

Cybersicurezza

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

254

vincitori cercati

AD 8

grado di assunzione

30 / 40 min

prova del settore

13 ott. 2026

termine di candidatura

eu-now.com

Dossier di preparazione · 19 blocchi di studio con le loro fonti ufficiali

Basato sul bando di concorso GU C/2026/4668 e sui testi ufficiali che coprono il suo allegato II

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

1 · Il concorso in un colpo d'occhio

EPSO/AD/430/26 è un concorso generale per titoli ed esami per **amministratori di grado AD 8** nelle istituzioni, negli organi e negli organismi dell'Unione. Due settori, e **ci si può candidare a uno solo**: intelligenza artificiale (240 vincitori cercati) e cbersicurezza (254). Voi puntate a la cbersicurezza: 254 posti nell'elenco di riserva.



Ciò che decide davvero: le tre prove di ragionamento e la prova Eufte sono porte — si passa o si esce. **Solo il punteggio del test del settore classifica i candidati**, e solo chi ottiene i punteggi più alti vede corretta la propria Eufte e verificata l'ammissibilità. Due terzi del vostro tempo di studio appartengono al settore.



Le cinque fasi. Solo il punteggio del test del settore ordina i candidati; tutto il resto è una soglia.

2 · Le cinque prove

Prova	Lingua	Domande	Durata	Punti	Soglia
Ragionamento verbale	1	20	35 min	0-20	10/20
Ragionamento numerico	1	10	20 min	0-10	10/20 con l'astratto
Ragionamento astratto	1	10	10 min	0-10	10/20 con il numerico
Test del settore	2	30	40 min	0-30	15/30 e tra i punteggi più alti
Eufte	2	—	40 min	0-10	5/10

La **lingua 1** è una delle 24 lingue ufficiali. La **lingua 2** è quella del test del settore e della prova Eufte. Occorre un C1 in una e un B2 nell'altra, e si scelgono nell'atto di candidatura. Le prove si svolgono a distanza con sorveglianza remota, e l'ordine delle sessioni può differire da quello del bando.

L'Eufte non è né una prova linguistica né una prova di conoscenze: EPSO pubblica prima della prova una documentazione su temi europei — la stessa che ricevete durante la prova — e voi svolgete un esercizio a partire da essa. La correzione avviene secondo griglie pubblicate.

La piattaforma d'esame

Le prove si svolgono su TAO, la piattaforma che EPSO usa per tutti i suoi esami. Arrivate sapendo dov'è ogni cosa: si perde meno tempo e nulla sorprende il giorno della prova.

EU Careers - Sample Test / Part I / Verbal Reasoning
Punteggio 42%

1. Elimination tool
2. Calculator
3. Scratchpad

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.

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

Schermata della domanda: navigatore delle domande in basso, segnalibro, orologio e strumenti in alto.

Verbal Reasoning

Test Configuration

Set

Verbal Reasoning

1013x2

2026

AC ± % ÷

Eliminazione delle risposte: barrate ciò che avete escluso.

Evidenziatore e righello di lettura per i testi lunghi.

Calcolatrice e blocco per appunti quando la prova li consente.

Schermate della piattaforma TAO utilizzata nelle prove EPSO.

L'elenco di riserva è pubblicato in ordine alfabetico, non per punteggio; vi figurano tutti i candidati a pari merito all'ultimo posto; e figurarvi non garantisce alcuna assunzione.

Fonti: bando di concorso GU C/2026/4668, sezioni 1, 4.2, 4.3.1, 4.3.2 (tabelle da 3 a 5), 4.3.3 e 4.3.4.

3 · Come sono le 30 domande

Il bando non pubblica né programma né bibliografia. Il contratto è l'**allegato II, «funzioni tipiche»**: tutto ciò che è esaminabile viene da lì, ed è per questo che il dossier lo scompone per intero. Trenta domande in 40 minuti, in lingua 2: **80 secondi a domanda**. Non c'è tempo per ricostruire nulla — si risponde con ciò che si riconosce.

Una situazione presa dal lavoro
Un'autorità nazionale rileva un incidente significativo in un soggetto essenziale...

- ☐ A · Notificare al CSIRT entro 72 ore
- ☒ B · Preallarme al CSIRT entro 24 ore
- ☐ C · Relazione finale alla Commissione entro un mese
- ☐ D · Notificare al gruppo di cooperazione

Ciò che decide la risposta

- CHI** è competente
CSIRT, autorità, Commissione...
- QUALE** obbligo esatto
preallarme, notifica, relazione
- IL NUMERO**
24 h · 72 h · un mese

I distrattori colpiscono uno dei tre:
il termine accanto, l'organo vicino,
l'obbligo di un'altra fase.

