

Ciberseguridad

Ámbito 2 · EPSO/AD/430/26 · grado AD 8

254

aprobados buscados

AD 8

grado de entrada

30 / 40 min

examen del ámbito

13 oct 2026

cierre de solicitudes

eu-now.com

Dossier de preparación · 19 bloques de estudio con sus fuentes oficiales

Elaborado sobre la convocatoria DO C/2026/4668 y los textos oficiales que cubren su Anexo II

[EU-now.com](https://eu-now.com)

1 · La oposición de un vistazo

EPSO/AD/430/26 es una oposición general por titulación y pruebas para **administradores de grado AD 8** de las instituciones, órganos y organismos de la Unión. Dos ámbitos, **solo se puede elegir uno**: inteligencia artificial (240 aprobados buscados) y ciberseguridad (254). Tú vas a ciberseguridad: 254 plazas en la lista de reserva.



Lo que decide todo: los tres tests de razonamiento y la redacción EUFTE son puertas de sí o no. **Solo la nota del MCQ del ámbito ordena a los candidatos**, y solo a los mejores se les corrige la EUFTE y se les comprueba la titulación. Dos tercios del tiempo de estudio, al ámbito.



Las cinco fases. Solo la puntuación del MCQ del ámbito ordena a los candidatos; el resto son puertas de sí o no.

2 · Las cinco pruebas

Prueba	Lengua	Preguntas	Duración	Puntos	Corte
Razonamiento verbal	1	20	35 min	0-20	10/20
Razonamiento numérico	1	10	20 min	0-10	10/20 junto con el abstracto
Razonamiento abstracto	1	10	10 min	0-10	10/20 junto con el numérico
MCQ del ámbito	2	30	40 min	0-30	15/30 y estar entre los mejores
EUFTE	2	—	40 min	0-10	5/10

Lengua 1 es cualquiera de las 24 oficiales. **Lengua 2** es la del MCQ del ámbito y la EUFTE. Hace falta C1 en una y B2 en la otra, y se eligen en el formulario. Las pruebas son a distancia con vigilancia remota, y el orden de convocatoria puede no ser el de la convocatoria.

La EUFTE no es un examen de idioma ni de conocimientos: EPSO publica documentación sobre asuntos de la Unión antes del examen, la misma que se entrega durante la prueba, y se responde a una consigna basada en ella. Se corrige con criterios publicados.

La plataforma del examen

Las pruebas se hacen en TAO, la plataforma que EPSO usa en todos sus exámenes. Conviene llegar sabiendo dónde está cada cosa: se pierde menos tiempo y no hay sorpresas el día de la prueba.

EU Careers - Sample Test / Part I / Verbal Reasoning
Pregunta 42x

Clock

All cells in the body have a specific structure and perform a specialised function, apart from stem cells. Stem cells have a number of remarkable properties. Unlike most specialised cells they are capable of replicating themselves many times. They can also develop into different types of specialised cells, such as muscle cells or red blood cells. These properties, in theory, mean that stem cells could repair the body, by multiplying and then replacing badly damaged tissue. It is believed that, in time, stem cell research could revolutionise medicine, as stem cells could be used to repair tissues or even to grow replacement organs.

Which of the following statements is correct?

☐ A. The only difference between stem cells and other cells is that stem cells do not perform a specialised function.

☐ B. A muscle cell that originated from a stem cell may transform back into a stem cell.

☐ C. Stem cells are the only cells that have the ability to repair themselves.

☐ D. Stem cells could repair damaged tissues by multiplying and then replacing damaged cells.

1. Elimination tool
2. Calculator
3. Scratchpad

Answered Answered and bookmarked Bookmarked

Back 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 OVERVIEW (16) Next

Bookmark tool

Pantalla de pregunta: navegador de preguntas abajo, marcador, reloj y herramientas arriba.

Verbal Reasoning

Test Configuration

Set

1013x2
2026

AC ± % ÷

Descartar opciones: tacha lo que ya has eliminado.

Resaltador y lector de líneas para enunciados largos.

Calculadora y bloc de notas donde la prueba los permite.

Capturas de la plataforma TAO utilizada en las pruebas de EPSO.

La lista de reserva se publica en orden alfabético, no por nota; los empates en la última plaza entran todos; y figurar en ella no garantiza contratación.

