TEST A2

EDICIÓN 2026

Técnico/a medio/a de informática

Ayuntamiento de Olot

«Bloc 6. Ciberseguretat i identitat digital»

Más de 450 Preguntas

467 de exámenes oficiales + 6 de refuerzo, marcadas

◆ Las soluciones de norma citan su artículo y su ley

5	3	2	180
de los 60 temas del programa oficial	preguntas de prueba de nivel	simulacros de examen	páginas

oposicionesexpress.com

Preguntas de procesos selectivos reales
Programa oficial de la convocatoria (DOGC)
Edición noviembre de 2026

Esto es una muestra

Tiene 43 páginas: el índice, cómo se ha hecho el libro, cómo usarlo y el test del tema 51 entero, con sus soluciones. El libro completo, de 180 páginas, sigue tema a tema el **programa oficial de la convocatoria de Técnico/a medio/a de informática del Ayuntamiento de Olot** (solo «Bloc 6. Ciberseguretat i identitat digital»: 5 de los 60 temas del programa).

El libro entero

34,90 €

PDF de 180 páginas: 473 preguntas con su solución explicada.

Pago único, impuestos incluidos. Se descarga al momento.

Consigue el libro completo

Escanea el código o pulsa la dirección: te lleva a la página del libro en oposicionesexpress.com, donde lo compras y lo descargas al momento en PDF.

oposicionesexpress.com/Test-Tecnico-a-medio-a-de-informatica-Ayuntamiento-de-Olot-A2.html

Precios a 3 de noviembre de 2026: si cambian, vale el que figure en la página de venta.

Índice

5 temas · 473 preguntas

Créditos y aviso legal 3

De dónde sale este libro 4

Cómo usar este libro 5

Prueba tu nivel 6

PARTE 1 · Test por temas 10

Tema 51 Serveis de seguretat de la informació (InfoSec): Objectius principals, eines, polítiques de seguretat i casos d'ús. 11

Tema 52 Certificats electrònics, signatura digital i infraestructura de clau pública (PKI). 46

Tema 53 Reglament EIDAS: Principis generals, tipus de signatura i novetats D'EIDAS2. 63

Tema 54 Seguretat de la informació: Introducció al concepte de còpia de seguretat i polítiques de backup. 72

Tema 55 Xarxes privades virtuals (VPN). Conceptes generals. 106

PARTE 2 · Simulacros de examen 142

Simulacro 1 50 preguntas 143

Simulacro 2 50 preguntas 162

Anexo: vigencia de los textos 180

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

Créditos y aviso legal

Edición noviembre de 2026

© 2026 oposicionesexpress.com. Todos los derechos reservados. La selección de preguntas, la estructura de tests, las soluciones anotadas y la maquetación de esta obra están protegidas por la legislación de propiedad intelectual.

Licencia de uso personal. Tu compra concede una licencia de uso personal e intransferible. No está permitida la reproducción total o parcial, la distribución, la comunicación pública, la cesión ni la reventa de este archivo sin autorización escrita del titular. Sí puedes fotocopiar para tu propio uso las hojas de respuestas.

Sin carácter oficial ni afiliación. Material de estudio independiente. No es una publicación oficial ni está afiliado, avalado o patrocinado por el Ayuntamiento de Olot, por ninguna otra Administración Pública, tribunal u organismo convocante, ni por la Agencia Estatal Boletín Oficial del Estado.

Alcance. Este libro sigue el programa oficial de la convocatoria de Técnico/a medio/a de informática del Ayuntamiento de Olot, publicada en el DOGC. Cubre solo «Bloc 6. Ciberseguretat i identitat digital»: 5 de los 60 temas del programa. Las bases pueden modificarse: contrasta siempre la publicación oficial.

Procedencia de las preguntas. Las preguntas de examen proceden de procesos selectivos reales convocados por Administraciones Públicas españolas; cada una indica su organismo convocante y, cuando consta, el año. Proceden de muchos organismos, no solo del Ayuntamiento de Olot.

Preguntas de refuerzo. Las 6 preguntas marcadas «Refuerzo» las ha elaborado haztefuncionario.com a partir del artículo que citan, y solo aparecen en los temas del programa sin preguntas de examen suficientes.

Resultados. Esta obra es una herramienta de preparación; el resultado depende de tu estudio y constancia.

Erratas. Si detectas un error en una pregunta o en una solución, escríbenos a oposiciones.dhm@gmail.com y lo corregimos en la siguiente actualización.

> **Actualizaciones de este libro**
>
> oposicionesexpress.com/Test-Tecnico-a-medio-a-de-informatica-Ayuntamiento-de-Olot-A2.html

De dónde sale este libro

Este libro sigue, tema a tema, el **programa oficial de la convocatoria de Técnico/a medio/a de informática del Ayuntamiento de Olot**, publicada en el DOGC. Cubre solo «Bloc 6. Ciberseguretat i identitat digital»: 5 de los 60 temas del programa. Cada tema que trae tiene su test, y todo el libro se apoya en preguntas que ya se han puesto en exámenes.

Las **467 preguntas de examen** de este libro proceden de procesos selectivos reales convocados por Administraciones Públicas españolas. Cada una indica su procedencia: el organismo convocante y, cuando consta, el año. Proceden de muchos organismos distintos, no solo del Ayuntamiento de Olot: son las que tratan las normas y materias de tu programa.

Cómo se ha elegido cada pregunta

1. **Pertenencia al tema.** Partimos de las 886 preguntas reales que haztefuncionario.com tiene enlazadas a los 5 temas de este programa que trae el libro, por la ley y los artículos que cubre cada tema.
2. **Filtros mecánicos.** Solo entran preguntas con sus 4 opciones completas, en castellano, sin duplicados y sin textos que desvelen la respuesta.
3. **Piso de fiabilidad.** Cada pregunta real lleva una nota interna de fiabilidad de su clave; las que no llegan al umbral se descartan, aunque el test quede más difícil de llenar.
4. **Artículo vigente.** Si una pregunta cita un artículo que hoy está derogado o ya no existe en el texto de la norma, no entra.
5. **Lo que más cae, primero.** Dentro de cada tema, cada artículo aporta preguntas en proporción a las veces que ha caído. Los temas más preguntados llevan hasta 100 preguntas; los que menos, 20.

Las preguntas de refuerzo

En 1 tema del programa no hay preguntas reales suficientes. Para que no se quede sin test, se completan con **6 preguntas de refuerzo**: las ha elaborado haztefuncionario.com a partir del artículo que citan, y pasan los mismos filtros mecánicos que las reales. Van siempre marcadas como «Refuerzo» y no entran en la prueba de nivel ni en los simulacros.

Qué encontrarás

Parte	Qué es
Prueba tu nivel	3 preguntas. Hazla antes de empezar: los temas de las que falles son tu mapa de estudio.
Parte 1 · 5 tests por tema	En el orden del programa oficial, con sus soluciones a continuación y una casilla de aciertos en cada una.
Parte 2 · 2 simulacros	Con el número de preguntas y el tiempo del formato de referencia de este libro.
Anexo de vigencia	Las normas del libro y de dónde se ha tomado su texto.

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

Cómo usar este libro

El examen de esta convocatoria

50	90	4	7,5
preguntas	minutos	opciones por pregunta	sobre 15 para superarlo

Formato orientativo: el formato del examen de esta convocatoria no consta; el de arriba es una referencia. Compruébalo en la publicación oficial. Dejar una pregunta en blanco no penaliza.

El orden que funciona

1. **Empieza por «Prueba tu nivel»**, sin apuntes y con el reloj en marcha. Corrígela y anota en qué temas fallas (cada solución dice su tema): ese es tu mapa de estudio.
2. **Trabaja los tests por tema**, empezando por tus temas débiles. Corrige con la clave rápida que abre cada página de soluciones y lee después las explicaciones.
3. **Reserva los simulacros para el final**, cronometrados y del tirón: tienen el número de preguntas y el tiempo del formato de referencia de este libro.
4. **Repite lo fallado**, un test con 1 de cada 4 respuestas falladas merece segunda vuelta antes de avanzar. Apunta los aciertos de cada vuelta en la casilla que abre las soluciones del tema.

> **Cómo se hace cada test**
>
> Escribe tu respuesta en la **casilla que hay junto a cada pregunta**. Las soluciones empiezan siempre en página nueva, así que no las ves mientras haces el test. Cuando termines, corrige con la clave rápida y apunta los aciertos.

Qué cubre y qué no

Cubre solo «Bloc 6. Ciberseguretat i identitat digital»: 5 de los 60 temas del programa. No incluye el resto del programa (55 temas). No incluye teoría: es material de entrenamiento. Contrasta siempre el temario y las bases en la publicación oficial de tu convocatoria.

La versión en pantalla

Las mismas preguntas, con corrección al instante y repaso de falladas, están en haztefuncionario.com, en la página de esta oposición.

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

Parte 1

Test por temas

5
tests, uno por tema

370
preguntas

364
reales de examen

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €**

Cómpralo aquí ›

Tema
51

Serveis de seguretat de la informació (InfoSec): Objectius principals, eines, polítiques de seguretat i casos d'ús.

100	100	0	180
preguntas en este test	reales de examen	de refuerzo	minutos recomendados

Estas preguntas salen de 16 organismos distintos y de exámenes de 2018 a 2026.

Escribe tu respuesta en la casilla que hay junto a cada pregunta. Las soluciones empiezan en página nueva: no las verás mientras haces el test.

1 **Según la Guía CCN-STIC 807 (Criptología de empleo en el Esquema Nacional de Seguridad), los esquemas de cifrado con autenticación (AE/AEAD) autorizados para uso recomendado basados en el cifrador de bloque AES son:**

A EAX, GCM y CBC.
B EAX, GCM y CCM.
C GCM, CCM y CTR.
D CBC, CFB y OFB.

Administración General del Estado, 2025 · Gestión de Sistemas e Informática (A2)

2 **Indique la respuesta correcta sobre tipos de ataque a un sistema de información:**

A El sniffing es la generación de tráfico utilizando un origen falseado.
B El spoofing es la captura del tráfico que circula por una red.
C Denegacion de servicio distribuida (DDoS) es un ataque a varios objetivos desde un solo punto, con la finalidad de degradar total o parcialmente los servicios prestados por esos recursos a sus usuarios legítimos.
D El barrido ("escaneo") de puertos es un ataque que trata de obtener información básica acerca de qué servicios se ofrecen en un determinado sistema, así como otros detalles técnicos del mismo.

Administración General del Estado, 2024 · Técnico Auxiliar de Informática (C1)

3 **¿Cuál de las siguientes afirmaciones sobre la recopilación y el análisis de incidencias en una organización con un SIEM (Security Information and Event Management) es falsa?**

A Permite reconocer amenazas y vulnerabilidades del sistema y generar alertas.
B Recopila y analiza un gran volumen de datos sobre aplicaciones, servidores y usuarios en tiempo real.
C Nos permite predecir cuándo se producirán nuevas amenazas en los sistemas.
D Nos ayuda a cumplir la normativa vigente sobre seguridad.

Generalitat de Catalunya, 2023 · Programador informático

MUESTRA GRATIS · Libro completo, 473 preguntas 34,90 €
Cómpralo aquí ›

4 **Señale qué afirmación es correcta con respecto a las soluciones de Ciberseguridad proporcionadas por el Centro Criptológico Nacional (CCN):**

- **A** CLARA, protección y trazabilidad del dato.
- **B** ELENA, Simulador de Técnicas de Cibervigilancia.
- **C** GLORIA, Gestión de eventos e información de seguridad.
- **D** MONICA, Gestor de logs para responder ante incidentes y amenazas.

Administración General del Estado, 2022 · Técnico Auxiliar de Informática (C1)

5 **¿Qué función realiza SOAR específicamente en la fase de contención de incidentes dentro de un SOC?:**

- **A** Generación de informes ejecutivos post-incidente
- **B** Normalización de logs heterogéneos
- **C** Orquestación automatizada de playbooks cross-tool
- **D** Creación de baselines de tráfico de red

Cortes de Aragón, 2026 · Técnico de Sistemas (A2)

6 **En el contexto de la ciberseguridad, ¿qué es una APT?**

- **A** Son ataques dirigidos a una entidad específica usando técnicas sofisticadas para explotar vulnerabilidades y de forma continuada en el tiempo.
- **B** Es un tipo de software antivirus diseñado para proteger sistemas operativos de amenazas conocidas.
- **C** Es un procedimiento estándar para actualizar contraseñas de manera periódica en una organización.
- **D** Es una herramienta de cifrado utilizada para proteger archivos y comunicaciones en redes empresariales.

Xunta de Galicia, 2025 · Escala de Sistemas y Tecnología de la Información (A1)

7 **En el contexto de la planificación de infraestructuras TIC, ¿cuál de los siguientes elementos es más relevante para asegurar la continuidad operativa de los servicios críticos?**

- **A** Utilización de entornos cloud públicos con escalabilidad automática.
- **B** Definición de un Plan de Continuidad de Servicios respaldado por análisis de impacto (BIA) y pruebas periódicas.
- **C** Alta disponibilidad mediante tolerancia a fallos definida en acuerdos contractuales.
- **D** Asignación dinámica de recursos sin necesidad de documentación formal.

Cortes de Aragón, 2025 · Analista de Sistemas (A1)

8 **Señale la respuesta correcta:**

- **A** Hyperledger es un hipervisor que crea y ejecuta máquinas virtuales.
- **B** Hyperledger es un proyecto de tecnología blockchain.
- **C** Hyperledger es un estándar global para anchos de banda inalámbricos LAN que operan con un rango de datos de 54 Mbps en la frecuencia de banda de 5 GHz.
- **D** Hyperledger es una red cableada LAN.