Anatomia di una domanda del settore: 80 secondi per riconoscere tre dati.

Le cinque trappole del formato

- **L'opzione più lunga.** Nelle prove ufficiali la risposta corretta è la più lunga solo circa 4 volte su 10: scegliere in base alla lunghezza non fa superare la prova.
- **L'assoluto.** «Sempre», «mai», «in ogni caso» segnalano di solito l'opzione falsa: il diritto dell'Unione vive di eccezioni.
- **L'attore scambiato.** L'obbligo è descritto correttamente, ma attribuito all'organo sbagliato. Leggete il soggetto prima del verbo.
- **Lo strumento vicino.** L'affermazione è vera, ma appartiene a un'altra norma, che non disciplina questo caso.
- **Il testo superato.** Una formulazione anteriore a una modifica. Studiate sempre il testo consolidato.

La scheda che funziona

A chi si applica	Cosa impone	Termini e cifre	Chi vigila
soggetti · prodotti	la condotta esatta	24 h · 72 h · soglia	e chi sanziona

Una scheda per strumento: quattro colonne, niente di più. È ciò che risponde in 80 secondi.

4 · Il programma, blocco per blocco

L'allegato II descrive funzioni, non materie. Eccole trasformate in blocchi di studio: che cosa entra, che cosa si confonde e dove è scritto. Ciò che non figura in un testo ufficiale non viene chiesto.



Il settore 2 è fatto di decisioni: quale controllo, quale termine e chi risponde quando accade qualcosa.

1 - Gestione del rischio e assurance di sicurezza

Quadri di rischio (RMF, CSF 2.0)

Controlli e monitoraggio

Vulnerabilità e test

Certificazione europea

2 - Architettura, progettazione e tecnologia

Zero trust, cloud e virtualizzazione

Identità e accessi

Crittografia e post-quantistica

Sviluppo sicuro e DevSecOps

Tecnologie emergenti

3 - Operazioni di sicurezza e risposta agli incidenti

Operazioni e rilevamento

Risposta e forense

Continuità e sanificazione

4 - Governance, politica e coordinamento

Istituzioni dell'Unione (2023/2841)

NIS2 ed esecuzione

Ciberresilienza

Cibersolidarietà

DORA

Politica e diritto penale

5 - Sensibilizzazione, competenze e consulenza

Formazione e profili ECSF

L'allegato II tradotto in blocchi di studio.

1 Cybersicurezza delle istituzioni dell'Unione — regolamento 2023/2841

Il quadro della casa in cui lavorerete. Ricorre spesso e si confonde sistematicamente con NIS2.

Che cosa entra

- Il quadro dell'articolo 6: approvato al più alto livello dirigenziale entro l'8 aprile 2025, esteso a infrastrutture locali, cloud, tecnologie operative e mobile, riesaminato almeno ogni quattro anni.
- La valutazione della maturità dell'articolo 7: entro l'8 luglio 2025 e poi almeno ogni due anni.
- Le misure dell'articolo 8 e il piano di cybersicurezza dell'articolo 9, rivisto ogni due anni.
- Il responsabile locale della cybersicurezza: compiti e linea di riporto.
- La segnalazione al CERT-UE prevista dall'articolo 21: preallarme entro 24 ore, notifica entro 72 ore, relazione finale entro un mese.
- L'IICB (articoli da 10 a 12) decide ed emana orientamenti; il CERT-UE (articolo 13) eroga servizi.

Che cosa si confonde

- Il CERT-UE non vigila, non sanziona e non è il CSIRT nazionale di nessuno: serve le entità dell'Unione.
- Le entità dell'Unione NON rientrano in NIS2: se lo scenario cita un'istituzione europea, la norma è il regolamento 2023/2841.
- Le informazioni classificate seguono un regime distinto, la decisione 2015/444, con i suoi contrassegni, le sue zone e i suoi uffici di registrazione.

Fonti: Regolamento (UE, Euratom) 2023/2841, articoli da 6 a 13 e 21 · Decisione (UE, Euratom) 2015/444

2 NIS2 e il regolamento di esecuzione 2024/2690

La norma di riferimento del settore e la fonte più ricca di domande su termini e soglie.

