Agenzia per la Cybersicurezza Nazionale

# Linee Guida CAD

## Definizione dei processi e delle procedure per la gestione degli incidenti di sicurezza informatica.

# Controllo di versione

| VERSIONE | DATA PUBBLICAZIONE | NOTE |
|---|---|---|
| 1.0 | Settembre 2025 | Prima versione. |

# INDICE

# 1. Introduzione

## 1.1. Premessa

La sicurezza informatica rappresenta un elemento essenziale per garantire la continuità operativa, la protezione delle informazioni e la resilienza delle organizzazioni. Incidenti di sicurezza, come ad esempio quelli dovuti a minacce quali *ransomware* o *DDOS*, possono infatti determinare impatti significativi sulle attività e i servizi di un'organizzazione in termini operativi, finanziari o reputazionali.

La gestione degli incidenti – intesa come l'insieme delle attività volte a rilevare tempestivamente un incidente, a rispondervi in modo appropriato ed efficiente, a ripristinare la situazione a prima del verificarsi dello stesso e a migliorare la capacità di rispondere a futuri incidenti tramite le lezioni apprese –è dunque una delle *capacità* determinanti per la sicurezza di un'organizzazione.

Per gestire gli incidenti in modo efficace è altresì cruciale adottare un approccio strutturato basato su processi e procedure chiaramente definiti in modo da creare un quadro organizzativo armonizzato e assicurare la coerenza e sistematicità delle varie attività. La definizione di processi e procedure permette altresì di garantire ripetibilità, facilitare la formazione e imparare dalle lezioni apprese.

## 1.2. Scopo e organizzazione del documento

Il presente documento si propone di fornire linee guida per la definizione di processi e procedure per gestire in modo efficace gli incidenti di sicurezza informatica. È stato redatto sulla base di quanto indicato dal **Piano Triennale per l'informatica nella Pubblica Amministrazione**[1] **2024-2026** di cui all'articolo 14-bis, comma 2, lettera b) del decreto legislativo 7 marzo 2005, n. 82 (cosiddetto CAD - Codice dell'Amministrazione Digitale), le cui linee d'azione istituzionali prevedono, per l'appunto, che **l'Agenzia per la Cybersicurezza Nazionale** fornisca le linee guida per la definizione dei processi e delle procedure per la gestione degli incidenti.

I destinatari delle presenti linee guida sono pertanto i soggetti di cui all'articolo 2, comma 2 del CAD (d'ora in avanti riferiti per brevità come **soggetti**), ossia:

a) le pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione, ivi comprese le autorità di sistema portuale, nonché le autorità amministrative indipendenti di garanzia, vigilanza e regolazione;
b) i gestori di servizi pubblici, ivi comprese le società quotate, in relazione ai servizi di pubblico interesse;
c) le società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n. 175, escluse le società quotate di cui all'articolo 2, comma 1, lettera p), del medesimo decreto che non rientrino nella categoria di cui alla lettera b).

[1] Il Piano Triennale per l'informatica nella Pubblica Amministrazione promuove la trasformazione digitale del Paese attraverso quella della Pubblica Amministrazione italiana.

Il documento, oltre al capitolo di introduzione, contiene i seguenti capitoli:

- **Processo per la gestione degli incidenti**: presenta un modello di processo per la gestione degli incidenti di sicurezza informatica con le relative fasi e sotto-fasi;
- **Procedure per la gestione degli incidenti:** esamina le principali caratteristiche delle procedure per la gestione degli incidenti.

Sono inoltre presenti le due seguenti appendici:

- **appendice A: obiettivi gestione incidenti**, riporta gli obiettivi di sicurezza più specificatamente connessi alla gestione degli incidenti;
- **appendice B: elenco attività processo e procedure**, elenca le attività del processo di gestione degli incidenti e le possibili procedure associate;
- **appendice C: playbook per la gestione degli incidenti**, esamina i *playbook* quali strumenti utilizzati per guidare la gestione di specifiche categorie di incidenti.

## 1.3. Termini e definizioni

Nella seguente tabella sono elencate le definizioni dei termini peculiari usati nel presente documento.

| TERMINE | DEFINIZIONE |
|---|---|
| Evento | Qualsiasi accadimento osservabile in una rete o sistema informativo. |
| Evento rilevante per la sicurezza | Evento di natura intenzionale o accidentale che potrebbe compromettere o che compromette la sicurezza dei sistemi informativi e di rete, in termini di disponibilità, autenticità, integrità o riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti o accessibili attraverso essi. |
| Falso positivo | Allarme segnalato da uno strumento di monitoraggio che non corrisponde ad un incidente. |
| Gestione degli incidenti di sicurezza informatica | Insieme di processi e procedure volti a prevenire, rilevare, analizzare, contenere un incidente di sicurezza, a rispondervi e recuperare da esso. |
| Incidente di sicurezza informatica | Evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi. |
| Indicatore di compromissione (IOC) | Informazione che descrive una minaccia o compromissione nota. |
| Minaccia informatica | Qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone. |
| Sistema informativo e di rete | 1. Una rete di comunicazione elettronica ai sensi dell'articolo 2, comma 1, lettera vv), del decreto legislativo 1° agosto 2003, n. 259; |

| TERMINE | DEFINIZIONE |
|---|---|
| | 2. Qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali;<br>3. I dati digitali conservati, elaborati, estratti o trasmessi per mezzo di reti o dispositivi di cui ai numeri 1) e 2), per il loro funzionamento, uso, protezione e manutenzione. |
| Tattiche, Tecniche, Procedure (TTPs) | Gli obiettivi di un attore malevolo durante una delle fasi dell'attacco, le modalità con le quali l'attore malevolo realizza una determinata Tattica e le modalità con le quali l'attore malevolo implementa una o più Tecniche. |
| Vulnerabilità | un punto debole, una suscettibilità o un difetto di prodotti ICT o servizi ICT che può essere sfruttato da una minaccia informatica. |

