



DOSSIER TECNICO DIDATTICO E DI VALUTAZIONE

ISO/IEC 27035 – Incident Management & Recovery

Corso + attestato

800,00 €

IVA/VAT esclusa

Codice corso

ISO27035-IMR

Durata minima

480 min

Soglia finale

70%

Edizione scheda

13/10/2026

1. Identità, finalità e perimetro del percorso

Percorso avanzato bilingue sulla gestione degli incidenti di sicurezza delle informazioni: preparazione, rilevazione, triage, analisi, contenimento, eradicazione, ripristino, coordinamento e lezioni apprese secondo la famiglia ISO/IEC 27035.

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; riferimenti di integrazione ISO/IEC 27001:2022 + Amd 1:2024 e ISO/IEC 27002:2022

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

- 10 moduli didattici strutturati
- tempo minimo tracciato: 480 min
- banca verifiche intermedie: 240 quesiti
- banca esame finale attiva: 180 quesiti
- esame finale: 30 quesiti selezionati dalla banca
- soglia di superamento: 70%
- 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 specialistico bilingue su ISO/IEC 27035 con 10 capitoli slide-based, 480 minuti minimi tracciati lato server, 24 quesiti intermedi per capitolo, 180 quesiti finali anti-ripetizione, scenari di triage, investigazione, containment, eradication, recovery, coordinamento e lessons learned.

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 Fondamenti, principi e ciclo di gestione dell'incidente

Tempo minimo: 45 min | Quesiti intermedi: 24

02 Governance, preparazione e capacità di risposta

Tempo minimo: 50 min | Quesiti intermedi: 24

03 Rilevazione, segnalazione e qualità delle informazioni iniziali

Tempo minimo: 45 min | Quesiti intermedi: 24

04 Triage, classificazione, severità e decisione

Tempo minimo: 50 min | Quesiti intermedi: 24

05 Analisi tecnica, investigazione ed evidenze

Tempo minimo: 55 min | Quesiti intermedi: 24

06 Risposta: contenimento, eradicazione e controllo del rischio

Tempo minimo: 55 min | Quesiti intermedi: 24

07 Recovery, ripristino controllato e ritorno alla normalità

Tempo minimo: 55 min | Quesiti intermedi: 24

08 Comunicazione, obblighi e coordinamento tra organizzazioni

Tempo minimo: 45 min | Quesiti intermedi: 24

09 Lezioni apprese, metriche, esercitazioni e miglioramento

Tempo minimo: 40 min | Quesiti intermedi: 24

10 Major incident simulation, recovery readiness e auditabilità

Tempo minimo: 40 min | Quesiti intermedi: 24

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**Fondamenti, principi e ciclo di gestione dell'incidente**

- Tempo minimo previsto: 45 min
- Banca di verifica intermedia disponibile: 24 quesiti

1. Obiettivo operativo del capitolo

Il percorso distingue evento, evento di sicurezza, incidente e crisi operativa, chiarendo finalità, confini e interazioni del processo di incident management. La gestione dell'incidente è un ciclo governato: preparare, rilevare e segnalare, valutare e decidere, rispondere, apprendere.

L'obiettivo è saper prendere decisioni sotto pressione mantenendo tracciabilità, proporzionalità e continuità tra processo di sicurezza, esigenze del business ed evidenze disponibili.

- Collega il tema alla fase corretta del ciclo di incident management.
- Distingui fatti, ipotesi, decisioni e risultati.
- Individua quali informazioni sono indispensabili prima di agire.

2. Collocazione nella famiglia ISO/IEC 27035

Il tema «Fondamenti, principi e ciclo di gestione dell'incidente» va letto nel quadro della famiglia ISO/IEC 27035: Parte 1 per principi e processo, Parte 2 per preparazione e lessons learned, Parte 3 per le operazioni di risposta ICT e Parte 4 per il coordinamento tra organizzazioni.

Il corso usa questi riferimenti come architettura operativa e li integra con il sistema di gestione della sicurezza delle informazioni.

- Non trattare la risposta come un'attività isolata del SOC.
- Mantieni chiari gli handover tra governance, team tecnico, business e soggetti esterni.
- Riesamina il processo quando cambiano rischi, tecnologia o dipendenze.

3. Processo operativo e criteri di decisione

Definire tassonomia, criteri di attivazione, responsabilità, autorità e interfacce con ISMS, risk management, business continuity, service management e crisis management.

Un buon processo definisce trigger, input minimi, livelli di autorità, criteri di escalation e condizioni di uscita. Nei momenti critici la decisione deve essere veloce ma ricostruibile.

- Definisci chi decide e su quale base.
- Stabilisci cosa deve essere registrato prima e dopo l'azione.
- Prevedi eccezioni controllate per scenari ad alta urgenza.
- Associa ogni azione a un criterio di successo verificabile.

4. Persone, ruoli e handover

IMT, IRT, SOC, IT operations, DPO/privacy, legale, comunicazione, continuità operativa e business owner possono avere ruoli diversi. La qualità dell'handover è spesso il vero punto debole.

Chiarezza non significa burocratizzare: significa sapere chi ha autorità per isolare, notificare, ripristinare, comunicare

e accettare il rischio residuo.

- RACI o matrice equivalente.
- Reperibilità e sostituzioni.
- Canali sicuri alternativi.
- Escalation tecnica e manageriale.
- Responsabilità nelle decisioni di recovery.

5. Evidenze e timeline

Politica, modello di processo, matrice ruoli, criteri di classificazione, workflow di escalation, registro eventi e collegamenti con rischio e continuità.

La timeline deve consentire di comprendere cosa si sapeva in ogni momento e perché una determinata decisione è stata presa. Evita ricostruzioni retroattive che confondono informazioni note all'epoca con informazioni scoperte successivamente.

- Timestamp sincronizzati.
- Fonte e affidabilità del dato.
- Decisione, owner e motivazione.
- Effetti dell'azione.
- Evidenze preservate prima di modificare il sistema quando pertinente.

6. Scenario applicativo

Un'anomalia viene chiusa come guasto tecnico, ma coinvolge credenziali privilegiate e dati sensibili. Il punto critico è riconoscere quando un evento diventa incidente e attivare il processo appropriato.

Analizza lo scenario separando prima i fatti dalle supposizioni. Poi indica l'obiettivo immediato, il rischio che vuoi limitare, l'azione proporzionata e l'evidenza che ti farà decidere se proseguire, cambiare strategia o fare rollback.

- Qual è il primo fatto verificabile?
- Quale decisione non può essere rinviata?
- Quale evidenza rischi di perdere agendo troppo presto?
- Quale funzione deve essere coinvolta prima del passo successivo?

7. Errori ricorrenti da evitare

Gli incidenti vengono spesso gestiti male non per assenza di strumenti, ma per decisioni non coordinate: severity definita troppo presto, contenimento senza valutare l'impatto, ripristino prima dell'eradicazione, comunicazioni incoerenti o chiusura senza verifica dell'efficacia.

Un processo maturo rende visibili questi errori e li trasforma in criteri di prevenzione.

- Non confondere "servizio ripristinato" con "incidente risolto".
- Non usare una sola fonte per confermare la portata.
- Non cancellare evidenze durante la remediation senza una decisione consapevole.
- Non chiudere l'incidente senza definire follow-up e owner.

8. Recovery e resilienza

Qualunque sia il tema del capitolo, la prospettiva di recovery deve essere considerata fin dall'inizio. Le decisioni di contenimento e analisi possono aumentare o ridurre il tempo di ripristino, mentre un recovery troppo rapido può reintrodurre compromissione o perdita di dati.

Recovery readiness significa avere criteri di go/no-go, baseline affidabili, backup testati, dipendenze note e monitoraggio rafforzato dopo il ritorno in servizio.

- Verifica prerequisiti di restore.
- Conferma integrità di configurazioni, credenziali e dati.
- Definisci un periodo di osservazione.
- Mantieni un piano di rollback.

9. Metriche e indicatori utili

Le metriche devono sostenere decisioni, non premiare la velocità a scapito della qualità. MTTD, MTTA e MTTR sono utili solo se letti insieme a severità, ricorrenza, incidenti riaperti, copertura di rilevazione e qualità del recovery.

Una metrica apparentemente positiva può nascondere sotto-segnalazione o chiusure premature.

- Tempo di rilevazione con distribuzione per severità.
- Tempo di contenimento e tempo di ripristino separati.
- Incidenti riaperti o ricorrenti.
- Azioni post-incident scadute.
- Esiti delle esercitazioni e gap ripetuti.

10. Audit e riesame della capacità

Un audit efficace segue un incidente o una simulazione dalla prima evidenza alla chiusura: trigger, classificazione, decisioni, azioni, recovery e lezioni apprese. L'obiettivo non è verificare che esista un piano, ma che la capacità funzioni in condizioni realistiche.

Campiona casi diversi per severità, tecnologia, sede e presenza di terze parti.

- Confronta playbook e comportamento reale.
- Verifica tempi e qualità degli handover.
- Cerca evidenza dell'efficacia delle azioni correttive.
- Valuta se i criteri sono stati applicati in modo coerente.

11. Decision lab

Immagina di ricevere nuove informazioni che cambiano la valutazione iniziale: un account privilegiato, un secondo tenant coinvolto, un backup sospetto o una notifica esterna. Decidi cosa deve essere riclassificato e quale azione diventa prioritaria.

La maturità si vede nella capacità di cambiare decisione senza perdere controllo e tracciabilità.

- Nuovo fatto.
- Impatto sulla severità.
- Decisione rivista.
- Autorizzazione necessaria.

- Evidenza da raccogliere.
- Effetto atteso e verifica.

12. Sintesi e preparazione al minitest

Per superare la verifica devi saper applicare «Fondamenti, principi e ciclo di gestione dell'incidente» a scenari nuovi. Le domande non premiano la memorizzazione di formule, ma la capacità di scegliere l'azione più difendibile sulla base di criteri, evidenze e rischio.