Che cosa entra

- I dieci ambiti di misure dell'articolo 21, paragrafo 2: analisi dei rischi, gestione degli incidenti, continuità operativa, sicurezza della catena di approvvigionamento, acquisizione e sviluppo, valutazione dell'efficacia, igiene informatica e formazione, crittografia, risorse umane e controllo degli accessi, autenticazione a più fattori.
- Le entità coperte dal regolamento di esecuzione: DNS, registri dei nomi di dominio di primo livello, cloud, centri dati, reti di distribuzione dei contenuti, fornitori di servizi gestiti e di servizi gestiti di sicurezza, mercati online, motori di ricerca, social network e prestatori di servizi fiduciari.
- I criteri di significatività dell'articolo 3: perdita diretta superiore a 500 000 EUR o al 5 % del fatturato, se inferiore; esfiltrazione di segreti commerciali; decesso o danno grave alla salute; accesso non autorizzato.
- La segnalazione per fasi dell'articolo 23: preallarme entro 24 ore, notifica dell'incidente entro 72 ore, relazione finale entro un mese.
- La responsabilità dell'organo di gestione (articolo 20) e la formazione obbligatoria.
- Le soglie per singolo servizio negli articoli da 5 a 14 del regolamento di esecuzione e le tredici sezioni del suo allegato.

Che cosa si confonde

- L'ENISA non vigila sulle entità: lo fanno le autorità nazionali competenti.
- Le misure dell'articolo 21 non sono gli obblighi di sicurezza del GDPR, per quanto si somiglino.
- Entità essenziali e importanti differiscono soprattutto per vigilanza e sanzioni, non per le misure in sé.

Fonti: Direttiva (UE) 2022/2555, articoli 20, 21 e 23 · Regolamento di esecuzione (UE) 2024/2690 · Orientamenti tecnici dell'ENISA 2025

3 Regolamento sulla ciberresilienza — regolamento 2024/2847

Prodotti con elementi digitali: classificazione, scadenze e chi risponde lungo la catena.

Che cosa entra

- La classificazione: prodotto ordinario, prodotto importante di classe I o II (articolo 7 e allegato III) e prodotto critico (articolo 8 e allegato IV).
- Le procedure di valutazione della conformità dell'articolo 32, secondo la classe.
- Gli obblighi del fabbricante: gestione delle vulnerabilità e periodo di assistenza dell'articolo 13, di almeno cinque anni salvo vita del prodotto più breve.
- La segnalazione dell'articolo 14 per le vulnerabilità attivamente sfruttate e gli incidenti gravi: preallarme entro 24 ore, notifica entro 72 ore, relazione finale entro 14 giorni, tramite la piattaforma unica di segnalazione dell'articolo 16.

- Il ruolo di curatore di software libero (articolo 24).
- Le date: applicazione generale l'11 dicembre 2027, obblighi di segnalazione dall'11 settembre 2026, disposizioni sugli organismi notificati dall'11 giugno 2026.

Che cosa si confonde

- La relazione finale del regolamento sulla ciberresilienza è dovuta in 14 giorni; quella di NIS2 in un mese. È lo scambio più frequente.
- La piattaforma unica di segnalazione è istituita dall'articolo 16, ma l'obbligo di segnalare sta nell'articolo 14.
- Un servizio interno di un'istituzione non è un prodotto immesso sul mercato.

Fonti: Regolamento (UE) 2024/2847, articoli 7, 8, 13, 14, 16, 24 e 32; allegati I, III e IV

4 Regolamento sulla ciber-solidarietà e piano generale dell'Unione

Risposta europea agli incidenti su vasta scala: tre parti e tre livelli.

Che cosa entra

- Il sistema europeo di allerta per la cibersecurity, con poli cibernetici nazionali e transfrontalieri (articoli da 3 a 9).
- Il meccanismo di emergenza per la cibersecurity: preparazione coordinata, riserva dell'UE per la cibersecurity e assistenza reciproca (articoli da 10 a 19).
- Il meccanismo europeo di riesame degli incidenti di cibersecurity, condotto dall'ENISA su richiesta della Commissione o di EU-CyCLONe (articolo 21).
- Chi può chiedere l'attivazione della riserva: gli Stati membri, le istituzioni, gli organi e gli organismi dell'Unione e i paesi terzi associati al programma Europa digitale.
- I livelli del piano generale (raccomandazione (UE) 2025/3445): tecnico nella rete di CSIRT, operativo in EU-CyCLONe, politico con l'attivazione dell'IPCR da parte della presidenza del Consiglio.

Che cosa si confonde

- Il livello politico non conduce la risposta tecnica: l'IPCR coordina decisioni, non contiene incidenti.
- EU-CyCLONe è operativo, non politico, e non sostituisce la rete di CSIRT.