## 1.4. Norme di riferimento

| NORMA | DESCRIZIONE |
|---|---|
| Codice dell'Amministrazione digitale – CAD | Decreto legislativo 7 marzo 2005, n. 82. Codice dell'amministrazione digitale. |
| Perimetro di Sicurezza Nazionale Cibernetica (PSNC) | Decreto-legge 21 settembre 2019, n. 105. Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica. |
| Legge 90/2024 | Legge 28 giugno 2024, n. 90. Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici. |
| Regolamento Cloud per la Pubblica Amministrazione | Decreto Direttoriale ACN n. 21007/24 del 27 giugno 2024 |
| Decreto NIS | Decreto legislativo 4 settembre 2024, n. 138. Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148. |

## 1.5. Documenti di riferimento

I seguenti documenti possono essere consultati per ulteriori approfondimenti sui temi trattati nelle presenti linee guida.

| TITOLO E INDIRIZZO DI PUBBLICAZIONE |
|---|
| NIST SP 800-61r2. Computer Security Incident Handling Guide. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf |
| NIST SP 800-61r3. Incident Response Recommendations and Considerations for Cybersecurity Risk Management. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf |

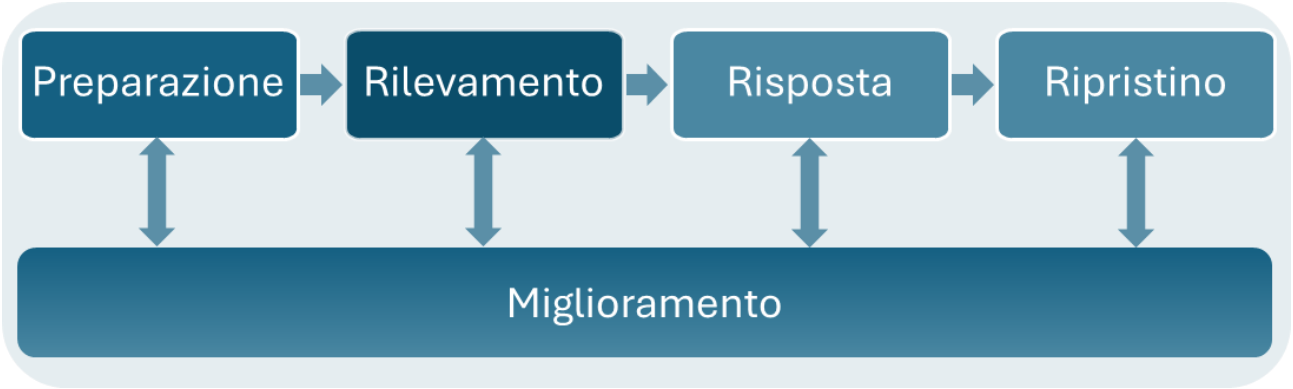
| |
|---|
| TTP-Based Hunting. https://www.mitre.org/sites/default/files/2021-11/prs-19-3892-ttp-based-hunting.pdf |
| Cybersecurity Incident & Vulnerability Response Playbooks. https://www.cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf |
| Framework Nazionale per la Cybersecurity e la Data Protection https://www.cybersecurityframework.it/ |

# 2. Processo per la gestione degli incidenti

In questo capitolo viene presentato un modello di processo per la gestione degli incidenti definito sulla base di quello riportato nel documento del NIST *Incident Response Recommendations and Considerations for Cybersecurity Risk Management SP 800-61r3*.

Il modello di processo è articolato nelle seguenti fasi che sono descritte nei successivi paragrafi del capitolo:

- **preparazione**: precede il verificarsi di un incidente e costituisce la base per una riposta efficace degli incidenti di sicurezza, include le attività di *governo*, *identificazione* e *protezione*;
- **rilevamento**: è volta a rilevare tempestivamente il verificarsi di un incidente;
- **risposta**: riguarda le attività vere e proprie di risposta all'incidente rilevato nella fase precedente, include le attività di *investigazione*, *notifica*, *contenimento* ed *eradicazione* dell'incidente;
- **ripristino**: consiste nel ripristino dei sistemi informativi e di rete oggetto di compromissione;
- **miglioramento**: individua le azioni da realizzare per migliorare il processo di gestione degli incidenti utilizzano le conoscenze acquisite durante l'esecuzione del processo. In considerazione del fatto che può essere acquisita conoscenza durante tutte le varie fasi del processo, la fase di *miglioramento* si estende lungo tutto il processo di gestione degli incidenti.




Il processo di gestione degli incidenti viene generalmente descritto e documentato nel cosiddetto **piano di gestione degli incidenti**, all'interno del quale sono indicate, ad esempio, le attività da porre in essere per la gestione dell'incidente, le strutture organizzative e tecniche coinvolte, gli strumenti da utilizzare e la reportistica da produrre.

Si osserva, inoltre, che il modello di processo sopra illustrato risulta allineato con la struttura del **Framework Nazionale per la Cybersecurity e la Data Protection (FNCS)**[2], organizzato nelle funzioni *Governo*, *Identificazione* e *Protezione* riguardanti le attività di preparazione e il miglioramento delle pratiche di gestione sulla base delle conoscenze acquisite nel rispondere agli incidenti, nonché *Rilevamento*, *Risposta* e *Ripristino*, relative alle attività di monitoraggio, risposta e ripristino dagli incidenti.

Il *Framework Nazionale* supporta le organizzazioni che necessitano di strategie e processi volti alla protezione dei dati personali e alla sicurezza *cyber*. L 'elemento principale è il cosiddetto *Framework Core* che indica una

[2] Per maggiori approfondimenti si può consultare la pagina web del framework https://www.cybersecurityframework.it/.

serie di *obiettivi di sicurezza* organizzati in una struttura gerarchica articolata in *funzioni*, *categorie* e *sottocategorie*.

Grazie all'allineamento del modello di processo con il *Framework Nazionale*, le attività poste in essere dai soggetti durante le varie fasi del processo di gestione degli incidenti sono coerenti con le misure di sicurezza previste dal quadro regolatorio cyber nazionale [3], in quanto tali misure sono state sviluppate in accordo al Framework[4].

Il Framework rappresenta, inoltre, uno strumento per implementare un'adeguata gestione del rischio *cyber*.

In tal senso, può essere utilizzato dalle organizzazioni per valutare il proprio livello di maturità in tema di gestione degli incidenti, sulla base degli *obiettivi di sicurezza* del Framework relativi alla gestione degli incidenti, e definire – in accordo al modello di processo qui presentato – le attività necessarie da porre in essere per raggiungere tali obiettivi.