Prima del test prova a spiegare come il tema influenza detection, decisione, risposta, recovery e miglioramento.

- Individua il criterio prima dell'azione.
- Separa remediation, recovery e chiusura.
- Cerca almeno due fonti indipendenti per le decisioni rilevanti.
- Verifica sempre l'efficacia dopo l'azione.

MODULO 02**Governance, preparazione e capacità di risposta**

- Tempo minimo previsto: 50 min
- Banca di verifica intermedia disponibile: 24 quesiti

1. Obiettivo operativo del capitolo

La preparazione rende possibile una risposta coerente sotto pressione. Comprende commitment, policy, piani, playbook, team, competenze, contatti, strumenti, comunicazioni e prove periodiche. La capacità va progettata prima dell'incidente, non durante.

L'obiettivo è saper prendere decisioni sotto pressione mantenendo tracciabilità, proporzionalità e continuità tra processo di sicurezza, esigenze del business ed evidenze disponibili.

- Collega il tema alla fase corretta del ciclo di incident management.
- Distingui fatti, ipotesi, decisioni e risultati.
- Individua quali informazioni sono indispensabili prima di agire.

2. Collocazione nella famiglia ISO/IEC 27035

Il tema «Governance, preparazione e capacità di risposta» va letto nel quadro della famiglia ISO/IEC 27035: Parte 1 per principi e processo, Parte 2 per preparazione e lessons learned, Parte 3 per le operazioni di risposta ICT e Parte 4 per il coordinamento tra organizzazioni.

Il corso usa questi riferimenti come architettura operativa e li integra con il sistema di gestione della sicurezza delle informazioni.

- Non trattare la risposta come un'attività isolata del SOC.
- Mantieni chiari gli handover tra governance, team tecnico, business e soggetti esterni.
- Riesamina il processo quando cambiano rischi, tecnologia o dipendenze.

3. Processo operativo e criteri di decisione

Costruire Incident Management Team e Incident Response Team, definire reperibilità, livelli di autorità, playbook, canali sicuri, fornitori, rapporti con autorità e criteri di mobilitazione.

Un buon processo definisce trigger, input minimi, livelli di autorità, criteri di escalation e condizioni di uscita. Nei momenti critici la decisione deve essere veloce ma ricostruibile.

- Definisci chi decide e su quale base.
- Stabilisci cosa deve essere registrato prima e dopo l'azione.
- Prevedi eccezioni controllate per scenari ad alta urgenza.
- Associa ogni azione a un criterio di successo verificabile.

4. Persone, ruoli e handover

IMT, IRT, SOC, IT operations, DPO/privacy, legale, comunicazione, continuità operativa e business owner possono avere ruoli diversi. La qualità dell'handover è spesso il vero punto debole.

Chiarezza non significa burocratizzare: significa sapere chi ha autorità per isolare, notificare, ripristinare, comunicare

e accettare il rischio residuo.

- RACI o matrice equivalente.
- Reperibilità e sostituzioni.
- Canali sicuri alternativi.
- Escalation tecnica e manageriale.
- Responsabilità nelle decisioni di recovery.

5. Evidenze e timeline

Roster aggiornato, matrice RACI, call tree, runbook, inventario strumenti, accordi con terze parti, esercitazioni e registri di formazione con verifica dell'efficacia.

La timeline deve consentire di comprendere cosa si sapeva in ogni momento e perché una determinata decisione è stata presa. Evita ricostruzioni retroattive che confondono informazioni note all'epoca con informazioni scoperte successivamente.

- Timestamp sincronizzati.
- Fonte e affidabilità del dato.
- Decisione, owner e motivazione.
- Effetti dell'azione.
- Evidenze preservate prima di modificare il sistema quando pertinente.

6. Scenario applicativo

Un ransomware colpisce nel fine settimana e nessuno sa chi può autorizzare lo shutdown di un sistema produttivo. La lacuna non è tecnica: è un difetto di preparazione e autorità.

Analizza lo scenario separando prima i fatti dalle supposizioni. Poi indica l'obiettivo immediato, il rischio che vuoi limitare, l'azione proporzionata e l'evidenza che ti farà decidere se proseguire, cambiare strategia o fare rollback.

- Qual è il primo fatto verificabile?
- Quale decisione non può essere rinviata?
- Quale evidenza rischi di perdere agendo troppo presto?
- Quale funzione deve essere coinvolta prima del passo successivo?

7. Errori ricorrenti da evitare

Gli incidenti vengono spesso gestiti male non per assenza di strumenti, ma per decisioni non coordinate: severity definita troppo presto, contenimento senza valutare l'impatto, ripristino prima dell'eradicazione, comunicazioni incoerenti o chiusura senza verifica dell'efficacia.

Un processo maturo rende visibili questi errori e li trasforma in criteri di prevenzione.

- Non confondere “servizio ripristinato” con “incidente risolto”.
- Non usare una sola fonte per confermare la portata.
- Non cancellare evidenze durante la remediation senza una decisione consapevole.
- Non chiudere l'incidente senza definire follow-up e owner.

8. Recovery e resilienza

Qualunque sia il tema del capitolo, la prospettiva di recovery deve essere considerata fin dall'inizio. Le decisioni di contenimento e analisi possono aumentare o ridurre il tempo di ripristino, mentre un recovery troppo rapido può reintrodurre compromissione o perdita di dati.

Recovery readiness significa avere criteri di go/no-go, baseline affidabili, backup testati, dipendenze note e monitoraggio rafforzato dopo il ritorno in servizio.

- Verifica prerequisiti di restore.
- Conferma integrità di configurazioni, credenziali e dati.
- Definisci un periodo di osservazione.
- Mantieni un piano di rollback.

9. Metriche e indicatori utili

Le metriche devono sostenere decisioni, non premiare la velocità a scapito della qualità. MTTD, MTTA e MTTR sono utili solo se letti insieme a severità, ricorrenza, incidenti riaperti, copertura di rilevazione e qualità del recovery.

Una metrica apparentemente positiva può nascondere sotto-segnalazione o chiusure premature.

- Tempo di rilevazione con distribuzione per severità.
- Tempo di contenimento e tempo di ripristino separati.
- Incidenti riaperti o ricorrenti.
- Azioni post-incident scadute.
- Esiti delle esercitazioni e gap ripetuti.

10. Audit e riesame della capacità

Un audit efficace segue un incidente o una simulazione dalla prima evidenza alla chiusura: trigger, classificazione, decisioni, azioni, recovery e lezioni apprese. L'obiettivo non è verificare che esista un piano, ma che la capacità funzioni in condizioni realistiche.

Campiona casi diversi per severità, tecnologia, sede e presenza di terze parti.

- Confronta playbook e comportamento reale.
- Verifica tempi e qualità degli handover.
- Cerca evidenza dell'efficacia delle azioni correttive.
- Valuta se i criteri sono stati applicati in modo coerente.

11. Decision lab

Immagina di ricevere nuove informazioni che cambiano la valutazione iniziale: un account privilegiato, un secondo tenant coinvolto, un backup sospetto o una notifica esterna. Decidi cosa deve essere riclassificato e quale azione diventa prioritaria.

La maturità si vede nella capacità di cambiare decisione senza perdere controllo e tracciabilità.

- Nuovo fatto.
- Impatto sulla severità.
- Decisione rivista.
- Autorizzazione necessaria.

- Evidenza da raccogliere.
- Effetto atteso e verifica.

12. Sintesi e preparazione al minitest

Per superare la verifica devi saper applicare «Governance, preparazione e capacità di risposta» a scenari nuovi. Le domande non premiano la memorizzazione di formule, ma la capacità di scegliere l'azione più difendibile sulla base di criteri, evidenze e rischio.

Prima del test prova a spiegare come il tema influenza detection, decisione, risposta, recovery e miglioramento.

- Individua il criterio prima dell'azione.
- Separa remediation, recovery e chiusura.
- Cerca almeno due fonti indipendenti per le decisioni rilevanti.
- Verifica sempre l'efficacia dopo l'azione.

MODULO 03**Rilevazione, segnalazione e qualità delle informazioni iniziali**

- Tempo minimo previsto: 45 min
- Banca di verifica intermedia disponibile: 24 quesiti

1. Obiettivo operativo del capitolo

Un incidente ben gestito parte da segnali raccolti, correlati e segnalati rapidamente. Fonti diverse — persone, log, EDR, SIEM, rete, cloud, fornitori, clienti — possono mostrare parti differenti dello stesso fenomeno.

L'obiettivo è saper prendere decisioni sotto pressione mantenendo tracciabilità, proporzionalità e continuità tra processo di sicurezza, esigenze del business ed evidenze disponibili.

- Collega il tema alla fase corretta del ciclo di incident management.
- Distingui fatti, ipotesi, decisioni e risultati.
- Individua quali informazioni sono indispensabili prima di agire.

2. Collocazione nella famiglia ISO/IEC 27035

Il tema «Rilevazione, segnalazione e qualità delle informazioni iniziali» va letto nel quadro della famiglia ISO/IEC 27035: Parte 1 per principi e processo, Parte 2 per preparazione e lessons learned, Parte 3 per le operazioni di risposta ICT e Parte 4 per il coordinamento tra organizzazioni.

Il corso usa questi riferimenti come architettura operativa e li integra con il sistema di gestione della sicurezza delle informazioni.

- Non trattare la risposta come un'attività isolata del SOC.
- Mantieni chiari gli handover tra governance, team tecnico, business e soggetti esterni.
- Riesamina il processo quando cambiano rischi, tecnologia o dipendenze.

3. Processo operativo e criteri di decisione

Definire canali di segnalazione, informazioni minime, priorità iniziale, sincronizzazione temporale, preservazione dei log e criteri per distinguere rumore, falso positivo, evento e incidente.

Un buon processo definisce trigger, input minimi, livelli di autorità, criteri di escalation e condizioni di uscita. Nei momenti critici la decisione deve essere veloce ma ricostruibile.