Administración General del Estado, 2022 · Gestión de Sistemas e Informática (A2)

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

9 **En materia de seguridad informática, ¿qué nombre recibe la técnica que consiste en manipular publicidad en línea con el objetivo de conseguir infectar dispositivos, de manera que, cuando el usuario accede a alguno de esos anuncios instala software malicioso sin ser consciente de ello?**

- **A** Crimeware.
- **B** Warshipping.
- **C** Malvertising.
- **D** Spyware.

Administración General del Estado, 2025 · Auxiliar Administrativo (C2)

10 **En el contexto de la seguridad de endpoints, ¿cuál es la principal diferencia entre un EPP (Endpoint Protection Platforms) y un EDR (Endpoint Detection Response)?**

- **A** Un EPP detecta ataques avanzados en tiempo real, mientras que un EDR previene ataques básicos.
- **B** Un EPP se enfoca en la prevención de amenazas conocidas, mientras que un EDR permite la detección y respuesta ante amenazas avanzadas.
- **C** Un EDR es solo una versión más antigua de EPP, sin diferencias funcionales.
- **D** Ambos sistemas tienen exactamente las mismas funciones, sin diferencias en su enfoque.

Junta de Andalucía, 2024 · Informática (A1)

11 **¿Cuál de las siguientes afirmaciones sobre gestión de ciberincidentes, amenazas y vectores de ataque es CORRECTA?.**

- **A** La gestión de ciberincidentes implica la preparación, identificación, contención, mitigación y recuperación de eventos de seguridad, mientras que las amenazas se refieren a posibles riesgos y los vectores de ataque son los métodos utilizados por los atacantes para explotar esas vulnerabilidades.
- **B** La seguridad perimetral es suficiente para proteger contra todos los vectores de ataque.
- **C** La formación y concienciación del personal en ciberseguridad no son herramientas efectivas para mitigar las amenazas.
- **D** Las amenazas y los vectores de ataque son sinónimos y se refieren a cualquier evento que cause un ciberincidente, mientras que la gestión de ciberincidentes se enfoca en la prevención de ataques antes de que ocurran.

Generalitat Valenciana, 2024 · Técnica en Sistemas y Tecnología de la Información (A2)

12 **Respecto a los marcos de referencia MITRE CVE y MITRE CWE, seleccione la respuesta correcta:**

- **A** CWE ofrece una nomenclatura estándar para vulnerabilidades de seguridad conocidas.
- **B** CVE es un sistema de categorías de debilidades del software.
- **C** CVE y CWE son sistemas equivalentes que categorizan vulnerabilidades utilizando la misma escala.
- **D** CVE incluye las versiones de software afectadas y posibles soluciones al fallo.

Generalitat Valenciana, 2023 · Sistemas y Tecnología de la Información (A1)

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

13 **¿Qué es un UTM (Unified Threat Management) según INCIBE?**

- **A** Un estándar que establece reglas y protocolos para la interoperabilidad de soluciones de seguridad corporativa.
- **B** Un dispositivo o solución que integra múltiples funciones de seguridad en una única plataforma.
- **C** Un estándar de seguridad que define la interoperabilidad de soluciones antivirus corporativas.
- **D** Una plataforma especializada en mitigación de ataques distribuidos de denegación de servicio (DDoS).

Administración General del Estado, 2025 · Gestión de Sistemas e Informática (A2)

14 **¿Cuál de las siguientes respuestas NO es una clasificación de los ciberincidentes registrada en la Guía para la Gestión de ciberincidentes del CCN-STIC-817?:**

- **A** Intento de intrusión.
- **B** Compromiso de la información.
- **C** Criptografía.
- **D** Contenido abusivo.

Generalitat Valenciana, 2024 · Superior de Gestión en Ingeniería Técnica Informática (A2)

15 **El ataque informático que consiste en modificar o sustituir el archivo del servidor de nombres de dominio (DNS) cambiando la dirección IP legítima de una entidad (comúnmente bancaria), de manera que cuando el usuario escribe el nombre de dominio de la entidad, el navegador lo redirige automáticamente a otra dirección IP con una web falsa que suplanta la identidad legítima, obteniendo ilícitamente las claves de acceso, se conoce como:**

- **A** Phishing.
- **B** Pharming.
- **C** Spoofing.
- **D** Sidejacking.

Junta de Andalucía, 2021 · Administrativo (C1)

16 **¿Cuál de los siguientes elementos tecnológicos representa un reto creciente en seguridad y gestión dentro de las organizaciones?**

- **A** El uso de dispositivos móviles y estrategias BYOD.
- **B** El uso de miniordenadores clásicos maquetados por el departamento de tecnologías.
- **C** La impresión centralizada en impresoras comunes o locales.
- **D** El uso de aplicaciones o paquetes ofimáticos estándar.

Administración General del Estado, 2025 · Gestión de Sistemas e Informática (A2)

PARTE 1

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

17 **¿Cuál es el nivel mínimo de recuperación que debe tener una actividad para que la consideremos como recuperada, aunque el nivel de servicio no sea el óptimo?**

- A ROL (Revised Operating Level).
- B RPO (Recovery Point Objective).
- C MTD (Maximum Tolerable Downtime).
- D RTO (Recovery Time Objective).

Administración General del Estado, 2022 · Gestión de Sistemas e Informática (A2)

18 **¿Cuál es una medida de carácter organizativo en la Protección del puesto de trabajo?**

- A Limitar los permisos de administración del equipo.
- B Restringir los puertos USB a puestos determinados.
- C La prohibición de publicar o compartir contraseñas.
- D Controlar y prohibir el acceso remoto hacia la propia organización.

Junta de Extremadura, 2023 · Auxiliar de Informática (C2)

19 **Indique cuál de las siguientes NO es una metodología o normativa de gestión de riesgos de seguridad de la información:**

- A MAGERIT
- B UNE-EN 12464-1:2022
- C ISO / IEC 27005:2022
- D NIST SP 800-30

Administración General del Estado, 2025 · Gestión de Sistemas e Informática (A2)

20 **Un parámetro manejado para definir la recuperación de un sistema de información ante un impacto es:**

- A Recovery Time Objective.
- B Recovery Plan Objective.
- C Occupant Emergency Plan.
- D Business Recovery Plan.

Cortes de Aragón, 2025 · Analista de Sistemas (A1)

21 **¿A qué se refiere el término "Movimiento Lateral" en el contexto de una intrusión?:**

- A Al desplazamiento del atacante entre distintos sistemas de una misma red una vez dentro.
- B A la exfiltración de datos hacia un servidor externo.
- C Al envío de correos electrónicos de phishing a otros departamentos.
- D Al cambio de la dirección IP de ataque para evitar el bloqueo del firewall.

Cortes de Aragón, 2026 · Técnico de Sistemas (A2)

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

22 **¿Cuál de las siguientes afirmaciones describe mejor el propósito de una auditoría informática?**

- **A** Evaluar la eficiencia de los procesos de negocio de una organización.
- **B** Revisar y mejorar la experiencia del usuario en aplicaciones de software.
- **C** Examinar y evaluar la seguridad, integridad y eficiencia de los sistemas de información de una organización.
- **D** Aconsejar el desarrollo de nuevas aplicaciones de software para mejorar la productividad.

Servicio Andaluz de Salud, 2025 · Técnico de Función Administrativa, Sistemas y Tecnología de la Información (A1)

23 **La guía CCN-STIC 817 sobre gestión de ciberincidentes, clasifica los mismos atendiendo a la ruta o camino que utiliza un atacante para tener acceso al activo atacado (vector de ataque). ¿Qué es un Ransonware?**

- **A** Es un ataque dirigido a poner fuera de servicio los sistemas, al objeto de causar daños en la productividad y/o la imagen de las instituciones atacadas.
- **B** Es un incidente relacionado con acciones fraudulentas derivadas de suplantación de identidad, en todas sus variantes.
- **C** Es un ataque dirigido a recabar información fundamental que permita avanzar en ataques más sofisticados, a través de ingeniería social o de identificación de vulnerabilidades.
- **D** Es un software cuyo objetivo es infiltrarse o dañar un ordenador, servidor u otro dispositivo de red, sin el conocimiento de su responsable o usuario y con finalidades muy diversas.

Gobierno de La Rioja, 2026 · Técnico Informático (C1)

24 **En el ámbito de la seguridad en las redes, indica cuál de estas parejas tipo de ataque/dimensión de seguridad a la que afecta, NO es correcta.**

- **A** Interrupción /disponibilidad.
- **B** Interceptación /disponibilidad.
- **C** Modificación /integridad.
- **D** Suplantación /autenticidad.

Gobierno de Aragón, 2024 · Técnico de Informática (A2)

25 **¿Qué elemento distingue principalmente el análisis cualitativo del cuantitativo en MAGERIT?**

- **A** El uso de escalas de valores discretos para valorar activos y amenazas.
- **B** La implementación de controles de seguridad específicos.
- **C** El tiempo necesario para realizar el análisis.
- **D** La necesidad de usar la herramienta PILAR.

Servicio Andaluz de Salud, 2025 · Técnico Medio de Gestión de Función Administrativa, Informática (A2)

26 **En la herramienta PILAR, utilizada para el análisis y gestión de riesgos en sistemas de información, ¿qué función principal desempeña el "perfil de seguridad"?**

- **A** Cuantifica el impacto financiero y reputacional de cada vulnerabilidad identificada.
- **B** Asigna responsables de seguridad dentro de la organización.
- **C** Genera un inventario detallado de todos los activos físicos de la infraestructura que hay que proteger.
- **D** Define los umbrales de seguridad que deben cumplir los sistemas en función de su categorización.

Servicio Andaluz de Salud, 2025 · Técnico de Función Administrativa, Sistemas y Tecnología de la Información (A1)

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

27 **¿Qué métrica clave de desempeño (KPI) evalúa objetivamente la eficacia operativa del departamento de auditoría informática?:**

- **A** Volumen total de informes de auditoría emitidos durante el ejercicio anual.
- **B** Porcentaje de riesgos críticos auditados vs plan anual y tasa de implementación de recomendaciones previas.
- **C** Horas facturables generadas por auditores.
- **D** Número agregado de certificaciones profesionales CISA obtenidas por el equipo.

Cortes de Aragón, 2026 · Técnico de Sistemas (A2)

28 **De acuerdo con el CCN-CERT, solo se autorizan los métodos de Key Exchange que proporcionen una fortaleza de seguridad de, al menos:**

- **A** 192 bits.
- **B** 128 bits.
- **C** 112 bits.
- **D** 256 bits.

Administración General del Estado, 2025 · Técnico Auxiliar de Informática (C1)

29 **¿Cuál de las siguientes es una de las capacidades que caracterizan un SIEM (Security Information and Event Management)?**

- **A** Correlación de eventos.
- **B** Descifrado e inspección profunda del contenido del tráfico de red cifrado (SSL/TLS) para la detección de amenazas ocultas.
- **C** Aplicación activa de parches de seguridad y gestión de la configuración en los activos de la red para remediar vulnerabilidades.
- **D** Simulación de ataques y ejecución de pruebas de penetración controladas.

Xunta de Galicia, 2025 · Gestión de Sistemas de Informática (A2)

30 **En cuanto a la gestión de incidencias según ISO 27001, ¿qué afirmación es FALSA?**

- **A** El trabajo de gestión de una incidencia se termina una vez que la incidencia se ha resuelto o mitigado.
- **B** El proceso de gestión de una incidencia da comienzo con la notificación de la misma por parte de la persona que la detecta.
- **C** Una vez detectado el incidente, se debe proceder a su clasificación.
- **D** Una vez el incidente se ha resuelto, se informará sobre su cierre a la persona que lo ha notificado.

Xunta de Galicia, 2022 · Escala de Sistemas y Tecnología de la Información (A1)

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

31 **¿Qué información está almacenada en la zona de seguridad del DNI electrónico, accesible en lectura por el ciudadano en los Puntos de Actualización del DNIe?**

- **A** El certificado de Firma (No Repudio).
- **B** El certificado de Autenticación (Digital Signature).
- **C** El certificado CA intermedia emisora.
- **D** La imagen de la fotografía.

Administración General del Estado, 2025 · Técnico Auxiliar de Informática (C1)

32 **¿Cuál de las siguientes es una definición acertada del concepto "vigilancia digital"?**

- **A** La vigilancia digital consiste en encontrar, analizar y rastrear cualquier información perjudicial para evitar que la amenaza se convierta en un problema real y de ese modo minimizar el impacto sobre la reputación corporativa.
- **B** La vigilancia digital consiste en obtener secretos sin el permiso del poseedor de la información (personal, sensible, propietaria o de naturaleza clasificada), de individuos, competidores, rivales, grupos, gobiernos y enemigos para ventaja personal, económica, política o militar a través del hackeo de redes privadas.
- **C** La vigilancia digital consiste en la búsqueda continua de productos, servicios, marcas y conceptos que estén creando tendencia en redes sociales de mercados extranjeros, con el fin de su análisis y posible réplica en el mercado local.
- **D** La vigilancia digital consiste en el conjunto de sistemas de vigilancia de una instalación que emiten sus datos a través de una conexión de internet/intranet a una plataforma de ciberseguridad centralizada.

Xunta de Galicia, 2022 · Escala de Sistemas y Tecnología de la Información (A1)

33 **Las auditorías técnicas que tienen por objeto participar en la investigación de fraudes, en actos conscientes y voluntarios en los cuales se eluden las normas legales se llaman:**

- **A** Auditorías forenses.
- **B** Auditorías de gestión.
- **C** Auditorías policiales.
- **D** Auditorías de regularidad.