Come riferimento per l'individuazione di tali obiettivi, in Appendice A sono riportati, in termini di categorie e sottocategorie del Framework[5], quelli più specificatamente connessi alla gestione degli incidenti.

## 2.1. Preparazione

La fase di *preparazione* – costituita dalle sotto-fasi di *governo*, *identificazione* e *protezione* discusse nelle successive sezioni del presente paragrafo – riguarda tutte le attività propedeutiche volte a garantire una gestione strutturata ed efficace degli incidenti di sicurezza quali, ad esempio, la definizione di politiche, l'assegnazione di ruoli e responsabilità, il censimento dei sistemi informativi e di rete, la definizione di misure di sicurezza atte a prevenire il verificarsi di un incidente o a mitigarne l'impatto.

### 2.1.1. Governo

In questa sotto-fase è definito il quadro strategico e organizzativo per la gestione degli incidenti, come, ad esempio, l'elaborazione di politiche per la gestione degli incidenti di sicurezza e l'assegnazione di ruoli e responsabilità.

Esempi di tematiche oggetto di politiche sono:

- Il piano di gestione degli incidenti;
- la categorizzazione, i livelli di impatto e la criticità degli incidenti;
- la notifica degli incidenti;
- la comunicazione interna ed esterna;
- la formazione e la sensibilizzazione del personale;
- la conformità normativa.

[3] Con riferimento, in particolare, al Perimetro di Sicurezza Nazionale Cibernetica, alla Legge 90/2024, al Regolamento Cloud per la Pubblica Amministrazione e al Decreto NIS.

[4] L'identificativo e la descrizione delle varie misure fanno riferimento, infatti, alle sottocategorie del Framework.

[5] Come osservato, categorie sottocategorie rappresentano infatti obiettivi di sicurezza con maggiore livello di dettaglio.

Con riferimento all'assegnazione dei ruoli e delle responsabilità, a seguire sono indicati, a titolo di esempio, ruoli e relative responsabilità generalmente presenti nel processo di gestione degli incidenti:

- **organizzazione per la sicurezza informatica**: governa il processo prendendo decisioni strategiche;
- **responsabile della gestione dell'incidente**: coordina e gestisce la risposta dell'incidente;
- **IRT (Incident Response Team)**: conduce le attività di investigazione, contenimento e ripristino;
- **SOC (Security Operation Center)**: effettua le attività di monitoraggio e analizza gli eventi rilevanti per la sicurezza;
- **ufficio IT**: gestisce l'infrastruttura informatica;
- **ufficio legale**: valuta gli obblighi legali;
- **ufficio comunicazione**: gestisce le attività di comunicazione.

In taluni casi, anche le terze parti possono svolgere un ruolo importante nel processo di gestione degli incidenti. Si pensi, ad esempio, a un fornitore di servizi di sicurezza gestiti (*managed security service provider* – MSSP) che esegue attività di analisi degli eventi rilevanti per la sicurezza o a un fornitore di servizi cloud che fornisce supporto nelle attività di ripristino dagli incidenti.

Pertanto, nell'ambito della gestione degli incidenti è fondamentale definire ruoli e responsabilità anche per le terze parti, che devono essere chiaramente definiti a livello contrattuale. In considerazione del livello di accesso ai sistemi che potrebbe avere un fornitore o della conoscenza che acquisisce nella gestione degli incidenti, è inoltre opportuno prevedere appositi termini contrattuali come, ad esempio, accordi di non divulgazione (NDA) e clausole di riservatezza.

Con riguardo alle figure professionali coinvolte nel processo di gestione degli incidenti, si può fare altresì riferimento alle linee guida per la realizzazione di CSIRT dell'Agenzia per la cybersicurezza nazionale[6].

Uno degli strumenti maggiormente utilizzati per l'assegnazione di ruoli e responsabilità, è la matrice di assegnazione responsabilità (cosiddetta *matrice RACI*) che permette di definire chiaramente ruoli e responsabilità per le varie attività di un processo. In particolare, RACI è un acronimo le cui lettere indicano la tipologia di responsabilità che un certo ruolo ha nell'ambito di una determinata attività:

- **Responsible (R)**: chi esegue operativamente l'attività.
- **Accountable (A)**: chi ha la responsabilità sul risultato dell'attività.
- **Consulted (C)**: chi viene consultato durante l'esecuzione dell'attività in quanto possiede conoscenze necessarie al completamento dell'attività.
- **Informed (I)**: chi è informato sull'avanzamento e il completamento dell'attività.

Per ogni attività deve essere presente almeno un *Responsible* in modo da individuare chi ha il compito di eseguire operativamente l'attività ed un solo *Accountable* in modo da definire chiaramente chi ha la responsabilità sul risultato dell'attività.

[6] Le linee guida sono pubblicate all'indirizzo https://www.acn.gov.it/portale/documents/d/guest/acn_linee_guida_csirt.

Per assegnare i ruoli e le responsabilità di un processo tramite matrici RACI sono preliminarmente individuati i ruoli – intesi come strutture organizzative o specifiche figure quale, ad esempio, quella del responsabile della gestione dell'incidente – e quindi assegnate la tipologia di responsabilità per le varie attività.

A seguire è riportato un esempio di matrice RACI per un generico processo costituito da n fasi.

| Fase | Attività | Ruolo 1 | Ruolo 2 | Ruolo m |
|---|---|---|---|---|
| Fase 1 | Attività 1 | A, R | C | I |
| Fase 1 | Attività 2 | R | A, R | – |
| Fase 1 | Attività … | A | R | C |
| Fase 2 | Attività 1 | A, R | I | C |
| Fase 2 | Attività 2 | I | – | A, R |
| Fase 2 | Attività … | A, R | I | I |
| Fase n | Attività 1 | C | I | A, R |
| Fase n | Attività 2 | R | – | A |
| Fase n | Attività … | A, R | C | C |

### 2.1.2. Identificazione

In questa sotto-fase è acquisita una conoscenza del contesto operativo al fine di pianificare in modo efficace la risposta agli incidenti. Le attività di *Identificazione* riguardano, ad esempio, l'inventario dei sistemi informativi e di rete (le informazioni relative a tale inventario permettono infatti di individuare i sistemi da proteggere, determinare le priorità per le attività di risposta e recupero e rilevare in modo più efficace gli incidenti) e l'individuazione di minacce e vulnerabilità (la conoscenza di minacce e vulnerabilità permette infatti di migliorare la prevenzione dell'incidente e favorire una risposta più rapida e mirata).

