por las Administraciones Públicas Adheridas.
   - **b)** Un registro físico de notificaciones para facilitar a los ciudadanos el acceso y comparecencia a sus notificaciones y/o comunicaciones emitidas por las Administraciones Públicas adheridas.
   - **c) Un Servicio electrónico de notificaciones para facilitar a los ciudadanos el acceso y comparecencia a sus notificaciones y/o comunicaciones emitidas por las Administraciones Públicas adheridas.**
   - **d)** Ninguna es correcta.

5. **Son empleados públicos quienes:**
   - **a)** Desempeñan funciones retribuidas en las Administraciones Públicas al servicio de los intereses particulares
   - **b)** Desempeñan funciones voluntarias en las Administraciones Públicas al servicio de los intereses generales
   - **c)** **Desempeñan funciones retribuidas en las Administraciones Públicas al servicio de los intereses generales**
   - **d)** Ninguna es correcta

6. **Un emisor firma un documento con su certificado X.509 y lo envía telemáticamente a un receptor ¿Qué debe usar el receptor para verificar la integridad del documento firmado?:**
   - **a)** La parte privada de su clave asimétrica
   - **b)** La parte pública de su clave asimétrica
   - **c)** La parte privada de la clave asimétrica del emisor
   - **d)** **La parte pública de la clave asimétrica del emisor**

7. **En Alcorcón, la máxima representación del municipio la ostenta:**
   - **a)** El Pleno
   - **b)** La Junta de Gobierno Local
   - **c)** **El alcalde o alcaldesa**
   - **d)** Los concejales

8. **Respecto a la seguridad en redes, indique qué es un "Exploit":**
   - **a)** **Es un malware diseñado para aprovechar la vulnerabilidad de un software**
   - **b)** Persona que accede a datos no autorizados
   - **c)** Adware que modifica la página de inicio de los navegadores de Internet sin el consentimiento del usuario
   - **d)** Software utilizado para la suplantación de la identidad de un usuario de la red

9. **En el Ayuntamiento de Alcorcón el alcalde o alcaldesa se elige:**
   - **a)** **Por los concejales**
   - **b)** Por el Gobernador civil
   - **c)** Por la ciudadanía en elecciones libres e iguales
   - **d)** Ninguna de las anteriores es correcta

10. **¿Qué es un "honeypot"?**
    - **a)** Un ataque de phishing
    - **b)** Una técnica de encriptación
    - **c)** **Un sistema para atraer a los atacantes**
    - **d)** Una técnica de ocultación de archivos

11. **¿Cómo se denomina el certificado que autentica la vinculación del sitio web, donde los usuarios realizan trámites y gestiones de manera digital, con una Administración Pública?**
    a) Certificado de sello electrónico
    b) **Certificado cualificado de Sede Electrónica**
    c) Certificado de pertenencia a una entidad
    d) Certificado digital de empleado público

12. **En el expediente de contratación, el documento que contiene la descripción de la realización de la prestación y define sus calidades y sus condiciones sociales y ambientales se denomina:**
    a) **Pliego de Prescripciones Técnicas**
    b) Anexo de determinaciones del contrato
    c) Memoria justificativa
    d) Pliego de Cláusulas administrativas

13. **¿Cuál de las tareas siguientes no es responsabilidad de un administrador de sistemas?:**
    a) Mantener y explotar los servidores
    b) Garantizar la continuidad en el funcionamiento del hardware de los servidores.
    c) Mantener actualizados los sistemas operativos y el software de base.
    d) **Analizar nuevas aplicaciones y herramientas útiles para los usuarios.**

14. **Señale la respuesta correcta en relación con los sistemas RAID:**
    a) Mejoran el rendimiento de todas las aplicaciones y aseguran más velocidad de acceso.
    b) **RAID 0 y RAID 1 no necesitan hacer el cálculo de la paridad**
    c) RAID 5 es más seguro que RAID 6
    d) RAID 1 mejora el rendimiento en escritura

