



DOSSIER TECNICO DIDATTICO E DI VALUTAZIONE

AI Security & Generative AI Risk – Enterprise Security Manager

Corso + attestato

780,00 €

IVA/VAT esclusa

Codice corso

AI-SEC-GENAI

Durata minima

424 min

Soglia finale

75%

Edizione scheda

13/10/2026

1. Identità, finalità e perimetro del percorso

Corso tecnico-manageriale sui rischi di sicurezza dei sistemi AI e GenAI: prompt injection, data leakage, model abuse, poisoning, supply chain, agentic AI, secure architecture, monitoring e governance del rischio.

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

NIST AI RMF 1.0; NIST AI 600-1 GenAI Profile; ISO/IEC 23894:2023; ISO/IEC 5338:2023; ISO/IEC 27001:2022; ISO/IEC 27090 in pubblicazione (riferimento evolutivo); OWASP guidance per LLM/GenAI

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 Threat model per AI e GenAI

Tempo minimo: 53 min | Quesiti intermedi: 32

02 Prompt injection, jailbreak e instruction hierarchy

Tempo minimo: 53 min | Quesiti intermedi: 32

03 Data leakage, privacy e secret protection

Tempo minimo: 53 min | Quesiti intermedi: 32

04 Model, data poisoning e integrity

Tempo minimo: 53 min | Quesiti intermedi: 32

05 RAG, vector database e knowledge security

Tempo minimo: 53 min | Quesiti intermedi: 32

06 Agentic AI, tool use e autonomous actions

Tempo minimo: 53 min | Quesiti intermedi: 32

07 AI supply chain, provider e model security

Tempo minimo: 53 min | Quesiti intermedi: 32

08 AI security testing, monitoring e incident response

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**Threat model per AI e GenAI**

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

Executive briefing

Distinguere asset e trust boundary di dati, prompt, embeddings, modelli, tool, agenti, API, vector store, plugin e sistemi downstream.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Costruire un threat model specifico per AI collegando attori, capacità, attack path, impatto e controlli esistenti.

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 un threat model specifico per AI collegando attori, capacità, attack path, impatto e controlli esistenti.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Architecture diagram, data flow, model inventory, trust-boundary map, misuse cases, attack tree and risk 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 copilota AI ha accesso a knowledge base e ticketing: valutare cosa accade se input non fidati influenzano chiamate a tool. 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 di componenti AI con threat model aggiornato dopo cambi architetturali.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Threat model copiato dal web; nessuna mappa trust boundary; sicurezza limitata al modello ignorando dati e integrazioni.

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 «Threat model per AI e GenAI».

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**Prompt injection, jailbreak e instruction hierarchy**

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

Executive briefing

Comprendere injection diretta/indiretta, jailbreak, conflitti di istruzioni e rischi derivanti da contenuti esterni trattati come istruzioni affidabili.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Separare istruzioni e dati, minimizzare privilegi, validare tool calls, usare content boundaries, policy enforcement e test avversariali.

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: Separare istruzioni e dati, minimizzare privilegi, validare tool calls, usare content boundaries, policy enforcement e test avversariali.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Red-team cases, policy tests, tool-call allowlist, prompt templates, injection telemetry and blocked-action evidence.

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 documento indicizzato contiene istruzioni malevole che il modello esegue durante RAG: progettare difese oltre al semplice filtro input. 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: Tasso di successo dei test injection e percentuale tool call soggette a autorizzazione server-side.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Affidarsi al system prompt; blacklist di frasi; tool con privilegi eccessivi; nessuna validazione dell'output prima dell'azione.

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 «Prompt injection,

jailbreak e instruction hierarchy”.

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**Data leakage, privacy e secret protection**

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

Executive briefing

Gestire rischio di prompt con dati sensibili, retention provider, training su input, embeddings, log, memorization, secret exposure e output inference.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Classificare dati, applicare DLP, minimizzazione, redaction, tenant controls, encryption, access control e policy di utilizzo dei provider.

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: Classificare dati, applicare DLP, minimizzazione, redaction, tenant controls, encryption, access control e policy di utilizzo dei provider.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Data classification, DLP rules, provider configuration, retention settings, access logs, privacy assessment and incident 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

Un dipendente incolla codice proprietario in un chatbot pubblico: gestire prevenzione, detection, risposta e revisione contrattuale. 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: Numero di policy violations su dati sensibili e percentuale flussi AI coperti da DLP/retention controls.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Policy “non inserire segreti” senza enforcement; log contenenti prompt completi; retention sconosciuta; embedding non classificati.

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 «Data leakage,

privacy e secret protection”.