- Definisci chi decide e su quale base.
- Stabilisci cosa deve essere registrato prima e dopo l'azione.
- Prevedi eccezioni controllate per scenari ad alta urgenza.
- Associa ogni azione a un criterio di successo verificabile.

4. Persone, ruoli e handover

IMT, IRT, SOC, IT operations, DPO/privacy, legale, comunicazione, continuità operativa e business owner possono avere ruoli diversi. La qualità dell'handover è spesso il vero punto debole.

Chiarezza non significa burocratizzare: significa sapere chi ha autorità per isolare, notificare, ripristinare, comunicare e accettare il rischio residuo.

- RACI o matrice equivalente.
- Reperibilità e sostituzioni.
- Canali sicuri alternativi.
- Escalation tecnica e manageriale.
- Responsabilità nelle decisioni di recovery.

5. Evidenze e timeline

Ticket, timestamp affidabili, log originali, alert correlati, fonte, asset coinvolti, account, indicatori tecnici, primo impatto e catena di escalation.

La timeline deve consentire di comprendere cosa si sapeva in ogni momento e perché una determinata decisione è stata presa. Evita ricostruzioni retroattive che confondono informazioni note all'epoca con informazioni scoperte successivamente.

- Timestamp sincronizzati.
- Fonte e affidabilità del dato.
- Decisione, owner e motivazione.
- Effetti dell'azione.
- Evidenze preservate prima di modificare il sistema quando pertinente.

6. Scenario applicativo

Il SIEM genera molti alert di autenticazione anomala e uno viene ignorato perché simile ai precedenti. Poco dopo emerge accesso a un repository critico: servono correlazione e qualità della prima valutazione.

Analizza lo scenario separando prima i fatti dalle supposizioni. Poi indica l'obiettivo immediato, il rischio che vuoi limitare, l'azione proporzionata e l'evidenza che ti farà decidere se proseguire, cambiare strategia o fare rollback.

- Qual è il primo fatto verificabile?
- Quale decisione non può essere rinviata?
- Quale evidenza rischi di perdere agendo troppo presto?
- Quale funzione deve essere coinvolta prima del passo successivo?

7. Errori ricorrenti da evitare

Gli incidenti vengono spesso gestiti male non per assenza di strumenti, ma per decisioni non coordinate: severity definita troppo presto, contenimento senza valutare l'impatto, ripristino prima dell'eradicazione, comunicazioni incoerenti o chiusura senza verifica dell'efficacia.

Un processo maturo rende visibili questi errori e li trasforma in criteri di prevenzione.

- Non confondere "servizio ripristinato" con "incidente risolto".
- Non usare una sola fonte per confermare la portata.
- Non cancellare evidenze durante la remediation senza una decisione consapevole.
- Non chiudere l'incidente senza definire follow-up e owner.

8. Recovery e resilienza

Qualunque sia il tema del capitolo, la prospettiva di recovery deve essere considerata fin dall'inizio. Le decisioni di contenimento e analisi possono aumentare o ridurre il tempo di ripristino, mentre un recovery troppo rapido può

reintrodurre compromissione o perdita di dati.

Recovery readiness significa avere criteri di go/no-go, baseline affidabili, backup testati, dipendenze note e monitoraggio rafforzato dopo il ritorno in servizio.

- Verifica prerequisiti di restore.
- Conferma integrità di configurazioni, credenziali e dati.
- Definisci un periodo di osservazione.
- Mantieni un piano di rollback.

9. Metriche e indicatori utili

Le metriche devono sostenere decisioni, non premiare la velocità a scapito della qualità. MTDD, MTTA e MTTR sono utili solo se letti insieme a severità, ricorrenza, incidenti riaperti, copertura di rilevazione e qualità del recovery.

Una metrica apparentemente positiva può nascondere sotto-segnalazione o chiusure premature.

- Tempo di rilevazione con distribuzione per severità.
- Tempo di contenimento e tempo di ripristino separati.
- Incidenti riaperti o ricorrenti.
- Azioni post-incident scadute.
- Esiti delle esercitazioni e gap ripetuti.

10. Audit e riesame della capacità

Un audit efficace segue un incidente o una simulazione dalla prima evidenza alla chiusura: trigger, classificazione, decisioni, azioni, recovery e lezioni apprese. L'obiettivo non è verificare che esista un piano, ma che la capacità funzioni in condizioni realistiche.

Campiona casi diversi per severità, tecnologia, sede e presenza di terze parti.

- Confronta playbook e comportamento reale.
- Verifica tempi e qualità degli handover.
- Cerca evidenza dell'efficacia delle azioni correttive.
- Valuta se i criteri sono stati applicati in modo coerente.

11. Decision lab

Immagina di ricevere nuove informazioni che cambiano la valutazione iniziale: un account privilegiato, un secondo tenant coinvolto, un backup sospetto o una notifica esterna. Decidi cosa deve essere riclassificato e quale azione diventa prioritaria.

La maturità si vede nella capacità di cambiare decisione senza perdere controllo e tracciabilità.

- Nuovo fatto.
- Impatto sulla severità.
- Decisione rivista.
- Autorizzazione necessaria.
- Evidenza da raccogliere.
- Effetto atteso e verifica.

12. Sintesi e preparazione al minitest

Per superare la verifica devi saper applicare «Rilevazione, segnalazione e qualità delle informazioni iniziali» a scenari nuovi. Le domande non premiano la memorizzazione di formule, ma la capacità di scegliere l'azione più difendibile sulla base di criteri, evidenze e rischio.

Prima del test prova a spiegare come il tema influenza detection, decisione, risposta, recovery e miglioramento.

- Individua il criterio prima dell'azione.
- Separa remediation, recovery e chiusura.
- Cerca almeno due fonti indipendenti per le decisioni rilevanti.
- Verifica sempre l'efficacia dopo l'azione.

MODULO 04**Triage, classificazione, severità e decisione**

- Tempo minimo previsto: 50 min
- Banca di verifica intermedia disponibile: 24 quesiti

1. Obiettivo operativo del capitolo

Il triage trasforma una segnalazione in una decisione operativa. Severità e priorità non coincidono automaticamente: occorre considerare impatto, urgenza, asset, dati, diffusione, persistenza, capacità dell'attaccante, requisiti legali e dipendenze.

L'obiettivo è saper prendere decisioni sotto pressione mantenendo tracciabilità, proporzionalità e continuità tra processo di sicurezza, esigenze del business ed evidenze disponibili.

- Collega il tema alla fase corretta del ciclo di incident management.
- Distingui fatti, ipotesi, decisioni e risultati.
- Individua quali informazioni sono indispensabili prima di agire.

2. Collocazione nella famiglia ISO/IEC 27035

Il tema «Triage, classificazione, severità e decisione» va letto nel quadro della famiglia ISO/IEC 27035: Parte 1 per principi e processo, Parte 2 per preparazione e lessons learned, Parte 3 per le operazioni di risposta ICT e Parte 4 per il coordinamento tra organizzazioni.

Il corso usa questi riferimenti come architettura operativa e li integra con il sistema di gestione della sicurezza delle informazioni.

- Non trattare la risposta come un'attività isolata del SOC.
- Mantieni chiari gli handover tra governance, team tecnico, business e soggetti esterni.
- Riesamina il processo quando cambiano rischi, tecnologia o dipendenze.

3. Processo operativo e criteri di decisione

Applicare criteri ripetibili, determinare il livello di risposta, stabilire escalation e obiettivi immediati, mantenendo la possibilità di riclassificare quando emergono nuove evidenze.

Un buon processo definisce trigger, input minimi, livelli di autorità, criteri di escalation e condizioni di uscita. Nei momenti critici la decisione deve essere veloce ma ricostruibile.

- Definisci chi decide e su quale base.
- Stabilisci cosa deve essere registrato prima e dopo l'azione.
- Prevedi eccezioni controllate per scenari ad alta urgenza.
- Associa ogni azione a un criterio di successo verificabile.

4. Persone, ruoli e handover

IMT, IRT, SOC, IT operations, DPO/privacy, legale, comunicazione, continuità operativa e business owner possono avere ruoli diversi. La qualità dell'handover è spesso il vero punto debole.

Chiarezza non significa burocratizzare: significa sapere chi ha autorità per isolare, notificare, ripristinare, comunicare

e accettare il rischio residuo.

- RACI o matrice equivalente.
- Reperibilità e sostituzioni.
- Canali sicuri alternativi.
- Escalation tecnica e manageriale.
- Responsabilità nelle decisioni di recovery.

5. Evidenze e timeline

Matrice severità, criteri di business impact, classificazione del dato, dipendenze, decision log, motivazione della priorità e timestamp delle riclassificazioni.

La timeline deve consentire di comprendere cosa si sapeva in ogni momento e perché una determinata decisione è stata presa. Evita ricostruzioni retroattive che confondono informazioni note all'epoca con informazioni scoperte successivamente.

- Timestamp sincronizzati.
- Fonte e affidabilità del dato.
- Decisione, owner e motivazione.
- Effetti dell'azione.
- Evidenze preservate prima di modificare il sistema quando pertinente.

6. Scenario applicativo

Un singolo account compromesso sembra “basso impatto”, ma appartiene a un amministratore cloud. La priorità cambia per privilegi, blast radius potenziale e capacità di persistenza.

Analizza lo scenario separando prima i fatti dalle supposizioni. Poi indica l'obiettivo immediato, il rischio che vuoi limitare, l'azione proporzionata e l'evidenza che ti farà decidere se proseguire, cambiare strategia o fare rollback.

- Qual è il primo fatto verificabile?
- Quale decisione non può essere rinviata?
- Quale evidenza rischi di perdere agendo troppo presto?
- Quale funzione deve essere coinvolta prima del passo successivo?

7. Errori ricorrenti da evitare

Gli incidenti vengono spesso gestiti male non per assenza di strumenti, ma per decisioni non coordinate: severity definita troppo presto, contenimento senza valutare l'impatto, ripristino prima dell'eradicazione, comunicazioni incoerenti o chiusura senza verifica dell'efficacia.