### 2.1.3. Protezione

In questa sotto-fase sono stabilite le misure, *tecnologiche* e *organizzative*, per abbassare la probabilità e limitare l'impatto degli incidenti.

Tra le misure di protezione *tecnologiche* sono comprese, ad esempio, quelle relative alla predisposizione degli strumenti di sicurezza per controllo degli accessi e per il monitoraggio, la configurazione dei sistemi informativi e di rete per l'acquisizione dei log, la pianificazione dei backup dei dati e delle configurazioni e la definizione delle soluzioni di *business continuity* e *disaster recovery*.

Ridurre il numero di incidenti consente di dedicare maggiori risorse alla risposta degli incidenti più critici e complessi, mentre limitare l'impatto dell'incidente rende generalmente meno complesse le attività di contenimento ed eradicazione, oltre a mitigare le conseguenze dell'attacco, in termini non solo di sistemi informativi e di rete compromessi, ma anche operativi, economici e reputazionali.

Tra le misure di protezione *organizzative* sono invece comprese la predisposizione dei modelli per la comunicazione interna ed esterna durante un incidente – incluse le comunicazioni e le notifiche alle autorità

competenti – prevedendo anche canali alternativi in caso di malfunzionamento dei canali di comunicazione principali e le attività di formazione del personale del personale in materia di sicurezza informatica con le relative esercitazioni.

## 2.2. Rilevamento

La fase di *rilevamento* è finalizzata a individuare e analizzare gli **eventi rilevanti per la sicurezza** al fine di identificare tempestivamente il verificarsi di un incidente e limitarne l'impatto e l'estensione.

Gli *eventi rilevanti per la sicurezza informatica* sono eventi di natura intenzionale o accidentale che *potrebbero* compromettere la sicurezza dei sistemi informativi e di rete e che necessitano pertanto di un'analisi (*triage*) al fine di verificare se si tratta di un incidente.

Esempi di eventi rilevanti per la sicurezza informatica sono:

- tentativi di autenticazioni su molteplici utenze di dominio da medesimi hostname/indirizzo IP;
- modifiche ai gruppi degli amministratori di dominio;
- autenticazioni da *hostname* e/o indirizzi IP identificati come IOC;
- richieste alle applicazioni web da user agent identificati come IOC;
- esecuzione di script che usano determinati comandi;
- accessi degli amministratori di dominio e/o in VPN al di fuori del normale orario lavorativo e/o da postazioni di lavoro diverse da quelle ordinarie;
- comunicazioni di rete sospette (verso *url* e/o indirizzi IP identificati come IOC);
- picco di traffico proveniente da molteplici indirizzi IP;
- saturazione della larghezza di banda in entrata.

Al fine di individuare gli eventi rilevanti per la sicurezza, è necessario prevedere **attività di monitoraggio** che possono essere realizzate secondo i seguenti approcci[7]:

- **proattivo**: gli eventi rilevanti per la sicurezza sono individuati, ad esempio, a seguito della ricerca di indizi di attività malevole sui sistemi[8], o dall'analisi dei bollettini di sicurezza condivisi dal CSIRT Italia, circa nuovi scenari di rischio, comportamenti anomali o attacchi in corso;
- **reattivo**: gli eventi rilevanti per la sicurezza sono individuati, ad esempio, in esito agli *allarmi* generati dagli strumenti di sicurezza o alle segnalazioni di attori interni (utenti che riportano malfunzionamenti o disservizi) e/o esterni come il CSIRT Italia.

[7] Per aumentare l'efficacia del monitoraggio, è opportuno adottare entrambi gli approcci.

[8] Si parla anche di *Threat Hunting* per indicare quelle metodologie di rilevamento che mirano ad *anticipare* le minacce, prima che causino danni, tramite la ricerca *attiva* di segni di compromissione all'interno di una rete o di un sistema informativo.

Le *attività di monitoraggio* sono pianificate e implementate sulla base di una preventiva analisi del rischio, svolta nella fase di preparazione, al fine di identificare i sistemi informativi e di rete maggiormente critici e le possibili vulnerabilità[9], e sono coerentemente allineate alle politiche previste per la gestione degli incidenti.

La ricerca di possibili indizi di attività malevole e la configurazione degli *allarmi* generati dagli strumenti di sicurezza si basano su *logiche di rilevamento* che possono essere definite in accordo alle seguenti metodologie:

- **IOC-based**: si basa sulla ricerca di indicatori di compromissione (caratteristiche statiche del malware come *hash*, nomi di file, librerie) nei log dei sistemi. Non permette di rilevare minacce che non sono caratterizzate dagli indicatori noti o che li cambiano.
- **anomaly-based:** si basa sul rilevamento di deviazioni da parte dei sistemi informativi o parti di essi dal loro comportamento *standard* attraverso l'analisi statistica, il *machine learning* e altre forme di analisi di grandi quantità di dati (*big data analysis*). Richiede generalmente una modellazione molto accurata del comportamento *standard* rispetto al quale rilevare deviazioni e, pertanto, potrebbe generare molti falsi positivi e richiedere investimenti significativi in termini di acquisizione dei dati e loro processamento;
- **TTP-based**: si basa sulla conoscenza delle tattiche, tecniche e procedure (TTPs) che un attore malevolo utilizza per raggiungere i propri obiettivi. È efficace perché le TTPs non cambiano frequentemente e sono comuni ai vari attori in quanto la tecnologia sulla quale opera l'attaccante vincola il numero e il tipo di tecniche che questi può utilizzare.

Gli eventi rilevanti per la sicurezza individuati sono quindi analizzati per verificare se si riferiscono a incidenti di sicurezza.

Il numero di eventi rilevanti per la sicurezza da analizzare può essere molto elevato e di complessa gestione senza il supporto di tecnologie automatizzate. A tal fine possono essere utilizzati strumenti di sicurezza come ad esempio il *SIEM*, il *SOAR* o l'*EDR*[10] che agevolano l'individuazione degli eventi rilevanti per la sicurezza.