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**Model, data poisoning e integrity**

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

Executive briefing

Proteggere training/fine-tuning data, feedback loop, model artefacts e pipeline da manipolazioni che alterano comportamento, backdoor o performance.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Applicare provenance, integrity checks, trusted sources, quarantine, validation, signed artefacts, controlled retraining e rollback.

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: Applicare provenance, integrity checks, trusted sources, quarantine, validation, signed artefacts, controlled retraining e rollback.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Dataset lineage, approval records, hashes/signatures, retraining logs, validation reports, rollback and anomaly evidence.

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

Feedback utente alimenta retraining automatico e viene manipolato da un gruppo coordinato: ridefinire trust e validation gate. 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 dataset/versioni modello con provenance e integrity verification prima del rilascio.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Retraining automatico senza gate; artefatti non firmati; fonti dati non tracciate; rollback non provato.

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 «Model, data

poisoning e integrity”.

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**RAG, vector database e knowledge security**

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

Executive briefing

Valutare rischi di access control, cross-tenant leakage, malicious documents, stale knowledge, poisoning e over-retrieval nei sistemi RAG.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Eseguire authorization prima e dopo retrieval, segmentare indici, validare ingestion, filtrare metadata, applicare least privilege e source attribution.

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: Eseguire authorization prima e dopo retrieval, segmentare indici, validare ingestion, filtrare metadata, applicare least privilege e source attribution.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Index access rules, ingestion workflow, source provenance, retrieval logs, permission tests and stale-content controls.

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 utente senza accesso al documento ottiene un riassunto tramite RAG: individuare dove l'autorizzazione è stata persa. 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: Tasso di retrieval non autorizzato nei test e percentuale fonti con owner/versione/provenance.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Permessi applicati solo alla UI; indice condiviso; ingestion da fonti non verificate; nessuna gestione dei contenuti scaduti.

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 «RAG, vector

database e knowledge security”.

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**Agentic AI, tool use e autonomous actions**

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

Executive briefing

Gestire rischi quando l'AI pianifica azioni, invoca tool, modifica sistemi, spende denaro o interagisce con account privilegiati.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Applicare least privilege, scoped credentials, approval gates, transaction limits, sandbox, idempotency, deterministic validation e kill switch.

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: Applicare least privilege, scoped credentials, approval gates, transaction limits, sandbox, idempotency, deterministic validation e kill switch.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Tool registry, permission matrix, approval logs, limits, sandbox configuration, transaction evidence and emergency-stop 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

Un agente può aprire ticket, eseguire script e inviare email: definire quali azioni richiedono conferma umana e quali limiti tecnici. 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 azioni ad alto impatto con approval gate e tasso di tool invocation bloccate per policy.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Credenziali condivise; tool generici; nessun limite transazionale; audit log non correlabile alla decisione del modello.

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 «Agentic AI, tool

use e autonomous actions”.

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**AI supply chain, provider e model security**

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

Executive briefing

Governare API provider, open-source model, fine-tuning service, libraries, model hub e dipendenze cloud rispetto a integrità, disponibilità, licensing e change risk.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Fare due diligence, pinning/versioning, artefact verification, contract controls, failover, rate-limit planning e change monitoring.

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: Fare due diligence, pinning/versioning, artefact verification, contract controls, failover, rate-limit planning e change monitoring.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Supplier assessment, model source, signatures/hashes, SBOM/ML-BOM where used, SLA, change notices and fallback 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

Un provider dismette un modello con breve preavviso: valutare business continuity e rischio di migrazione forzata. 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: Quota di componenti AI con versione tracciata, provenance verificata e fallback definito.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Latest version automatica in produzione; modello scaricato senza verifica; dipendenza singola senza exit plan.

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 «AI supply chain, provider e model security».

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**AI security testing, monitoring e incident response**

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

Executive briefing

Integrare red teaming, abuse testing, security regression, telemetry, anomaly detection, incident response e lessons learned per sistemi AI.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Definire test library, release gate, runtime monitoring, abuse signals, incident taxonomy, evidence preservation, rollback e communication plan.

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 test library, release gate, runtime monitoring, abuse signals, incident taxonomy, evidence preservation, rollback e communication plan.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Red-team report, regression results, telemetry dashboards, incident timelines, evidence packs, rollback and corrective actions.

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 jailbreak noto ricompare dopo update del modello: decidere se il problema è test coverage, change management o control effectiveness. 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: Regression escape rate, time to contain AI security incidents and closure rate of red-team findings.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Red team solo prima del go-live; nessun security regression; telemetry di sicurezza assente; incidenti AI non correlati alle versioni.

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 «AI security testing, monitoring e incident response».

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: AI-SEC-GENAI
- 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.