Xunta de Galicia, 2022 · Escala de Sistemas y Tecnología de la Información (A1)

34 **¿Qué tarea dentro del Método de Análisis de Riesgos MAGERIT, tiene como objetivos estimar la frecuencia de ocurrencia de cada amenaza sobre cada activo y estimar la degradación que causaría la amenaza en cada dimensión del activo?**

- **A** MAR.21: Identificación de las Amenazas.
- **B** MAR.22: Caracterización de las Amenazas.
- **C** MAR.21: Análisis de Riesgos.
- **D** MAR.22: Valoración de las Amenazas.

Servicio Andaluz de Salud, 2022 · Técnico de Función Administrativa, Sistemas y Tecnología de la Información (A1)

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

35 **En el contexto de la gestión de riesgos basada en el marco NIST SP 800-30 y el uso de herramientas GRC (Governance, Risk and Compliance), ¿qué función cumple específicamente un Mapa de Calor (Heat Map) en el análisis cualitativo de riesgos?**

- **A** Determinar la temperatura física de los CPDs para predecir fallos en el hardware mediante protocolos SNMP.
- **B** Visualizar la priorización de los riesgos mediante una matriz que cruza los valores de probabilidad de ocurrencia e impacto potencial.
- **C** Calcular el tiempo medio entre fallos (MTBF) de los activos críticos basándose en un histórico de incidentes.
- **D** Generar un inventario automático de activos (Discovery) mediante el escaneo de puertos y servicios activos en la red.

Administración General del Estado, 2025 · Gestión de Sistemas e Informática (A2)

36 **De acuerdo con el estándar Common Vulnerability Scoring System CVSS versión 4.0, una vulnerabilidad con una puntuación base CVSS de 7.5 se califica de gravedad:**

- **A** Baja.
- **B** Media.
- **C** Alta.
- **D** Crítica.

Junta de Castilla y León, 2026 · Ingeniero de Telecomunicación (A1)

37 **¿Cuál de las siguientes afirmaciones describe mejor la Metodología MAGERIT 3.0 en relación con su enfoque y utilidad?.**

- **A** MAGERIT 3.0 es exclusivamente una metodología para la gestión de riesgos en proyectos de desarrollo de software.
- **B** MAGERIT 3.0 es un método que se centra en la gestión de riesgos de seguridad de la información y proporciona un enfoque estructurado para identificar, analizar y mitigar riesgos en sistemas de información.
- **C** MAGERIT 3.0 es un marco para la gestión de riesgos en el ámbito financiero y económico de las organizaciones, principalmente en entidades bancarias y financieras.
- **D** MAGERIT 3.0 es una guía para la gestión de riesgos en el área de recursos humanos y se enfoca en la evaluación de riesgos laborales y de seguridad en el trabajo.

Generalitat Valenciana, 2024 · Técnica en Sistemas y Tecnología de la Información (A2)

38 **Según MAGERIT, ¿cuál es la diferencia clave entre un análisis de impacto y un análisis de riesgos en la gestión de seguridad?**

- **A** El análisis de impacto se centra en las consecuencias de una amenaza, mientras que el análisis de riesgos considera tanto la probabilidad como el impacto.
- **B** El análisis de impacto sólo evalúa daños económicos, mientras que el análisis de riesgos considera factores técnicos y organizativos.
- **C** El análisis de riesgos se aplica únicamente a sistemas informáticos, mientras que el análisis de impacto se enfoca en la continuidad del negocio.
- **D** El análisis de impacto es opcional en MAGERIT, mientras que el análisis de riesgos es obligatorio.

Servicio Andaluz de Salud, 2025 · Técnico de Función Administrativa, Sistemas y Tecnología de la Información (A1)

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

39 **En cuanto a un ataque DDoS:**

- **A** Se produce cuando un grupo de personas o automatismos se unen para optimizar los recursos propios de una empresa.
- **B** Se produce cuando un grupo de personas o automatismos protegen un servidor u ordenador mediante la implantación de soluciones de protección de redes.
- **C** Es gracias a DDoS que las empresas pueden llegar a estar totalmente protegidas de cualquier virus.
- **D** Se produce cuando un grupo de personas o automatismos atacan un servidor u ordenador desde uno o muchos equipos a la vez.

Generalitat de Catalunya, 2023 · Programador informático

40 **¿Cuál de las siguientes no es una fase en un plan director de seguridad?**

- **A** Conocer la situación actual
- **B** Conocer la situación presupuestaria
- **C** Conocer la estrategia de la organización.
- **D** Clasificación y priorización.

Junta de Comunidades de Castilla-La Mancha, 2025 · Escala Superior de Sistemas y Tecnologías de la Información (A1)

41 **De acuerdo con el CCN-CERT, ¿cuál de los siguientes NO se considera un mecanismo de Autenticación Multi-Factor (MFA)?**

- **A** Contraseña + Token OTP (One Time Password).
- **B** Escáner de Iris + Huella dactilar.
- **C** Contraseña + Escáner de Iris.
- **D** Tarjeta de identificación + Reconocimiento facial.

Administración General del Estado, 2025 · Técnico Auxiliar de Informática (C1)

42 **¿Qué NO debe incluir la implementación de un plan de continuidad de negocio dentro de un Sistema de Gestión de la Seguridad de la Información?**

- **A** Designar y formar a las personas que deben intervenir en cada caso.
- **B** Documentar y construir procedimientos de actuación en cada caso.
- **C** Aportar una definición del alcance del Sistema de Gestión de la Seguridad de la Información.
- **D** Establecer una estructura de gestión y sus niveles de competencia dentro del plan de continuidad.

Xunta de Galicia, 2022 · Escala de Sistemas y Tecnología de la Información (A1)

43 **Señalar qué característica NO es correcta respecto del concepto RIESGO, de acuerdo a la metodología Magerit v3.**

- **A** El riesgo es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.
- **B** El riesgo puede ser acumulado, potencial y repercutido.
- **C** El riesgo es la causa potencial de un incidente que puede causar daños a un sistema de información.
- **D** El riesgo se puede estimar a partir del estudio de los activos, amenazas y salvaguardas.

Gobierno de Aragón, 2024 · Técnico de Informática (A2)

PARTE 1

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

44 **¿Cuál de las siguientes afirmaciones sobre la seguridad de las bases de datos en la nube es correcta?**

- **A** Las bases de datos en la nube son inmunes a los ataques
- **B** La seguridad de las bases de datos en la nube es responsabilidad exclusiva del proveedor de servicios en la nube
- **C** Las bases de datos en la nube son inherentemente más seguras que las bases de datos locales
- **D** Los usuarios deben implementar medidas de seguridad adicionales para proteger sus datos en la nube

Junta de Andalucía, 2025 · Informática (C1)

45 **En el diseño de una arquitectura de red segura, ¿qué configuración perimetral permite aislar los servidores que ofrecen servicios al exterior, impidiendo que una intrusión en estos comprometa directamente la red interna?**

- **A** La implementación de una red privada virtual (VPN) de acceso remoto para todos los usuarios externos.
- **B** La creación de una zona desmilitarizada (DMZ) mediante el uso de cortafuegos que segmenten el tráfico.
- **C** El uso de un único sistema de detección de intrusiones (IDS) configurado en modo promiscuo en el núcleo de la red.
- **D** La asignación de direcciones IP públicas directamente a los terminales de los usuarios internos.

Administración General del Estado, 2025 · Técnico Auxiliar de Informática (C1)

46 **Según la metodología MAGERIT v3, ¿en qué consiste el impacto acumulado de una amenaza sobre un activo?**

- **A** Es la medida que establece la probabilidad de que ocurra un daño sobre el activo y todos aquellos de los que él depende.
- **B** Se trata de la estimación del conjunto de riesgos que afectan a un activo, de forma acumulada en el tiempo, dado un horizonte temporal predefinido.
- **C** Es el inverso del valor estimado de la degradación sufrida por un activo, tanto en caso de que llegue a producirse una amenaza como si ésta aún no ha tenido lugar.
- **D** Es la medida de la pérdida de valor acumulado, es decir, la degradación del valor del propio activo y todos aquellos que dependen de él.

Junta de Castilla y León, 2024 · Técnico Superior de Informática

47 **Un ataque Zero-day:**

- **A** aprovecha una vulnerabilidad de un software antes de que se publiquen y apliquen los parches que la corrigen
- **B** intercepta mensajes entre dos victimas poniéndose el atacante en medio de la comunicación
- **C** es el uso de la línea telefónica convencional y de la ingeniería social para engañar personas y obtener información delicada como puede ser información financiera o información útil para el robo de identidad
- **D** es un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar

Junta de Andalucía, 2020 · Informática (A1)

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

48 **¿A qué área del mundo TIC hacen referencia los conceptos RTO y RPO?**

- **A** Son conceptos relacionados con los planes de contingencia.
- **B** Son conceptos relacionados con el desarrollo de aplicaciones.
- **C** Son conceptos relacionados con el estándar de redes Ethernet.
- **D** Son conceptos relacionados con VoIP.

Parlamento de Navarra, 2022 · Técnico de Grado Medio en Sistemas Informáticos

49 **Respecto a la metodología MAGERIT y la gestión de riesgos, el riesgo calculado tomando en consideración el valor propio de un activo y el valor de los activos que depende de él se denomina:**

- **A** Riesgo inherente
- **B** Riesgo repercutido
- **C** Riesgo acumulado
- **D** Riesgo total

Junta de Andalucía, 2021 · Informática (A1)

50 **Al diseñar un sistema de información con altos requisitos de seguridad, ¿cuál de las siguientes buenas prácticas suele recomendarse?**

- **A** No emplear cifrado para agilizar el tráfico de datos.
- **B** Implementar mecanismos de autenticación y autorización, además de cifrar los datos.
- **C** Permitir conexiones anónimas sin restricciones para facilitar la puesta en marcha.
- **D** Todas las respuestas anteriores son correctas.

Servicio Andaluz de Salud, 2025 · Técnico de Función Administrativa, Sistemas y Tecnología de la Información (A1)

51 **En el contexto de la detección de ciberincidentes, ¿qué es un precursor?**

- **A** Un indicio de que un incidente ya se ha producido.
- **B** Un registro obligatorio tras cerrar un incidente.
- **C** Un indicio de que un incidente podría ocurrir en el futuro.
- **D** Un nivel de peligrosidad asignado por el CCN-CERT.

Administración General del Estado, 2025 · Gestión de Sistemas e Informática (A2)

52 **Durante la elaboración del Plan de Recuperación ante Desastres (DRP) de un CPD se definen los siguientes objetivos: RPO (Objetivo de Punto de Recuperación) = 10 minutos y RTO (Objetivo de Tiempo de Recuperación) = 1 hora. ¿Cuál de las siguientes interpretaciones es correcta?**

- **A** El sistema puede perder hasta 1 hora de datos y tardar 10 minutos en recuperarse tras un desastre.
- **B** No se perderá ningún dato ante un desastre y la recuperación será inmediata gracias al RPO de 10 minutos.
- **C** El sistema puede perder hasta 10 minutos de datos y debe restaurarse completamente en un máximo de 1 hora.
- **D** La recuperación completa requiere exactamente 1 hora, independientemente de la complejidad del incidente.

Administración General del Estado, 2025 · Gestión de Sistemas e Informática (A2)

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

53 **La situación que se crea cuando una persona persigue a otra de forma obsesiva a través de mensajes digitales, llamadas telefónicas, etc., se denomina:**

A Stalking.
B Sextorsión.
C Ciberacoso.
D Las opciones a) y c) son correctas.

Junta de Andalucía, 2021 · Psicólogo

54 **¿Cuál de las siguientes opciones es una práctica recomendada para eliminar información de soportes electrónicos antes de desecharlos, según INCIBE?**

A Guardar los dispositivos en un almacén cerrado durante al menos 6 meses antes de desecharlos.
B Formatear el dispositivo una sola vez, no siendo necesario verificar el resultado.
C Usar procesos de desmagnetización o destrucción física del soporte.
D Enviar el dispositivo a un punto limpio para su posterior reciclaje.

Junta de Comunidades de Castilla-La Mancha, 2025 · Escala Administrativa de Informática (C1)

55 **¿En qué consiste la técnica de spoofing?**

A Consiste en usurpar una identidad electrónica para ocultar la propia identidad y así poder cometer delitos en Internet.
B Consiste en conectar dispositivos de hardware al sistema informático de manera incorrecta y sin autorización.
C Es una técnica para desbloquear y acceder a sitios web restringidos en línea.
D Es un proceso para hacer que los archivos o programas parezcan más atractivos o interesantes de lo que realmente son.

Generalitat de Catalunya, 2023 · Programador informático

56 **En el contexto de la gestión de escritorio en una gran organización, ¿cuál de las siguientes estrategias de seguridad puede suponer un mayor impacto en la organización debido a un contexto heterogéneo con diversidad de plataformas y dispositivos, y a la necesidad de mantener un equilibrio entre la productividad del usuario y la seguridad de la organización en cada uno de ellos?**

A Implementar una política de bloqueo completo de todos los puertos USB en todas las estaciones de trabajo.
B Desarrollar un sistema MDM de gestión de dispositivos móviles que garantice la seguridad y el cumplimiento normativo en todos los dispositivos corporativos.
C Aplicar una política de "desconfianza por defecto" que restrinja todas las comunicaciones externas desde las estaciones de trabajo, permitiendo solo conexiones a sitios web específicos.
D Establecer un sistema de gestión unificada que asegure que todas las estaciones de trabajo, independientemente del sistema operativo, cumplan con las políticas de seguridad y las actualizaciones de software.