15. **¿A qué se refieren las siglas ACID en una transacción de base de datos?**
    a) Availability, capacity isolation, durability
    b) Availability, consistency, isolation, durability
    c) Availability, consistency, interaction, durability
    d) **Atomicity, consistency, isolation, durability**

16. **¿Qué es un PaaS?**
    a) ***Sistema de cloud computing* que proporciona a los usuarios un entorno de nube (*cloud*) en el que pueden desarrollar, gestionar y distribuir aplicaciones.**
    b) Es un sistema seguro de almacenamiento de contraseñas en entornos corporativos
    c) Es un sistema de gestión de bases de datos relacional utilizado sobre todo en entornos distribuidos.
    d) Es un lenguaje de programación que incide sobre todo en aspectos de seguridad de las aplicaciones.

17. **Se indica a un empleado municipal del Ayuntamiento que tiene que instalar en su teléfono inteligente con sistema operativo Android una aplicación de autenticación avanzada para poder acceder a la VPN ¿Qué finalidad puede tener?**
    a) Disponer de un antivirus avanzado en el teléfono inteligente.
    b) Asegurarse de que el usuario puede autenticar el desbloqueo del teléfono inteligente con una característica biométrica.
    c) Utilizar esa aplicación para acceder directamente al escritorio remoto del empleado municipal.
    d) **El uso de múltiple factor de autenticación.**

18. **¿Cuándo serán objeto de una auditoría regular ordinaria los sistemas de información obligados por el Esquema Nacional de Seguridad?:**
    a) Nunca, sólo debe hacerse una auditoría en el momento de su implantación.
    b) Una vez cada cinco años.
    c) **Al menos cada dos años.**
    d) Siempre que se produzcan modificaciones sustanciales en los sistemas de información que puedan repercutir en las medidas de seguridad requeridas.

19. **¿Debe publicar la Administración del Ayuntamiento de Alcorcón un inventario de sus actividades de tratamiento de datos personales?:**
    a) No, nunca
    b) Sí, cuando se traten de datos a gran escala
    c) **Sí, en cualquier caso**
    d) No, aunque puede publicarlo si así lo estima conveniente

20. **¿Qué herramienta del CCN-CERT permite la gestión de ciberincidentes?**
    a) VANESA
    b) IRIS
    c) **LUCIA**
    d) CARMEN

21. **¿Qué concepto corresponde al hecho de asegurar que los usuarios autorizados tengan acceso, cuando lo requieran, a la información y sus activos asociados según la norma ISO 27001?**
    a) Seguridad
    b) Integridad
    c) **Disponibilidad**
    d) Confidencialidad

22. **¿Qué guías técnicas proporciona el CCN-CERT para implementar el ENS?**
    a) Guías Serie 27000.
    b) Guías Serie 9000.
    c) Guías Serie 500.
    d) **Guías Serie 800.**

23. **Según el Esquema Nacional de Seguridad, la categoría de un sistema de información se dice que es ALTA, cuando:**
    a) Las consecuencias de un incidente de seguridad puedan suponer un perjuicio a la organización
    b) Solo si todas sus dimensiones de seguridad alcanzan el nivel ALTO
    c) **Alguna de sus dimensiones de seguridad alcanza el nivel ALTO**
    d) No han existido durante dos años incidentes de seguridad

24. **¿Cuál es la mejor definición de un Datalake?**
    a) Repositorio distribuido de datos estructurados y no estructurados.
    b) **Repositorio centralizado de datos estructurados y no estructurados.**
    c) Repositorio centralizado de datos estructurados.
    d) Repositorio multidimensional para el análisis de datos.