Fuentes: convocatoria DO C/2026/4668, secciones 1, 4.2, 4.3.1, 4.3.2 (tablas 3 a 5), 4.3.3 y 4.3.4.

3 · Cómo son las 30 preguntas

La convocatoria no publica temario ni bibliografía. El contrato es el **Anexo II, «funciones típicas»**: de ahí sale todo lo preguntable, y por eso este dossier lo desglosa entero. Son 30 preguntas en 40 minutos, en lengua 2: **80 segundos por pregunta**. No hay tiempo de deducir desde cero, se contesta con lo que se reconoce.

Enunciado con un caso de trabajo

Una autoridad nacional detecta un incidente significativo en una entidad esencial...

- ☐ A · Notificar en 72 horas al CSIRT
- ☒ B · Alerta temprana en 24 horas al CSIRT
- ☐ C · Informe final en un mes a la Comisión
- ☐ D · Notificar al Grupo de Cooperación

Lo que decide la respuesta

- 1** QUIÉN es competente
CSIRT, autoridad, Comisión...
- 2** QUÉ obligación exacta
alerta, notificación, informe
- 3** EL NÚMERO
24 h · 72 h · un mes

Los distractores atacan uno de los tres: el plazo de al lado, el órgano vecino, la obligación de otra fase.

Anatomía de una pregunta del ámbito: 80 segundos para reconocer tres datos.

Las cinco trampas del formato

- **La opción más larga.** En los exámenes oficiales la correcta es la más larga solo unas 4 de cada 10 veces: elegir por longitud no aprueba.
- **El absoluto.** «Siempre», «nunca», «en todos los casos» suelen marcar la opción falsa: el Derecho de la Unión vive de excepciones.
- **El actor cambiado.** La obligación está bien descrita pero colgada de otro organismo. Lee el sujeto antes que el verbo.
- **El instrumento vecino.** La afirmación es cierta, pero de otra norma que no aplica a ese caso.
- **El derecho superado.** Redacciones anteriores a una modificación. Estudia siempre texto consolidado.

La ficha que sí sirve

A quién se aplica	Qué obliga	Plazos y cifras	Quién vigila
entidades · productos	la conducta exacta	24 h · 72 h · umbral	y quién sanciona

La ficha por instrumento: cuatro columnas y nada más. Es lo que se contesta en 80 segundos.

4 · El temario, bloque a bloque

El Anexo II describe funciones, no materias. Aquí están traducidas a bloques de estudio: qué entra, qué se confunde y dónde está escrito. Lo que no aparece en un texto oficial no se pregunta.



El ámbito 2 va de decisiones: qué control, qué plazo y quién responde cuando algo pasa.

1 · Gestión de riesgos y aseguramiento

Marcos de riesgo (RMF, CSF 2.0)

Controles y monitorización

Vulnerabilidades y pruebas

Certificación europea

2 · Arquitectura, diseño y tecnología

Confianza cero, nube y virtualización

Identidad y accesos

Criptografía y poscuántica

Desarrollo seguro y DevSecOps

Tecnologías emergentes

3 · Operaciones y respuesta a incidentes

Operaciones y detección

Respuesta e informática forense

Continuidad y saneamiento

4 · Gobernanza, política y coordinación

Instituciones de la UE (2023/2841)

NIS2 y ejecución

Cyber Resilience Act

Cyber Solidarity Act

DORA

Política y derecho penal

5 · Concienciación, capacidades y asesoría

Formación y perfiles ECSF

El Anexo II traducido a bloques de estudio.

1 Ciberseguridad de las instituciones de la UE — Reglamento 2023/2841

El marco de la casa donde vas a trabajar. Cae con frecuencia porque es el único régimen que se aplica a las entidades de la Unión, y se confunde sistemáticamente con NIS2.

Qué entra

- Marco del artículo 6: aprobado bajo el nivel más alto de dirección antes del 8 de abril de 2025, con alcance sobre local, nube, tecnología operativa y móvil, y revisión al menos cada cuatro años.
- Evaluación de madurez del artículo 7: antes del 8 de julio de 2025 y al menos cada dos años.
- Medidas del artículo 8 y plan de ciberseguridad del artículo 9, revisado cada dos años.
- Responsable local de ciberseguridad: funciones y a quién reporta.
- Notificación a CERT-EU del artículo 21: alerta temprana en 24 horas, notificación en 72 horas, informe final en un mes.
- IICB (artículos 10 a 12): decide, emite directrices y puede dirigir recomendaciones; CERT-EU (artículo 13): presta servicios.