Un processo maturo rende visibili questi errori e li trasforma in criteri di prevenzione.

- Non confondere “servizio ripristinato” con “incidente risolto”.
- Non usare una sola fonte per confermare la portata.
- Non cancellare evidenze durante la remediation senza una decisione consapevole.
- Non chiudere l'incidente senza definire follow-up e owner.

8. Recovery e resilienza

Qualunque sia il tema del capitolo, la prospettiva di recovery deve essere considerata fin dall'inizio. Le decisioni di contenimento e analisi possono aumentare o ridurre il tempo di ripristino, mentre un recovery troppo rapido può reintrodurre compromissione o perdita di dati.

Recovery readiness significa avere criteri di go/no-go, baseline affidabili, backup testati, dipendenze note e monitoraggio rafforzato dopo il ritorno in servizio.

- Verifica prerequisiti di restore.
- Conferma integrità di configurazioni, credenziali e dati.
- Definisci un periodo di osservazione.
- Mantieni un piano di rollback.

9. Metriche e indicatori utili

Le metriche devono sostenere decisioni, non premiare la velocità a scapito della qualità. MTTD, MTTA e MTTR sono utili solo se letti insieme a severità, ricorrenza, incidenti riaperti, copertura di rilevazione e qualità del recovery.

Una metrica apparentemente positiva può nascondere sotto-segnalazione o chiusure premature.

- Tempo di rilevazione con distribuzione per severità.
- Tempo di contenimento e tempo di ripristino separati.
- Incidenti riaperti o ricorrenti.
- Azioni post-incident scadute.
- Esiti delle esercitazioni e gap ripetuti.

10. Audit e riesame della capacità

Un audit efficace segue un incidente o una simulazione dalla prima evidenza alla chiusura: trigger, classificazione, decisioni, azioni, recovery e lezioni apprese. L'obiettivo non è verificare che esista un piano, ma che la capacità funzioni in condizioni realistiche.

Campiona casi diversi per severità, tecnologia, sede e presenza di terze parti.

- Confronta playbook e comportamento reale.
- Verifica tempi e qualità degli handover.
- Cerca evidenza dell'efficacia delle azioni correttive.
- Valuta se i criteri sono stati applicati in modo coerente.

11. Decision lab

Immagina di ricevere nuove informazioni che cambiano la valutazione iniziale: un account privilegiato, un secondo tenant coinvolto, un backup sospetto o una notifica esterna. Decidi cosa deve essere riclassificato e quale azione diventa prioritaria.

La maturità si vede nella capacità di cambiare decisione senza perdere controllo e tracciabilità.

- Nuovo fatto.
- Impatto sulla severità.
- Decisione rivista.
- Autorizzazione necessaria.

- Evidenza da raccogliere.
- Effetto atteso e verifica.

12. Sintesi e preparazione al minitest

Per superare la verifica devi saper applicare «Triage, classificazione, severità e decisione» a scenari nuovi. Le domande non premiano la memorizzazione di formule, ma la capacità di scegliere l'azione più difendibile sulla base di criteri, evidenze e rischio.

Prima del test prova a spiegare come il tema influenza detection, decisione, risposta, recovery e miglioramento.

- Individua il criterio prima dell'azione.
- Separa remediation, recovery e chiusura.
- Cerca almeno due fonti indipendenti per le decisioni rilevanti.
- Verifica sempre l'efficacia dopo l'azione.

MODULO 05**Analisi tecnica, investigazione ed evidenze**

- Tempo minimo previsto: 55 min
- Banca di verifica intermedia disponibile: 24 quesiti

1. Obiettivo operativo del capitolo

L'analisi deve costruire una cronologia affidabile e distinguere fatti, ipotesi e conclusioni. L'obiettivo operativo è capire cosa è successo, cosa è ancora attivo, quali sistemi sono coinvolti e quali azioni sono sicure senza distruggere evidenze utili.

L'obiettivo è saper prendere decisioni sotto pressione mantenendo tracciabilità, proporzionalità e continuità tra processo di sicurezza, esigenze del business ed evidenze disponibili.

- Collega il tema alla fase corretta del ciclo di incident management.
- Distingui fatti, ipotesi, decisioni e risultati.
- Individua quali informazioni sono indispensabili prima di agire.

2. Collocazione nella famiglia ISO/IEC 27035

Il tema «Analisi tecnica, investigazione ed evidenze» va letto nel quadro della famiglia ISO/IEC 27035: Parte 1 per principi e processo, Parte 2 per preparazione e lessons learned, Parte 3 per le operazioni di risposta ICT e Parte 4 per il coordinamento tra organizzazioni.

Il corso usa questi riferimenti come architettura operativa e li integra con il sistema di gestione della sicurezza delle informazioni.

- Non trattare la risposta come un'attività isolata del SOC.
- Mantieni chiari gli handover tra governance, team tecnico, business e soggetti esterni.
- Riesamina il processo quando cambiano rischi, tecnologia o dipendenze.

3. Processo operativo e criteri di decisione

Preservare evidenze, documentare acquisizioni, validare fonti, correlare indicatori, ricostruire timeline, individuare root entry point e distinguere causa, vettore, impatto e persistenza.

Un buon processo definisce trigger, input minimi, livelli di autorità, criteri di escalation e condizioni di uscita. Nei momenti critici la decisione deve essere veloce ma ricostruibile.

- Definisci chi decide e su quale base.
- Stabilisci cosa deve essere registrato prima e dopo l'azione.
- Prevedi eccezioni controllate per scenari ad alta urgenza.
- Associa ogni azione a un criterio di successo verificabile.

4. Persone, ruoli e handover

IMT, IRT, SOC, IT operations, DPO/privacy, legale, comunicazione, continuità operativa e business owner possono avere ruoli diversi. La qualità dell'handover è spesso il vero punto debole.

Chiarezza non significa burocratizzare: significa sapere chi ha autorità per isolare, notificare, ripristinare, comunicare

e accettare il rischio residuo.

- RACI o matrice equivalente.
- Reperibilità e sostituzioni.
- Canali sicuri alternativi.
- Escalation tecnica e manageriale.
- Responsabilità nelle decisioni di recovery.

5. Evidenze e timeline

Hash, immagini o esportazioni forensi quando pertinenti, log grezzi, timeline, IOC, query, note dell'analista, chain of custody e decisioni su raccolta e conservazione.

La timeline deve consentire di comprendere cosa si sapeva in ogni momento e perché una determinata decisione è stata presa. Evita ricostruzioni retroattive che confondono informazioni note all'epoca con informazioni scoperte successivamente.

- Timestamp sincronizzati.
- Fonte e affidabilità del dato.
- Decisione, owner e motivazione.
- Effetti dell'azione.
- Evidenze preservate prima di modificare il sistema quando pertinente.

6. Scenario applicativo

Un host viene formattato subito per ripristinarlo. Il servizio torna online, ma si perde la possibilità di capire la persistenza e l'estensione dell'attacco: recovery e investigazione devono essere coordinate.

Analizza lo scenario separando prima i fatti dalle supposizioni. Poi indica l'obiettivo immediato, il rischio che vuoi limitare, l'azione proporzionata e l'evidenza che ti farà decidere se proseguire, cambiare strategia o fare rollback.

- Qual è il primo fatto verificabile?
- Quale decisione non può essere rinviata?
- Quale evidenza rischi di perdere agendo troppo presto?
- Quale funzione deve essere coinvolta prima del passo successivo?

7. Errori ricorrenti da evitare

Gli incidenti vengono spesso gestiti male non per assenza di strumenti, ma per decisioni non coordinate: severity definita troppo presto, contenimento senza valutare l'impatto, ripristino prima dell'eradicazione, comunicazioni incoerenti o chiusura senza verifica dell'efficacia.

Un processo maturo rende visibili questi errori e li trasforma in criteri di prevenzione.

- Non confondere "servizio ripristinato" con "incidente risolto".
- Non usare una sola fonte per confermare la portata.
- Non cancellare evidenze durante la remediation senza una decisione consapevole.
- Non chiudere l'incidente senza definire follow-up e owner.

8. Recovery e resilienza

Qualunque sia il tema del capitolo, la prospettiva di recovery deve essere considerata fin dall'inizio. Le decisioni di contenimento e analisi possono aumentare o ridurre il tempo di ripristino, mentre un recovery troppo rapido può reintrodurre compromissione o perdita di dati.

Recovery readiness significa avere criteri di go/no-go, baseline affidabili, backup testati, dipendenze note e monitoraggio rafforzato dopo il ritorno in servizio.

- Verifica prerequisiti di restore.
- Conferma integrità di configurazioni, credenziali e dati.
- Definisci un periodo di osservazione.
- Mantieni un piano di rollback.

9. Metriche e indicatori utili

Le metriche devono sostenere decisioni, non premiare la velocità a scapito della qualità. MTTD, MTTA e MTTR sono utili solo se letti insieme a severità, ricorrenza, incidenti riaperti, copertura di rilevazione e qualità del recovery.

Una metrica apparentemente positiva può nascondere sotto-segnalazione o chiusure premature.

- Tempo di rilevazione con distribuzione per severità.
- Tempo di contenimento e tempo di ripristino separati.
- Incidenti riaperti o ricorrenti.
- Azioni post-incident scadute.
- Esiti delle esercitazioni e gap ripetuti.

10. Audit e riesame della capacità

Un audit efficace segue un incidente o una simulazione dalla prima evidenza alla chiusura: trigger, classificazione, decisioni, azioni, recovery e lezioni apprese. L'obiettivo non è verificare che esista un piano, ma che la capacità funzioni in condizioni realistiche.

Campiona casi diversi per severità, tecnologia, sede e presenza di terze parti.

- Confronta playbook e comportamento reale.
- Verifica tempi e qualità degli handover.
- Cerca evidenza dell'efficacia delle azioni correttive.
- Valuta se i criteri sono stati applicati in modo coerente.