25. **Conforme al artículo 17 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administrativo Común de las Administraciones Públicas, los documentos electrónicos deberán conservarse en un formato que permite garantizar, señale la respuesta INCORRECTA:**
    a) La integridad del documento
    b) La conservación del documento
    c) **La consulta durante un período determinado**
    d) La autenticidad del documento

26. **¿Qué norma ISO es equivalente al ENS en cuanto a gestión de la seguridad de la información?**
    a) **ISO 27001**
    b) ISO 9001
    c) ISO 22301
    d) ISO 20000

27. **Dentro del contexto de la evaluación de seguridad de aplicaciones web, ¿Cuál de las siguientes prácticas se emplea específicamente para identificar debilidades y fallos que podrían ser explotados por un atacante?**
    a) Firewalling
    b) **Pentesting**
    c) Monitoreo de tráfico
    d) Cifrado

28. **¿Qué herramienta se utiliza para identificar y analizar vulnerabilidades de seguridad en sistemas operativos, aplicaciones y dispositivos de red?**
    a) Nmap
    b) Metasploit
    c) Wireshark
    d) **Nessus**

29. **¿Cuál de las siguientes no es una característica de los microservicios?**
    a) La diversidad tecnológica que puede combinarse con los microservicios
    b) El aislamiento de fallos
    c) **Los microservicios son una arquitectura fuertemente acoplada, al contrario que las arquitecturas monolíticas**
    d) Suele ser un sistema distribuido

30. **¿Cuál de las siguientes afirmaciones describe la tecnología blockchain?**
    a) Tecnología diseñada para el almacenamiento y procesamiento de grandes cantidades de datos
    b) Tecnología que garantiza la seguridad y la privacidad de las comunicaciones en línea
    c) **Tecnología de registro distribuido que permite la creación de registros inmutables**
    d) Tecnología diseñada para el tratamiento de datos en tiempo real

31. **Indique cuál de las siguientes expresiones NO ES CORRECTA para KERBEROS:**
    a) **Se basa en criptografía de clave asimétrica y no requiere un tercero de confianza**
    b) Es un protocolo de autenticación por red que permite que dos entidades de la misma se demuestre su identidad de manera segura
    c) Se basa en el intercambio de tickets de servicio
    d) Puede implementarse tanto en entornos Linux como en entornos Windows

32. **¿Qué hace el comando arp -a?**
    a) Muestra la configuración de red
    b) Muestra las conexiones de red activas
    c) Prueba el acceso a un dispositivo concreto de la red
    d) **Muestra una tabla de direcciones IP y MAC de los dispositivos conectados a una red local**

33. **¿Cuál es la principal ventaja de implementar Tiering en un sistema de almacenamiento empresarial?**
    a) Reducir la cantidad de hardware necesario al eliminar la redundancia
    b) Sustituir completamente el almacenamiento basado en discos mecánicos
    c) Minimizar el impacto de fallos de hardware al distribuir datos en múltiples discos físicos
    d) **Maximizar el rendimiento priorizando el acceso a los datos más utilizados en capas de almacenamiento más rápidas**

34. **¿Qué característica de seguridad proporciona SELinux en sistemas Linux?**
    a) Control de acceso basado en permisos tradicionales de usuario/grupo
    b) **Control de acceso obligatorio (MAC) con políticas de seguridad reforzadas**
    c) Protección de red mediante filtrado de paquetes
    d) Encriptación de discos de manera nativa en el kernel

35. **¿Cuál es la función principal del archivo de configuración /etc/fstab en sistemas Linux?**
    a) Configurar las interfaces de red
    b) **Definir los sistemas de archivos que deben montarse al inicio**
    c) Configurar las políticas de seguridad de SELinux
    d) Establecer las variables de entorno del sistema

36. **¿Qué metodología se utiliza para el análisis de riesgos en el ámbito de las Administraciones Públicas en España?:**
    a) PRINCE2
    b) ITIL
    c) **MAGERIT**
    d) COBIT

37. **¿Qué sistema se utiliza de forma específica para detectar intrusiones en una red?**
    a) **IDS**
    b) IPS
    c) Firewall
    d) NMAP

38. **¿Qué algoritmo de cifrado es simétrico?**
    a) RSA (Rivest-Shamir-Adleman)
    b) **AES (Advanced Encryption Standar)**
    c) ECC (Elliptic Curve Cryptography)
    d) SHA (Secure Hash Algorithm)

39. **En el ámbito de la ciberseguridad, ¿Cuál de las siguientes soluciones tecnológicas es fundamental para la recopilación, análisis y respuesta a incidentes de seguridad, facilitando la gestión de eventos y la detección de anomalías?**
    a) EDR
    b) NAC
    c) **SIEM**
    d) SOAR