Fonti: Regolamento (UE) 2025/38 · Raccomandazione (UE) 2025/3445 del Consiglio

5 Certificazione europea — regolamento sulla cibersicurezza e schema EUCC

Il quadro di certificazione: livelli, volontarietà e ripartizione dei ruoli.

Che cosa entra

- I livelli di affidabilità dell'articolo 52 — di base, sostanziale ed elevato — e la valutazione che ciascuno richiede.
- La volontarietà sancita dall'articolo 56, salvo diversa disposizione del diritto dell'Unione o nazionale.
- I ruoli: l'ENISA prepara gli schemi candidati (articolo 49), gli organismi di valutazione della conformità certificano (articolo 60), le autorità nazionali vigilano (articolo 58) e l'ECCG consiglia (articolo 62).
- Lo schema EUCC (regolamento di esecuzione 2024/482): criteri comuni e CEM, il livello sostanziale corrisponde ad AVA_VAN 1-2 e quello elevato ad AVA_VAN 3-5, senza autovalutazione, certificati validi fino a cinque anni.
- Gli obblighi del titolare sulla gestione delle vulnerabilità e i motivi di revoca.

Che cosa si confonde

- L'ENISA non rilascia certificati: prepara gli schemi.
- La certificazione non è obbligatoria per impostazione predefinita; affermarlo è un distrattore classico.
- L'EUCC non ammette autovalutazione, a differenza di alcuni schemi di livello di base.

Fonti: Regolamento (UE) 2019/881, articoli 49, 52, 56, 58, 60 e 62 · Regolamento di esecuzione (UE) 2024/482

6 DORA e il settore finanziario

Compare come quadro settoriale: imparate la mappa e il confine con NIS2, non i dettagli.

Che cosa entra

- I cinque pilastri: gestione del rischio informatico (capo II), gestione e segnalazione degli incidenti (III), test di resilienza operativa digitale, compresi i test di penetrazione guidati dalla minaccia (IV), rischio di terzi con autorità di sorveglianza capofila per i fornitori critici (V) e condivisione delle informazioni (VI).
- La responsabilità dell'organo di gestione ai sensi dell'articolo 5.
- Il regolamento delegato 2024/1774 precisa il quadro di gestione del rischio informatico.
- Il rapporto con NIS2: DORA è *lex specialis* per le entità finanziarie.

Che cosa si confonde

- Le autorità europee di vigilanza non vigilano su una singola banca: lo fanno le autorità nazionali competenti.
- Una relazione su un incidente grave ai sensi di DORA non è una notifica NIS2, e i termini differiscono.

Fonti: Regolamento (UE) 2022/2554, articolo 5 e capi da II a VI · Regolamento delegato (UE) 2024/1774

7 Politica dell'Unione e diritto penale

Domande di attribuzione: che cosa dice ciascuno strumento e di chi è la competenza.

Che cosa entra

- La strategia per la cibersicurezza del 2020: resilienza e sovranità tecnologica; capacità operativa di prevenire, dissuadere e reagire; un ciberspazio globale e aperto.
- Il regime di sanzioni cibernetiche del regolamento (UE) 2019/796: attacchi informatici con effetti significativi, inserimento in elenco da parte del Consiglio, congelamento attuato dagli Stati membri.
- La direttiva 2013/40: accesso illecito, interferenza sui sistemi e sui dati, intercettazione, strumenti; circostanze aggravanti come le botnet o le infrastrutture critiche; punti di contatto attivi 24 ore su 24.
- L'accademia delle competenze per la cibersicurezza (COM(2023) 207) e i suoi quattro pilastri.

Che cosa si confonde

- Le sanzioni le decide il Consiglio; il diritto penale lo applicano gli Stati membri. I due piani non si mescolano.
- L'accademia non è un organo con poteri: è un'iniziativa politica.

Fonti: JOIN(2020) 18 · Regolamento (UE) 2019/796 · Direttiva 2013/40/UE · COM(2023) 207

8 Quadri di gestione del rischio — RMF, SP 800-30 e CSF 2.0

L'ossatura tecnica. L'esame chiede l'ordine delle fasi e il prodotto di ciascuna.