Servicio Andaluz de Salud, 2025 · Técnico Medio de Gestión de Función Administrativa, Administración General (A2)

MUESTRA GRATIS · Libro completo, 473 preguntas 34,90 €
Cómpralo aquí ›

57 **Según la Guía de Seguridad de las TIC CCN-STIC 817 del Esquema Nacional de Seguridad, los indicios de que nos encontramos ante un ciberincidente pueden provenir de dos tipos de fuentes: los precursores y los indicadores. ¿Cuál es la diferencia entre ambos?**

- **A** Un precursor es un indicio de que seguro que ocurrirá un incidente en el futuro. Un indicador es un indicio de que un incidente ocurrió o está ocurriendo ahora.
- **B** Un precursor es un indicio de que puede ocurrir un incidente en el futuro. Un indicador es un indicio de que un incidente puede haber ocurrido o puede estar ocurriendo ahora.
- **C** Un precursor es un indicio de que un incidente puede haber ocurrido o puede estar ocurriendo ahora. Un indicador es un indicio de que un incidente puede ocurrir en el futuro.
- **D** Un precursor es un indicio de que se originó un incidente. Un indicador es un indicio de que un incidente puede originarse en el futuro.

Generalitat Valenciana, 2025 · Técnico facultativo en Sistemas y Tecnología de la Información (A2)

58 **Se considera que un UTM (Unified Threat Management) es:**

- **A** Un protocolo de gestión de amenazas.
- **B** Lo mismo que un firewall de nueva generación (NGFW).
- **C** Un dispositivo que combina múltiples funciones o servicios de seguridad (como firewall, antivirus, filtrado de contenido) en un solo dispositivo.
- **D** Un protocolo de nivel de transporte.

Administración General del Estado, 2022 · Gestión de Sistemas e Informática (A2)

59 **Señala el objetivo principal del control de flujo de datos, la notarización y la auditoría en el contexto de la seguridad de la información.**

- **A** Garantizar la disponibilidad de los datos en todo momento.
- **B** Prevenir el acceso no autorizado a los datos sensibles.
- **C** Proteger los datos contra pérdidas o daños.
- **D** Facilitar la colaboración y el intercambio de datos entre diferentes usuarios.

Xunta de Galicia, 2023 · Escala Técnica Auxiliar de Informática (C1)

60 **Señale la respuesta incorrecta sobre la elaboración de Planes de Seguridad según la Metodología MAGERIT:**

- **A** La tarea PS1 identifica los proyectos de seguridad traduciendo las decisiones de tratamiento de los riesgos en acciones concretas.
- **B** Una vez identificados los proyectos de seguridad se realiza la planificación de estos.
- **C** Los factores para ordenar los proyectos de seguridad en el tiempo son la criticidad de los impactos, el coste, la disponibilidad de personal propio y el presupuesto.
- **D** El Plan de seguridad no incluye un cronograma sino una lista de tareas.

Generalitat Valenciana, 2023 · Sistemas y Tecnología de la Información (A1)

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

61 **El MFA (Multi-Factor Authentication) o Autenticación Multifactor es un mecanismo de control de acceso que requiere que el usuario proporcione dos o más factores de verificación antes de concederle acceso a un sistema, red o aplicación. ¿Cuáles de los siguientes no es considerado como un factor clásico en MFA?**

- **A** Contraseña (algo que sabes).
- **B** Código SMS en el móvil (algo que tienes).
- **C** Huella dactilar (algo que eres).
- **D** Ubicación geográfica (lugar donde estás).

Junta de Andalucía, 2025 · Informática (A2)

62 **En gestión de continuidad de negocio, ¿qué es un BIA (Business Impact Analysis)?**

- **A** Es una métrica ampliamente utilizada para calcular el tiempo máximo tolerable de inactividad del negocio.
- **B** Es un proceso de análisis de las funciones del negocio y del efecto que una interrupción de la actividad empresarial podría tener sobre ellas.
- **C** Es el plan que define los pasos que se requieren para el restablecimiento de los procesos de negocio después de una interrupción.
- **D** Es una herramienta del CCN-CERT que permite realizar un análisis global de riesgos de ciberseguridad de una organización.

Junta de Comunidades de Castilla-La Mancha, 2025 · Escala Superior de Sistemas y Tecnologías de la Información (A1)

63 **Indique la respuesta incorrecta respecto a la Gestión de Ciberincidentes:**

- **A** Para la notificación de los incidentes de ciberseguridad se utilizará como criterio de referencia el Nivel de peligrosidad.
- **B** Los incidentes de Ingeniería Social no se incluyen en la taxonomía de gestión de incidentes por no darse directamente en los sistemas TIC.
- **C** El indicador de impacto de un ciberincidente se determinará evaluando las consecuencias que este ciberincidente ha tenido en las funciones y actividades de la organización afectada, en sus activos o en los individuos afectados.
- **D** Los organismos públicos tienen la obligación de notificar a su CERT de referencia todos aquellos que se categorizan con un nivel CRÍTICO, MUY ALTO o ALTO.

Generalitat Valenciana, 2023 · Sistemas y Tecnología de la Información (A1)

64 **En el ámbito de la seguridad de las tecnologías de la información, señale la respuesta INCORRECTA en relación con la inteligencia de fuentes abiertas (OSINT):**

- **A** Se trata de un conjunto de técnicas y herramientas para recopilar información pública, correlacionar los datos y procesarlos.
- **B** Consta de las siguientes fases: requisitos, fuentes de información, adquisición, procesamiento, análisis y presentación.
- **C** Maltego o TheHarvester son ejemplos de herramientas OSINT.
- **D** El sistema operativo KALNIX está diseñado específicamente para la aplicación de técnicas OSINT.

Junta de Andalucía, 2021 · Ingeniero de Telecomunicación (A1)

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

65 **¿Cuál de los siguientes tipos de virus se caracteriza por ocultar su presencia al modificar los archivos infectados de manera que su tamaño permanezca igual?**

- **A** Virus de Macro.
- **B** Virus de sobreescritura.
- **C** Virus de boot.
- **D** Virus de compañía.

Xunta de Galicia, 2023 · Escala Técnica Auxiliar de Informática (C1)

66 **Según MAGERIT, ¿Cuál de las siguientes podría ser una definición de Riesgo?**

- **A** Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización
- **B** Intento de destruir, exponer, alterar o inhabilitar un sistema de información o la información que el sistema maneja, o violar alguna política de seguridad de alguna otra manera
- **C** Consecuencia que sobre un activo tiene la materialización de una amenaza
- **D** Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización

Junta de Comunidades de Castilla-La Mancha, 2020 · Escala Superior de Sistemas y Tecnologías de la Información (A1)

67 **¿Cuál de los siguientes sistemas correspondería con un sistema de autenticación fuerte?**

- **A** Un sistema que utilice usuario y contraseña.
- **B** Un sistema que utilice usuario, contraseña y token digital.
- **C** Un sistema que utilice identificación biométrica.
- **D** Un sistema que utilice usuario y código numérico.

Administración General del Estado, 2022 · Gestión de Sistemas e Informática (A2)

68 **Una infección de tipo Mirai es un ataque dirigido a dispositivos IoT vulnerables, en el que estos son infectados por un malware llamado Mirai para convertirlos en parte de una botnet. ¿Qué medidas de seguridad debemos adoptar para prevenir infecciones de este tipo en nuestros dispositivos?**

- **A** Segmentar la red IoT.
- **B** Cambiar las credenciales por defecto de dispositivos IoT.
- **C** Deshabilitar servicios innecesarios (como Telnet).
- **D** Todas la anteriores respuestas son correctas

Junta de Andalucía, 2025 · Informática (A2)

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

69 **Según la Guía CCN-STIC 804 (ENS. Guía de implantación), el conjunto de procedimientos operativos de seguridad [ORG.3] debe cubrir un determinado porcentaje de las actividades rutinarias, así como aquellas tareas que se realizan con poca frecuencia, pero exigen seguir unos pasos determinados muy precisos. Dicho porcentaje será de, al menos:**

- **A** El 60 % de las actividades rutinarias.
- **B** El 90 % de las actividades rutinarias.
- **C** El 80 % de las actividades rutinarias.
- **D** El 70 % de las actividades rutinarias.

Administración General del Estado, 2025 · Gestión de Sistemas e Informática (A2)

70 **¿Qué característica de seguridad ofrece UEFI?**

- **A** Arranque seguro.
- **B** Antivirus integrado.
- **C** Firewall por hardware.
- **D** Cifrado de disco automático.

Junta de Comunidades de Castilla-La Mancha, 2025 · Escala Administrativa de Informática (C1)

71 **En relación al ámbito de la seguridad de la red de una organización, podríamos afirmar que:**

- **A** IDS (Intrusion Detection System) es un servidor en la red que bloquea los accesos no autorizados.
- **B** IPS (Intrusion Prevention System) es un software que se utiliza para un análisis forense de los ataques y accesos no autorizados.
- **C** SIEM (Security Information and Event Management) es un software que engloba la gestión de información de seguridad y la gestión de eventos.
- **D** IGS (Intrusion Gateway System) combina las tareas de un IDS y un IPS, proporcionando un análisis en tiempo real de las alertas de seguridad generadas por los distintos dispositivos hardware y software de la red.

Administración General del Estado, 2024 · Gestión de Sistemas e Informática (A2)

72 **En la aplicación, se requiere implementar un sistema de autenticación robusto para proteger el acceso a los datos de los pacientes. ¿Cuál de las siguientes combinaciones de factores de autenticación NO se considera una buena práctica de seguridad?**

- **A** Contraseña + token de hardware (generador de códigos).
- **B** Contraseña + dato biométrico (huella dactilar).
- **C** Contraseña + pregunta de seguridad + fecha de nacimiento.
- **D** Contraseña + código de verificación enviado por SMS.

Servicio Andaluz de Salud, 2025 · Técnico Medio de Gestión de Función Administrativa, Informática (A2)

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

73 **¿Cuál de los siguientes NO es un ataque de suplantación de identidad?**

- **A** Hijacking.
- **B** Smurf.
- **C** IP-spoofing.
- **D** Phising.

Administración General del Estado, 2022 · Gestión de Sistemas e Informática (A2)

74 **Sea un activo valorado en 1.000.000 €, que es víctima de una amenaza que lo degrada un 90%, y las salvaguardas tienen un 90% de eficacia sobre el impacto, señale cuál de las siguientes es correcta:**

- **A** El impacto es de cuantía 90.000 €
- **B** El impacto residual es de cuantía 90.000 €
- **C** El riesgo residual es 90.000 €
- **D** El riesgo acumulado es 90.000 €

Servicio Andaluz de Salud, 2021 · Técnico Medio de Gestión de Función Administrativa, Informática (A2)

75 **En el contexto de una investigación forense:**

- **A** Se debe trabajar con el disco duro original para dejar constancia del trabajo realizado
- **B** Se debe trabajar con una copia de los ficheros del disco duro realizada desde el sistema operativo y configurando el acceso a disco en modo de sólo lectura
- **C** Se debe trabajar con un clonado o copia bit a bit del disco duro
- **D** Se debe trabajar con el disco duro original pero realizando previamente una imagen forense y dejando constancia mediante el cálculo del hash

Junta de Andalucía, 2021 · Informática (A1)

76 **¿Cuál de las siguientes opciones describe el concepto de "vulnerabilidad de día cero"?**

- **A** Es un tipo de vulnerabilidad que permite el acceso no autorizado por un problema de compatibilidad inicial entre elementos del sistema
- **B** Es un tipo de vulnerabilidad que se explota después de una actualización del sistema
- **C** Es un tipo de vulnerabilidad desconocida para el proveedor y sin parche disponible
- **D** Es un tipo de vulnerabilidad que se puede corregir sin necesidad de implementar un parche de seguridad

Junta de Castilla y León, 2025 · Ingeniero de Telecomunicación (A1)

77 **Usando el concepto de impacto repercutido según se describe en la metodología Magerit v3: Sea un activo A valorado en 500.000, que depende de otro activo B en un 30%, (el valor de B es de 200.000). Si B es víctima de una amenaza que lo degrada un 90%, A sufre un impacto repercutido de cuantía:**

- **A** 54.000
- **B** 135.000
- **C** 330.000
- **D** 150.000

Gobierno de Aragón, 2025 · Técnico de Informática (A2)

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

78 **Cuál de las siguientes es unna norma internacional emitida por la Organización Internacional de Normalización (ISO) que describe cómo gestionar la seguridad de la información en una organización. Es certificable.**

A ISO 27000
B ISO 27001
C ISO 27002
D ISO 33000

Junta de Andalucía, 2020 · Informática (A1)

79 **Según la Metodología MAGERIT, ¿qué concepto se refiere al daño sobre un activo derivado de la materialización de la amenaza?**

A Impacto.
B Exposición.
C Vulnerabilidad.
D Salvaguarda.

Junta de Castilla y León, 2026 · Técnico Superior de Informática

80 **En el ámbito de la seguridad informática, ¿en qué consiste la técnica conocida como "pharming"?**

A En el envío masivo de correos electrónicos para obtener claves bancarias.
B En la infección de un equipo mediante un troyano que cifra los archivos pidiendo un rescate.
C En la redirección del tráfico de un sitio web legítimo a otro fraudulento, mediante la alteración del DNS o del archivo hosts del equipo de la víctima.
D En la observación física de un usuario mientras introduce su contraseña en un terminal a través de cámaras de seguridad y sistemas de vigilancia remota.