Lo que más se confunde

- CERT-EU no supervisa ni sanciona ni es el CSIRT nacional de nadie: asiste a las entidades de la Unión.
- Las entidades de la Unión NO están bajo NIS2; si el enunciado habla de una institución europea, la norma es la 2023/2841.

- Información clasificada: la Decisión 2015/444 es un régimen aparte, con sus marcados, zonas y registros.

Fuentes: Reglamento (UE, Euratom) 2023/2841, artículos 6 a 13 y 21 · Decisión (UE, Euratom) 2015/444

2 NIS2 y el Reglamento de Ejecución 2024/2690

La norma de referencia del sector y la mayor fuente de preguntas de plazos y umbrales.

Qué entra

- Las diez áreas de medidas del artículo 21(2): análisis de riesgos, gestión de incidentes, continuidad, seguridad de la cadena de suministro, adquisición y desarrollo, evaluación de eficacia, higiene y formación, criptografía, seguridad del personal y control de accesos, autenticación multifactor.
- Entidades cubiertas por el Reglamento de Ejecución: DNS, registros de dominios de primer nivel, nube, centros de datos, redes de distribución de contenidos, proveedores de servicios gestionados y de seguridad gestionados, mercados en línea, buscadores, redes sociales y prestadores de servicios de confianza.
- Criterios de significatividad del artículo 3: pérdida directa superior a 500.000 euros o al 5 % del volumen de negocio (lo que sea menor), exfiltración de secretos comerciales, muerte o daño grave a la salud, acceso no autorizado.
- Escalonado del artículo 23: alerta temprana en 24 horas, notificación de incidente en 72 horas, informe final en un mes.
- Responsabilidad del órgano de dirección (artículo 20) y formación obligatoria.
- Umbrales por servicio de los artículos 5 a 14 del Reglamento de Ejecución y las trece secciones de su anexo.

Lo que más se confunde

- ENISA no supervisa entidades: supervisan las autoridades nacionales competentes.
- Las medidas del artículo 21 no son las medidas de seguridad del RGPD, aunque se parezcan.
- Entidad esencial e importante se diferencian sobre todo en el régimen de supervisión y sanción, no en las medidas.

Fuentes: Directiva (UE) 2022/2555, artículos 20, 21 y 23 · Reglamento de Ejecución (UE) 2024/2690 · Guía técnica de ENISA 2025

3 Cyber Resilience Act — Reglamento 2024/2847

Productos con elementos digitales. Preguntas de clasificación, de plazos y de quién responde en la cadena.

Qué entra

- Clasificación: producto por defecto, importante de clase I o II (artículo 7 y anexo III) y crítico (artículo 8 y anexo IV).
- Rutas de evaluación de la conformidad del artículo 32 según la clase.
- Deberes del fabricante: gestión de vulnerabilidades y periodo de soporte del artículo 13, al menos cinco años salvo vida útil menor.
- Notificación del artículo 14: vulnerabilidad explotada activamente e incidente grave, con alerta temprana en 24 horas, notificación en 72 horas e informe final en 14 días, por la plataforma única del artículo 16.
- Figura del administrador de código abierto (artículo 24).
- Fechas: aplicación general el 11 de diciembre de 2027, obligaciones de notificación desde el 11 de septiembre de 2026, organismos notificados desde el 11 de junio de 2026.

Lo que más se confunde

- El informe final del CRA es a los 14 días; el de NIS2, al mes. Es el intercambio de plazos más habitual.
- La plataforma única de notificación se crea en el artículo 16, pero la obligación de notificar está en el 14.
- Un servicio interno de una institución no es un producto puesto en el mercado.

Fuentes: Reglamento (UE) 2024/2847, artículos 7, 8, 13, 14, 16, 24 y 32; anexos I, III y IV

4 Cyber Solidarity Act y plan director de gestión de crisis

Respuesta europea a incidentes a gran escala: tres piezas y tres niveles.

