



DOSSIER TECNICO DIDATTICO E DI VALUTAZIONE

Cyber Incident Response & Crisis Management – ISO/IEC 27035 / NIST SP 800-61r3

Corso + attestato

780,00 €

IVA/VAT esclusa

Codice corso

IR-27035-CYBER

Durata minima

424 min

Soglia finale

75%

Edizione scheda

13/10/2026

1. Identità, finalità e perimetro del percorso

Percorso avanzato per CSIRT/SOC, CISO, incident manager e dirigenti sulla preparazione, detection, triage, containment, eradication, recovery, comunicazione di crisi e miglioramento post-incident.

La presente scheda tecnica estesa descrive il percorso così come pubblicato nella CIWZ Academy alla data di emissione. Riunisce finalità, riferimenti, architettura didattica, contenuti dei moduli, sistema delle verifiche, criteri di superamento e condizioni di attestazione. Il documento non sostituisce i testi ufficiali delle norme, delle leggi, delle linee guida o degli schemi richiamati.

2. Riferimenti normativi, regolamentari e tecnici

ISO/IEC 27035-1:2023; ISO/IEC 27035-2:2023; ISO/IEC 27035-3:2020; ISO/IEC 27035-4:2024; NIST SP 800-61 Rev.3 (2025); NIST CSF 2.0; NIS2/D.Lgs. 138/2024 ove applicabili

I riferimenti sono utilizzati come quadro di studio e di valutazione nei limiti del contenuto pubblicato e delle fonti disponibili. Per l'applicazione professionale prevalgono sempre le versioni ufficiali e vigenti dei documenti richiamati.

3. Architettura didattica e sistema di verifica

- 8 moduli didattici strutturati
- tempo minimo tracciato: 424 min
- banca verifiche intermedie: 256 quesiti
- banca esame finale attiva: 240 quesiti
- esame finale: 30 quesiti selezionati dalla banca
- soglia di superamento: 75%
- Accesso al percorso attraverso il profilo Academy personale o tramite assegnazione aziendale.
- Studio sequenziale dei moduli, con registrazione server-side dell'avanzamento e del tempo minimo previsto.

- Verifiche intermedie associate ai moduli per controllare comprensione, capacità applicativa e qualità del ragionamento.
- Sblocco dell'esame finale solo dopo il completamento dei requisiti previsti dal percorso.
- Esame finale protetto, composto dalla piattaforma mediante selezione dalla banca attiva del corso.
- Registrazione dell'esito e, quando previsto, possibilità di richiedere l'attestato finale.

4. Informazioni tecniche ufficiali di catalogo

Scheda tecnica del corso

Percorso CIWZ Academy executive/professionale con contenuti originali, lezioni tracciate lato server, 8 moduli, verifiche intermedie randomizzate, Secure Proctor negli assessment e banca finale scenario-based. Accesso gratuito; eventuale costo solo per emissione del certificato dopo il superamento.

5. Programma analitico del percorso

Il programma seguente è ricavato dai moduli attivi pubblicati nella piattaforma. Per ciascun modulo sono indicati il tempo minimo e la consistenza della banca di verifica intermedia disponibile.

01 Incident response governance e preparazione

Tempo minimo: 53 min | Quesiti intermedi: 32

02 Detection, logging e triage

Tempo minimo: 53 min | Quesiti intermedi: 32

03 Scoping, analysis e incident classification

Tempo minimo: 53 min | Quesiti intermedi: 32

04 Containment strategy e decisioni sotto pressione

Tempo minimo: 53 min | Quesiti intermedi: 32

05 Eradication, recovery e validation

Tempo minimo: 53 min | Quesiti intermedi: 32

06 Forensic readiness e digital evidence durante l'incidente

Tempo minimo: 53 min | Quesiti intermedi: 32

07 Comunicazione, notifica e crisis leadership

Tempo minimo: 53 min | Quesiti intermedi: 32

08 Post-incident review, lessons learned e resilience improvement

Tempo minimo: 53 min | Quesiti intermedi: 32

6. Contenuti sviluppati modulo per modulo

Le pagine seguenti descrivono in modo analitico i contenuti effettivamente associati a ciascun modulo della piattaforma. La struttura è concepita per consentire a candidato, azienda, HR, Quality, HSE o CISO di comprendere con precisione cosa viene studiato e verificato.