Junta de Castilla y León, 2026 · Auxiliar Administrativo (C2)

81 **Dentro de las amenazas dirigidas al puesto del usuario, ¿en qué consiste la técnica de "Pharming" para la obtención ilícita de credenciales?**

A En la alteración del proceso de resolución de nombres (fichero hosts o caché DNS) para redirigir al usuario a una página web falsa, incluso si este escribe la dirección correcta en el navegador.
B En el envío masivo de correos electrónicos suplantando la identidad de una entidad financiera para que el usuario pinche en un enlace malicioso.
C En la instalación de un programa malicioso que registra todas las pulsaciones de teclas realizadas en un dispositivo infectado.
D En el uso de técnicas de ingeniería social telefónica con las que se suplanta la identidad de una empresa, organización o persona de confianza, con el fin de obtener información personal y sensible.

Administración General del Estado, 2025 · Técnico Auxiliar de Informática (C1)

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

82 **¿Qué tipo de ataque informático es la Denegación de Servicio (DoS) y la Denegación de Servicio Distribuida (DDoS)?**

- **A** Ataque de fuerza bruta
- **B** Ataque de repetición
- **C** Ataque combinado
- **D** Ataque de registro

Principado de Asturias, 2018 · Técnico de Intervención de Bomberos

83 **En un análisis forense de un sistema comprometido, se identifica un malware que utiliza una técnica de persistencia basada en la modificación del Master Boot Record (MBR). ¿Qué tipo de malware es más probable que esté involucrado?**

- **A** MBRZero, debido a su capacidad de cifrar el sistema de archivos.
- **B** Bootkit, por su ejecución previa al cargador del sistema operativo.
- **C** SpyBootRec, por su capacidad de monitorear actividades del usuario.
- **D** AdwareMaster, por su integración en aplicaciones de arranque.

Xunta de Galicia, 2025 · Gestión de Sistemas de Informática (A2)

84 **¿Cuál de las siguientes opciones describe correctamente la técnica "Right to Left Override" (RLO) utilizada en ataques por correo electrónico?**

- **A** Es una técnica que cifra los archivos adjuntos para evitar su detección por antivirus.
- **B** Consiste en usar macros ocultas en documentos de texto para ejecutar código malicioso.
- **C** Utiliza un carácter Unicode especial para alterar visualmente el nombre de los archivos adjuntos y ocultar su verdadera extensión.
- **D** Se basa en el envío masivo de correos para saturar la bandeja de entrada y ocultar mensajes legítimos.

Gobierno de Navarra, 2025 · Oficial de Sistemas Informáticos (C1)

85 **De los siguientes escenarios, ¿cuál representa una técnica de ingeniería social?:**

- **A** Un antivirus detectando malware en segundo plano.
- **B** Un atacante llama haciéndose pasar por soporte técnico para obtener acceso remoto.
- **C** Un usuario instala manualmente un software legítimo.
- **D** Un error de red impide el acceso a una página web segura.

Junta de Comunidades de Castilla-La Mancha, 2025 · Administrativo (C1)

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

86 **La norma ISO 27701:**

- **A** Es el estándar para que las organizaciones puedan implementar sistemas de gestión de seguridad de la información.
- **B** Permite a las organizaciones crear un sistema de gestión de información de privacidad (PIMS) y obtener la certificación en determinadas prácticas de privacidad.
- **C** Es incompatible con la norma ISO 27001.
- **D** Un protocolo de nivel de transporte.

Administración General del Estado, 2022 · Gestión de Sistemas e Informática (A2)

87 **¿En qué caso se puede utilizar el navegador de la estación de trabajo, ya sea dentro o fuera de la jornada laboral?**

- **A** Para consultar páginas web que no tengan relación directa con las funciones y tareas asignadas, incluidas páginas web de vídeos en línea.
- **B** Para descargar archivos o programas que no estén justificados en el ejercicio de sus funciones y tareas encomendadas, incluida música, vídeo y juegos.
- **C** Para conectarse a chats, foros de discusión, grupos de trabajo o cualquier aplicación interactiva, así como para participar en juegos en línea.
- **D** Para casos relacionados directamente con las tareas y funciones encomendadas y con la autorización del órgano competente.

Generalitat de Catalunya, 2023 · Recepcionista

88 **Según la metodología MAGERIT v3, ¿cuál de las siguientes opciones NO es un tipo de salvaguarda con efecto preventivo o reductor de la probabilidad de ocurrencia de una amenaza?**

- **A** Disuasoria.
- **B** Minimizadora.
- **C** Eliminatoria.
- **D** Preventiva.

Junta de Castilla y León, 2024 · Técnico Superior de Informática

89 **¿Cuál es el primer paso en la elaboración de un Plan de Recuperación ante Desastres (DRP)?**

- **A** Implementar una solución de respaldo.
- **B** Realizar pruebas de conmutación de los servicios.
- **C** Identificar los activos críticos y el impacto de su interrupción.
- **D** Definir los pasos a seguir en caso de desastre.

Junta de Andalucía, 2025 · Informática (A2)

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

90 **Según la Norma UNE-ISO/IEC 27001:2017, la facultad de un control para lograr los objetivos de seguridad para la que fue diseñado se denomina:**

A Eficiencia de un control.
B Finalidad de un control.
C Idoneidad de un control.
D Eficacia de un control.

Xunta de Galicia, 2022 · Escala de Sistemas y Tecnología de la Información (A1)

91 **Seleccione la respuesta verdadera sobre los términos empleados para definir la estrategia de continuidad y recuperación en un sistema de información:**

A El término RLO determina el impacto que tiene que un proceso permanezca detenido hasta ser restaurado.
B El término MTD determina el impacto que tiene que un proceso permanezca detenido hasta ser restaurado.
C El término RPO determina el impacto que tiene que un proceso permanezca detenido hasta ser restaurado.
D El término RTO determina el tiempo que un proceso permanece detenido hasta ser restaurado.

Generalitat Valenciana, 2023 · Técnico superior de gestión en Ingeniería Técnica Informática (A2)

92 **Señale la opción correcta respecto a las soluciones EMM (Enterprise Mobility Management) para sistemas de movilidad:**

A MAM permite administrar las aplicaciones en los dispositivos móviles de una organización.
B MIM tiene como papel fundamental la seguridad de contenidos.
C MDM no implica la instalación de perfiles únicos.
D MCM permite gestionar la securización del correo electrónico móvil.

Servicio Andaluz de Salud, 2022 · Técnico Medio de Gestión de Función Administrativa, Informática (A2)

93 **¿Cuál de las siguientes opciones es la más adecuada?**

A Las listas de control de acceso (ACL) se deben colocar cerca del destino si son extendidas y cerca del origen si son estándar.
B Tanto las listas de control de acceso (ACL) estándar como extendidas se deben colocar cerca del origen.
C Tanto las listas de control de acceso (ACL) estándar como extendidas se deben colocar cerca del destino.
D Las listas de control de acceso (ACL) se deben colocar cerca del destino si son estándar.

Administración General del Estado, 2022 · Gestión de Sistemas e Informática (A2)

94 **En la relación que establecemos con la empresa proveedora del cloud:**

A Deberíamos requerir evidencias de que existe un plan de continuidad de negocio.
B Los SLA (acuerdos de nivel de servicio) solo dependen de nosotros como cliente.
C El hecho de que la empresa proveedora disponga de la certificación ISO 27001 no nos aporta nada en este tipo de servicio.
D En términos generales, cuando el nivel de abstracción disminuye, también disminuye el control que tiene el cliente sobre la infraestructura.

Generalitat de Catalunya, 2023 · Analista informático

MUESTRA GRATIS · Libro completo, 473 preguntas 34,90 €
Cómpralo aquí ›

95 **¿Cuál de las siguientes técnicas de detección de malware es utilizada por algunos programas antivirus avanzados para identificar amenazas desconocidas?**

- **A** Firma de virus.
- **B** Análisis heurístico.
- **C** Protección en tiempo real.
- **D** Protección firewall.

Xunta de Galicia, 2023 · Escala Técnica Auxiliar de Informática (C1)

96 **Durante la fase de seguridad activa en el proceso de conexión remota a un sistema de información crítico, un organismo público adopta autenticación multifactor (MFA), establecimiento de túneles cifrados y verificación de la integridad de los dispositivos. ¿Cuál es el objetivo principal de esta combinación de medidas en la fase previa al acceso lógico a los recursos internos?**

- **A** Garantizar que la identidad del usuario, la confidencialidad del canal de comunicación y la integridad del dispositivo que se conecta se encuentran en un estado de seguridad aceptable antes de permitir el acceso a recursos sensibles.
- **B** Reducir el consumo de recursos del sistema central al delegar la autenticación en los dispositivos de los usuarios, confiando en que el cifrado por sí mismo garantiza que solo se conecten usuarios legítimos.
- **C** Asegurar que el sistema pueda rastrear en todo momento la ubicación física exacta del usuario, utilizando la información de la VPN y las credenciales, lo que permite bloquear conexiones desde otros países.
- **D** Permitir que cualquier dispositivo pueda conectarse libremente al sistema, siempre que el usuario recuerde una contraseña compleja, ya que las otras medidas se centran exclusivamente en proteger el canal y no al usuario.

Govern de les Illes Balears, 2026 · Facultativo Técnico de Informática (A2)

97 **En la seguridad en la nube, ¿cuál de las siguientes afirmaciones es cierta?**

- **A** La virtualización no es útil para aumentar la seguridad de los procesos que se ejecutan en la nube.
- **B** Cifrar los datos no aporta una seguridad adicional.
- **C** Los mecanismos de seguridad son responsabilidad del proveedor.
- **D** La segmentación de datos se puede considerar un mecanismo de seguridad.

Generalitat de Catalunya, 2023 · Analista informático

98 **¿Cuál es una de las principales ventajas técnicas de TLS 1.3 respecto a TLS 1.2?**

- **A** Aumenta el número de pasos de verificación en el handshake para asegurar que la clave sea más larga.
- **B** Elimina el uso de certificados digitales, basándose únicamente en contraseñas de un solo uso (OTP).
- **C** Obliga a que el cliente y el servidor se encuentren en la misma subred física.
- **D** Permite completar el handshake en un solo viaje de ida y vuelta (1-RTT), reduciendo la latencia.

Administración General del Estado, 2025 · Técnico Auxiliar de Informática (C1)

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

99 **En seguridad de la información, ¿cuál es el objetivo principal del modelo Bell-LaPadula?**

- **A** Integridad de los datos
- **B** Disponibilidad de los recursos
- **C** Confidencialidad de la información
- **D** Autenticación de usuarios

Junta de Comunidades de Castilla-La Mancha, 2025 · Escala Técnica de Sistemas e Informática (A2)

100 **Como solución para la protección de los equipos contra software malicioso utilizan Symantec Endpoint Protection (SEP). Si desde la plataforma de gestión de activos corporativa se programa la tarea de ejecución del Sylink del SEP, se utilizará para:**

- **A** Desplegar el Job.
- **B** Indicar cuál es el servidor al que tienen que apuntar los equipos clientes para su gestión.
- **C** Programar el despliegue.
- **D** Lanzar la directiva GPO.

Servicio Andaluz de Salud, 2022 · Técnico Medio de Gestión de Función Administrativa, Informática (A2)

PARTE 1

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

Soluciones — Tema 51

Serveis de seguretat de la informació (InfoSec): Objectius principals…

Clave rápida

Corrige aquí antes de leer las explicaciones.

1 **B**	2 **D**	3 **C**	4 **B**	5 **C**	6 **A**	7 **B**	8 **B**	9 **C**	10 **B**
11 **A**	12 **D**	13 **B**	14 **C**	15 **B**	16 **A**	17 **A**	18 **C**	19 **B**	20 **A**
21 **A**	22 **C**	23 **D**	24 **B**	25 **A**	26 **D**	27 **B**	28 **C**	29 **A**	30 **A**
31 **D**	32 **A**	33 **A**	34 **D**	35 **B**	36 **C**	37 **B**	38 **A**	39 **D**	40 **B**
41 **B**	42 **C**	43 **C**	44 **D**	45 **B**	46 **D**	47 **A**	48 **A**	49 **C**	50 **B**
51 **C**	52 **C**	53 **D**	54 **C**	55 **A**	56 **D**	57 **B**	58 **C**	59 **B**	60 **D**
61 **D**	62 **B**	63 **B**	64 **D**	65 **B**	66 **D**	67 **B**	68 **D**	69 **C**	70 **A**
71 **C**	72 **C**	73 **B**	74 **B**	75 **C**	76 **C**	77 **B**	78 **B**	79 **A**	80 **C**
81 **A**	82 **C**	83 **B**	84 **C**	85 **B**	86 **B**	87 **D**	88 **B**	89 **C**	90 **D**
91 **D**	92 **A**	93 **D**	94 **A**	95 **B**	96 **A**	97 **D**	98 **D**	99 **C**	100 **B**

Aciertos

1.ª vuelta _____ / 100

2.ª vuelta _____ / 100

1 — **B**

Criptografía Básica Los modos de cifrado con autenticación integrada combinan confidencialidad e integridad en una única operación. Sobre el cifrador de bloque de referencia, los esquemas reconocidos para uso recomendado son los que aportan autenticación del mensaje junto al cifrado. Entre ellos figuran los modos que generan y verifican una etiqueta de autenticación asociada. Los modos que solo proporcionan confidencialidad, como el encadenamiento de bloques, la realimentación de cifrado, la realimentación de salida o el contador, no ofrecen autenticación por sí mismos y por tanto no se consideran de cifrado autenticado.

2 — **D**

Amenazas y Vulnerabilidades El barrido o escaneo de puertos consiste en un ataque cuyo objetivo es obtener información básica sobre qué servicios ofrece un determinado sistema, además de otros detalles técnicos del mismo, revelando puertos abiertos y posibles vulnerabilidades. Las demás afirmaciones intercambian o falsean definiciones. La captura del tráfico que circula por una red corresponde al sniffing, mientras que la generación de tráfico con un origen falseado describe el spoofing. La denegación de servicio distribuida se caracteriza por proceder de múltiples puntos coordinados contra un objetivo, no desde un único origen.