Qué entra

- Sistema europeo de alerta de ciberseguridad con centros nacionales y transfronterizos (artículos 3 a 9).
- Mecanismo de emergencia: preparación coordinada, reserva de ciberseguridad de la UE y asistencia mutua (artículos 10 a 19).
- Mecanismo europeo de revisión de incidentes, que ejecuta ENISA a petición de la Comisión o de EU-CyCLONe (artículo 21).
- Quién puede pedir el despliegue de la reserva: Estados miembros, instituciones y órganos de la Unión y terceros países asociados al programa Europa Digital.
- Niveles del plan director (Recomendación 2025/3445): técnico en la red de CSIRT, operativo en EU-CyCLONe, político con la activación del IPCR por la Presidencia del Consejo.

Lo que más se confunde

- El nivel político no dirige la respuesta técnica: el IPCR coordina decisiones, no contiene incidentes.
- EU-CyCLONe es operativo, no político, y no sustituye a la red de CSIRT.

Fuentes: Reglamento (UE) 2025/38 · Recomendación (UE) 2025/3445

5 Certificación europea — Ley de Ciberseguridad y esquema EUCC

Marco de certificación: niveles, voluntariedad y reparto de papeles.

Qué entra

- Niveles de garantía del artículo 52: básico, sustancial y alto, con el tipo de evaluación que exige cada uno.
- Voluntariedad del artículo 56, salvo que el Derecho de la Unión o nacional disponga otra cosa.
- Papeles: ENISA prepara esquemas candidatos (artículo 49), los organismos de evaluación certifican (artículo 60), las autoridades nacionales supervisan (artículo 58) y el ECCG asesora (artículo 62).
- Esquema EUCC (Reglamento de Ejecución 2024/482): Common Criteria y CEM, sustancial equivale a AVA_VAN 1-2 y alto a AVA_VAN 3-5, sin autoevaluación, certificados de hasta cinco años.
- Obligaciones del titular del certificado en gestión de vulnerabilidades y supuestos de retirada.

Lo que más se confunde

- ENISA no emite certificados: prepara los esquemas.
- La certificación no es obligatoria por defecto; decirlo es un distractor clásico.
- En EUCC no hay autoevaluación, a diferencia de otros esquemas de nivel básico.

Fuentes: Reglamento (UE) 2019/881, artículos 49, 52, 56, 58, 60 y 62 · Reglamento de Ejecución (UE) 2024/482

6 DORA y el sector financiero

Aparece como marco sectorial: conviene el mapa y la frontera con NIS2, no el detalle fino.

Qué entra

- Los cinco pilares: gestión del riesgo TIC (capítulo II), gestión y notificación de incidentes (III), pruebas de resiliencia operativa digital incluidas las dirigidas por amenazas (IV), riesgo de terceros con supervisores principales para los proveedores críticos (V) y compartición de información (VI).
- Responsabilidad del órgano de dirección del artículo 5.
- El Reglamento Delegado 2024/1774 detalla el marco de gestión del riesgo TIC.
- Relación con NIS2: DORA es *lex specialis* para las entidades financieras.

Lo que más se confunde

- Las autoridades europeas de supervisión no supervisan directamente a un banco: lo hacen las autoridades nacionales competentes.
- La notificación de incidente grave de DORA no es la notificación de NIS2, ni comparte plazos.

Fuentes: Reglamento (UE) 2022/2554, artículos 5 y capítulos II a VI · Reglamento Delegado (UE) 2024/1774

7 Política y derecho penal de la UE

Preguntas de atribución: qué dice cada instrumento y de quién es la competencia.

Qué entra

- Estrategia de Ciberseguridad de 2020: resiliencia y soberanía tecnológica, capacidad operativa para prevenir, disuadir y responder, y un ciberespacio global y abierto.
- Régimen de sanciones del Reglamento 2019/796: ciberataques con efecto significativo, inclusión en lista por el Consejo, congelación ejecutada por los Estados miembros.
- Directiva 2013/40: acceso ilegal, interferencia en sistemas y datos, interceptación, herramientas; agravantes como redes de bots o infraestructura crítica; puntos de contacto disponibles 24 horas.
- Academia de Capacidades de Ciberseguridad (COM(2023) 207) y sus cuatro pilares.

Lo que más se confunde

- Las sanciones las decide el Consejo; el derecho penal lo aplican los Estados miembros. No se mezclan.
- La Academia no es un organismo con potestades: es una iniciativa política.

Fuentes: JOIN(2020) 18 · Reglamento (UE) 2019/796 · Directiva 2013/40/UE · COM(2023) 207

8 Marcos de gestión de riesgos — RMF, SP 800-30 y CSF 2.0

La columna vertebral técnica. Se pregunta el orden de los pasos y la salida de cada uno.