MODULO 01**Incident response governance e preparazione**

- Tempo minimo previsto: 53 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Costruire policy, team, ruoli, reperibilità, escalation, autorità decisionale, playbook, asset context, contatti e dipendenze prima che l'incidente avvenga.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Definire CSIRT operating model, severity criteria, war room, legal/privacy liaison, executive escalation, evidence handling e vendor coordination.

Metodo operativo

Applicare un ciclo strutturato: definire contesto e finalità, stabilire criteri prima della decisione, assegnare responsabilità, eseguire i controlli, raccogliere evidenze e riesaminare il risultato. Nel tema specifico: Definire CSIRT operating model, severity criteria, war room, legal/privacy liaison, executive escalation, evidence handling e vendor coordination.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: IR plan, call tree, RACI, playbooks, contact lists, tabletop results, tooling readiness and evidence procedures.

Decisioni, rischio e proporzionalità

La decisione deve essere proporzionata a criticità, esposizione, impatto, affidabilità delle informazioni e requisiti applicabili. Documentare assunzioni, livello di confidenza, eccezioni e condizioni che richiedono rivalutazione.

Caso applicativo

L'incidente avviene di notte e nessuno sa chi può autorizzare l'isolamento di un sistema critico: correggere governance e decision rights. Separare i fatti dalle ipotesi, indicare i dati mancanti, scegliere l'azione iniziale e definire quale evidenza dimostrerà che la decisione è stata efficace.

Indicatori e weak signals

Un indicatore utile deve avere formula, fonte, frequenza, owner, soglia e decisione associata. Per questo modulo monitorare almeno: Tempo medio di attivazione del team e percentuale playbook testati nell'ultimo ciclo.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Piano non testato; numeri di telefono obsoleti; responsabilità implicite; autorità di containment non definita.

Laboratorio decisionale

Scenario: una condizione cambia improvvisamente (tecnologia, fornitore, requisito, volume, minaccia o responsabilità). Costruire una risposta in cinque passaggi: impatto, criterio, decisione, evidenza, riesame. Applicarla a «Incident response

governance e preparazione”.

Preparazione alla verifica

Prima del test, verificare di saper spiegare il tema senza leggere le slide, motivare una scelta in uno scenario ambiguo, identificare almeno due evidenze indipendenti e distinguere una risposta sostanziale da una puramente documentale.

MODULO 02**Detection, logging e triage**

- Tempo minimo previsto: 53 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Trasformare alert, log, threat intelligence e segnalazioni in eventi valutabili con contesto, priorità e preservazione delle prime evidenze.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Definire data sources, sincronizzazione temporale, triage queue, enrichment, severity, false-positive handling e escalation criteria.

Metodo operativo

Applicare un ciclo strutturato: definire contesto e finalità, stabilire criteri prima della decisione, assegnare responsabilità, eseguire i controlli, raccogliere evidenze e riesaminare il risultato. Nel tema specifico: Definire data sources, sincronizzazione temporale, triage queue, enrichment, severity, false-positive handling e escalation criteria.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: SIEM/EDR evidence, alert history, timestamps, asset criticality, triage notes, source reliability and preserved artefacts.

Decisioni, rischio e proporzionalità

La decisione deve essere proporzionata a criticità, esposizione, impatto, affidabilità delle informazioni e requisiti applicabili. Documentare assunzioni, livello di confidenza, eccezioni e condizioni che richiedono rivalutazione.

Caso applicativo

Un alert EDR sembra benigno ma coincide con account privilegiato e traffico anomalo: evitare chiusura prematura basata su un solo segnale. Separare i fatti dalle ipotesi, indicare i dati mancanti, scegliere l'azione iniziale e definire quale evidenza dimostrerà che la decisione è stata efficace.

Indicatori e weak signals

Un indicatore utile deve avere formula, fonte, frequenza, owner, soglia e decisione associata. Per questo modulo monitorare almeno: MTTD, triage latency, false-positive rate e percentuale alert critici con enrichment completo.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Alert fatigue; orologi non sincronizzati; chiusura senza note; assenza di asset context e threat intelligence.