Tali strumenti devono essere opportunamente configurati al fine di ridurre gli *allarmi* che non corrispondono ad incidenti, generalmente indicati come **falsi positivi**. Per ridurre il numero di *falsi positivi*, nella fase di *miglioramento* è opportuno effettuare un *tuning* delle logiche di rilevamento sulla base dell'analisi effettuata sui falsi positivi. Ad esempio, nel caso di falsi positivi persistenti, si potrà valutare la possibilità di aggiornare le logiche di rilevamento in modo da escludere tali eventi da quelli segnalati.

La Cyber Threat Intelligence (CTI) può supportare l'individuazione tempestiva di attività malevole, limitarne l'impatto e ridurre i tempi di riposta e ripristino.

---

[9] Possibili strategie per individuare i sistemi informativi e di rete maggiormente critici e le vulnerabilità sono rispettivamente la *Crown Jewel Analysis (CJA)* e la *Threat Model (TM)*.

[10] Il SIEM (*Security Information and Event Management*), il SOAR (*Security Orchestration, Automation and Response)* e l'EDR (*Endpoint Detection Response*) sono strumenti di sicurezza utilizzati, rispettivamente, per la raccolta e analisi dei log, l'automazione e il coordinamento delle attività di risposta agli incidenti e il rilevamento e la risposta delle minacce presenti sugli *endpoint*.

La **Cyber Threat Intelligence** si occupa della raccolta, analisi e diffusione di informazioni sulle minacce cyber e, vulnerabilità con l'obiettivo di prevenire, rilevare e rispondere agli attacchi informatici.

Possono essere individuate le seguenti categorie di Threat Intelligence:

- **strategica**: è un'informazione di alto livello, destinata ai responsabili delle decisioni. Generalmente non è un'informazione tecnica, può riguardare aspetti come l'impatto economico di una attività cyber, i pattern di attacco e le aree che potrebbero influire sulle decisioni aziendali ad alto livello;
- **operativa**: è un'informazione che tratta specifici attacchi imminenti contro l'organizzazione ed è di competenza del personale di sicurezza di alto livello;
- **tattica**: si riferisce a tattiche, tecniche e procedure (TTP) e fornisce informazioni su come gli avversari portano avanti i propri attacchi;
- **technical**: riguarda i dati utilizzati dagli strumenti tecnici per il monitoraggio e l'analisi delle compromissioni; ad esempio, un indirizzo IP legato a un server di comando e controllo o l'*hash* di un *malware* rilevato su un *endpoint*.

Nel caso in cui l'analisi di un evento rilevante per la sicurezza abbia effettivamente determinato che è relativo a un incidente, viene dichiarato l'incidente e si passa alla successiva fase di *risposta*.

## 2.3. Risposta

La fase di *risposta* – costituita dalle sotto-fasi di *investigazione*, *notifica*, *contenimento* ed *eradicazione* discusse nelle successive sezioni del presente paragrafo – inizia nel momento in cui è stato dichiarato l'incidente e rappresenta la fase centrale del processo di gestione degli incidenti.

Con riferimento alle varie sotto-fasi, si osserva che le stesse non seguono generalmente un ordine lineare ma tendono piuttosto a essere realizzate in parallelo, in modo strettamente interlacciato. Inoltre, non tutte devono essere necessariamente implementante per ogni tipo di evento: potrebbero esserci infatti eventi che non richiedono attività di *contenimento* e/o *eradicazione*, come, ad esempio, nel caso di eventi per i quali non c'è stato alcun impatto.

### 2.3.1. Investigazione

In questa sotto-fase viene esaminato in modo approfondito l'incidente. L'obiettivo è ricostruire possibilmente l'intera sequenza degli eventi occorsi (cosiddetta *cyber kill chain*), individuare la causa dell'incidente e valutare l'estensione della compromissione.

Considerato che le successive attività potrebbero far emergere nuovi elementi informativi tali da richiedere lo svolgimento di ulteriori attività di analisi e approfondimento per ricostruire la dinamica dell'incidente, potrebbe essere necessario tornare nuovamente alla sotto-fase di investigazione nel corso delle attività di risposta. Ad esempio, a seguito della notifica di incidente allo CSIRT Italia, questo potrebbe fornire nuovi elementi, quali indicatori di compromissione, per proseguire le attività di investigazione, o, ancora, durante la fase di eradicazione potrebbe essere rilevato un nuovo artefatto malevolo, che potrebbe richiedere di svolgere ulteriori approfondimenti sulla causa o sull'estensione dell'incidente.

Le attività di investigazione riguardano, ad esempio:

- l'acquisizione delle evidenze forensi;
- la valutazione del perimetro compromesso in termini di comprensione del contesto e dell'estensione dell'incidente;
- la caratterizzazione dell'incidente almeno in termini di categoria (ad esempio, *ransomware* oppure *DDOS*), impatto e severità;
- l'esame dell'incidente tramite acquisizione di log dei sistemi, artefatti ed evidenze rilevati, correlazione di eventi e attività dell'attaccante, predisposizione della *timeline* degli eventi occorsi, identificazione del vettore di attacco e della possibile causa dell'incidente, individuazione e documentazione degli IOC;
- la definizione delle prime attività di risposta dell'incidente come, ad esempio, eventuali azioni di contenimento preventivo (e.g. disabilitazione delle utenze compromesse, isolamento dei sistemi compromessi dalla rete, blocco dei flussi di comunicazione da e verso gli indicatori di compromissione);
- la valutazione del supporto di terze parti per la gestione dell'incidente (ad esempio supporto per le indagini forensi);
- la valutazione della presenza di ulteriori vettori di attacco e meccanismi di persistenza multipli.

Con riferimento alla caratterizzazione dell'incidente, al fine di disporre di un *linguaggio comune* si può far riferimento alla tassonomia cyber dell'Agenzia per la cybersicurezza nazionale[11].

### 2.3.2. Notifica

In questa sotto-fase si procede a notificare, obbligatoriamente se previsto dalle normative vigenti, l'occorrenza dell'incidente alle autorità competenti e a comunicarlo alle parti, interne ed esterne, interessate.