3 — **C**

Ciberseguridad: Principios Un SIEM centraliza y analiza registros y eventos de seguridad para detectar indicios de amenazas, identificar vulnerabilidades y generar alertas. También puede facilitar el cumplimiento de obligaciones de seguridad mediante la recopilación y conservación de información. Sin embargo, detectar patrones o alertar sobre riesgos no significa predecir cuándo aparecerán amenazas nuevas.

4 — **B**

Ciberseguridad: Principios Las herramientas de ciberseguridad del Centro Criptológico Nacional tienen funciones específicas. El simulador de técnicas de cibervigilancia se identifica con el nombre Elena, por lo que esa correspondencia resulta correcta. La herramienta de auditoría de cumplimiento en sistemas Windows recibe otro nombre, luego asociarla con la protección y trazabilidad del dato es incorrecto. Las soluciones de gestión de eventos e información de seguridad y de gestión de registros aparecen intercambiadas en las restantes opciones. Solo la referida al simulador ofrece la asociación exacta.

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

5
C

Ciberseguridad: Principios SOAR permite coordinar y automatizar acciones de respuesta mediante playbooks que conectan distintas herramientas de seguridad. En la contención, esa orquestación ayuda a ejecutar de forma coordinada las medidas previstas para limitar el incidente. No se limita a normalizar registros ni a elaborar informes posteriores.

6
A

Amenazas y Vulnerabilidades APT significa amenaza persistente avanzada. Se caracteriza por dirigirse a una entidad concreta y emplear técnicas sofisticadas para comprometer sus sistemas. Además, la operación suele mantenerse de forma continuada en el tiempo, en lugar de limitarse a una acción puntual.

7
B

Gestión de Servicios TI e ITIL La continuidad operativa exige identificar qué servicios son críticos y qué consecuencias tendría su interrupción. El análisis de impacto en el negocio (BIA) aporta esa información y permite definir medidas y prioridades dentro de un plan de continuidad. Las pruebas periódicas ayudan a comprobar que el plan puede aplicarse cuando se produce una incidencia.

8
B

Criptografía Básica Hyperledger es un proyecto de código abierto impulsado por la Fundación Linux dedicado al desarrollo de tecnologías de cadena de bloques empresariales. Agrupa herramientas, marcos y bibliotecas destinados a construir libros de contabilidad distribuidos aplicables a distintos sectores. No es un programa de virtualización ni una infraestructura de red física o inalámbrica. Su finalidad es ofrecer soluciones colaborativas basadas en registros compartidos y contratos inteligentes para entornos corporativos.

9
C

Malware y Protección Antivirus La técnica descrita consiste en insertar código malicioso dentro de anuncios publicitarios en línea. Cuando la persona interactúa con esos anuncios, o incluso al cargarse en la página, se descarga e instala programa dañino en el dispositivo sin conocimiento del usuario. El término combina las palabras inglesas para publicidad y software malicioso. Otras opciones designan realidades distintas, como programas espía que recopilan información o el envío físico de dispositivos comprometidos por correo. Por ello, la denominación correcta corresponde a la manipulación fraudulenta de la publicidad digital.

10
B

Seguridad de Puestos y Endpoint Un EPP se centra principalmente en prevenir amenazas, por ejemplo mediante la detección y el bloqueo de malware conocido. Un EDR observa la actividad de los dispositivos para detectar comportamientos sospechosos y facilitar la investigación y respuesta ante amenazas avanzadas. Por ello, cumplen funciones relacionadas, pero tienen enfoques distintos y complementarios.

11
A

Amenazas y Vulnerabilidades La gestión de ciberincidentes comprende las actuaciones necesarias para prepararse, identificar y contener incidentes, así como mitigarlos y recuperar los sistemas. Una amenaza es un posible riesgo para la seguridad, mientras que un vector de ataque es la vía o el método empleado para materializarlo. La seguridad perimetral por sí sola no cubre todos los riesgos, y la formación del personal también ayuda a mitigarlos.

12
D

Amenazas y Vulnerabilidades CVE identifica vulnerabilidades de seguridad conocidas y sus fichas pueden recoger los productos y versiones afectados, así como referencias a información sobre posibles soluciones. CWE, en cambio, organiza debilidades o defectos del software que pueden dar lugar a vulnerabilidades. Por ello, ambos marcos tienen finalidades distintas y no utilizan una escala equivalente.

13
B

Cortafuegos y Redes Privadas Virtuales La gestión unificada de amenazas consiste en un dispositivo o solución que integra varias funciones de seguridad dentro de una misma plataforma. Reúne capacidades como cortafuegos, detección y prevención de intrusiones, antivirus, filtrado de contenidos y redes privadas virtuales. Su finalidad es simplificar la administración de la seguridad en las organizaciones al centralizar en un único punto la protección frente a distintos tipos de amenazas. No se trata de un estándar de interoperabilidad ni de una herramienta exclusiva para mitigar ataques de denegación de servicio.

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

14
C

Amenazas y Vulnerabilidades Las clasificaciones de ciberincidentes identifican tipos de sucesos, como los intentos de intrusión, el compromiso de la información o el contenido abusivo. La criptografía, en cambio, es una disciplina y una técnica de protección de la información, no una categoría de ciberincidente en esa clasificación. Por eso no pertenece a las categorías indicadas en la guía.

15
B

Amenazas y Vulnerabilidades La clave está en la manipulación del sistema que traduce nombres de dominio en direcciones numéricas: aunque el usuario teclee correctamente la dirección del banco, el navegador lo desvía a una página falsa que copia la original para robar las claves. Esta técnica de redirección encubierta se distingue del engaño por correo o mensaje fraudulento, que requiere que la víctima pulse un enlace. Aquí no hace falta error del usuario: el desvío se produce alterando la propia resolución de nombres.

16
A

Seguridad de Puestos y Endpoint El acceso desde dispositivos móviles personales al entorno corporativo plantea un desafío creciente para la seguridad y la gestión. La estrategia que permite emplear equipos propios de la persona empleada multiplica la superficie de exposición y la diversidad de plataformas. Esto complica el control de configuraciones, actualizaciones y protección de la información. Las alternativas basadas en equipos maquetados internamente, la impresión tradicional o el uso de suites ofimáticas estándar constituyen escenarios controlados y estables. Por ello, la movilidad con equipos personales es la que concentra el mayor reto actual.

17
A

Gestión de Servicios TI e ITIL En la gestión de la continuidad de negocio, el nivel de operación revisado identifica el rendimiento mínimo con el que una actividad puede considerarse recuperada, aun cuando el servicio no alcance su estado óptimo. Este parámetro fija el umbral aceptable de funcionamiento durante la fase de recuperación. Se diferencia del objetivo de tiempo, que mide cuándo debe restaurarse la actividad, del objetivo de punto, que limita la pérdida de datos, y del periodo máximo tolerable de interrupción. Por ello, representa el grado mínimo de operatividad exigible tras un incidente grave.

18
C

Seguridad de Puestos y Endpoint La prohibición de publicar o compartir contraseñas es una medida organizativa porque establece una pauta de conducta para las personas usuarias. En cambio, limitar permisos de administración o restringir puertos USB son medidas de configuración o control técnico. La norma interna sobre contraseñas ayuda a evitar accesos no autorizados.

19
B

Ciberseguridad: Principios La gestión de riesgos de seguridad de la información se apoya en marcos y metodologías específicas. Entre ellas figuran la metodología nacional de análisis y gestión de riesgos, la norma internacional dedicada al riesgo de seguridad de la información y la guía estadounidense sobre evaluación de riesgos. En cambio, la norma europea sobre iluminación en lugares de trabajo interiores regula parámetros lumínicos y ergonómicos, sin relación alguna con la protección de activos de información ni con el análisis de amenazas y vulnerabilidades. Por ello no constituye una metodología ni normativa de gestión de riesgos.

20
A

Gestión de Servicios TI e ITIL El Recovery Time Objective (RTO) establece el tiempo máximo objetivo para recuperar un sistema o servicio tras una interrupción. Es un parámetro de continuidad del negocio que ayuda a determinar cuánto puede durar la indisponibilidad antes de que el impacto resulte inaceptable. Se diferencia del objetivo de punto de recuperación, que se refiere a la pérdida de datos admisible.

21
A

Amenazas y Vulnerabilidades El movimiento lateral es la fase en la que un atacante, tras obtener acceso inicial, se desplaza entre distintos sistemas o recursos de la misma red. El objetivo suele ser ampliar el acceso, localizar información o alcanzar sistemas de mayor valor. No consiste en sacar datos fuera de la red ni en cambiar la dirección IP desde la que se ataca.

22
C

Gestión de Servicios TI e ITIL Una auditoría informática examina los sistemas de información y los controles asociados para valorar si protegen adecuadamente los datos y funcionan de forma íntegra y eficiente. También permite identificar riesgos, debilidades y posibles mejoras. Su propósito no se limita a evaluar procesos de negocio ni a diseñar aplicaciones.

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

23 **D**

Malware y Protección Antivirus El ransomware es una modalidad de software malicioso, por lo que queda comprendido en la descripción general de un programa que se infiltra o causa daños sin conocimiento del usuario. Su rasgo característico es bloquear o cifrar datos y exigir un rescate para recuperarlos. La descripción ofrecida es amplia y no recoge específicamente esa exigencia de rescate.

24 **B**

Ciberseguridad: Principios La interceptación consiste en acceder o captar información sin autorización, por lo que afecta a la confidencialidad. La disponibilidad se ve comprometida principalmente por ataques de interrupción, que impiden acceder a un servicio o recurso. Las demás parejas relacionan correctamente la modificación con la integridad y la suplantación con la autenticidad.

25 **A**

Ciberseguridad: Principios El análisis cualitativo expresa las valoraciones mediante categorías o escalas discretas, en lugar de calcularlas necesariamente con magnitudes numéricas precisas. Esto permite estimar activos, amenazas e impactos de forma comparativa, aunque con menor precisión cuantitativa. El análisis cuantitativo, por su parte, utiliza valores numéricos para medirlos.

26 **D**

Esquema Nacional de Seguridad En PILAR, el perfil de seguridad fija los requisitos o umbrales que debe alcanzar un sistema según la categoría de seguridad que le corresponda. Sirve para orientar el análisis de riesgos y valorar las medidas necesarias para protegerlo. No es un inventario de activos ni una asignación de responsables.

27 **B**

Redes, Internet y Ciberseguridad La eficacia del departamento se valora mejor midiendo si audita los riesgos prioritarios conforme a lo previsto y si las recomendaciones producen mejoras. El porcentaje de riesgos críticos cubiertos refleja el cumplimiento del plan y la tasa de implementación muestra el seguimiento de los resultados. El volumen de informes o de horas, por sí solo, no demuestra que la auditoría esté reduciendo riesgos.

28 **C**

Criptografía Básica Las directrices de seguridad nacionales exigen que los métodos de intercambio de claves autorizados ofrezcan una fortaleza mínima equivalente a 112 bits. Ese umbral asegura resistencia frente a ataques de fuerza bruta con la capacidad de cálculo actual. Se descartan así los mecanismos de establecimiento de claves considerados débiles. La exigencia se aplica al establecimiento de claves en los protocolos de comunicación cifrada. Valores inferiores no resultan admisibles por su nivel de vulnerabilidad frente a las amenazas presentes.

29 **A**

Ciberseguridad: Principios Un SIEM recopila y centraliza registros y eventos de distintos sistemas y dispositivos. La correlación permite relacionar esos datos para detectar patrones o indicios de incidentes que podrían pasar inadvertidos al analizarlos por separado. Por ello, es una capacidad característica de este tipo de herramienta.

30 **A**

Ciberseguridad: Principios Resolver o mitigar el incidente no necesariamente pone fin a su gestión. También deben completarse las actuaciones posteriores previstas, como documentar lo ocurrido, comunicar el cierre y extraer conclusiones para mejorar la respuesta. Por eso es falsa la afirmación de que el trabajo termina en cuanto se resuelve o mitiga la incidencia.

31 **D**

Firma y Certificado Electrónico El documento nacional de identidad electrónico distribuye su información en tres zonas dentro del chip. La zona pública contiene el certificado de la autoridad de certificación intermedia emisora, las claves de intercambio seguro y el certificado de componente. La zona privada guarda los certificados de firma y de autenticación, accesibles mediante dicha clave personal. La zona de seguridad solo puede leerla el titular en los puntos de actualización habilitados y almacena los datos de filiación, la imagen de la fotografía y la imagen de la firma manuscrita.

32 **A**

Ciberseguridad: Principios La vigilancia digital consiste en localizar y analizar de forma continuada información que pueda perjudicar a una organización. Su finalidad es detectar amenazas antes de que se materialicen y reducir el daño que podrían causar a su reputación. No se refiere necesariamente a robar secretos ni a vigilar instalaciones mediante cámaras conectadas.

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

33
A

Sistemas Informáticos Las auditorías forenses se orientan a investigar hechos que pueden constituir fraude u otras actuaciones deliberadas contrarias a las normas. Su finalidad es analizar indicios y evidencias para esclarecer lo sucedido. Por ello, este tipo de auditoría se distingue de las auditorías de gestión o de regularidad, centradas en otros objetivos.