Laboratorio decisionale

Scenario: una condizione cambia improvvisamente (tecnologia, fornitore, requisito, volume, minaccia o responsabilità). Costruire una risposta in cinque passaggi: impatto, criterio, decisione, evidenza, riesame. Applicarla a «Detection, logging e triage».

Preparazione alla verifica

Prima del test, verificare di saper spiegare il tema senza leggere le slide, motivare una scelta in uno scenario ambiguo, identificare almeno due evidenze indipendenti e distinguere una risposta sostanziale da una puramente documentale.

MODULO 03**Scoping, analysis e incident classification**

- Tempo minimo previsto: 53 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Determinare cosa è successo, quando, quali asset/account/dati sono coinvolti, quale accesso persiste e quale impatto attuale/potenziale deve guidare le decisioni.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Costruire timeline, hypotheses, evidence matrix, blast radius, attacker objectives, confidence level e classification rationale.

Metodo operativo

Applicare un ciclo strutturato: definire contesto e finalità, stabilire criteri prima della decisione, assegnare responsabilità, eseguire i controlli, raccogliere evidenze e riesaminare il risultato. Nel tema specifico: Costruire timeline, hypotheses, evidence matrix, blast radius, attacker objectives, confidence level e classification rationale.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Timeline, IOC, affected asset list, identity evidence, network traces, hypothesis log, confidence and severity decisions.

Decisioni, rischio e proporzionalità

La decisione deve essere proporzionata a criticità, esposizione, impatto, affidabilità delle informazioni e requisiti applicabili. Documentare assunzioni, livello di confidenza, eccezioni e condizioni che richiedono rivalutazione.

Caso applicativo

Un singolo endpoint mostra infostealer ma le credenziali sono riutilizzate su cloud: ampliare scope oltre l'host compromesso. Separare i fatti dalle ipotesi, indicare i dati mancanti, scegliere l'azione iniziale e definire quale evidenza dimostrerà che la decisione è stata efficace.

Indicatori e weak signals

Un indicatore utile deve avere formula, fonte, frequenza, owner, soglia e decisione associata. Per questo modulo monitorare almeno: Tempo per stabilire blast radius con livello di confidenza dichiarato.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Scoping limitato al primo asset; ipotesi confuse con fatti; severity decisa solo dal malware name.

Laboratorio decisionale

Scenario: una condizione cambia improvvisamente (tecnologia, fornitore, requisito, volume, minaccia o responsabilità). Costruire una risposta in cinque passaggi: impatto, criterio, decisione, evidenza, riesame. Applicarla a «Scoping, analysis e incident classification».

Preparazione alla verifica

Prima del test, verificare di saper spiegare il tema senza leggere le slide, motivare una scelta in uno scenario ambiguo, identificare almeno due evidenze indipendenti e distinguere una risposta sostanziale da una puramente documentale.

MODULO 04**Containment strategy e decisioni sotto pressione**

- Tempo minimo previsto: 53 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Bilanciare riduzione del danno, business continuity, preservazione delle evidenze e possibilità di osservare l'attaccante senza aumentare il rischio.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Scegliere containment immediato o graduato, segmentazione, credential reset, isolation, blocks e compensazioni con decision log.

Metodo operativo

Applicare un ciclo strutturato: definire contesto e finalità, stabilire criteri prima della decisione, assegnare responsabilità, eseguire i controlli, raccogliere evidenze e riesaminare il risultato. Nel tema specifico: Scegliere containment immediato o graduato, segmentazione, credential reset, isolation, blocks e compensazioni con decision log.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Containment plan, approvals, actions, timestamp, impact assessment, evidence snapshots and communication records.

Decisioni, rischio e proporzionalità

La decisione deve essere proporzionata a criticità, esposizione, impatto, affidabilità delle informazioni e requisiti applicabili. Documentare assunzioni, livello di confidenza, eccezioni e condizioni che richiedono rivalutazione.

Caso applicativo

Isolare subito un server può fermare produzione e distruggere volatilità utile: decidere in base a rischio, criticità e alternative. Separare i fatti dalle ipotesi, indicare i dati mancanti, scegliere l'azione iniziale e definire quale evidenza dimostrerà che la decisione è stata efficace.