Che cosa entra

- Le sette fasi dell'RMF (SP 800-37r2): preparare, categorizzare, selezionare, attuare, valutare, autorizzare e monitorare, con il prodotto di ogni fase.
- La valutazione del rischio secondo la SP 800-30r1: fonti di minaccia, eventi di minaccia, vulnerabilità e condizioni predisponenti, probabilità e impatto; il processo preparare-condurre-comunicare-mantenere; i tre livelli organizzativi.
- Il CSF 2.0 (CSWP 29): sei funzioni, tra cui Govern, categorie e sottocategorie, profili attuale e obiettivo, e livelli da 1 a 4.
- I modelli di maturità: a che cosa servono e in che cosa differiscono da una valutazione del rischio.

Che cosa si confonde

- Le funzioni del CSF non sono le fasi dell'RMF, né i requisiti della ISO 27001.
- I livelli del CSF descrivono il rigore della governance, non un punteggio di sicurezza.

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

9 Controlli, valutazione e monitoraggio continuo

Ciò che l'allegato II chiama operazioni e metriche di valutazione della sicurezza.

Che cosa entra

- Le famiglie di controlli della SP 800-53r5 e la differenza tra un controllo di base e il suo potenziamento.
- Le baseline e gli orientamenti di adattamento sono passati alla SP 800-53B; la r5 ne conserva i concetti: perimetro, controlli compensativi e parametri definiti dall'organizzazione.
- I metodi di valutazione della SP 800-53A: esaminare, intervistare e testare, e la prova che ciascuno produce.
- Il monitoraggio continuo (SP 800-137): definire la strategia, istituire, attuare, analizzare e riferire, rispondere, riesaminare e aggiornare; tre livelli; che cosa determina la frequenza.
- La misurazione (SP 800-55): metriche di attuazione, di efficacia e di impatto.

Che cosa si confonde

- Un audit annuale non è monitoraggio continuo.
- Una metrica che non innesca alcuna decisione non è una metrica di sicurezza, ma solo un numero.

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

10 Gestione delle vulnerabilità e test di sicurezza

Distinguate le tecniche per obiettivo, perimetro e prova — e sappiate quale norma le impone.

Che cosa entra

- Scansione, test di penetrazione e red teaming: che cosa cerca ciascuno e che cosa consegna.
- Le fasi della SP 800-115: pianificazione, scoperta, attacco e relazione; tecniche di esame, identificazione e analisi degli obiettivi, convalida delle vulnerabilità.
- La gestione delle patch in azienda (SP 800-40r4): risposte al rischio — accettare, attenuare, trasferire o evitare; gruppi di manutenzione; ciclo di vita della patch.
- I livelli dell'OWASP ASVS 5.0 e le categorie di test del WSTG 4.2.
- L'innescio giuridico: allegati 6.5 e 6.10 del regolamento di esecuzione 2024/2690.

Che cosa si confonde

- Una scansione non è un test di penetrazione: obiettivo e prova sono diversi.
- Il regolamento di esecuzione fonda i test sul rischio, non li impone incondizionatamente.

Fonti: NIST SP 800-115 · SP 800-40r4 · OWASP ASVS 5.0 e WSTG 4.2 · Regolamento di esecuzione (UE) 2024/2690

11 Architettura di sicurezza — zero trust, cloud e virtualizzazione

Concetti di architettura con un lessico molto preciso.

Che cosa entra

- I principi e i componenti logici della SP 800-207: il motore delle politiche decide, l'amministratore delle politiche istituisce e il punto di applicazione applica.
- Le fonti che alimentano l'algoritmo di fiducia: diagnostica continua, conformità di settore, intelligence sulle minacce, log di attività e SIEM.
- Gli approcci: governance rafforzata dell'identità, micro-segmentazione e perimetro definito dal software; le varianti di distribuzione: agente e gateway, gateway di enclave, portale di risorse e sandboxing delle applicazioni.
- Le minacce proprie di un'architettura zero trust (sezione 5).
- Cloud e virtualizzazione: SP 800-145 per i modelli, SP 800-144 per la responsabilità condivisa e SP 800-125 per l'hypervisor.

Che cosa si confonde

- Zero trust non è un prodotto né un perimetro di rete: è una strategia di decisione a ogni accesso.
- La transizione è graduale e parte dai beni di maggior valore; sostituire tutto in una volta è la falsa opzione tipica.

Fonti: NIST SP 800-207 · SP 800-145, 800-144 e 800-125

12 Gestione delle identità e degli accessi

I livelli di affidabilità sono il terreno preferito dei distrattori.