34
D

Amenazas y Vulnerabilidades En MAGERIT, la tarea MAR.22 corresponde a la valoración de las amenazas. En ella se estima con qué frecuencia puede materializarse cada amenaza sobre cada activo y qué degradación provocaría en sus distintas dimensiones. La identificación de amenazas es una tarea diferente y no realiza esas estimaciones.

35
B

Ciberseguridad: Principios Un mapa de calor es una herramienta de representación visual empleada en el análisis cualitativo de riesgos. Su finalidad consiste en priorizar los riesgos identificados mediante una matriz que combina dos dimensiones fundamentales. La primera es la probabilidad de que la amenaza se materialice. La segunda es el impacto potencial que produciría sobre la organización. El cruce de ambos valores genera zonas de color que reflejan la severidad relativa de cada riesgo. Esta visualización facilita a los responsables la toma de decisiones sobre el tratamiento y la asignación de recursos.

36
C

Amenazas y Vulnerabilidades En CVSS versión 4.0, las puntuaciones base de 7,0 a 8,9 corresponden al nivel de gravedad alto. Una puntuación de 7,5 queda dentro de ese intervalo. La categoría crítica se reserva para puntuaciones superiores, a partir de 9,0.

37
B

Ciberseguridad: Principios MAGERIT 3.0 es una metodología para analizar y gestionar los riesgos que afectan a los sistemas de información. Ofrece un enfoque estructurado para identificar activos y amenazas, valorar riesgos y determinar medidas de tratamiento. No se limita al desarrollo de software ni a los ámbitos financiero o laboral.

38
A

Ciberseguridad: Principios El análisis de impacto determina las consecuencias que tendría la materialización de una amenaza sobre los activos o servicios. El análisis de riesgos es más amplio: combina ese impacto con la probabilidad de que ocurra el escenario de amenaza. Por eso, ambos análisis se relacionan, pero no miden exactamente lo mismo.

39
D

Amenazas y Vulnerabilidades Un ataque DDoS consiste en dirigir tráfico desde múltiples equipos hacia un servidor o servicio para sobrecargarlo y dificultar o impedir que responda a los usuarios legítimos. Los equipos pueden actuar de forma coordinada, a menudo sin que sus propietarios lo sepan. El carácter distribuido del ataque deriva precisamente de que procede de varios sistemas.

40
B

Ciberseguridad: Principios Un plan director de seguridad suele partir del análisis de la situación actual y de la estrategia de la organización, para después clasificar y priorizar las necesidades de seguridad. La situación presupuestaria puede influir en la planificación y en la viabilidad de las medidas. Sin embargo, no constituye por sí misma una fase habitual del plan.

41
B

Ciberseguridad: Principios La autenticación multifactor exige combinar credenciales de categorías distintas: algo que se sabe, algo que se posee y algo que se es. Combinar el escáner de iris con la huella dactilar une dos elementos que pertenecen a la misma categoría, los rasgos biométricos inherentes a la persona. Al no aportar factores de naturaleza diferente, no constituye una autenticación multifactor genuina. Las demás combinaciones sí mezclan factores de tipo distinto, como conocimiento con posesión, conocimiento con biometría o posesión con biometría, y por ello sí son válidas como esquemas de varios factores.

42
C

Ciberseguridad: Principios La definición del alcance delimita qué partes de la organización y qué actividades cubre el Sistema de Gestión de la Seguridad de la Información. Es un elemento de planificación del propio sistema, no una actuación que deba incluirse al implementar el plan de continuidad de negocio. La implementación de este plan sí requiere organizar a las personas, sus competencias y los procedimientos de actuación.

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

43
C

Ciberseguridad: Principios El riesgo expresa el grado de exposición a que una amenaza afecte a los activos y cause daños; puede estimarse considerando activos, amenazas y salvaguardas. La causa potencial de un incidente es la amenaza, no el riesgo. Por eso, atribuir esa definición al riesgo es incorrecto.

44
D

Ciberseguridad: Principios El uso de una base de datos en la nube no elimina los riesgos de seguridad ni hace que los datos sean inmunes a los ataques. Por ello, quienes utilizan el servicio deben aplicar medidas adicionales para proteger la información, como controlar los accesos y configurar adecuadamente la seguridad. La protección requiere atención tanto al servicio utilizado como a la gestión que hacen sus usuarios.

45
B

Cortafuegos y Redes Privadas Virtuales Una zona desmilitarizada constituye un segmento de red intermedio donde se ubican los servidores que ofrecen servicios accesibles desde el exterior. Se implementa mediante cortafuegos que separan tres áreas: la red externa, la propia zona intermedia y la red interna. Con esta segmentación, si un atacante compromete un servidor expuesto, permanece confinado en ese segmento y no accede directamente a los recursos internos protegidos. Una red privada virtual solo cifra conexiones remotas, un sistema de detección únicamente vigila sin aislar y asignar direcciones públicas a los terminales internos aumenta la exposición.

46
D

Amenazas y Vulnerabilidades El impacto acumulado expresa la pérdida de valor que se produce al considerar la degradación del activo y la de los activos que dependen de él. Así, refleja las consecuencias encadenadas de una amenaza sobre el conjunto de activos relacionado. No mide la probabilidad de que ocurra el daño ni la acumulación de riesgos a lo largo del tiempo.

47
A

Amenazas y Vulnerabilidades Un ataque zero-day explota una vulnerabilidad para la que todavía no se han publicado o aplicado parches correctores. Esto permite atacar sistemas antes de que puedan protegerse mediante la actualización correspondiente. El término alude al escaso margen de tiempo disponible para corregir la vulnerabilidad.

48
A

Gestión de Servicios TI e ITIL RTO (Recovery Time Objective) establece el tiempo máximo previsto para recuperar un servicio tras una interrupción. RPO (Recovery Point Objective) fija hasta qué momento deben poder recuperarse los datos, expresado como pérdida de información admisible. Ambos son objetivos fundamentales de los planes de contingencia y recuperación.

49
C

Ciberseguridad: Principios En MAGERIT, el riesgo acumulado considera el valor propio del activo y el de los activos que dependen de él. Así, refleja el impacto que podría alcanzar a través de esos activos dependientes. Se distingue del riesgo repercutido, que tiene en cuenta los activos de los que depende el activo analizado.

50
B

Ciberseguridad: Principios Un sistema con altos requisitos de seguridad debe verificar quién accede y qué acciones puede realizar cada usuario. La autenticación identifica al usuario y la autorización limita sus permisos. El cifrado protege la confidencialidad de los datos frente a accesos no autorizados.

51
C

Amenazas y Vulnerabilidades En la gestión de ciberincidentes se distinguen dos tipos de señales de alerta. Un precursor es un indicio que sugiere que un incidente de seguridad podría producirse en el futuro. Por el contrario, un indicador es una señal que revela que un incidente ya ha ocurrido o está ocurriendo en ese momento. Reconocer los precursores permite adoptar medidas preventivas antes de que la amenaza se materialice, reforzando la vigilancia y la protección de los sistemas afectados.

52
C

Mantenimiento y Soporte de Equipos El objetivo de punto de recuperación fija la cantidad máxima de datos que puede perderse tras un incidente. Un valor de diez minutos admite perder solo esa franja de información. El objetivo de tiempo de recuperación establece el plazo máximo para restaurar el servicio. Un valor de una hora obliga a dejar el sistema operativo dentro de 60 minutos. Ambos objetivos resultan independientes y complementarios en la planificación de continuidad. La interpretación válida combina pérdida limitada y restauración dentro del plazo señalado.

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

53
D

Delitos Informáticos El stalking consiste en perseguir o acosar de manera insistente y obsesiva a una persona, también mediante llamadas y mensajes digitales. Cuando ese hostigamiento se realiza por medios digitales, puede describirse asimismo como ciberacoso. Por eso, ambos términos encajan en la situación planteada.

54
C

Seguridad de Puestos y Endpoint Para impedir que la información pueda recuperarse después de desechar un soporte, se pueden emplear métodos de eliminación segura. Entre ellos están la desmagnetización, adecuada para los soportes magnéticos, y la destrucción física del dispositivo. El método debe ser eficaz para el tipo de soporte del que se trate.

55
A

Amenazas y Vulnerabilidades El spoofing consiste en falsificar o suplantar una identidad electrónica para que una comunicación o actividad parezca proceder de otra persona, dispositivo o sistema. Esta suplantación puede utilizarse para ocultar la identidad real y facilitar ataques o fraudes. No consiste en conectar hardware de forma incorrecta ni en desbloquear sitios web.

56
D

Seguridad de Puestos y Endpoint Una gestión unificada permite aplicar de forma coherente las políticas de seguridad y las actualizaciones en equipos con distintos sistemas operativos. Esto ayuda a mantener un nivel común de protección sin recurrir a restricciones idénticas que puedan perjudicar innecesariamente la productividad. En una organización heterogénea, coordinar la seguridad de todos los puestos es el reto de mayor alcance.

57
B

Esquema Nacional de Seguridad Un precursor es un indicio que apunta a que un incidente podría producirse en el futuro, pero no confirma que ya haya sucedido. Un indicador, en cambio, sugiere que el incidente puede haber ocurrido o estar ocurriendo en ese momento. La diferencia depende, por tanto, de si el indicio anticipa un posible incidente o apunta a uno actual o pasado.

58
C

Cortafuegos y Redes Privadas Virtuales Un sistema de gestión unificada de amenazas es una solución de seguridad que integra en un único dispositivo varias funciones de protección de red. Reúne prestaciones como cortafuegos, antivirus, prevención de intrusiones y filtrado de contenidos web dentro de una misma plataforma. Esta agrupación simplifica la administración y reduce costes frente a la implantación de equipos independientes para cada servicio. No constituye un protocolo ni opera en un nivel concreto de transporte. Aunque comparte objetivos con las soluciones de nueva generación, ambos conceptos no resultan equivalentes.

59
B

Ciberseguridad: Principios El control del flujo de datos limita cómo y quién puede acceder a la información, mientras que la auditoría permite revisar las actividades realizadas. La notarización aporta evidencias sobre operaciones o datos. En conjunto, estos mecanismos ayudan a impedir accesos no autorizados a información sensible.

60
D

Ciberseguridad: Principios El Plan de Seguridad de MAGERIT sí incorpora una planificación temporal de los proyectos, por lo que no se limita a enumerar tareas. El cronograma permite ordenar las actuaciones y fijar cuándo deben realizarse. Para establecer esa planificación se tienen en cuenta factores como la criticidad, el coste, los recursos disponibles y el presupuesto.

61
D

Ciberseguridad: Principios Los factores clásicos de autenticación se agrupan en algo que el usuario sabe, algo que tiene y algo que es. La contraseña, el código recibido en el móvil y la huella dactilar corresponden a esas tres categorías. La ubicación geográfica es un dato contextual que puede utilizarse para evaluar el riesgo, pero no es uno de los factores clásicos.

62
B

Gestión de Servicios TI e ITIL El BIA analiza las funciones del negocio y las consecuencias que tendría una interrupción sobre ellas. Este análisis ayuda a comprender qué actividades son críticas y qué efectos tendría su falta de disponibilidad. No es el plan de recuperación, sino un análisis que sirve de base para preparar la continuidad del negocio.

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

63
B

Ciberseguridad: Principios La afirmación es incorrecta porque los incidentes de ingeniería social sí se contemplan en la gestión de ciberincidentes. Aunque puedan dirigirse inicialmente a personas, pueden comprometer la seguridad de la organización y deben poder notificarse y clasificarse. Por tanto, no se excluyen de la taxonomía por no afectar directamente a sistemas TIC.

64
D

Amenazas y Vulnerabilidades OSINT consiste en recopilar y analizar información de fuentes abiertas, y existen herramientas específicas para realizar esas tareas. «KALNIX» no es un sistema operativo diseñado específicamente para OSINT. Kali Linux, cuyo nombre puede confundirse con el indicado, es una distribución orientada a pruebas de seguridad y auditoría, aunque incluya herramientas aprovechables para OSINT.

65
B

Malware y Protección Antivirus Un virus de sobreescritura infecta un archivo sustituyendo parte o todo su contenido. Al conservar el tamaño del archivo, puede ocultar una señal que ayudaría a advertir la infección. Esta característica lo distingue de otros tipos de virus.

66
D

Ciberseguridad: Principios En MAGERIT, el riesgo expresa el grado de exposición a que una amenaza se materialice sobre uno o varios activos y cause daños o perjuicios a la organización. No es la causa potencial del incidente —la amenaza— ni el daño que se produce cuando esta se materializa. Por eso se formula como una estimación de esa exposición.

67
B

Ciberseguridad: Principios La autenticación fuerte requiere combinar al menos dos factores independientes de naturaleza distinta, como algo que se conoce y algo que se posee. Un sistema que exige usuario y contraseña junto con un token digital reúne el factor de conocimiento y el factor de posesión, cumpliendo así el requisito de multifactor. Los mecanismos que emplean únicamente usuario y contraseña, solo un código numérico o exclusivamente un rasgo biométrico se apoyan en un único factor y no alcanzan la consideración de autenticación reforzada.

68
D

Malware y Protección Antivirus Mirai suele aprovechar dispositivos IoT mal protegidos, especialmente cuando conservan credenciales conocidas o exponen servicios vulnerables. Cambiar las credenciales predeterminadas dificulta el acceso no autorizado, y deshabilitar servicios innecesarios reduce la superficie de ataque. La segmentación de la red limita la propagación del malware y el impacto de una infección.

69
C

Esquema Nacional de Seguridad El conjunto de procedimientos operativos de seguridad debe documentar y cubrir, como referencia mínima, el 80% de las actividades rutinarias de la organización. También ha de recoger las tareas de ejecución poco frecuente que exigen seguir pasos muy precisos por su relevancia para la seguridad. Este umbral orienta la medida organizativa correspondiente en la guía de implantación del Esquema Nacional de Seguridad. Su finalidad es garantizar que la operación diaria quede reflejada en instrucciones claras, aplicables y verificables. El resto de porcentajes propuestos no responde a esa referencia.