11. Decision lab

Immagina di ricevere nuove informazioni che cambiano la valutazione iniziale: un account privilegiato, un secondo tenant coinvolto, un backup sospetto o una notifica esterna. Decidi cosa deve essere riclassificato e quale azione diventa prioritaria.

La maturità si vede nella capacità di cambiare decisione senza perdere controllo e tracciabilità.

- Nuovo fatto.
- Impatto sulla severità.
- Decisione rivista.
- Autorizzazione necessaria.

- Evidenza da raccogliere.
- Effetto atteso e verifica.

12. Sintesi e preparazione al minitest

Per superare la verifica devi saper applicare «Analisi tecnica, investigazione ed evidenze» a scenari nuovi. Le domande non premiano la memorizzazione di formule, ma la capacità di scegliere l'azione più difendibile sulla base di criteri, evidenze e rischio.

Prima del test prova a spiegare come il tema influenza detection, decisione, risposta, recovery e miglioramento.

- Individua il criterio prima dell'azione.
- Separa remediation, recovery e chiusura.
- Cerca almeno due fonti indipendenti per le decisioni rilevanti.
- Verifica sempre l'efficacia dopo l'azione.

MODULO 06**Risposta: contenimento, eradicazione e controllo del rischio**

- Tempo minimo previsto: 55 min
- Banca di verifica intermedia disponibile: 24 quesiti

1. Obiettivo operativo del capitolo

La risposta deve ridurre il danno senza introdurre rischi maggiori. Il contenimento limita la propagazione; l'eradicazione rimuove cause e persistenze note; entrambe richiedono decisioni, criteri di successo e controllo degli effetti collaterali.

L'obiettivo è saper prendere decisioni sotto pressione mantenendo tracciabilità, proporzionalità e continuità tra processo di sicurezza, esigenze del business ed evidenze disponibili.

- Collega il tema alla fase corretta del ciclo di incident management.
- Distingui fatti, ipotesi, decisioni e risultati.
- Individua quali informazioni sono indispensabili prima di agire.

2. Collocazione nella famiglia ISO/IEC 27035

Il tema «Risposta: contenimento, eradicazione e controllo del rischio» va letto nel quadro della famiglia ISO/IEC 27035: Parte 1 per principi e processo, Parte 2 per preparazione e lessons learned, Parte 3 per le operazioni di risposta ICT e Parte 4 per il coordinamento tra organizzazioni.

Il corso usa questi riferimenti come architettura operativa e li integra con il sistema di gestione della sicurezza delle informazioni.

- Non trattare la risposta come un'attività isolata del SOC.
- Mantieni chiari gli handover tra governance, team tecnico, business e soggetti esterni.
- Riesamina il processo quando cambiano rischi, tecnologia o dipendenze.

3. Processo operativo e criteri di decisione

Scegliere tra isolamento, blocco, revoca, segmentazione, sospensione, workaround e remediation definitiva, valutando impatto operativo, rischio residuo, evidenze e dipendenze.

Un buon processo definisce trigger, input minimi, livelli di autorità, criteri di escalation e condizioni di uscita. Nei momenti critici la decisione deve essere veloce ma ricostruibile.

- Definisci chi decide e su quale base.
- Stabilisci cosa deve essere registrato prima e dopo l'azione.
- Prevedi eccezioni controllate per scenari ad alta urgenza.
- Associa ogni azione a un criterio di successo verificabile.

4. Persone, ruoli e handover

IMT, IRT, SOC, IT operations, DPO/privacy, legale, comunicazione, continuità operativa e business owner possono avere ruoli diversi. La qualità dell'handover è spesso il vero punto debole.

Chiarezza non significa burocratizzare: significa sapere chi ha autorità per isolare, notificare, ripristinare, comunicare e accettare il rischio residuo.

- RACI o matrice equivalente.
- Reperibilità e sostituzioni.
- Canali sicuri alternativi.
- Escalation tecnica e manageriale.
- Responsabilità nelle decisioni di recovery.

5. Evidenze e timeline

Action log, autorizzazioni, host/account isolati, IOC bloccati, configurazioni modificate, vulnerabilità corrette, indicatori di persistenza e verifiche post-eradicazione.

La timeline deve consentire di comprendere cosa si sapeva in ogni momento e perché una determinata decisione è stata presa. Evita ricostruzioni retroattive che confondono informazioni note all'epoca con informazioni scoperte successivamente.

- Timestamp sincronizzati.
- Fonte e affidabilità del dato.
- Decisione, owner e motivazione.
- Effetti dell'azione.
- Evidenze preservate prima di modificare il sistema quando pertinente.

6. Scenario applicativo

Bloccare un intero segmento ferma l'attaccante ma interrompe un servizio essenziale. Il team deve scegliere un contenimento proporzionato e documentare rischio e motivazione.

Analizza lo scenario separando prima i fatti dalle supposizioni. Poi indica l'obiettivo immediato, il rischio che vuoi limitare, l'azione proporzionata e l'evidenza che ti farà decidere se proseguire, cambiare strategia o fare rollback.

- Qual è il primo fatto verificabile?
- Quale decisione non può essere rinviata?
- Quale evidenza rischi di perdere agendo troppo presto?
- Quale funzione deve essere coinvolta prima del passo successivo?

7. Errori ricorrenti da evitare

Gli incidenti vengono spesso gestiti male non per assenza di strumenti, ma per decisioni non coordinate: severity definita troppo presto, contenimento senza valutare l'impatto, ripristino prima dell'eradicazione, comunicazioni incoerenti o chiusura senza verifica dell'efficacia.

Un processo maturo rende visibili questi errori e li trasforma in criteri di prevenzione.

- Non confondere "servizio ripristinato" con "incidente risolto".
- Non usare una sola fonte per confermare la portata.
- Non cancellare evidenze durante la remediation senza una decisione consapevole.
- Non chiudere l'incidente senza definire follow-up e owner.

8. Recovery e resilienza

Qualunque sia il tema del capitolo, la prospettiva di recovery deve essere considerata fin dall'inizio. Le decisioni di contenimento e analisi possono aumentare o ridurre il tempo di ripristino, mentre un recovery troppo rapido può

reintrodurre compromissione o perdita di dati.

Recovery readiness significa avere criteri di go/no-go, baseline affidabili, backup testati, dipendenze note e monitoraggio rafforzato dopo il ritorno in servizio.

- Verifica prerequisiti di restore.
- Conferma integrità di configurazioni, credenziali e dati.
- Definisci un periodo di osservazione.
- Mantieni un piano di rollback.

9. Metriche e indicatori utili

Le metriche devono sostenere decisioni, non premiare la velocità a scapito della qualità. MTDD, MTTA e MTTR sono utili solo se letti insieme a severità, ricorrenza, incidenti riaperti, copertura di rilevazione e qualità del recovery.

Una metrica apparentemente positiva può nascondere sotto-segnalazione o chiusure premature.

- Tempo di rilevazione con distribuzione per severità.
- Tempo di contenimento e tempo di ripristino separati.
- Incidenti riaperti o ricorrenti.
- Azioni post-incident scadute.
- Esiti delle esercitazioni e gap ripetuti.

10. Audit e riesame della capacità

Un audit efficace segue un incidente o una simulazione dalla prima evidenza alla chiusura: trigger, classificazione, decisioni, azioni, recovery e lezioni apprese. L'obiettivo non è verificare che esista un piano, ma che la capacità funzioni in condizioni realistiche.

Campiona casi diversi per severità, tecnologia, sede e presenza di terze parti.

- Confronta playbook e comportamento reale.
- Verifica tempi e qualità degli handover.
- Cerca evidenza dell'efficacia delle azioni correttive.
- Valuta se i criteri sono stati applicati in modo coerente.

11. Decision lab

Immagina di ricevere nuove informazioni che cambiano la valutazione iniziale: un account privilegiato, un secondo tenant coinvolto, un backup sospetto o una notifica esterna. Decidi cosa deve essere riclassificato e quale azione diventa prioritaria.

La maturità si vede nella capacità di cambiare decisione senza perdere controllo e tracciabilità.

- Nuovo fatto.
- Impatto sulla severità.
- Decisione rivista.
- Autorizzazione necessaria.
- Evidenza da raccogliere.
- Effetto atteso e verifica.

12. Sintesi e preparazione al minitest

Per superare la verifica devi saper applicare «Risposta: contenimento, eradicazione e controllo del rischio» a scenari nuovi. Le domande non premiano la memorizzazione di formule, ma la capacità di scegliere l'azione più difendibile sulla base di criteri, evidenze e rischio.

Prima del test prova a spiegare come il tema influenza detection, decisione, risposta, recovery e miglioramento.

- Individua il criterio prima dell'azione.
- Separa remediation, recovery e chiusura.
- Cerca almeno due fonti indipendenti per le decisioni rilevanti.
- Verifica sempre l'efficacia dopo l'azione.

MODULO 07**Recovery, ripristino controllato e ritorno alla normalità**

- Tempo minimo previsto: 55 min
- Banca di verifica intermedia disponibile: 24 quesiti

1. Obiettivo operativo del capitolo

Il recovery non è semplicemente “riaccendere”. Occorre dimostrare che la causa è stata trattata, che i sistemi sono affidabili, che i dati sono integri e che il ritorno in esercizio non reintroduce l'incidente. L'interfaccia con continuità operativa e disaster recovery è essenziale.

L'obiettivo è saper prendere decisioni sotto pressione mantenendo tracciabilità, proporzionalità e continuità tra processo di sicurezza, esigenze del business ed evidenze disponibili.

- Collega il tema alla fase corretta del ciclo di incident management.
- Distingui fatti, ipotesi, decisioni e risultati.
- Individua quali informazioni sono indispensabili prima di agire.

2. Collocazione nella famiglia ISO/IEC 27035

Il tema «Recovery, ripristino controllato e ritorno alla normalità» va letto nel quadro della famiglia ISO/IEC 27035: Parte 1 per principi e processo, Parte 2 per preparazione e lessons learned, Parte 3 per le operazioni di risposta ICT e Parte 4 per il coordinamento tra organizzazioni.