Qué entra

- Los siete pasos del RMF (SP 800-37r2): preparar, categorizar, seleccionar, implantar, evaluar, autorizar y monitorizar, con el producto de cada paso.
- Evaluación de riesgos de SP 800-30r1: fuentes de amenaza, eventos, vulnerabilidades y condiciones predisponentes, probabilidad e impacto; proceso preparar, conducir, comunicar y mantener; los tres niveles de la organización.
- CSF 2.0 (CSWP 29): seis funciones con Govern incorporada, categorías y subcategorías, perfiles actual y objetivo, y niveles 1 a 4.
- Modelos de madurez: para qué sirven y en qué se diferencian de una evaluación de riesgos.

Lo que más se confunde

- Las funciones del CSF no son los pasos del RMF, ni las cláusulas de ISO 27001.
- Los niveles del CSF describen rigor de gobernanza, no una nota de seguridad.

Fuentes: NIST SP 800-37r2 · NIST SP 800-30r1 · NIST CSWP 29

9 Controles, evaluación y monitorización continua

Lo que el Anexo II llama operaciones de evaluación y métricas.

Qué entra

- Familias de SP 800-53r5 y diferencia entre control base y mejora del control.
- Las líneas base y la guía de adaptación se trasladaron a SP 800-53B; en r5 quedan los conceptos: alcance, controles compensatorios y parámetros definidos por la organización.
- Procedimientos de SP 800-53A: examinar, entrevistar y probar, y qué evidencia produce cada método.
- Monitorización continua (SP 800-137): definir estrategia, establecer, implantar, analizar e informar, responder, revisar y actualizar; tres niveles; qué marca la frecuencia.
- Medición (SP 800-55): medidas de implantación, de eficacia y de impacto.

Lo que más se confunde

- Una auditoría anual no es monitorización continua.
- Una métrica que no dispara una decisión no es una métrica de seguridad, es un número.

Fuentes: NIST SP 800-53r5 · SP 800-53A r5 · SP 800-137 · SP 800-55

10 Gestión de vulnerabilidades y pruebas de seguridad

Distinguir técnicas por objetivo, alcance y evidencia, y saber qué norma las exige.

Qué entra

- Escaneo, prueba de penetración y equipo rojo: qué busca cada uno y qué entrega.
- Fases de SP 800-115: planificación, descubrimiento, ataque e informe; técnicas de revisión, de identificación y análisis del objetivo y de validación de vulnerabilidades.
- Gestión de parches empresarial (SP 800-40r4): respuestas al riesgo aceptar, mitigar, transferir o evitar; grupos de mantenimiento; ciclo de vida del parche.
- OWASP ASVS 5.0 por niveles y las categorías de prueba de la guía WSTG 4.2.
- El disparador legal: anexos 6.5 y 6.10 del Reglamento de Ejecución 2024/2690.

Lo que más se confunde

- Un escaneo no es una prueba de penetración: cambia el objetivo y la evidencia.
- El anexo del Reglamento de Ejecución hace las pruebas basadas en riesgo, no obligatorias sin más.

Fuentes: NIST SP 800-115 · SP 800-40r4 · OWASP ASVS 5.0 y WSTG 4.2 · RE (UE) 2024/2690

11 Arquitectura de seguridad — confianza cero, nube y virtualización

Conceptos de arquitectura con vocabulario muy concreto.

Qué entra

- Principios y componentes lógicos de SP 800-207: el motor de políticas decide, el administrador de políticas establece y el punto de aplicación ejecuta.
- Fuentes que alimentan el algoritmo de confianza: diagnóstico continuo, cumplimiento sectorial, inteligencia de amenazas, registros de actividad y SIEM.
- Enfoques: gobernanza reforzada de la identidad, microsegmentación y perímetro definido por software; variantes de despliegue: agente y pasarela, pasarela de enclave, portal de recursos y aislamiento de aplicaciones.
- Amenazas específicas a una arquitectura de confianza cero (sección 5).
- Nube y virtualización: SP 800-145 para modelos, SP 800-144 para responsabilidad compartida y SP 800-125 para el hipervisor.

Lo que más se confunde

- La confianza cero no es un producto ni un perímetro de red: es una estrategia de decisión por acceso.
- La transición es incremental y empieza por los activos de mayor valor; sustituir todo de golpe es la opción falsa típica.