40. **¿Qué tipo de ataque consiste en la explotación de vulnerabilidades en aplicaciones web?**
    a) **SQL Injection**
    b) DDoS
    c) Phishing
    d) Hijacking

41. **En el contexto de la arquitectura de servicios en la nube, ¿Cuál de las siguientes configuraciones se caracteriza por la integración de infraestructuras locales con recursos de una nube pública, permitiendo una mayor flexibilidad y escalabilidad en la gestión de datos y aplicaciones?**
    a) Nube privada de múltiples inquilinos
    b) Nube pública con recursos compartidos
    c) Nube comunitaria con gobernanza colaborativa
    d) **Nube híbrida**

42. **En el contexto de la gestión de aplicaciones mediante contenedores, ¿Cuál de las siguientes herramientas es específicamente conocida por su capacidad para empaquetar, distribuir y ejecutar aplicaciones en entornos de contenedores, siendo fundamental en la adopción de arquitecturas basadas en microservicios?**
    a) Proxmox
    b) VMware y vSphere
    c) **Docker**
    d) Citrix

43. **¿Qué solución se utiliza para la gestión de dispositivos móviles en una organización?**
    a) **MDM**
    b) EDR
    c) UEM
    d) CASB

44. **¿Qué tipo de ataque es común en dispositivos IoT debido a su falta de seguridad?**
    a) Man-in-the-Middle
    b) SQL Injection
    c) Phishing
    d) **Ataque de denegación de servicio distribuido (DDoS)**

45. **¿Cuál de las siguientes herramientas SIEM proporciona capacidades de correlación de eventos en tiempo real?**
    a) Metasploit
    b) **IBM QRadar**
    c) QualysGuard
    d) PILAR

46. **¿Cuál de los siguientes servicios e infraestructuras comunes propuestos por la AGE hace referencia al Servicio Compartido de Gestión de Notificaciones?**
    a) ALMACEN
    b) SARA
    c) Cl@ve
    d) **NOTIFIC@**

47. **En el contexto de SIEM, ¿Qué significa SOAR?**
    a) **Security Orchestration, Automation and Response**
    b) System Operations and Active Response
    c) Security Operations Automated Reporting
    d) System Orchestration and Risk Analysis

48. **¿Qué método de autenticación es más seguro para VPN?**
    a) Usuario y contraseña
    b) Certificado digital
    c) **Autenticación multifactor con certificado y token**
    d) Dirección IP estática

49. **En el contexto de copias de seguridad, ¿Qué es RPO?**
    a) El tiempo máximo de recuperación
    b) **La cantidad máxima de datos que se pueden perder**
    c) El número de copias a mantener
    d) La frecuencia de backup

50. **En el contexto de bastionado de Windows, ¿Qué son las GPOs?**
    a) Grupos de Permisos de Operación
    b) **Objetos de Políticas de Grupo**
    c) Gestión de Políticas de Operación
    d) Guías de Procedimientos Organizativos

51. **En el contexto de autenticación, ¿Qué es MFA?:**
    a) Multiple Firewall Authentication
    b) Managed File Access
    c) **Multi Factor Authentication**
    d) Mobile First Authentication

52. **¿Qué caracteriza a una red DMZ?**
    a) Red interna segura
    b) **Zona entre red interna y externa**
    c) Red externa pública
    d) Red de backup

53. **¿Qué herramienta se utiliza comúnmente para la explotación de vulnerabilidades en pruebas de penetración?**
    a) **Metasploit**
    b) Wireshark
    c) Nmap
    d) Nessus

54. **¿Qué herramienta del CCN-CERT se utiliza para el análisis de riesgos?:**
    a) LUCIA
    b) METRICA 3
    c) LORETO
    d) **PILAR**

55. **¿Cuál es el principal objetivo de un sistema EDR (Endpoint Detectiona and Response)?**
    a) Cifrar el tráfico de red
    b) **Monitorizar y responder a amenazas en endpoints**
    c) Gestionar contraseñas de usuario
    d) Configurar políticas de firewall