Che cosa entra

- IAL, AAL e FAL, da 1 a 3: che cosa esige ciascun livello in materia di verifica dell'identità, autenticazione e federazione.
- Le regole sugli autenticatori della SP 800-63B-4: autenticazione a più fattori, resistenza al phishing, autenticatori sincronizzabili e riautenticazione.
- Gli accessi privilegiati con la SP 800-53r5: AC-2 gestione degli account, AC-5 separazione dei compiti e AC-6 privilegio minimo; allegato 11.3 del regolamento di esecuzione 2024/2690.
- I servizi fiduciari eIDAS: firma elettronica avanzata e qualificata, sigillo e validazione temporale qualificati, portafoglio europeo di identità digitale, e i loro effetti giuridici.

Che cosa si confonde

- AAL2 non è AAL3: cambiano la resistenza al phishing e il tipo di autenticatore.
- Una firma avanzata non è qualificata: solo la qualificata ha l'effetto di una firma autografa.

Fonti: NIST SP 800-63-4 (A, B e C) · SP 800-53r5 · Regolamento (UE) 910/2014 consolidato

13 Crittografia, gestione delle chiavi e transizione post-quantistica

Cifre, stati e processi: molto esaminabile e facile da sbagliare.

Che cosa entra

- Il ciclo di vita e gli stati di una chiave; i fattori che fissano un criptoperiodo (SP 800-57 parte 1, sezione 5.3).
- I tipi di chiave e la protezione che ciascuno richiede.
- La forza di sicurezza e gli orientamenti sulla transizione tra algoritmi (sezione 5.6).
- Le norme post-quantistiche: FIPS 203 ML-KEM per l'incapsulamento di chiavi, FIPS 204 ML-DSA e FIPS 205 SLH-DSA per le firme.
- Che cosa chiede davvero la raccomandazione (UE) 2024/1101: un sottogruppo del gruppo di cooperazione NIS, una tabella di marcia coordinata entro due anni, piani nazionali di transizione, schemi ibridi e un riesame entro tre anni.

Che cosa si confonde

- Un meccanismo di incapsulamento di chiavi non è uno schema di firma: ML-KEM e ML-DSA non sono intercambiabili.
- La raccomandazione dell'Unione non fissa scadenze di migrazione: inventarle è l'errore più ripetuto.

Fonti: NIST SP 800-57 parte 1 r5 · FIPS 203, 204 e 205 · Raccomandazione (UE) 2024/1101

14 Sviluppo sicuro e DevSecOps

L'allegato II lo chiama sviluppo sicuro; la fonte è il SSDF.

Che cosa entra

- I quattro gruppi del SSDF (SP 800-218): preparare l'organizzazione, proteggere il software, produrre software ben protetto e rispondere alle vulnerabilità.
- La sicurezza nella catena di integrazione e distribuzione continue (SP 800-204C) e i cinque tipi di codice: applicativo, servizi applicativi, infrastruttura come codice, politica come codice e osservabilità come codice.
- I controlli della service mesh e dove si collocano.
- L'ingegneria della sicurezza dei sistemi (SP 800-160 vol. 1 r1): processi della ISO 15288, affidabilità e dossier di assurance.
- Gli ancoraggi giuridici: allegati 6.2 e 6.3 del regolamento di esecuzione 2024/2690 e requisiti del regolamento sulla ciberresilienza.

Che cosa si confonde

- Una sola scansione a fine ciclo non è DevSecOps.
- Infrastruttura come codice e politica come codice sono anch'esse codice da proteggere: è l'omissione abituale.

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

15 Operazioni di sicurezza — log, rilevamento e intelligence sulle minacce

SOC, monitoraggio e panorama delle minacce.

Che cosa entra

- La gestione dei log (SP 800-92): generazione, conservazione e analisi; i ruoli di syslog e del SIEM; politiche per ambiente; difficoltà ricorrenti.
- La condivisione di informazioni sulle minacce (SP 800-150): indicatori contro tattiche, tecniche e procedure; consumare, usare, organizzare e produrre; convalida e definizione delle priorità.
- Il protocollo dei semafori per la diffusione: rosso, ambra, verde e bianco.
- Il panorama delle minacce dell'ENISA e la sua metodologia: attori, tecniche e settori più colpiti.

Che cosa si confonde

- Un indicatore di compromissione non è una tattica: il primo scade, la seconda descrive un comportamento.
- Il SIEM non genera i log: li riceve. Confonderlo cambia la risposta.

Fonti: NIST SP 800-92 · SP 800-150 · Panorama delle minacce dell'ENISA 2025 e metodologia CTL

16 Risposta agli incidenti e informatica forense

È qui che si confondono più spesso le fasi e l'ordine delle azioni.