Il corso usa questi riferimenti come architettura operativa e li integra con il sistema di gestione della sicurezza delle informazioni.

- Non trattare la risposta come un'attività isolata del SOC.
- Mantieni chiari gli handover tra governance, team tecnico, business e soggetti esterni.
- Riesamina il processo quando cambiano rischi, tecnologia o dipendenze.

3. Processo operativo e criteri di decisione

Definire criteri di go/no-go, priorità di ripristino, clean restore, validation, heightened monitoring, rollback, owner del servizio e periodo di osservazione prima della chiusura.

Un buon processo definisce trigger, input minimi, livelli di autorità, criteri di escalation e condizioni di uscita. Nei momenti critici la decisione deve essere veloce ma ricostruibile.

- Definisci chi decide e su quale base.
- Stabilisci cosa deve essere registrato prima e dopo l'azione.
- Prevedi eccezioni controllate per scenari ad alta urgenza.
- Associa ogni azione a un criterio di successo verificabile.

4. Persone, ruoli e handover

IMT, IRT, SOC, IT operations, DPO/privacy, legale, comunicazione, continuità operativa e business owner possono avere ruoli diversi. La qualità dell'handover è spesso il vero punto debole.

Chiarezza non significa burocratizzare: significa sapere chi ha autorità per isolare, notificare, ripristinare, comunicare

e accettare il rischio residuo.

- RACI o matrice equivalente.
- Reperibilità e sostituzioni.
- Canali sicuri alternativi.
- Escalation tecnica e manageriale.
- Responsabilità nelle decisioni di recovery.

5. Evidenze e timeline

Backup validati, restore test, baseline note, vulnerability closure, credential reset, monitoring rafforzato, business acceptance, RTO/RPO quando applicabili e decisione di ritorno in servizio.

La timeline deve consentire di comprendere cosa si sapeva in ogni momento e perché una determinata decisione è stata presa. Evita ricostruzioni retroattive che confondono informazioni note all'epoca con informazioni scoperte successivamente.

- Timestamp sincronizzati.
- Fonte e affidabilità del dato.
- Decisione, owner e motivazione.
- Effetti dell'azione.
- Evidenze preservate prima di modificare il sistema quando pertinente.

6. Scenario applicativo

Un database viene ripristinato da un backup tecnicamente valido ma precedente all'ultima sincronizzazione. Il recovery deve bilanciare integrità, perdita dati, dipendenze e priorità del business.

Analizza lo scenario separando prima i fatti dalle supposizioni. Poi indica l'obiettivo immediato, il rischio che vuoi limitare, l'azione proporzionata e l'evidenza che ti farà decidere se proseguire, cambiare strategia o fare rollback.

- Qual è il primo fatto verificabile?
- Quale decisione non può essere rinviata?
- Quale evidenza rischi di perdere agendo troppo presto?
- Quale funzione deve essere coinvolta prima del passo successivo?

7. Errori ricorrenti da evitare

Gli incidenti vengono spesso gestiti male non per assenza di strumenti, ma per decisioni non coordinate: severity definita troppo presto, contenimento senza valutare l'impatto, ripristino prima dell'eradicazione, comunicazioni incoerenti o chiusura senza verifica dell'efficacia.

Un processo maturo rende visibili questi errori e li trasforma in criteri di prevenzione.

- Non confondere “servizio ripristinato” con “incidente risolto”.
- Non usare una sola fonte per confermare la portata.
- Non cancellare evidenze durante la remediation senza una decisione consapevole.
- Non chiudere l'incidente senza definire follow-up e owner.

8. Recovery e resilienza

Qualunque sia il tema del capitolo, la prospettiva di recovery deve essere considerata fin dall'inizio. Le decisioni di contenimento e analisi possono aumentare o ridurre il tempo di ripristino, mentre un recovery troppo rapido può reintrodurre compromissione o perdita di dati.

Recovery readiness significa avere criteri di go/no-go, baseline affidabili, backup testati, dipendenze note e monitoraggio rafforzato dopo il ritorno in servizio.

- Verifica prerequisiti di restore.
- Conferma integrità di configurazioni, credenziali e dati.
- Definisci un periodo di osservazione.
- Mantieni un piano di rollback.

9. Metriche e indicatori utili

Le metriche devono sostenere decisioni, non premiare la velocità a scapito della qualità. MTTD, MTTA e MTTR sono utili solo se letti insieme a severità, ricorrenza, incidenti riaperti, copertura di rilevazione e qualità del recovery.

Una metrica apparentemente positiva può nascondere sotto-segnalazione o chiusure premature.

- Tempo di rilevazione con distribuzione per severità.
- Tempo di contenimento e tempo di ripristino separati.
- Incidenti riaperti o ricorrenti.
- Azioni post-incident scadute.
- Esiti delle esercitazioni e gap ripetuti.

10. Audit e riesame della capacità

Un audit efficace segue un incidente o una simulazione dalla prima evidenza alla chiusura: trigger, classificazione, decisioni, azioni, recovery e lezioni apprese. L'obiettivo non è verificare che esista un piano, ma che la capacità funzioni in condizioni realistiche.

Campiona casi diversi per severità, tecnologia, sede e presenza di terze parti.

- Confronta playbook e comportamento reale.
- Verifica tempi e qualità degli handover.
- Cerca evidenza dell'efficacia delle azioni correttive.
- Valuta se i criteri sono stati applicati in modo coerente.

11. Decision lab

Immagina di ricevere nuove informazioni che cambiano la valutazione iniziale: un account privilegiato, un secondo tenant coinvolto, un backup sospetto o una notifica esterna. Decidi cosa deve essere riclassificato e quale azione diventa prioritaria.

La maturità si vede nella capacità di cambiare decisione senza perdere controllo e tracciabilità.

- Nuovo fatto.
- Impatto sulla severità.
- Decisione rivista.
- Autorizzazione necessaria.

- Evidenza da raccogliere.
- Effetto atteso e verifica.

12. Sintesi e preparazione al minitest

Per superare la verifica devi saper applicare «Recovery, ripristino controllato e ritorno alla normalità» a scenari nuovi. Le domande non premiano la memorizzazione di formule, ma la capacità di scegliere l'azione più difendibile sulla base di criteri, evidenze e rischio.

Prima del test prova a spiegare come il tema influenza detection, decisione, risposta, recovery e miglioramento.

- Individua il criterio prima dell'azione.
- Separa remediation, recovery e chiusura.
- Cerca almeno due fonti indipendenti per le decisioni rilevanti.
- Verifica sempre l'efficacia dopo l'azione.

MODULO 08**Comunicazione, obblighi e coordinamento tra organizzazioni**

- Tempo minimo previsto: 45 min
- Banca di verifica intermedia disponibile: 24 quesiti

1. Obiettivo operativo del capitolo

Gli incidenti attraversano spesso confini organizzativi. La comunicazione deve essere autorizzata, accurata, tempestiva e coerente. ISO/IEC 27035-4 aggiunge la prospettiva del coordinamento tra più organizzazioni e dei relativi effetti sui processi interni.

L'obiettivo è saper prendere decisioni sotto pressione mantenendo tracciabilità, proporzionalità e continuità tra processo di sicurezza, esigenze del business ed evidenze disponibili.

- Collega il tema alla fase corretta del ciclo di incident management.
- Distingui fatti, ipotesi, decisioni e risultati.
- Individua quali informazioni sono indispensabili prima di agire.

2. Collocazione nella famiglia ISO/IEC 27035

Il tema «Comunicazione, obblighi e coordinamento tra organizzazioni» va letto nel quadro della famiglia ISO/IEC 27035: Parte 1 per principi e processo, Parte 2 per preparazione e lessons learned, Parte 3 per le operazioni di risposta ICT e Parte 4 per il coordinamento tra organizzazioni.

Il corso usa questi riferimenti come architettura operativa e li integra con il sistema di gestione della sicurezza delle informazioni.

- Non trattare la risposta come un'attività isolata del SOC.
- Mantieni chiari gli handover tra governance, team tecnico, business e soggetti esterni.
- Riesamina il processo quando cambiano rischi, tecnologia o dipendenze.

3. Processo operativo e criteri di decisione

Mappare soggetti interni ed esterni, criteri di notifica, canali, livello di dettaglio condivisibile, responsabilità di coordinamento, gestione delle dipendenze e allineamento dei messaggi.

Un buon processo definisce trigger, input minimi, livelli di autorità, criteri di escalation e condizioni di uscita. Nei momenti critici la decisione deve essere veloce ma ricostruibile.

- Definisci chi decide e su quale base.
- Stabilisci cosa deve essere registrato prima e dopo l'azione.
- Prevedi eccezioni controllate per scenari ad alta urgenza.
- Associa ogni azione a un criterio di successo verificabile.

4. Persone, ruoli e handover

IMT, IRT, SOC, IT operations, DPO/privacy, legale, comunicazione, continuità operativa e business owner possono avere ruoli diversi. La qualità dell'handover è spesso il vero punto debole.

Chiarezza non significa burocratizzare: significa sapere chi ha autorità per isolare, notificare, ripristinare, comunicare

e accettare il rischio residuo.

- RACI o matrice equivalente.
- Reperibilità e sostituzioni.
- Canali sicuri alternativi.
- Escalation tecnica e manageriale.
- Responsabilità nelle decisioni di recovery.

5. Evidenze e timeline

Communication matrix, contatti autorità/CSIRT/fornitori, decision log, notifiche, messaggi approvati, accordi di condivisione e registri di coordinamento.

La timeline deve consentire di comprendere cosa si sapeva in ogni momento e perché una determinata decisione è stata presa. Evita ricostruzioni retroattive che confondono informazioni note all'epoca con informazioni scoperte successivamente.

- Timestamp sincronizzati.
- Fonte e affidabilità del dato.
- Decisione, owner e motivazione.
- Effetti dell'azione.
- Evidenze preservate prima di modificare il sistema quando pertinente.