Fuentes: NIST SP 800-207 · SP 800-145, 800-144 y 800-125

12 Identidad y accesos

Los niveles de garantía son el terreno favorito de los distractores.

Qué entra

- IAL, AAL y FAL, cada uno del 1 al 3: qué exige cada nivel en verificación de identidad, autenticación y federación.
- Reglas de autenticadores de SP 800-63B-4: multifactor, resistentes al phishing, autenticadores sincronizables y reautenticación.
- Accesos privilegiados con SP 800-53r5: AC-2 gestión de cuentas, AC-5 separación de funciones y AC-6 mínimo privilegio; anexo 11.3 del Reglamento de Ejecución 2024/2690.
- Servicios de confianza de eIDAS: firma avanzada frente a cualificada, sello y sello de tiempo cualificados, cartera europea de identidad digital, y sus efectos jurídicos.

Lo que más se confunde

- AAL2 no es AAL3: cambia la resistencia al phishing y el tipo de autenticador.
- Firma avanzada no equivale a cualificada: solo la cualificada tiene el efecto de firma manuscrita.

Fuentes: NIST SP 800-63-4 (A, B y C) · SP 800-53r5 · Reglamento (UE) 910/2014 consolidado

13 Criptografía, claves y transición poscuántica

Cifras, estados y procesos: material muy preguntable y fácil de inventar mal.

Qué entra

- Ciclo de vida y estados de la clave; qué factores fijan el criptoperiodo (SP 800-57 parte 1, sección 5.3).
- Tipos de clave y necesidades de protección de cada uno.
- Fortaleza de seguridad y guía de transición de algoritmos (sección 5.6).
- Estándares poscuánticos: FIPS 203 ML-KEM para encapsulado de claves, FIPS 204 ML-DSA y FIPS 205 SLH-DSA para firma.
- Qué pide de verdad la Recomendación 2024/1101: un subgrupo del Grupo de Cooperación, una hoja de ruta coordinada en dos años, planes nacionales de transición, esquemas híbridos y revisión en tres años.

Lo que más se confunde

- Un mecanismo de encapsulado de claves no es un esquema de firma: ML-KEM y ML-DSA no son intercambiables.
- La recomendación europea no fija fechas límite de migración: inventarlas es el error más repetido.

Fuentes: NIST SP 800-57 parte 1 r5 · FIPS 203, 204 y 205 · Recomendación (UE) 2024/1101

14 Desarrollo seguro y DevSecOps

El Anexo II lo llama desarrollo seguro; la fuente es el SSDF.

Qué entra

- Los cuatro grupos del SSDF (SP 800-218): preparar la organización, proteger el software, producir software bien asegurado y responder a las vulnerabilidades.
- Seguridad en la cadena de integración y despliegue continuo (SP 800-204C) y los cinco tipos de código: aplicación, servicios de aplicación, infraestructura como código, política como código y observabilidad como código.
- Controles de malla de servicios y dónde se colocan.
- Ingeniería de seguridad de sistemas (SP 800-160 vol. 1 r1): procesos de ISO 15288, confiabilidad y caso de aseguramiento.
- Conexión legal: anexos 6.2 y 6.3 del Reglamento de Ejecución 2024/2690 y requisitos del CRA.

Lo que más se confunde

- Un escaneo al final del ciclo no es DevSecOps.
- La infraestructura como código y la política como código también son código a proteger: es el olvido típico.

Fuentes: NIST SP 800-218 · SP 800-204C · SP 800-160 vol. 1 r1

15 Operaciones de seguridad — registros, detección e inteligencia

SOC, monitorización y panorama de amenazas.

Qué entra

- Gestión de registros (SP 800-92): generación, almacenamiento y análisis; papel del syslog y del SIEM; políticas por entorno; dificultades habituales.
- Ciclo de compartición de información (SP 800-150): indicadores frente a tácticas, técnicas y procedimientos; consumir, usar, organizar y producir; validación y priorización.
- Protocolo de semáforo para la difusión: rojo, ámbar, verde y blanco.
- Panorama de amenazas de ENISA y su metodología: actores, técnicas y sectores más afectados.

Lo que más se confunde

- Un indicador de compromiso no es una táctica: el primero caduca, la segunda describe comportamiento.
- El SIEM no genera los registros: los recibe. Confundirlo cambia la respuesta.

