



DOSSIER TECNICO DIDATTICO E DI VALUTAZIONE

Digital & Computer Forensics Investigator – Enterprise DFIR

Corso + attestato

2.800,00 €

IVA/VAT esclusa

Codice corso

DFIR-FORENSICS-PRO

Durata minima

480 min

Soglia finale

75%

Edizione scheda

13/10/2026

1. Identità, finalità e perimetro del percorso

Percorso professionale di computer forensics e digital evidence per analisti DFIR, incident responder, auditor e consulenti: forensic readiness, acquisizione, preservazione, analisi host/network/cloud, timeline, chain of custody, reporting e qualità metodologica.

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 27037:2012 (vigente, in revisione); ISO/IEC 27041:2015; ISO/IEC 27042:2015; ISO/IEC 27043:2015; NIST SP 800-86; ISO/IEC 27035-1:2023; GDPR e normativa nazionale applicabile alla raccolta/trattamento delle evidenze

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: 480 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 Forensic readiness, legal authority e investigation planning

Tempo minimo: 60 min | Quesiti intermedi: 32

02 Identificazione, raccolta, acquisizione e preservazione

Tempo minimo: 60 min | Quesiti intermedi: 32

03 Metodo investigativo, validazione strumenti e repeatability

Tempo minimo: 60 min | Quesiti intermedi: 32

04 File system, artefatti endpoint e memory forensics

Tempo minimo: 60 min | Quesiti intermedi: 32

05 Network, email e cloud forensics

Tempo minimo: 60 min | Quesiti intermedi: 32

06 Timeline analysis, hypothesis testing e attribution discipline

Tempo minimo: 60 min | Quesiti intermedi: 32

07 Malware triage e compromise analysis

Tempo minimo: 60 min | Quesiti intermedi: 32

08 Reporting, expert communication e quality assurance

Tempo minimo: 60 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**Forensic readiness, legal authority e investigation planning**

- Tempo minimo previsto: 60 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Preparare persone, processi, logging, sincronizzazione temporale, strumenti, storage e autorizzazioni affinché un'indagine possa partire rapidamente e produrre evidenze utilizzabili.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Definire scope, authority, objectives, constraints, privacy/legal liaison, evidence sources, preservation priority and investigation 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 scope, authority, objectives, constraints, privacy/legal liaison, evidence sources, preservation priority and investigation plan.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Forensic readiness plan, authorization record, source map, tool list, time reference, retention policy and investigation objectives.

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'indagine interna nasce da sospetto insider ma coinvolge caselle personali e BYOD: chiarire authority, proporzionalità e fonti prima di acquisire. 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 tra autorizzazione e preservazione delle fonti volatili/critiche.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Acquisire prima di definire authority; logging non sincronizzato; strumenti non validati; retention insufficiente rispetto ai tempi di discovery.

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, legal authority e investigation planning».

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**Identificazione, raccolta, acquisizione e preservazione**

- Tempo minimo previsto: 60 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Applicare principi di ISO/IEC 27037 per identificare potenziali evidenze, raccoglierle/acquisirle con metodo appropriato e preservarne integrità e tracciabilità.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Scegliere live vs dead acquisition, priorità di volatilità, write protection, imaging, hashing, labeling, packaging, transport and secure storage.

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 live vs dead acquisition, priorità di volatilità, write protection, imaging, hashing, labeling, packaging, transport and secure storage.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Acquisition worksheet, source identifiers, hash values, tool/version, timestamps, chain of custody and storage 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 laptop cifrato e acceso contiene sessioni cloud attive: bilanciare volatile acquisition, rischio di alterazione e valore dell'accesso corrente. 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 acquisizioni con hash verificato e chain of custody completa al primo controllo.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Spegnerne automaticamente ogni host; nessun hash; etichette ambigue; copie di lavoro create direttamente dall'originale.

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 «Identificazione,

raccolta, acquisizione e preservazione”.

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**Metodo investigativo, validazione strumenti e repeatability**

- Tempo minimo previsto: 60 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Assicurare che metodo e strumenti siano fit for purpose, documentati, validati e utilizzati in modo da consentire scrutinio indipendente, ripetibilità e riproducibilità dove pertinenti.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Definire requirements, known limitations, test dataset, validation record, analyst procedure, quality review and alternative verification methods.

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 requirements, known limitations, test dataset, validation record, analyst procedure, quality review and alternative verification methods.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Tool validation record, version/hash, configuration, known limitations, test results, peer review and method 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

Due tool producono timestamp diversi sullo stesso artefatto: identificare timezone/parse assumptions e verificare con fonte indipendente. 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 strumenti critici con validazione aggiornata e finding analitici sottoposti a peer review.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Fiducia nel brand del tool; aggiornamenti senza revalidation; screenshot come unica evidenza; procedure non versionate.

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 «Metodo investigativo, validazione strumenti e repeatability».

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**File system, artefatti endpoint e memory forensics**

- Tempo minimo previsto: 60 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Interpretare filesystem, metadata, registry/configuration, event logs, browser, execution artefacts, persistence, deleted data e memoria volatile in relazione all'ipotesi investigativa.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Correlare più artefatti, gestire timestamp, file carving, process/network memory evidence, user activity and anti-forensics indicators.