56. **¿Cuál es la principal diferencia entre IDS e IPS?**
    a) **El IPS puede bloquear tráfico automáticamente**
    b) El IDS analiza más protocolos
    c) El IPS solo funciona en modo pasivo
    d) El IDS requiere más recursos

57. **En el contexto de análisis de vulnerabilidades, ¿Qué es un falso positivo?**
    a) **Un hallazgo que identifica incorrectamente una vulnerabilidad que no existe en realidad**
    b) Una vulnerabilidad que ha sido correctamente identificada, pero su impacto es mínimo y no requiere acción inmediata
    c) Una vulnerabilidad real que no ha sido detectada por el sistema de análisis
    d) Un error de configuración que impide la correcta detección de vulnerabilidades

58. **En las Guías Serie 800 del CCN-CERT, ¿cuál es la recomendación principal para la gestión de los riesgos asociados con el teletrabajo en las administraciones públicas?**
    a) Permitir el teletrabajo sin restricciones tecnológicas para agilizar procesos
    b) **Implementar soluciones seguras de acceso remoto con autenticación multifactor y cifrado**
    c) Limitar el acceso remoto solo a las áreas que no manejan información sensible
    d) Reemplazar el teletrabajo con presencialidad para garantizar mayor control

59. **En relación con los procedimientos de notificación de incidentes de seguridad, ¿Qué elementos deben ser reportados según las directrices del ENS?**
    a) Sólo el impacto económico del incidente
    b) **La descripción del incidente, los impactos, y las medidas correctivas adoptadas**
    c) Sólo la identidad de los responsables del ataque
    d) Los incidentes relacionados con la pérdida de información confidencial únicamente.

60. **Con respecto al concepto de "continuidad de negocio" en términos de gestión de crisis. Elige la definición más adecuada:**
    a) **La capacidad de una organización para seguir funcionando tras un evento disruptivo mediante la implementación de procesos y recursos adecuados**
    b) La capacidad de una organización para seguir produciendo bienes en caso de crisis
    c) La capacidad de una organización para mantener la relación con sus proveedores durante una crisis
    d) La capacidad de minimizar el impacto en los costes de operaciones no relacionadas con el negocio

61. **¿Cuál de los siguientes describe con más precisión una Amenaza Persistente Avanzada?**
    - **a)** Un ataque masivo de denegación de servicio distribuido destinado a tumbar un sitio web
    - **b)** **Un ataque cibernético altamente dirigido y persistente que busca infiltrarse y mantener el acceso a la red de la víctima durante un largo periodo de tiempo, con el objetivo de robar información sensible**
    - **c)** Un ataque realizado por una aplicación de malware que explota una vulnerabilidad conocida
    - **d)** Un ataque de phishing que roba las credenciales de un usuario específico

62. **Según el artículo 66 de la Constitución Española, ¿a quién representan las Cortes Generales?**
    - **a)** **Al pueblo español**
    - **b)** A las circunscripciones electorales
    - **c)** A los municipios
    - **d)** A las Comunidades Autónomas

63. **Según el artículo 16 de la Constitución Española, se podrá obligar a alguien a declarar sobre su ideología, religión o creencias:**
    - **a)** Siempre que sea necesario para aclarar un delito
    - **b)** Cuando los jueces lo ordenen
    - **c)** En caso de terrorismo
    - **d)** **Nunca**

64. **¿Qué implica la interoperabilidad en la Administración Electrónica?**
    - **a)** La exclusión de la tecnología en la administración pública
    - **b)** La incompatibilidad de sistemas y documentos electrónicos
    - **c)** **La capacidad de los sistemas de información de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos**
    - **d)** La restricción de acceso a documentos públicos