Che cosa entra

- Il ciclo di vita della SP 800-61r3 costruito sul CSF 2.0: preparazione (Govern, Identify, Protect) e lezioni apprese, rispetto alle fasi di risposta (Detect, Respond, Recover), con la tabella di corrispondenza al precedente modello in quattro fasi.
- Il processo forense della SP 800-86: raccolta, esame, analisi e relazione; dati volatili per primi; integrità e catena di custodia.
- Le fonti di dati: file, sistemi operativi, traffico di rete e applicazioni.
- I termini di segnalazione al CERT-UE dell'articolo 21 del regolamento 2023/2841 e il coordinamento dell'articolo 22.

Che cosa si confonde

- Eradicare prima di acquisire le prove distrugge il caso: l'ordine conta ed è oggetto d'esame.
- Il ripristino non è la chiusura: le lezioni apprese fanno parte della preparazione all'incidente successivo.

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

17 Continuità, piani di emergenza e sanificazione dei supporti

Elenchi chiusi e parametri: punti rapidi se li si conosce.

Che cosa entra

- I tipi di piano della SP 800-34r1: continuità operativa, continuità delle operazioni, comunicazione di crisi, protezione delle infrastrutture critiche, risposta agli incidenti informatici, ripristino in caso di disastro, piano di emergenza del sistema informativo e piano di emergenza per gli occupanti.
- RTO, RPO e tempo massimo tollerabile di inattività, ricavati dall'analisi di impatto sull'attività.
- Le strategie di ripristino: metodi di backup e siti freddi, tiepidi, caldi, mobili e speculari.
- La sanificazione dei supporti (SP 800-88r2): cancellare, purgare e distruggere; cancellazione crittografica e sue condizioni; l'albero decisionale della sezione 4.3 per tipo di supporto, riutilizzo e categorizzazione di riservatezza FIPS 199.

Che cosa si confonde

- Il RTO non è il RPO: uno misura il tempo di ritorno, l'altro quanti dati ci si può permettere di perdere.
- Cancellare non è purgare, e la smagnetizzazione non funziona sulla memoria flash, che non immagazzina nulla per via magnetica.

Fonti: NIST SP 800-34r1 · SP 800-88r2

18 Sensibilizzazione, formazione e professioni della cibersecurity

Chiude l'allegato II e si risolve in fretta se si conoscono gli elenchi.

Che cosa entra

- Il programma di apprendimento della SP 800-50r1: analisi dei fabbisogni; piano e strategia; analisi e progettazione; sviluppo e attuazione; valutazione e miglioramento.
- Sensibilizzazione contro formazione per ruolo: obiettivo diverso, misurazione diversa.
- I dodici profili di ruolo dell'ECSF dell'ENISA e il quadro NICE (SP 800-181r1) con i suoi ruoli professionali e i suoi enunciati di compiti, conoscenze e abilità.
- Gli inneschi giuridici: articolo 20, paragrafo 2, di NIS2, allegato 8 del regolamento di esecuzione 2024/2690 e articolo 8, paragrafo 1, lettera p), del regolamento 2023/2841.

Che cosa si confonde

- Un corso online una volta l'anno non è un programma: mancano l'analisi dei fabbisogni e la misurazione.
- Non inventate profili ECSF: l'elenco è chiuso e i distrattori spesso ne aggiungono uno falso.

Fonti: NIST SP 800-50r1 · SP 800-181r1 · ECSF dell'ENISA

19 Tecnologie emergenti — IA nella sicurezza e preparazione quantistica

Il ponte verso l'altro settore di questo concorso.

Che cosa entra

- I tre livelli del quadro multilivello dell'ENISA: fondamenti di cibersicurezza, fondamenti di IA e livello settoriale.
- Le classi di attacco del NIST AI 100-2 che contano quando un SOC adotta l'apprendimento automatico o strumenti basati su grandi modelli linguistici.
- Le voci del Top 10 OWASP LLM da controllare per prime in un'organizzazione.
- La preparazione quantistica: inventario crittografico, agilità, schemi ibridi e processo della raccomandazione (UE) 2024/1101.

Che cosa si confonde

- Uno strumento di apprendimento automatico non sostituisce un controllo: lo completa.
- Non esistono scadenze europee di migrazione post-quantistica: esiste un processo con tappe di pianificazione.