Indicatori e weak signals

Un indicatore utile deve avere formula, fonte, frequenza, owner, soglia e decisione associata. Per questo modulo monitorare almeno: Tempo alla containment efficace e numero di azioni urgenti eseguite senza approvazione prevista.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Containment riflessivo senza impatto analysis; reset password non coordinati; nessuna documentazione delle decisioni.

Laboratorio decisionale

Scenario: una condizione cambia improvvisamente (tecnologia, fornitore, requisito, volume, minaccia o responsabilità). Costruire una risposta in cinque passaggi: impatto, criterio, decisione, evidenza, riesame. Applicarla a «Containment strategy e decisioni sotto pressione».

Preparazione alla verifica

Prima del test, verificare di saper spiegare il tema senza leggere le slide, motivare una scelta in uno scenario ambiguo, identificare almeno due evidenze indipendenti e distinguere una risposta sostanziale da una puramente documentale.

MODULO 05**Eradication, recovery e validation**

- Tempo minimo previsto: 53 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Rimuovere persistence/root cause tecnica, ripristinare servizi da fonti affidabili e validare che l'ambiente sia sicuro prima di dichiarare la normalizzazione.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Definire clean-build criteria, patching, credential rotation, restore, heightened monitoring, staged return and business validation.

Metodo operativo

Applicare un ciclo strutturato: definire contesto e finalità, stabilire criteri prima della decisione, assegnare responsabilità, eseguire i controlli, raccogliere evidenze e riesaminare il risultato. Nel tema specifico: Definire clean-build criteria, patching, credential rotation, restore, heightened monitoring, staged return and business validation.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Rebuild records, patch evidence, credential reset, restore tests, validation checklist, monitoring results and service acceptance.

Decisioni, rischio e proporzionalità

La decisione deve essere proporzionata a criticità, esposizione, impatto, affidabilità delle informazioni e requisiti applicabili. Documentare assunzioni, livello di confidenza, eccezioni e condizioni che richiedono rivalutazione.

Caso applicativo

Ripristinare backup precedente senza eliminare le credenziali rubate può ricreare compromissione: coordinare recovery e eradication. Separare i fatti dalle ipotesi, indicare i dati mancanti, scegliere l'azione iniziale e definire quale evidenza dimostrerà che la decisione è stata efficace.

Indicatori e weak signals

Un indicatore utile deve avere formula, fonte, frequenza, owner, soglia e decisione associata. Per questo modulo monitorare almeno: Tempo di recovery validato e percentuale sistemi ripristinati con control validation completata.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Recovery = "sistema online"; nessuna validation; ritorno simultaneo di tutti i servizi; monitoraggio ridotto troppo presto.

Laboratorio decisionale

Scenario: una condizione cambia improvvisamente (tecnologia, fornitore, requisito, volume, minaccia o responsabilità). Costruire una risposta in cinque passaggi: impatto, criterio, decisione, evidenza, riesame. Applicarla a «Eradication, recovery e validation».

Preparazione alla verifica

Prima del test, verificare di saper spiegare il tema senza leggere le slide, motivare una scelta in uno scenario ambiguo, identificare almeno due evidenze indipendenti e distinguere una risposta sostanziale da una puramente documentale.

MODULO 06**Forensic readiness e digital evidence durante l'incidente**

- Tempo minimo previsto: 53 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Integrare raccolta e preservazione delle evidenze nell'incident response senza rallentare inutilmente il containment, mantenendo tracciabilità e integrità.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Definire priorità di volatilità, imaging/log export, hash, chain of custody, time source, evidence repository e access control.

Metodo operativo

Applicare un ciclo strutturato: definire contesto e finalità, stabilire criteri prima della decisione, assegnare responsabilità, eseguire i controlli, raccogliere evidenze e riesaminare il risultato. Nel tema specifico: Definire priorità di volatilità, imaging/log export, hash, chain of custody, time source, evidence repository e access control.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Acquisition notes, hashes, chain of custody, tool/version records, time source, evidence storage and analyst notes.

Decisioni, rischio e proporzionalità

La decisione deve essere proporzionata a criticità, esposizione, impatto, affidabilità delle informazioni e requisiti applicabili. Documentare assunzioni, livello di confidenza, eccezioni e condizioni che richiedono rivalutazione.