Con riguardo agli obblighi di notifica verso l'Agenzia per la Cybersicurezza Nazionale si faccia riferimento alla guida alla notifica degli incidenti al CSIRT Italia[12].

Nel caso in cui il soggetto non sia tenuto ai sensi della normativa vigente a notificare l'incidente allo CSIRT Italia, è sempre possibile procedere alla notifica volontaria attraverso la piattaforma di notifica del CSIRT Italia.

In accordo alle politiche definite a riguardo, si procede inoltre a comunicare l'incidente alle parti interne (come, ad esempio, i vertici del soggetto o l'ufficio legale) ed esterne (come, ad esempio, utenti impattati, fornitori o altri soggetti coinvolti) interessate.

### 2.3.3. Contenimento

In questa sotto-fase viene circoscritto il perimetro dell'attacco in modo da limitare l'impatto dell'incidente ed evitarne l'estensione ad altri sistemi informativi e di rete. Se al termine della sotto-fase si rilevano ancora evidenze di compromissione, sarà necessario tornare alla sotto-fase di *investigazione*.

Le attività di contenimento riguardano, ad esempio:

[11] La tassonomia è pubblicata all'indirizzo https://www.acn.gov.it/portale/w/la-tassonomia-cyber-dellacn.

[12] La guida è pubblicata all'indirizzo https://www.acn.gov.it/portale/w/guida-alla-notifica-degli-incidenti-informatici.

- la definizione della strategia di contenimento tenendo conto almeno dell'esigenza di preservare le evidenze, dei requisiti di disponibilità dei servizi (livelli di servizio attesi), delle risorse umane e finanziarie disponibili, delle tempistiche;
- l'isolamento dei sistemi e i segmenti di rete coinvolti nell'incidente prevedendo almeno di: implementare regole sui sistemi perimetrali in base agli indicatori di compromissione individuati, bloccare gli accessi non autorizzati e le sorgenti dei malware, disabilitare account compromessi;
- il monitoraggio delle eventuali attività malevole a seguito delle azioni di contenimento;
- la verifica della presenza di ulteriori possibili meccanismi di persistenza;
- l'aggiornamento della timeline dell'attacco con le evidenze rilevate in questa fase.

Al fine di garantire tracciabilità e coerenza delle azioni intraprese, è opportuno redigere un piano delle attività di contenimento all'interno del quale documentare almeno le seguenti informazioni:

- sistemi informativi e di rete impattati dalle attività;
- obiettivi delle attività di contenimento;
- attività di contenimento individuate e loro motivazioni;
- strutture tecniche e organizzative coinvolte nelle attività di contenimento;
- impatto stimato sull'operatività delle attività di contenimento;
- modalità di verifica dell'efficacia delle attività di contenimento;
- esiti attesi delle attività di contenimento.

### 2.3.4. Eradicazione

In questa sotto-fase viene rimossa ogni capacità di controllo e persistenza nella rete da parte dell'attaccante. Se al termine della sotto-fase sono rilevate ancora attività malevole, sarà necessario tornare alla sotto-fase di *Investigazione*.

Le attività di eradicazione riguardano, ad esempio:

- la bonifica delle credenziali utilizzate dall'attaccante;
- la rimozione degli artefatti malevoli dai sistemi e dalle reti interessate;
- la bonifica dei sistemi compromessi;
- la risoluzione o mitigazione delle vulnerabilità sfruttate dall'attaccante;
- l'installazione degli aggiornamenti, in particolare quelli di sicurezza;
- il monitoraggio delle eventuali reazioni dell'attaccante alle attività di eradicazione;
- l'aggiornamento della timeline dell'attacco con le evidenze rilevate in questa fase;
- l'esecuzione di ulteriori scansioni per verificare la presenza di malware.

Al fine di garantire tracciabilità e coerenza delle azioni intraprese, è opportuno redigere un piano delle attività di eradicamento all'interno del quale documentare almeno le seguenti informazioni:

- sistemi informativi e di rete impattati dalle attività;
- obiettivi delle attività di eradicazione;

- attività di eradicazione individuate e loro motivazioni;
- strutture tecniche e organizzative coinvolte nelle attività di eradicazione;
- modalità di verifica dell'efficacia delle attività di eradicazione;
- esiti attesi delle attività di eradicazione.

## 2.4. Ripristino

La fase di *ripristino* è finalizzata a riportare i sistemi informativi allo stato antecedente all'incidente, assicurandosi che tutto funzioni regolarmente.

Le attività di questa fase riguardano, ad esempio:

- la creazione di *golden/clean image*[13];
- la reinstallazione dei i sistemi a partire dalle *golden/clean image*;
- il ricollegamento in rete dei sistemi informativi e di rete bonificati;
- il monitoraggio dei sistemi per verificare l'efficacia delle attività.

Al fine di garantire tracciabilità e coerenza delle azioni intraprese, è opportuno redigere un piano delle attività di ripristino all'interno del quale documentare almeno le seguenti informazioni:

- sistemi informativi e di rete impattati;
- obiettivi delle attività di ripristino;
- attività di ripristino individuate e loro motivazioni;
- strutture tecniche e organizzative coinvolte nelle attività di ripristino;
- modalità di verifica dell'efficacia delle attività di ripristino;
- esiti attesi delle attività di ripristino.

## 2.5. Miglioramento

La fase di *miglioramento* è finalizzata a incrementare la capacità di gestione degli incidenti e riguarda attività quali, ad esempio, l'analisi post-incidente, le esercitazioni, la revisione delle procedure, l'aggiornamento delle politiche e la condivisione delle conoscenze acquisite.

A tal fine, sono ad esempio organizzate le cosiddette riunioni di *lesson learned* in cui si ha l'opportunità di trarre insegnamenti alla luce di quanto emerso durante la gestione dell'incidente, dalle azioni intraprese e dalla loro efficacia e di individuare gli interventi correttivi e di potenziamento. Nell'ambito di tali riunioni sono generalmente affrontate tematiche quali, ad esempio:

- la valutazione sulla corretta esecuzione delle procedure previste e della loro adeguatezza;
- le criticità emerse durante l'esecuzione del processo di risposta;

[13] Per immagine *golden o clean* si intende la copia originale e ben configurata di un sistema informativo che può essere utilizzata per ripristinare il sistema ad uno stato consistente, funzionante e non compromesso dal punto di vista della sicurezza).