Fuentes: NIST SP 800-92 · SP 800-150 · ENISA Threat Landscape 2025 y metodología CTL

16 Respuesta a incidentes y forense digital

Donde más se confunden fases y orden de actuación.

Qué entra

- Ciclo de vida de SP 800-61r3 apoyado en el CSF 2.0: preparación (Govern, Identify, Protect) y lecciones aprendidas frente a las fases de respuesta (Detect, Respond, Recover), con la tabla que mapea el modelo anterior de cuatro fases.
- Proceso forense de SP 800-86: recolección, examen, análisis e informe; datos volátiles primero; integridad y cadena de custodia.
- Fuentes de datos: ficheros, sistema operativo, tráfico de red y aplicaciones.
- Plazos de notificación a CERT-EU del artículo 21 del Reglamento 2023/2841 y la coordinación del artículo 22.

Lo que más se confunde

- Erradicar antes de capturar la evidencia destruye el caso: el orden importa y se pregunta.
- Recuperar no es cerrar: las lecciones aprendidas son parte de la preparación del siguiente incidente.

Fuentes: NIST SP 800-61r3 · SP 800-86 · Reglamento (UE, Euratom) 2023/2841

17 Continuidad, contingencia y saneamiento de soportes

Listas cerradas y parámetros: preguntas rápidas si se conocen.

Qué entra

- Tipos de plan de SP 800-34r1: continuidad de negocio, continuidad de operaciones, comunicación de crisis, protección de infraestructura crítica, respuesta a incidentes cibernéticos, recuperación ante desastres, contingencia del sistema y emergencia de ocupantes.
- RTO, RPO y tiempo máximo tolerable de interrupción, derivados del análisis de impacto.
- Estrategias de recuperación: métodos de copia y sitios frío, templado, caliente, móvil y espejo.
- Saneamiento de soportes (SP 800-88r2): borrar, purgar y destruir; borrado criptográfico y sus condiciones previas; el flujo de decisión de la sección 4.3 según tipo de soporte, reutilización y categorización FIPS 199.

Lo que más se confunde

- RTO no es RPO: uno mide tiempo de vuelta, el otro cuánta información se puede perder.
- Borrar no es purgar, y la desmagnetización no sirve para memoria flash, que no guarda datos magnéticamente.

Fuentes: NIST SP 800-34r1 · SP 800-88r2

18 Concienciación, formación y perfiles profesionales

Cierra el Anexo II y se contesta rápido con las listas bien aprendidas.

Qué entra

- Programa de aprendizaje de SP 800-50r1: análisis de necesidades; plan y estrategia; análisis y diseño; desarrollo e implantación; evaluación y mejora.
- Concienciación frente a formación por rol: objetivo y medición distintos.
- Los doce perfiles del marco ECSF de ENISA y el marco NICE (SP 800-181r1) con sus roles y enunciados de tareas, conocimientos y habilidades.
- Disparadores legales: artículo 20(2) de NIS2, anexo 8 del Reglamento de Ejecución 2024/2690 y artículo 8(1)(p) del Reglamento 2023/2841.

Lo que más se confunde

- Un curso anual en línea no es un programa: falta el análisis de necesidades y la medición.
- No inventar perfiles del ECSF: la lista es cerrada y los distractores suelen añadir uno falso.

Fuentes: NIST SP 800-50r1 · SP 800-181r1 · ENISA ECSF

19 Tecnologías emergentes — IA en seguridad y preparación cuántica

El puente con el otro ámbito de la convocatoria.

Qué entra

- Las tres capas del marco multicapa de ENISA: fundamentos de ciberseguridad, fundamentos de IA y capa sectorial.
- Clases de ataque de NIST AI 100-2 que importan cuando un SOC adopta aprendizaje automático o herramientas con modelos de lenguaje.
- Los riesgos de OWASP para aplicaciones LLM que se controlan primero en una organización.
- Preparación cuántica: inventario criptográfico, agilidad, esquemas híbridos y el proceso de la Recomendación 2024/1101.

Lo que más se confunde

- Una herramienta de aprendizaje automático no sustituye a un control: lo complementa.
- No existen fechas límite europeas de migración poscuántica: existe un proceso con hitos de planificación.