Fonti: Quadro multilivello dell'ENISA · NIST AI 100-2 · OWASP LLM Top 10 · Raccomandazione (UE) 2024/1101

5 · Come studiarlo in otto settimane



Otto settimane permettono due passaggi sul programma, se si risponde a domande fin dal primo giorno.

settimana	1	2	3	4	5	6	7	8
Mappa e schede								
Studio blocco per blocco								
Blocchi deboli e cifre								
Simulazioni a tempo								
Ripasso e ragionamento								

Ripartizione: due terzi al settore, un terzo al ragionamento. Il settore vi classifica; il ragionamento si limita a eliminare. E dalla settimana 3 rispondete a domande lo stesso giorno in cui studiate il blocco: leggere senza rispondere non fissa nulla.

6 · Biblioteca ufficiale

Tutto ciò che segue è pubblico e citabile. Una preparazione seria non ha bisogno di altro, e nessun manuale commerciale sostituisce il testo consolidato.

Documento	A che cosa serve
Regolamento (UE, Euratom) 2023/2841 e decisione 2015/444	Cybersicurezza delle entità dell'Unione e informazioni classificate UE.
Direttiva (UE) 2022/2555 e regolamento di esecuzione 2024/2690	Misure, soglie di significatività e termini di segnalazione.
Regolamento (UE) 2024/2847 — ciberresilienza	Prodotti con elementi digitali, classi e segnalazione.
Regolamento (UE) 2025/38 e raccomandazione (UE) 2025/3445	Riserva per la cybersicurezza e gestione delle crisi.
Regolamento (UE) 2019/881 e regolamento di esecuzione 2024/482	Certificazione europea e schema EUCC.
Regolamento (UE) 2022/2554 e regolamento delegato 2024/1774	DORA e il quadro di gestione del rischio informatico.
JOIN(2020) 18 · Regolamento 2019/796 · Direttiva 2013/40 · COM(2023) 207	Strategia, sanzioni, diritto penale e competenze.
NIST SP 800-37r2 · SP 800-30r1 · CSWP 29	Quadro di gestione del rischio, valutazione e CSF 2.0.
NIST SP 800-53r5 · 800-53A r5 · 800-137 · 800-55	Controlli, valutazione, monitoraggio continuo e metriche.
NIST SP 800-115 · 800-40r4 · OWASP ASVS e WSTG	Test di sicurezza e gestione delle patch.
NIST SP 800-207 · 800-144/145/146 · 800-125	Zero trust, cloud e virtualizzazione.
NIST SP 800-63-4 (A, B, C) e regolamento 910/2014	Identità, autenticazione e servizi fiduciari.
NIST SP 800-57 p.1 r5 · FIPS 203/204/205 · Raccomandazione 2024/1101	Chiavi, post-quantistica e tabella di marcia europea.
NIST SP 800-218 · 800-204C · 800-160 v1r1	Sviluppo sicuro, CI/CD e ingegneria della sicurezza dei sistemi.
NIST SP 800-92 · 800-150 · Panorama delle minacce dell'ENISA 2025	Log, intelligence sulle minacce e panorama.
NIST SP 800-61r3 · 800-86 · 800-34r1 · 800-88r2	Incidenti, forense, continuità e sanificazione.
NIST SP 800-50r1 · SP 800-181r1 · ECSF dell'ENISA	Sensibilizzazione, formazione e profili professionali.

7 · Prima di dichiararvi pronti

- Tenete separati i termini di NIS2, del regolamento sulla ciberresilienza e del 2023/2841, relazione finale compresa?
- Sapete chi vigila, chi certifica e chi assiste in ciascun quadro europeo?
- Sapete elencare le sette fasi dell'RMF e le sei funzioni del CSF 2.0 con il loro prodotto?
- Distinguate scansione, test di penetrazione e red teaming per obiettivo e prova?
- Sono chiari IAL, AAL e FAL, e le tre norme post-quantistiche con la loro funzione?
- Sapete perché la smagnetizzazione non sanifica la memoria flash e che cosa richiede la cancellazione crittografica?
- Avete fatto tre simulazioni di 30 domande in 40 minuti, nella vostra lingua 2?

Allenatevi con domande di questo settore, nelle cinque lingue dell'esame.

Banca EPSO/AD/430/26 cbersicurezza, con la spiegazione e l'articolo dietro ogni risposta: eu-now.com/specialist/cybersecurity



E quando qualcosa non torna, chiedete. In EU-now, EUgenio risponde con la norma davanti e cita l'articolo da cui viene la risposta: la differenza tra sapere di aver sbagliato e sapere perché.

Cifre e scadenze provengono dal bando pubblicato nella Gazzetta ufficiale (C/2026/4668) e dai testi ufficiali citati. In caso di rettifica pubblicata da EPSO, prevale la Gazzetta ufficiale.