6. Scenario applicativo

Un fornitore cloud vede l'attività malevola prima del cliente, mentre un partner teme di condividere IOC per ragioni contrattuali. Il coordinamento deve essere preparato e governato prima della crisi.

Analizza lo scenario separando prima i fatti dalle supposizioni. Poi indica l'obiettivo immediato, il rischio che vuoi limitare, l'azione proporzionata e l'evidenza che ti farà decidere se proseguire, cambiare strategia o fare rollback.

- Qual è il primo fatto verificabile?
- Quale decisione non può essere rinviata?
- Quale evidenza rischi di perdere agendo troppo presto?
- Quale funzione deve essere coinvolta prima del passo successivo?

7. Errori ricorrenti da evitare

Gli incidenti vengono spesso gestiti male non per assenza di strumenti, ma per decisioni non coordinate: severity definita troppo presto, contenimento senza valutare l'impatto, ripristino prima dell'eradicazione, comunicazioni incoerenti o chiusura senza verifica dell'efficacia.

Un processo maturo rende visibili questi errori e li trasforma in criteri di prevenzione.

- Non confondere “servizio ripristinato” con “incidente risolto”.
- Non usare una sola fonte per confermare la portata.
- Non cancellare evidenze durante la remediation senza una decisione consapevole.
- Non chiudere l'incidente senza definire follow-up e owner.

8. Recovery e resilienza

Qualunque sia il tema del capitolo, la prospettiva di recovery deve essere considerata fin dall'inizio. Le decisioni di contenimento e analisi possono aumentare o ridurre il tempo di ripristino, mentre un recovery troppo rapido può reintrodurre compromissione o perdita di dati.

Recovery readiness significa avere criteri di go/no-go, baseline affidabili, backup testati, dipendenze note e monitoraggio rafforzato dopo il ritorno in servizio.

- Verifica prerequisiti di restore.
- Conferma integrità di configurazioni, credenziali e dati.
- Definisci un periodo di osservazione.
- Mantieni un piano di rollback.

9. Metriche e indicatori utili

Le metriche devono sostenere decisioni, non premiare la velocità a scapito della qualità. MTTD, MTTA e MTTR sono utili solo se letti insieme a severità, ricorrenza, incidenti riaperti, copertura di rilevazione e qualità del recovery.

Una metrica apparentemente positiva può nascondere sotto-segnalazione o chiusure premature.

- Tempo di rilevazione con distribuzione per severità.
- Tempo di contenimento e tempo di ripristino separati.
- Incidenti riaperti o ricorrenti.
- Azioni post-incident scadute.
- Esiti delle esercitazioni e gap ripetuti.

10. Audit e riesame della capacità

Un audit efficace segue un incidente o una simulazione dalla prima evidenza alla chiusura: trigger, classificazione, decisioni, azioni, recovery e lezioni apprese. L'obiettivo non è verificare che esista un piano, ma che la capacità funzioni in condizioni realistiche.

Campiona casi diversi per severità, tecnologia, sede e presenza di terze parti.

- Confronta playbook e comportamento reale.
- Verifica tempi e qualità degli handover.
- Cerca evidenza dell'efficacia delle azioni correttive.
- Valuta se i criteri sono stati applicati in modo coerente.

11. Decision lab

Immagina di ricevere nuove informazioni che cambiano la valutazione iniziale: un account privilegiato, un secondo tenant coinvolto, un backup sospetto o una notifica esterna. Decidi cosa deve essere riclassificato e quale azione diventa prioritaria.

La maturità si vede nella capacità di cambiare decisione senza perdere controllo e tracciabilità.

- Nuovo fatto.
- Impatto sulla severità.
- Decisione rivista.
- Autorizzazione necessaria.

- Evidenza da raccogliere.
- Effetto atteso e verifica.

12. Sintesi e preparazione al minitest

Per superare la verifica devi saper applicare «Comunicazione, obblighi e coordinamento tra organizzazioni» a scenari nuovi. Le domande non premiano la memorizzazione di formule, ma la capacità di scegliere l'azione più difendibile sulla base di criteri, evidenze e rischio.

Prima del test prova a spiegare come il tema influenza detection, decisione, risposta, recovery e miglioramento.

- Individua il criterio prima dell'azione.
- Separa remediation, recovery e chiusura.
- Cerca almeno due fonti indipendenti per le decisioni rilevanti.
- Verifica sempre l'efficacia dopo l'azione.

MODULO 09**Lezioni apprese, metriche, esercitazioni e miglioramento**

- Tempo minimo previsto: 40 min
- Banca di verifica intermedia disponibile: 24 quesiti

1. Obiettivo operativo del capitolo

La chiusura amministrativa non equivale alla chiusura del rischio. Le lezioni apprese trasformano l'incidente in miglioramento: cause, controlli, processo, ruoli, strumenti, comunicazioni e formazione devono essere riesaminati con evidenze.

L'obiettivo è saper prendere decisioni sotto pressione mantenendo tracciabilità, proporzionalità e continuità tra processo di sicurezza, esigenze del business ed evidenze disponibili.

- Collega il tema alla fase corretta del ciclo di incident management.
- Distingui fatti, ipotesi, decisioni e risultati.
- Individua quali informazioni sono indispensabili prima di agire.

2. Collocazione nella famiglia ISO/IEC 27035

Il tema «Lezioni apprese, metriche, esercitazioni e miglioramento» va letto nel quadro della famiglia ISO/IEC 27035: Parte 1 per principi e processo, Parte 2 per preparazione e lessons learned, Parte 3 per le operazioni di risposta ICT e Parte 4 per il coordinamento tra organizzazioni.

Il corso usa questi riferimenti come architettura operativa e li integra con il sistema di gestione della sicurezza delle informazioni.

- Non trattare la risposta come un'attività isolata del SOC.
- Mantieni chiari gli handover tra governance, team tecnico, business e soggetti esterni.
- Riesamina il processo quando cambiano rischi, tecnologia o dipendenze.

3. Processo operativo e criteri di decisione

Condurre post-incident review, separare blame da accountability, aggiornare risk assessment, SoA, playbook e training, definire azioni con owner, scadenze e verifica successiva dell'efficacia.

Un buon processo definisce trigger, input minimi, livelli di autorità, criteri di escalation e condizioni di uscita. Nei momenti critici la decisione deve essere veloce ma ricostruibile.

- Definisci chi decide e su quale base.
- Stabilisci cosa deve essere registrato prima e dopo l'azione.
- Prevedi eccezioni controllate per scenari ad alta urgenza.
- Associa ogni azione a un criterio di successo verificabile.

4. Persone, ruoli e handover

IMT, IRT, SOC, IT operations, DPO/privacy, legale, comunicazione, continuità operativa e business owner possono avere ruoli diversi. La qualità dell'handover è spesso il vero punto debole.

Chiarezza non significa burocratizzare: significa sapere chi ha autorità per isolare, notificare, ripristinare, comunicare

e accettare il rischio residuo.

- RACI o matrice equivalente.
- Reperibilità e sostituzioni.
- Canali sicuri alternativi.
- Escalation tecnica e manageriale.
- Responsabilità nelle decisioni di recovery.

5. Evidenze e timeline

PIR report, cause analysis, action tracker, aggiornamento rischi/controlli, metriche MTTD/MTTA/MTTR lette con cautela, esiti di esercitazioni e verifiche delle azioni.

La timeline deve consentire di comprendere cosa si sapeva in ogni momento e perché una determinata decisione è stata presa. Evita ricostruzioni retroattive che confondono informazioni note all'epoca con informazioni scoperte successivamente.

- Timestamp sincronizzati.
- Fonte e affidabilità del dato.
- Decisione, owner e motivazione.
- Effetti dell'azione.
- Evidenze preservate prima di modificare il sistema quando pertinente.

6. Scenario applicativo

Il tempo medio di risposta migliora, ma aumentano gli incidenti riaperti. La metrica positiva non dimostra da sola efficacia: occorre leggere qualità della soluzione e ricorrenza.

Analizza lo scenario separando prima i fatti dalle supposizioni. Poi indica l'obiettivo immediato, il rischio che vuoi limitare, l'azione proporzionata e l'evidenza che ti farà decidere se proseguire, cambiare strategia o fare rollback.

- Qual è il primo fatto verificabile?
- Quale decisione non può essere rinviata?
- Quale evidenza rischi di perdere agendo troppo presto?
- Quale funzione deve essere coinvolta prima del passo successivo?

7. Errori ricorrenti da evitare

Gli incidenti vengono spesso gestiti male non per assenza di strumenti, ma per decisioni non coordinate: severity definita troppo presto, contenimento senza valutare l'impatto, ripristino prima dell'eradicazione, comunicazioni incoerenti o chiusura senza verifica dell'efficacia.

Un processo maturo rende visibili questi errori e li trasforma in criteri di prevenzione.

- Non confondere “servizio ripristinato” con “incidente risolto”.
- Non usare una sola fonte per confermare la portata.
- Non cancellare evidenze durante la remediation senza una decisione consapevole.
- Non chiudere l'incidente senza definire follow-up e owner.

8. Recovery e resilienza

Qualunque sia il tema del capitolo, la prospettiva di recovery deve essere considerata fin dall'inizio. Le decisioni di contenimento e analisi possono aumentare o ridurre il tempo di ripristino, mentre un recovery troppo rapido può reintrodurre compromissione o perdita di dati.

Recovery readiness significa avere criteri di go/no-go, baseline affidabili, backup testati, dipendenze note e monitoraggio rafforzato dopo il ritorno in servizio.

- Verifica prerequisiti di restore.
- Conferma integrità di configurazioni, credenziali e dati.
- Definisci un periodo di osservazione.
- Mantieni un piano di rollback.

9. Metriche e indicatori utili

Le metriche devono sostenere decisioni, non premiare la velocità a scapito della qualità. MTTD, MTTA e MTTR sono utili solo se letti insieme a severità, ricorrenza, incidenti riaperti, copertura di rilevazione e qualità del recovery.