Caso applicativo

Un admin esegue comandi di troubleshooting prima dell'acquisizione: documentare alterazioni e valutare l'affidabilità dell'evidenza residua. Separare i fatti dalle ipotesi, indicare i dati mancanti, scegliere l'azione iniziale e definire quale evidenza dimostrerà che la decisione è stata efficace.

Indicatori e weak signals

Un indicatore utile deve avere formula, fonte, frequenza, owner, soglia e decisione associata. Per questo modulo monitorare almeno: Percentuale incidenti maggiori con evidence pack completo e chain of custody senza gap.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Screenshot al posto di acquisizioni; hash assenti; tool version non registrata; evidenze su share comune modificabile.

Laboratorio decisionale

Scenario: una condizione cambia improvvisamente (tecnologia, fornitore, requisito, volume, minaccia o responsabilità). Costruire una risposta in cinque passaggi: impatto, criterio, decisione, evidenza, riesame. Applicarla a «Forensic readiness e digital evidence durante l'incidente».

Preparazione alla verifica

Prima del test, verificare di saper spiegare il tema senza leggere le slide, motivare una scelta in uno scenario ambiguo, identificare almeno due evidenze indipendenti e distinguere una risposta sostanziale da una puramente documentale.

MODULO 07**Comunicazione, notifica e crisis leadership**

- Tempo minimo previsto: 53 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Coordinare management, legale, privacy, clienti, autorità, assicurazione, fornitori e comunicazione esterna con messaggi coerenti e decisioni tracciate.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Definire audience, owner, approval, facts/unknowns, cadence, notification triggers, spokesperson and secure channels.

Metodo operativo

Applicare un ciclo strutturato: definire contesto e finalità, stabilire criteri prima della decisione, assegnare responsabilità, eseguire i controlli, raccogliere evidenze e riesaminare il risultato. Nel tema specifico: Definire audience, owner, approval, facts/unknowns, cadence, notification triggers, spokesperson and secure channels.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Situation reports, decision log, notification records, stakeholder matrix, approved statements and communication timeline.

Decisioni, rischio e proporzionalità

La decisione deve essere proporzionata a criticità, esposizione, impatto, affidabilità delle informazioni e requisiti applicabili. Documentare assunzioni, livello di confidenza, eccezioni e condizioni che richiedono rivalutazione.

Caso applicativo

Il management vuole comunicare “nessuna esfiltrazione” prima che l'analisi sia conclusa: gestire incertezza senza creare false rassicurazioni. Separare i fatti dalle ipotesi, indicare i dati mancanti, scegliere l'azione iniziale e definire quale evidenza dimostrerà che la decisione è stata efficace.

Indicatori e weak signals

Un indicatore utile deve avere formula, fonte, frequenza, owner, soglia e decisione associata. Per questo modulo monitorare almeno: Tempo di produzione del primo situation report affidabile e numero di messaggi corretti/ritirati per errori.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Messaggi assoluti con dati incompleti; canali non sicuri; notifiche gestite senza coordinamento con timeline tecnica.

Laboratorio decisionale

Scenario: una condizione cambia improvvisamente (tecnologia, fornitore, requisito, volume, minaccia o responsabilità). Costruire una risposta in cinque passaggi: impatto, criterio, decisione, evidenza, riesame. Applicarla a «Comunicazione, notifica e crisis leadership».

Preparazione alla verifica

Prima del test, verificare di saper spiegare il tema senza leggere le slide, motivare una scelta in uno scenario ambiguo, identificare almeno due evidenze indipendenti e distinguere una risposta sostanziale da una puramente documentale.

MODULO 08**Post-incident review, lessons learned e resilience improvement**

- Tempo minimo previsto: 53 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Trasformare incidenti in miglioramento misurabile, distinguendo root cause tecniche, organizzative e di governance e verificando che le azioni riducano il rischio.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Condurre PIR senza blame, costruire causal chain, prioritizzare azioni, aggiornare risk register/playbook/detection e testare l'efficacia.

Metodo operativo

Applicare un ciclo strutturato: definire contesto e finalità, stabilire criteri prima della decisione, assegnare responsabilità, eseguire i controlli, raccogliere evidenze e riesaminare il risultato. Nel tema specifico: Condurre PIR senza blame, costruire causal chain, prioritizzare azioni, aggiornare risk register/playbook/detection e testare l'efficacia.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: PIR report, root-cause analysis, action register, risk updates, control changes, new detection rules and effectiveness tests.