- l'identificazione di ruoli, responsabilità, interlocutori e autorità non chiari o non definiti;
- le proposte migliorative per la condivisione delle informazioni;
- la necessità di ulteriori strumenti o risorse per migliorare il rilevamento e il processo di gestione e risposta agli incidenti;
- le attività da realizzare per prevenire il ripetersi di incidenti simili;
- gli indicatori di compromissione (IOC) rilevati da monitorare;
- la valutazione dell'adeguatezza delle misure di sicurezza esistenti;
- l'identificazione delle politiche e delle procedure da modificare per evitare il ripetersi di incidenti simili.

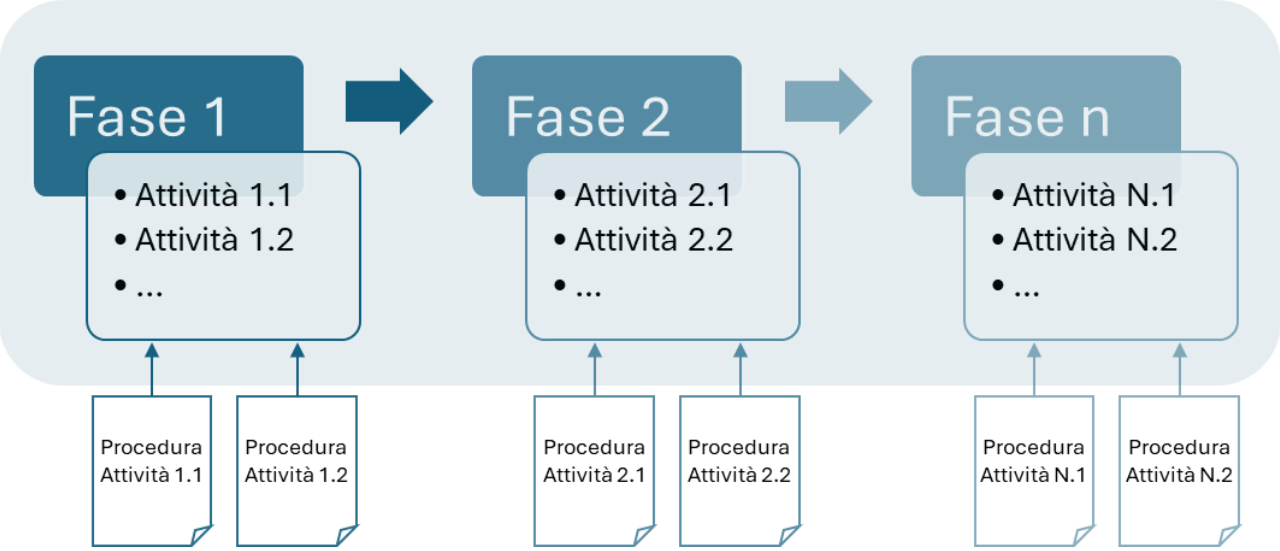
Gli esiti di tali riunioni sono la base per definire gli interventi di miglioramento necessari per risolvere le questioni emerse durante la gestione dell'incidente e possono comprendere, ad esempio, l'aggiornamento delle procedure di politiche e procedure, l'implementazione di nuove logiche di rilevamento e la previsione di specifiche attività di formazione.

Le attività di miglioramento includono inoltre la valutazione periodica (tramite, ad esempio, autovalutazioni o valutazioni di terzi) delle prestazioni – anche attraverso l'utilizzo di indicatori e metriche (*Key Performance Indicator - KPI*[14]) – della gestione degli incidenti e la conduzione di esercitazioni e test sul piano di gestione degli incidenti.

[14] Esempi di KPI sono il *Mean Time to Detect (MTTD)* definito come il tempo medio impiegato per rilevare un incidente e il *Mean Time to Resolution/Repair (MTTR)* definito come il tempo medio necessario per risolvere un incidente.

# 3. Procedure per la gestione degli incidenti

L'uso di procedure per la gestione degli incidenti consente di guidare le attività del processo di gestione degli incidenti in modo strutturato, migliorando l'efficienza operativa, riducendo il rischio di errori e in conformità con le politiche stabilite. L'obiettivo di una procedura è garantire una risposta coerente e ripetibile a fronte di situazioni critiche od operative.




Esempi di procedure per la gestione degli incidenti sono:

- **procedura per la notifica degli incidenti**: definisce le modalità, le tempistiche e i canali di comunicazione attraverso cui notificare un incidente di sicurezza alle autorità competenti;
- **procedura per la configurazione degli allarmi**: stabilisce i parametri e le soglie per la generazione automatica di allarmi da parte dei sistemi di monitoraggio, al fine di rilevare comportamenti anomali o potenziali minacce;
- **procedura per l'acquisizione delle evidenze forensi**: descrive le procedure per l'acquisizione, la conservazione e la documentazione delle evidenze digitali;
- **procedura per la bonifica dei sistemi compromessi**: dettaglia le azioni da intraprendere per rimuovere gli artefatti malevoli e risolvere le vulnerabilità dai sistemi informativi e di rete oggetto di compromissione;
- **procedura per il ripristino dei sistemi a partire dai backup**: indica le modalità operative per il recupero dell'operatività dei sistemi attraverso il ripristino dei dati e delle configurazioni a partire dai backup precedentemente effettuati.

Le procedure sono strutturate secondo un formato standard[15] che prevede la presenza di elementi ricorrenti quali ad esempio:

- **titolo e versione**: indica l'oggetto della procedura e il suo numero di versione;

[15] Procedure formalizzate che forniscono istruzioni dettagliate su come eseguire specifiche attività sono anche denominate **SOP (Standard Operating Procedure)**.