Una metrica apparentemente positiva può nascondere sotto-segnalazione o chiusure premature.

- Tempo di rilevazione con distribuzione per severità.
- Tempo di contenimento e tempo di ripristino separati.
- Incidenti riaperti o ricorrenti.
- Azioni post-incident scadute.
- Esiti delle esercitazioni e gap ripetuti.

10. Audit e riesame della capacità

Un audit efficace segue un incidente o una simulazione dalla prima evidenza alla chiusura: trigger, classificazione, decisioni, azioni, recovery e lezioni apprese. L'obiettivo non è verificare che esista un piano, ma che la capacità funzioni in condizioni realistiche.

Campiona casi diversi per severità, tecnologia, sede e presenza di terze parti.

- Confronta playbook e comportamento reale.
- Verifica tempi e qualità degli handover.
- Cerca evidenza dell'efficacia delle azioni correttive.
- Valuta se i criteri sono stati applicati in modo coerente.

11. Decision lab

Immagina di ricevere nuove informazioni che cambiano la valutazione iniziale: un account privilegiato, un secondo tenant coinvolto, un backup sospetto o una notifica esterna. Decidi cosa deve essere riclassificato e quale azione diventa prioritaria.

La maturità si vede nella capacità di cambiare decisione senza perdere controllo e tracciabilità.

- Nuovo fatto.
- Impatto sulla severità.
- Decisione rivista.
- Autorizzazione necessaria.

- Evidenza da raccogliere.
- Effetto atteso e verifica.

12. Sintesi e preparazione al minitest

Per superare la verifica devi saper applicare «Lezioni apprese, metriche, esercitazioni e miglioramento» a scenari nuovi. Le domande non premiano la memorizzazione di formule, ma la capacità di scegliere l'azione più difendibile sulla base di criteri, evidenze e rischio.

Prima del test prova a spiegare come il tema influenza detection, decisione, risposta, recovery e miglioramento.

- Individua il criterio prima dell'azione.
- Separa remediation, recovery e chiusura.
- Cerca almeno due fonti indipendenti per le decisioni rilevanti.
- Verifica sempre l'efficacia dopo l'azione.

MODULO 10**Major incident simulation, recovery readiness e auditabilità**

- Tempo minimo previsto: 40 min
- Banca di verifica intermedia disponibile: 24 quesiti

1. Obiettivo operativo del capitolo

Il modulo finale integra l'intero ciclo in una simulazione decisionale: detection, triage, analisi, contenimento, eradicazione, recovery, comunicazione, coordinamento e miglioramento. L'obiettivo è dimostrare una capacità ripetibile, non una sequenza teorica.

L'obiettivo è saper prendere decisioni sotto pressione mantenendo tracciabilità, proporzionalità e continuità tra processo di sicurezza, esigenze del business ed evidenze disponibili.

- Collega il tema alla fase corretta del ciclo di incident management.
- Distingui fatti, ipotesi, decisioni e risultati.
- Individua quali informazioni sono indispensabili prima di agire.

2. Collocazione nella famiglia ISO/IEC 27035

Il tema «Major incident simulation, recovery readiness e auditabilità» va letto nel quadro della famiglia ISO/IEC 27035: Parte 1 per principi e processo, Parte 2 per preparazione e lessons learned, Parte 3 per le operazioni di risposta ICT e Parte 4 per il coordinamento tra organizzazioni.

Il corso usa questi riferimenti come architettura operativa e li integra con il sistema di gestione della sicurezza delle informazioni.

- Non trattare la risposta come un'attività isolata del SOC.
- Mantieni chiari gli handover tra governance, team tecnico, business e soggetti esterni.
- Riesamina il processo quando cambiano rischi, tecnologia o dipendenze.

3. Processo operativo e criteri di decisione

Eseguire tabletop e technical exercise, definire inject, criteri di successo, osservatori, decision log, recovery checkpoints, escalation e post-exercise action plan.

Un buon processo definisce trigger, input minimi, livelli di autorità, criteri di escalation e condizioni di uscita. Nei momenti critici la decisione deve essere veloce ma ricostruibile.

- Definisci chi decide e su quale base.
- Stabilisci cosa deve essere registrato prima e dopo l'azione.
- Prevedi eccezioni controllate per scenari ad alta urgenza.
- Associa ogni azione a un criterio di successo verificabile.

4. Persone, ruoli e handover

IMT, IRT, SOC, IT operations, DPO/privacy, legale, comunicazione, continuità operativa e business owner possono avere ruoli diversi. La qualità dell'handover è spesso il vero punto debole.

Chiarezza non significa burocratizzare: significa sapere chi ha autorità per isolare, notificare, ripristinare, comunicare

e accettare il rischio residuo.

- RACI o matrice equivalente.
- Reperibilità e sostituzioni.
- Canali sicuri alternativi.
- Escalation tecnica e manageriale.
- Responsabilità nelle decisioni di recovery.

5. Evidenze e timeline

Scenario, timeline, decisioni, log tecnici, tempi, handover, escalation, recovery evidence, comunicazioni, debrief, gap register e follow-up fino alla chiusura efficace.

La timeline deve consentire di comprendere cosa si sapeva in ogni momento e perché una determinata decisione è stata presa. Evita ricostruzioni retroattive che confondono informazioni note all'epoca con informazioni scoperte successivamente.

- Timestamp sincronizzati.
- Fonte e affidabilità del dato.
- Decisione, owner e motivazione.
- Effetti dell'azione.
- Evidenze preservate prima di modificare il sistema quando pertinente.

6. Scenario applicativo

Durante una simulazione il team contiene correttamente il malware ma non coinvolge il business owner prima del restore. Il gap dimostra che la maturità dipende anche dalle interfacce, non solo dalla competenza tecnica.

Analizza lo scenario separando prima i fatti dalle supposizioni. Poi indica l'obiettivo immediato, il rischio che vuoi limitare, l'azione proporzionata e l'evidenza che ti farà decidere se proseguire, cambiare strategia o fare rollback.

- Qual è il primo fatto verificabile?
- Quale decisione non può essere rinviata?
- Quale evidenza rischi di perdere agendo troppo presto?
- Quale funzione deve essere coinvolta prima del passo successivo?

7. Errori ricorrenti da evitare

Gli incidenti vengono spesso gestiti male non per assenza di strumenti, ma per decisioni non coordinate: severity definita troppo presto, contenimento senza valutare l'impatto, ripristino prima dell'eradicazione, comunicazioni incoerenti o chiusura senza verifica dell'efficacia.

Un processo maturo rende visibili questi errori e li trasforma in criteri di prevenzione.

- Non confondere “servizio ripristinato” con “incidente risolto”.
- Non usare una sola fonte per confermare la portata.
- Non cancellare evidenze durante la remediation senza una decisione consapevole.
- Non chiudere l'incidente senza definire follow-up e owner.

8. Recovery e resilienza

Qualunque sia il tema del capitolo, la prospettiva di recovery deve essere considerata fin dall'inizio. Le decisioni di contenimento e analisi possono aumentare o ridurre il tempo di ripristino, mentre un recovery troppo rapido può reintrodurre compromissione o perdita di dati.

Recovery readiness significa avere criteri di go/no-go, baseline affidabili, backup testati, dipendenze note e monitoraggio rafforzato dopo il ritorno in servizio.

- Verifica prerequisiti di restore.
- Conferma integrità di configurazioni, credenziali e dati.
- Definisci un periodo di osservazione.
- Mantieni un piano di rollback.

9. Metriche e indicatori utili

Le metriche devono sostenere decisioni, non premiare la velocità a scapito della qualità. MTTD, MTTA e MTTR sono utili solo se letti insieme a severità, ricorrenza, incidenti riaperti, copertura di rilevazione e qualità del recovery.

Una metrica apparentemente positiva può nascondere sotto-segnalazione o chiusure premature.

- Tempo di rilevazione con distribuzione per severità.
- Tempo di contenimento e tempo di ripristino separati.
- Incidenti riaperti o ricorrenti.
- Azioni post-incident scadute.
- Esiti delle esercitazioni e gap ripetuti.

10. Audit e riesame della capacità

Un audit efficace segue un incidente o una simulazione dalla prima evidenza alla chiusura: trigger, classificazione, decisioni, azioni, recovery e lezioni apprese. L'obiettivo non è verificare che esista un piano, ma che la capacità funzioni in condizioni realistiche.

Campiona casi diversi per severità, tecnologia, sede e presenza di terze parti.

- Confronta playbook e comportamento reale.
- Verifica tempi e qualità degli handover.
- Cerca evidenza dell'efficacia delle azioni correttive.
- Valuta se i criteri sono stati applicati in modo coerente.

11. Decision lab

Immagina di ricevere nuove informazioni che cambiano la valutazione iniziale: un account privilegiato, un secondo tenant coinvolto, un backup sospetto o una notifica esterna. Decidi cosa deve essere riclassificato e quale azione diventa prioritaria.

La maturità si vede nella capacità di cambiare decisione senza perdere controllo e tracciabilità.

- Nuovo fatto.
- Impatto sulla severità.
- Decisione rivista.
- Autorizzazione necessaria.

- Evidenza da raccogliere.
- Effetto atteso e verifica.

12. Sintesi e preparazione al minitest

Per superare la verifica devi saper applicare «Major incident simulation, recovery readiness e auditabilità» a scenari nuovi. Le domande non premiano la memorizzazione di formule, ma la capacità di scegliere l'azione più difendibile sulla base di criteri, evidenze e rischio.

Prima del test prova a spiegare come il tema influenza detection, decisione, risposta, recovery e miglioramento.

- Individua il criterio prima dell'azione.
- Separa remediation, recovery e chiusura.
- Cerca almeno due fonti indipendenti per le decisioni rilevanti.
- Verifica sempre l'efficacia dopo l'azione.

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: 180 quesiti attivi.
- Soglia di superamento pubblicata per il corso: 70%.
- 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: 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: ISO27035-IMR
- 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.