Decisioni, rischio e proporzionalità

La decisione deve essere proporzionata a criticità, esposizione, impatto, affidabilità delle informazioni e requisiti applicabili. Documentare assunzioni, livello di confidenza, eccezioni e condizioni che richiedono rivalutazione.

Caso applicativo

Dopo un ransomware si compra un nuovo tool ma restano identity governance e backup design invariati: valutare se la causa è stata affrontata. Separare i fatti dalle ipotesi, indicare i dati mancanti, scegliere l'azione iniziale e definire quale evidenza dimostrerà che la decisione è stata efficace.

Indicatori e weak signals

Un indicatore utile deve avere formula, fonte, frequenza, owner, soglia e decisione associata. Per questo modulo monitorare almeno: Recurrence rate per causa e percentuale azioni PIR chiuse con verifica di efficacia.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: PIR descrittivo; colpa individuale; azioni senza owner; lessons learned non integrate in rischio, training e test.

Laboratorio decisionale

Scenario: una condizione cambia improvvisamente (tecnologia, fornitore, requisito, volume, minaccia o responsabilità). Costruire una risposta in cinque passaggi: impatto, criterio, decisione, evidenza, riesame. Applicarla a «Post-incident

review, lessons learned e resilience improvement”.

Preparazione alla verifica

Prima del test, verificare di saper spiegare il tema senza leggere le slide, motivare una scelta in uno scenario ambiguo, identificare almeno due evidenze indipendenti e distinguere una risposta sostanziale da una puramente documentale.

7. Sistema di verifica, esame finale e criteri di superamento

- Le verifiche intermedie sono collegate ai singoli moduli e costituiscono un controllo progressivo dell'apprendimento prima dell'accesso alla prova finale.
- La prova finale è composta da 30 quesiti selezionati dalla banca attiva del corso. La piattaforma applica una logica anti-ripetizione per i nuovi tentativi quando la consistenza della banca lo consente.
- Consistenza della banca finale rilevata al momento della generazione: 240 quesiti attivi.
- Soglia di superamento pubblicata per il corso: 75%.
- Le domande sono finalizzate a verificare non soltanto il richiamo mnemonico, ma anche interpretazione, applicazione, selezione delle evidenze, valutazione di scenari e qualità della decisione, in funzione della materia trattata.

8. Tracciamento, continuità didattica e integrità della sessione

- Lo stato del percorso, i moduli completati e il tempo registrato sono gestiti lato server quando il corso utilizza la modalità formativa Academy.
- La piattaforma consente la ripresa del percorso dal punto registrato e conserva gli esiti delle verifiche previste.
- Le sessioni di verifica possono essere soggette ai controlli di integrità e proctoring attivati dalla piattaforma e descritti nelle regole di utilizzo applicabili.
- Gli eventi tecnici e di integrità sono elementi di supporto alla valutazione e non sostituiscono il giudizio professionale quando è prevista una revisione umana.

9. Attestazione, utilizzo e limiti del documento

L'attestato CIWZ, quando previsto dal percorso e richiesto dopo il superamento, documenta il risultato ottenuto nel percorso o nella prova CIWZ indicata. Non sostituisce automaticamente certificazioni di persona, iscrizioni ad albi, abilitazioni professionali, qualifiche legali o credenziali rilasciate da organismi o soggetti terzi quando tali requisiti sono previsti dallo schema applicabile.

10. Condizioni economiche e fiscali

- Corso + attestato: 780,00 € IVA/VAT esclusa.
- La UAE VAT viene applicata ai clienti UAE secondo i dati di fatturazione e la normativa fiscale applicabile.
- Eventuali condizioni commerciali specifiche, convenzioni o ordini aziendali prevalgono sul prezzo pubblico solo se formalmente accettati da Certificato IWZ FZCO.

11. Controllo documentale della scheda

- Documento generato automaticamente dalla CIWZ Academy sulla base dei dati del corso pubblicati al momento della richiesta.
- Codice corso: IR-27035-CYBER
- Lingua documento: IT
- Data di generazione: 13/10/2026
- Per l'applicazione normativa e professionale fanno fede le fonti ufficiali vigenti e le eventuali procedure/schema applicabili.