Fuentes: ENISA multilayer framework · NIST AI 100-2 · OWASP LLM Top 10 · Recomendación (UE) 2024/1101

5 · Cómo estudiarlo en ocho semanas



Ocho semanas dan para dos vueltas al temario si se contesta desde el principio.

semana	1	2	3	4	5	6	7	8
Mapa y fichas								
Estudio por bloques								
Bloques flojos y cifras								
Simulacros cronometrados								
Repaso y razonamiento								

Reparto: dos tercios al ámbito y un tercio al razonamiento. El ámbito ordena; el razonamiento solo elimina. Y desde la semana 3, preguntas el mismo día que se estudia el bloque: leer sin contestar no fija nada.

6 · Biblioteca oficial

Todo lo que sigue es público y citable. Ninguna preparación sería necesita más, y ningún manual comercial sustituye al texto consolidado.

Documento	Para qué
Reglamento (UE, Euratom) 2023/2841 y Decisión 2015/444	Ciberseguridad de las entidades de la Unión e información clasificada.
Directiva (UE) 2022/2555 y Reglamento de Ejecución 2024/2690	Medidas, umbrales de significatividad y plazos de notificación.
Reglamento (UE) 2024/2847 — Cyber Resilience Act	Productos con elementos digitales, clases y notificación.
Reglamento (UE) 2025/38 y Recomendación (UE) 2025/3445	Reserva de ciberseguridad y gestión de crisis.
Reglamento (UE) 2019/881 y Reglamento de Ejecución 2024/482	Certificación europea y esquema EUCC.
Reglamento (UE) 2022/2554 y Delegado 2024/1774	DORA y marco de gestión del riesgo TIC.
JOIN(2020) 18 · Reglamento 2019/796 · Directiva 2013/40 · COM(2023) 207	Estrategia, sanciones, derecho penal y capacidades.
NIST SP 800-37r2 · SP 800-30r1 · CSWP 29	Marco de gestión de riesgos, evaluación y CSF 2.0.
NIST SP 800-53r5 · 800-53A r5 · 800-137 · 800-55	Controles, evaluación, monitorización continua y métricas.
NIST SP 800-115 · 800-40r4 · OWASP ASVS y WSTG	Pruebas de seguridad y gestión de parches.
NIST SP 800-207 · 800-144/145/146 · 800-125	Confianza cero, nube y virtualización.
NIST SP 800-63-4 (A, B, C) y Reglamento 910/2014	Identidad, autenticación y servicios de confianza.
NIST SP 800-57 p.1 r5 · FIPS 203/204/205 · Recomendación 2024/1101	Claves, poscuántica y hoja de ruta europea.
NIST SP 800-218 · 800-204C · 800-160 v1r1	Desarrollo seguro, CI/CD e ingeniería de seguridad.
NIST SP 800-92 · 800-150 · ENISA Threat Landscape 2025	Registros, inteligencia de amenazas y panorama.
NIST SP 800-61r3 · 800-86 · 800-34r1 · 800-88r2	Incidentes, forense, continuidad y saneamiento.
NIST SP 800-50r1 · SP 800-181r1 · ENISA ECSF	Concienciación, formación y perfiles profesionales.

7 · Antes de darte por preparado

- ¿Tienes los plazos de NIS2, del CRA y del 2023/2841 sin mezclarlos, incluido el informe final?

- ¿Sabes quién supervisa, quién certifica y quién asiste en cada marco europeo?
- ¿Recitas los siete pasos del RMF y las seis funciones del CSF 2.0 con su salida?
- ¿Distingues escaneo, prueba de penetración y equipo rojo por objetivo y evidencia?
- ¿Tienes claros IAL, AAL y FAL y los tres estándares poscuánticos con su función?
- ¿Sabes por qué la desmagnetización no sana memoria flash y qué es el borrado criptográfico?
- ¿Has hecho tres simulacros de 30 preguntas en 40 minutos, en tu lengua 2?

Practica con preguntas de este ámbito, en los cinco idiomas del examen.

Banco de ciberseguridad de EPSO/AD/430/26, con la explicación y el artículo detrás de cada respuesta: eu-now.com/specialist/cybersecurity



Y cuando algo falle, pregúntalo. En EU-now, EUgenio responde con la norma delante y cita el artículo del que sale la respuesta: es la diferencia entre saber que fallaste y saber por qué.

Cifras y plazos proceden de la convocatoria publicada en el Diario Oficial (C/2026/4668) y de los textos oficiales citados. Si EPSO publica una corrección de errores, manda el Diario Oficial.