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: Correlare più artefatti, gestire timestamp, file carving, process/network memory evidence, user activity and anti-forensics indicators.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Timeline sources, parsed artefacts, memory image, process tree, persistence evidence, deleted-file recovery 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 file malevolo non esiste più ma rimangono execution artefacts, network connections e persistence: costruire una conclusione senza sovrainterpretare. 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 medio di fonti indipendenti a supporto di un finding critico.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Conclusioni da un singolo artefatto; timezone ignorata; metadata trattati come prova assoluta; memory acquisition effettuata troppo tardi.

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 «File system,

artefatti endpoint e memory forensics”.

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**Network, email e cloud forensics**

- Tempo minimo previsto: 60 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Analizzare packet/log/flow, DNS, proxy, VPN, email headers, identity provider, SaaS/cloud audit e API evidence considerando retention e shared-responsibility.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Preservare log rapidamente, correlare identity/network/cloud, verificare source reliability, tenant context, timestamps and provider limitations.

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: Preservare log rapidamente, correlare identity/network/cloud, verificare source reliability, tenant context, timestamps and provider limitations.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: PCAP/flow, DNS/proxy logs, mail trace, IdP audit, cloud activity logs, provider export metadata and retention 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

L'account compromesso usa token validi senza login interattivo: ricostruire sessione cloud e source IP senza affidarsi ai soli sign-in event. 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: Copertura temporale delle fonti e percentuale incidenti con log critici preservati prima della scadenza retention.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Scaricare log senza metadata di export; confondere NAT/proxy con utente; ignorare service principal e token refresh.

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 «Network, email e cloud forensics».

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**Timeline analysis, hypothesis testing e attribution discipline**

- Tempo minimo previsto: 60 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Costruire super-timeline, separare fatti da inferenze, usare livelli di confidenza e testare ipotesi alternative per evitare bias investigativi.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Normalizzare timezone, correlare fonti, registrare hypothesis/evidence, cercare disconfirming evidence and document uncertainty.

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: Normalizzare timezone, correlare fonti, registrare hypothesis/evidence, cercare disconfirming evidence and document uncertainty.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Normalized timeline, evidence matrix, hypothesis log, confidence ratings, alternative explanations and peer-review comments.

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

Una sequenza sembra mostrare esfiltrazione ma il traffico coincide con backup schedato: testare ipotesi alternativa prima di concludere. 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 finding critici con fonte indipendente e confidence statement esplicito.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Narrativa costruita troppo presto; confirmation bias; timestamp non normalizzati; attribution personale basata su username.

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 «Timeline analysis, hypothesis testing e attribution discipline».

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**Malware triage e compromise analysis**

- Tempo minimo previsto: 60 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Eseguire triage statico/dinamico proporzionato e collegare IOC, comportamento, persistence, credential access e command-and-control all'indagine senza trasformare il corso in reverse engineering specialistico.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Usare hashing, strings/metadata, sandbox, YARA/IOC where appropriate, behaviour timeline and containment implications, preserving samples securely.

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: Usare hashing, strings/metadata, sandbox, YARA/IOC where appropriate, behaviour timeline and containment implications, preserving samples securely.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Sample hash, source, sandbox report, behaviour indicators, network IOC, persistence evidence and secure-sample handling log.

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 sample è classificato come commodity malware ma usa persistence custom: valutare se il label del vendor descrive davvero il caso. 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 da sample collection a IOC actionable verificato e distribuito.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Caricare sample sensibili su servizi pubblici senza autorizzazione; fidarsi del nome antivirus; IOC senza scadenza/contesto.

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 «Malware triage e

compromise analysis”.

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**Reporting, expert communication e quality assurance**

- Tempo minimo previsto: 60 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Produrre report che distinguano evidenze, metodo, risultati, limitazioni, inferenze e conclusioni, comprensibili a management, legali e tecnici e sottoponibili a scrutinio.

Obiettivi professionali

Al termine del modulo il partecipante deve saper trasformare il tema in decisioni, controlli e verifiche. Focus operativo: Usare struttura ripetibile, source reference, confidence, exhibits, peer review, versioning and secure distribution; evitare linguaggio assoluto oltre l'evidenza.

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: Usare struttura ripetibile, source reference, confidence, exhibits, peer review, versioning and secure distribution; evitare linguaggio assoluto oltre l'evidenza.

Evidenze e auditabilità

La qualità professionale si dimostra con evidenze coerenti e ricostruibili, non con la sola esistenza di procedure. Evidenze chiave: Final report, executive summary, evidence index, exhibits, method annex, limitation statement, peer-review record and distribution log.

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'analista sa che un utente "probabilmente" ha eseguito un'azione ma l'evidenza prova solo l'account: formulare conclusione proporzionata. 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 report critici peer-reviewed e numero di correzioni post-emissione per errori metodologici.

Errori ricorrenti

Evitare approcci meramente formali. Criticità tipiche: Conclusioni senza source reference; limitazioni omesse; linguaggio certo su inferenze; report tecnici incomprensibili al decisore.

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 «Reporting, expert communication e quality assurance».

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: 2.800,00 € 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: DFIR-FORENSICS-PRO
- 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.