65. **En un ataque APT (Amenaza Persistente Avanzada), ¿Cuál es el objetivo principal del "lateral movement" una vez que un atacante ha comprometido un sistema inicial dentro de la red de la víctima?**
    - **a)** Desplazarse entre los sistemas comprometidos y utilizar técnicas de cifrado para protegerlos contra la detección de los administradores de red
    - **b)** Proteger los sistemas comprometidos contra posibles descubrimientos utilizando herramientas de cifrado
    - **c)** **Desplazarse entre sistemas dentro de la red interna para acceder a datos valiosos y persistir en el entorno**
    - **d)** Desplazarse hacia otros sistemas con el fin de lanzar un ataque de denegación de servicio (DDoS) y paralizar las operaciones de la víctima

66. **¿Cuál de las siguientes prácticas es la más recomendable para proteger las copias de seguridad contra un ataque de ransomware?:**
    a) **Mantener las copias de seguridad desconectadas de la red y en almacenamiento físico, fuera del alcance de posibles ataques**
    b) Programar copias de seguridad solo una vez al mes para evitar ataques rápidos
    c) Implementar cifrado de extremo a extremo en todas las copias de seguridad sin importar el método de almacenamiento
    d) Permitir que las copias de seguridad se realicen únicamente desde redes internas no expuestas a Internet

67. **¿Qué técnica es clave para fomentar la concienciación en seguridad entre los usuarios y evitar el phishing en un entorno corporativo?**
    a) Permitir que los usuarios tomen decisiones sobre la seguridad sin intervención del departamento de TI
    b) **Realización de simulaciones periódicas de phishing para educar a los empleados sobre cómo identificar correos electrónicos fraudulentos**
    c) Bloqueo de todos los correos electrónicos de origen desconocido
    d) Implementación de filtros de contenido que eviten la visualización de enlaces sospechosos

68. **En relación con la gestión de almacenamiento removible en una organización, ¿Cuál de las siguientes prácticas de DLP es más efectiva para prevenir fugas de datos mediante dispositivos USB no autorizados sin afectar la productividad de los empleados?**
    a) Bloquear completamente el acceso a todos los dispositivos USB sin excepciones
    b) **Permitir solo dispositivos USB encriptados que sean previamente registrados y autorizados por el sistema de DLP**
    c) Monitorear únicamente el tráfico de dispositivos USB conectados, sin realizar ninguna acción correctiva automática
    d) Permitir el acceso sin restricciones a dispositivos USB, pero exigir que se realicen copias de seguridad periódicas de los datos almacenados

69. **¿Para qué se utiliza la herramienta FIRe?**
    a) Para almacenar apoderamientos electrónicos
    b) Para el envío de notificaciones internas
    c) Para el archivado rápido de expedientes
    d) **Para la firma electrónica de documentos**

70. **¿Qué es el principio de "menor privilegio"?**
    a) La idea de que los usuarios deben estructurarse de acuerdo a un organigrama para el desempeño de sus actividades
    b) **La idea de otorgar, exclusivamente, los permisos y derechos necesarios y suficientes a un usuario para desempeñar sus actividades**
    c) La idea de que únicamente el usuario administrador debe tener acceso a la información confidencial de una organización
    d) La idea de conceder acceso ilimitado a los administradores para realizar tareas críticas sin restricciones

71. **En el análisis forense de una APT, ¿qué herramienta avanzada sería más adecuada para detectar la ejecución de un "shellcode" que ha sido inyectado en la memoria del sistema sin ser detectado por los antivirus tradicionales?**
    a) Wireshark
    b) Metasploit
    c) **Volatility**
    d) Nmap

72. **¿Cuál de las siguientes es una de las características clave de un Next-Generation Firewall (NGFW) en comparación con un cortafuegos tradicional de red?**
    a) Un NGFW solo realiza inspección de tráfico en la capa de red
    b) **Un NGFW puede identificar aplicaciones específicas a través de inspección profunda de paquetes y bloquea ataques basados en el comportamiento**
    c) Un NGFW no realiza inspección de tráfico SSL/TLS
    d) Un NGRW se limita a bloquear el acceso no autorizado a través de una simple lista blanca

73. **¿Cuál de las siguientes soluciones permite el intercambio de asientos electrónicos de registro entre las Administraciones Públicas?**
    a) FACe
    b) IAE_AAPP
    c) ADA
    d) **SIR**