70
A

Hardware: Unidad Central y CPU UEFI puede incorporar Secure Boot o arranque seguro, que comprueba la autenticidad de los componentes de software que se ejecutan durante el inicio. Así, dificulta que se carguen programas de arranque no autorizados, como ciertos tipos de malware. No es, por sí mismo, un antivirus ni un cortafuegos.

71
C

Ciberseguridad: Principios La gestión de información y eventos de seguridad combina dos funciones complementarias en una única plataforma. Por un lado, recopila, almacena y analiza los datos de seguridad procedentes de múltiples fuentes de la organización. Por otro, correla y gestiona en tiempo real los eventos generados por los distintos dispositivos y aplicaciones de la red. Un sistema de detección de intrusiones solo alerta, sin bloquear por sí mismo el tráfico. Un sistema de prevención de intrusiones sí interviene activamente frente a las amenazas. La opción restante describe un sistema inexistente en la práctica profesional.

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

72
C

Ciberseguridad: Principios Las preguntas de seguridad y la fecha de nacimiento suelen ser datos personales previsibles o fáciles de averiguar, por lo que no constituyen factores robustos. Aunque se añadan a una contraseña, no aportan una segunda comprobación suficientemente independiente y resistente. La autenticación multifactor debe combinar factores distintos y difíciles de suplantar.

73
B

Amenazas y Vulnerabilidades La suplantación de identidad busca hacerse pasar por otra entidad, usuario o dirección para engañar a los sistemas o a las personas. El secuestro de sesión, la falsificación de direcciones de red y el fraude por correo electrónico persiguen suplantar identidades legítimas. En cambio, existe un ataque que satura una red mediante el envío masivo de peticiones amplificadas con respuesta hacia la víctima, provocando denegación de servicio. Este último no pretende hacerse pasar por nadie, sino agotar los recursos disponibles del objetivo.

74
B

Ciberseguridad: Principios La amenaza degrada el activo en un 90 %, por lo que el impacto inicial es de 900.000 €. Las salvaguardas reducen ese impacto en un 90 %, es decir, en 810.000 €. El impacto residual que permanece tras aplicar las salvaguardas es, por tanto, de 90.000 €; para calcular el riesgo haría falta conocer también la probabilidad de que se materialice la amenaza.

75
C

Ciberseguridad: Principios En una investigación forense se analiza una copia bit a bit para evitar modificar el disco original. El clonado conserva también los datos que no son visibles mediante una copia ordinaria de archivos. Así se preserva la evidencia y se puede trabajar sobre una réplica.

76
C

Amenazas y Vulnerabilidades Una vulnerabilidad de día cero es un fallo de seguridad que el proveedor todavía desconoce y para el que, por tanto, no hay un parche disponible. Puede ser aprovechada antes de que exista una solución que permita corregirla. El nombre alude a que el proveedor no ha dispuesto de tiempo para desarrollar y distribuir una corrección.

77
B

Ciberseguridad: Principios El impacto repercutido sobre A se calcula aplicando a su valor la dependencia respecto de B y la degradación sufrida por B. Así, 500.000 × 0,30 × 0,90 = 135.000. El valor propio de B no interviene en este cálculo, porque se parte del valor del activo A afectado.

78
B

Ciberseguridad: Principios La ISO/IEC 27001 establece los requisitos para implantar y mantener un sistema de gestión de la seguridad de la información. Es una norma certificable, de modo que una organización puede acreditar que su sistema cumple esos requisitos. La ISO/IEC 27002, en cambio, proporciona directrices y controles de seguridad, pero no es la norma certificable de requisitos.

79
A

Amenazas y Vulnerabilidades En MAGERIT, el impacto expresa el daño que sufre un activo cuando se materializa una amenaza. Permite valorar las consecuencias de esa materialización sobre el activo. No debe confundirse con la vulnerabilidad, que es una debilidad que puede facilitar el éxito de una amenaza.

80
C

Amenazas y Vulnerabilidades El pharming consiste en desviar a la víctima desde una dirección web legítima hacia una página fraudulenta. Para hacerlo, se altera la resolución DNS o el archivo hosts del equipo, de modo que el nombre de dominio conduce a una dirección distinta. Así, la víctima puede llegar al sitio falso sin advertir inicialmente la redirección.

81
A

Amenazas y Vulnerabilidades El pharming consiste en manipular el proceso de resolución de nombres de dominio para desviar al usuario hacia sitios web fraudulentos. La manipulación puede afectar al fichero hosts local o a la caché del servicio de nombres. El efecto es que, aunque la persona escriba correctamente la dirección en el navegador, acaba en una página falsa diseñada para capturar credenciales. Se diferencia del envío masivo de correos, que corresponde al phishing, del registro de pulsaciones propio de un keylogger, y de la suplantación telefónica característica del vishing.

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

82
C

Amenazas y Vulnerabilidades La denegación de servicio busca impedir que los usuarios legítimos accedan a un sistema o servicio, agotando sus recursos o saturando sus comunicaciones. Se considera un ataque combinado cuando se emplean conjuntamente distintas técnicas o fuentes para provocar esa interrupción. En la modalidad distribuida, el tráfico procede de varios equipos coordinados, lo que refuerza el ataque.

83
B

Malware y Protección Antivirus Un bootkit modifica componentes del arranque para ejecutarse antes de que se cargue el sistema operativo. Al intervenir en el MBR, puede iniciar su código durante las primeras fases del arranque y mantener así la persistencia. Por eso, un malware que modifica el MBR encaja con este tipo.

84
C

Amenazas y Vulnerabilidades Right to Left Override (RLO) es un carácter Unicode de control que altera la dirección visual de parte del texto. En un nombre de archivo puede hacer que la extensión se muestre en un orden engañoso y parezca distinta de la real. Así, el archivo puede aparentar ser de un tipo inofensivo cuando su extensión verdadera indica otro tipo.

85
B

Amenazas y Vulnerabilidades La ingeniería social consiste en manipular a una persona para que revele información o facilite una acción que favorezca al atacante. Hacerse pasar por el servicio de soporte técnico para conseguir acceso remoto es un ejemplo de suplantación y engaño. Los otros escenarios describen actividades legítimas o problemas técnicos, no una manipulación de la víctima.

86
B

Ciberseguridad: Principios La norma internacional de gestión de la privacidad amplía el marco de gestión de la seguridad de la información para incorporar el tratamiento de datos personales. Permite implantar un sistema de gestión de información de privacidad y obtener certificación sobre determinadas prácticas protectoras. Funciona como extensión del estándar general de seguridad y de su código de buenas prácticas, con el que resulta plenamente compatible. No constituye un protocolo de nivel de transporte ni establece por sí sola el sistema de seguridad de la información.

87
D

Internet: Navegación y Servicios El navegador de la estación de trabajo debe utilizarse para actividades relacionadas directamente con las funciones y tareas encomendadas. Además, el uso indicado requiere la autorización del órgano competente. La navegación por motivos particulares o para descargar contenidos ajenos al trabajo no queda comprendida en ese uso autorizado.

88
B

Amenazas y Vulnerabilidades Las salvaguardas minimizadoras reducen el impacto de una amenaza si llega a materializarse, pero no actúan sobre la probabilidad de que ocurra. Las medidas disuasorias, eliminatorias y preventivas sí pueden evitar o reducir esa probabilidad. Por eso, la minimización no pertenece al grupo señalado en la pregunta.

89
C

Sistemas Informáticos La planificación de la recuperación comienza por identificar qué activos son críticos y qué consecuencias tendría que dejaran de estar disponibles. Ese análisis permite establecer prioridades y orientar las medidas de recuperación. Sin conocer el impacto de una interrupción, no se pueden definir adecuadamente las soluciones ni los procedimientos.

90
D

Ciberseguridad: Principios La eficacia expresa en qué medida un control consigue los objetivos de seguridad para los que fue diseñado. Se refiere, por tanto, a su capacidad para producir el resultado previsto, no solo a los recursos empleados ni a su finalidad. Por eso, la denominación correcta es eficacia del control.

91
D

Gestión de Servicios TI e ITIL El RTO (Recovery Time Objective) establece el tiempo objetivo para restablecer un proceso o servicio tras una interrupción. Por eso se relaciona con cuánto puede permanecer detenido antes de recuperarse. El RPO, en cambio, se refiere al punto temporal hasta el que deben recuperarse los datos.

92
A

Seguridad de Puestos y Endpoint MAM significa gestión de aplicaciones móviles y permite administrar las aplicaciones instaladas en los dispositivos de una organización. Se distingue de MDM, que se ocupa de la gestión de los propios dispositivos. Por eso, la afirmación sobre MAM describe correctamente una función de las soluciones EMM.

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

93
D

Cortafuegos y Redes Privadas Virtuales Las listas de control de acceso estándar filtran únicamente en función de la dirección de origen, por lo que su ubicación recomendada es lo más cerca posible del destino para no bloquear tráfico legítimo. En cambio, las listas extendidas pueden filtrar por origen, destino, protocolo y puerto, de modo que conviene situarlas cerca del origen para descartar cuanto antes el tráfico no deseado y ahorrar ancho de banda. Por ello, la afirmación que sitúa las estándar próximas al destino refleja correctamente la práctica recomendada.

94
A

Ciberseguridad: Principios Al contratar servicios en la nube, conviene comprobar que el proveedor dispone de un plan de continuidad de negocio y de evidencias de que puede mantener o recuperar el servicio ante interrupciones. Los acuerdos de nivel de servicio deben atender a las obligaciones y necesidades de ambas partes. Además, una menor abstracción suele implicar más control del cliente sobre la infraestructura, no menos.

95
B

Malware y Protección Antivirus El análisis heurístico busca indicios de malware a partir de características o comportamientos sospechosos. A diferencia de la detección basada en firmas, no necesita que la amenaza esté previamente identificada en una base de datos. Por eso puede ayudar a detectar amenazas desconocidas o variantes nuevas.

96
A

Ciberseguridad: Principios La autenticación multifactor aporta garantías adicionales sobre la identidad de quien solicita el acceso. El túnel cifrado protege la confidencialidad de las comunicaciones, mientras que la comprobación del dispositivo permite verificar su integridad. En conjunto, estas medidas ayudan a determinar si la conexión reúne condiciones de seguridad antes de acceder a recursos sensibles.

97
D

Ciberseguridad: Principios La segmentación de datos permite separar la información en partes o entornos diferenciados y limitar el acceso entre ellos. Esto puede reducir la exposición de los datos y contener el impacto de un acceso no autorizado. En la nube, la seguridad no recae exclusivamente en el proveedor: las responsabilidades se distribuyen según el servicio y su configuración.

98
D

Criptografía Básica La versión 1.3 del protocolo de seguridad en la capa de transporte optimiza el establecimiento de conexión reduciéndolo a un único intercambio de ida y vuelta. Esta mejora disminuye la latencia frente a la versión anterior, que requería dos intercambios. Además, incorpora la reanudación con cero intercambios en sesiones ya conocidas. No suprime los certificados digitales ni exige que ambos extremos compartan subred física. Tampoco añade pasos de verificación adicionales, sino que simplifica el proceso conservando y reforzando la seguridad criptográfica.

99
C

Ciberseguridad: Principios Bell-LaPadula es un modelo de control de acceso diseñado para proteger la confidencialidad de la información. Organiza los datos y los usuarios según niveles de seguridad y limita las operaciones para evitar que información clasificada llegue a usuarios no autorizados. Su objetivo principal no es proteger la integridad ni la disponibilidad.

100
B

Malware y Protección Antivirus Sylink es el componente de Symantec Endpoint Protection que contiene la información de comunicación y configuración del cliente. Al ejecutarlo, el equipo cliente recibe la referencia del servidor de gestión al que debe conectarse. Por tanto, sirve para indicar a qué servidor tienen que apuntar los equipos para su gestión.

MUESTRA GRATIS · Libro completo, 473 preguntas **34,90 €** **Cómpralo aquí ›**

El libro completo

Esta muestra trae el test del tema 51, con sus soluciones. El libro completo sigue, tema a tema, el **programa oficial de la convocatoria de Técnico/a medio/a de informática del Ayuntamiento de Olot** (solo «Bloc 6. Ciberseguretat i identitat digital»: 5 de los 60 temas del programa) y trae:

- **473** preguntas con su solución explicada
- **467** reales de examen
- **5** temas con su test
- **180** páginas en PDF

Además de las 467 reales, 6 preguntas de refuerzo en 1 tema sin preguntas de examen suficientes, marcadas una a una.

Parte	Qué es
Prueba tu nivel	3 preguntas, con su hoja de respuestas, sus soluciones y «Tu resultado»: por dónde empezar a estudiar.
Parte 1 · 5 tests por tema	Uno por cada tema que trae del programa oficial de la convocatoria, de 20 a 100 preguntas: 370 preguntas con sus soluciones explicadas y su casilla de aciertos.
Parte 2 · 2 simulacros	100 preguntas reales con un formato habitual en convocatorias de este tipo; cada uno con su hoja de respuestas y sus soluciones.
Anexo de vigencia	Las normas del libro y de dónde se ha tomado su texto.

Consigue el libro completo

Escanea el código o pulsa la dirección: te lleva a la página del libro en oposicionesexpress.com, donde lo compras y lo descargas al momento en PDF. Pago único.

oposicionesexpress.com/Test-Tecnico-a-medio-a-de-informatica-Ayuntamiento-de-Olot-A2.html