74. **En el contexto de la seguridad de redes inalámbricas, ¿Cuál de los siguientes protocolos es fundamental para establecer un método seguro de autenticación y cifrado, garantizando la protección de las comunicaciones en entornos Wi-Fi?**
    a) 801.a
    b) EAP
    c) **WPA3**
    d) WEP

75. **¿Qué protocolo se utiliza para la comunicación segura en dispositivos IoT?**
    a) **MQTT**
    b) SIOTC
    c) TFTP
    d) DNS

76. **¿Cuál de estas afirmaciones sobre accesibilidad es cierta con las guías del W3C?:**
    a) Una página web accesible debe contener solo texto
    b) Una página web accesible no debe utilizar colores
    c) Una página web accesible debe utilizar un único tipo de letra establecido en estas guías
    d) **Una página web accesible debe tener textos equivalentes para cualquier elemento no textual**

77. **En un entorno de backup en la nube de proveedor, ¿Qué técnica de seguridad es la más eficaz para garantizar la confidencialidad de los datos?:**
    a) Implementación de control de acceso basado en roles (RBAC)
    b) **Cifrado de extremo a extremo (end-to-end encryption)**
    c) Autenticación multifactor para todos los usuarios que acceden a los backups
    d) Uso de una red privada virtual (VPN) para proteger los datos en tránsito

78. **En relación con el modelo "BYOD", señale cuál de las siguientes afirmaciones es correcta:**
    a) No procede la implantación de un modelo BYOD a través del uso de contenedores
    b) **Suele acompañarse del despliegue de tecnologías EMM (Enterprise Mobility Management) en la organización, para el control y la gestión de sus dispositivos móviles**
    c) Consiste en que el empleado pueda utilizar su ordenador corporativo en el ámbito personal
    d) Son las siglas de "Bring Your Own Data"

79. **En un sistema de comunicaciones móviles, si un dispositivo es propiedad de una organización y gestionado en su totalidad por la misma, es puesto a disposición del usuario exclusivamente para el desempeño de sus funciones profesionales, entonces estamos hablando de un modelo:**
    a) BYOT
    b) BYOD
    c) COPE
    d) **COBO**

80. **En el contexto de gestión de identidades, ¿qué es OIDC?**
    - **a)** Un protocolo de cifrado
    - **b)** **Un protocolo de autenticación basado en OAuth 2.0**
    - **c)** Un sistema de backup
    - **d)** Un firewall

PREGUNTAS DE RESERVA (ESTAS PREGUNTAS NO COMPUTARAN A NO SER QUE SE ANULE ALGUNA DE LAS PREGUNTAS ANTERIORES)

81. **¿De qué tipo es esta dirección? 3002:0bd6::0000:0000:ee00:0033:6778**
    - **a)** IPv4
    - **b)** **IPv6**
    - **c)** MAC
    - **d)** Puerto

82. **¿Qué elemento de Windows permite la implementación de políticas de grupo para gestionar la configuración de los equipos en una red?**
    - **a)** **Active Directory**
    - **b)** BitLocker
    - **c)** Windows Defender
    - **d)** PowerShell

83. **¿Qué topologías es posible encontrar en Ethernet?**
    - **a)** **Bus, árbol o estrella**
    - **b)** Solo bus
    - **c)** Bus o estrella
    - **d)** Solo estrella

84. **¿Qué protocolo se utiliza típicamente para Single Sign-On empresarial?**
    - **a)** Oauth
    - **b)** **SAML**
    - **c)** RPC
    - **d)** LDAPS

85. **¿Cuál es el principal objetivo en el proceso de recolección y conservación de evidencias digitales en un proceso forense?**
    - **a)** **Asegurar la validez de las evidencias para su posterior análisis sin alterar su integridad**
    - **b)** Crear copias exactas de los dispositivos involucrados para realizar un análisis posterior sin riesgos
    - **c)** Copiar toda la información disponible en los dispositivos, independientemente de su relevancia, para asegurar que no se omita evidencia
    - **d)** Eliminar cualquier dato irrelevante para facilitar la revisión de las evidencias