- **ambito di applicazione**: definisce il contesto operativo, le aree e i soggetti a cui la procedura si rivolge;
- **attività operative**: elenca in ordine sequenziale le azioni e i controlli da svolgere per garantire la corretta esecuzione della procedura;
- **strumenti utilizzati**: descrive gli strumenti necessari per l'implementazione della procedura.
- **ruoli e responsabilità**: specifica le figure coinvolte e le relative responsabilità nell'esecuzione della procedura;

Le procedure devono essere aggiornate e testate periodicamente per garantirne la coerenza con l'evoluzione del contesto tecnico e normativo e verificarne l'applicabilità, l'accuratezza e l'efficacia; possono essere inoltre utilizzate per formare il personale su come agire correttamente a fronte di specifiche attività operative.

A seguire è riportato, a titolo di esempio [16], una procedura per il ripristino dei sistemi a partire dai backup.

### Titolo e versione

- Procedura per il ripristino dei sistemi a partire dai backup. V.1.0 – 01/10/2025.

### Ambito di applicazione

- La procedura in questione definisce le modalità operative per il ripristino dei sistemi informativi e di rete dell'organizzazione a partire dai backup in caso di malfunzionamenti, guasti hardware/software, incidenti di sicurezza o perdita di dati. L'obiettivo è garantire il ripristino sicuro, completo e verificabile dei sistemi informativi e di rete, minimizzando tempi di inattività e perdita di dati

### Attività operative

- Confermare la necessità del ripristino.
- Notificare alle parti interessate l'avvio della procedura.
- Identificare i sistemi informativi di rete da ripristinare.
- Selezionare il backup più recente valido e sicuro.
- Verificare l'integrità dei supporti di backup.
- Preparare gli account e le credenziali necessari per il ripristino.
- Avviare il processo di ripristino dal backup selezionato.
- Monitorare lo stato del ripristino per eventuali errori o anomalie.
- Verificare l'integrità dei dati ripristinati,
- Controllare il corretto funzionamento dei sistemi informativi e di rete ripristinati anche in termini di accesso degli utenti.
- Documentare l'esito del ripristino, eventuali problemi riscontrati e azioni correttive adottate.
- Notificare alle parti interessate gli esiti e la chiusura della procedura di ripristino.

[16] La procedura è presentata per l'appunto a titolo esemplificativo e non ha carattere esaustivo.

## Strumenti utilizzati

- Software di backup e ripristino.
- Storage o supporti di backup (NAS, SAN, *cloud storage*, ecc.).
- Console di gestione dei sistemi e dei server.
- Strumenti di verifica integrità dati (*checksum*, log di ripristino).
- Documentazione dei backup e procedure operative interne.

## Ruoli e responsabilità[17]

| Attività | OSI | RGI | IRT | SOC | IT | LEG | COM |
|---|---|---|---|---|---|---|---|
| *OSI: organizzazione sicurezza informatica, RGI: responsabile gestione incidenti, IRT: Incident Response Team, SOC: Security Operation Center, IT: Ufficio IT, LEG: ufficio legale, COM: ufficio comunicazione.* | | | | | | | |
| Confermare la necessità del ripristino. | C | A | R | C | C | C | I |
| Notificare alle parti interessate avvio procedura. | I | A | I | I | I | I | R |
| Identificare i sistemi informativi di rete da ripristinare. | I | A | R | C | C | – | – |
| Selezionare il backup più recente valido e sicuro. | A | C | C | C | R | – | – |
| Verificare l'integrità dei supporti di backup. | A | C | C | – | R | – | – |
| Preparare gli account e le credenziali necessari per il ripristino. | A | C | C | C | R | – | – |
| Avviare il processo di ripristino dal backup selezionato. | A | C | C | C | R | I | I |
| Monitorare lo stato del ripristino per eventuali errori o anomalie. | A | C | C | C | R | – | – |
| Verificare l'integrità dei dati ripristinati, | A | C | C | C | R | – | – |
| Controllare il corretto funzionamento dei sistemi informativi e di rete ripristinati anche in termini di accesso degli utenti. | A | R | C | C | R | – | – |
| Documentare l'esito del ripristino, eventuali problemi riscontrati e azioni correttive adottate. | A | R | I | I | R | – | – |
| Notificare alle parti interessate gli esiti e la chiusura della procedura di ripristino. | A | R | C | I | I | I | I |

[17] I ruoli riportati sono quelli indicati a titolo esemplificativo nel paragrafo Governo. I ruoli e le responsabilità assegnati sono a carattere puramente indicativo e dovranno essere effettivamente determinati dall'organizzazione sulla base del proprio contesto tecnico-organizzativo.

# Appendice A: obiettivi gestione incidenti

Nella seguente tabella sono riportati gli obiettivi di sicurezza più specificatamente connessi alla gestione degli incidenti, riportati in termini di codice e descrizione delle categorie e sottocategorie del Framework Nazionale.

Tale specificità è stata valutata sulla base della priorità assegnata alle categorie e sottocategorie nel documento del NIST *Incident Response Recommendations and Considerations for Cybersecurity Risk Management SP 800-61r3*[18] considerando, in particolare, categorie e sottocategorie contrassegnate con priorità alta[19].

| CODICE | DESCRIZIONE |
|---|---|
| GV.PO | La politica di cybersecurity dell'organizzazione è stabilita, comunicata e applicata. |
| ID.RA-02 | Le informazioni di cyber threat intelligence sono ricevute da forum e fonti di condivisione delle informazioni. |
| ID.RA-05 | Minacce, vulnerabilità, probabilità e impatti sono utilizzati per comprendere il rischio inerente e per informare la prioritizzazione della risposta al rischio. |
| ID.RA-06 | Le risposte al rischio sono scelte, prioritizzate, pianificate, monitorate e comunicate. |
| ID.IM-02 | Sono identificati miglioramenti in esito ai test e alle esercitazioni di sicurezza, compresi quelli effettuati in coordinamento con i fornitori e le terze parti interessate. |
| ID.IM-03 | Sono identificati miglioramenti dall'esecuzione di processi, procedure e attività operativi. |
| ID.IM-04 | I piani di risposta agli incidenti e gli altri piani di cybersecurity che impattano le operazioni sono stabiliti, comunicati, mantenuti e migliorati. |
| PR.DS-11 | I backup dei dati sono creati, protetti, mantenuti e verificati. |
| DE.CM | Gli asset sono monitorati per individuare anomalie, indicatori di compromissione e altri eventi potenzialmente avversi. |
| DE.CM-01 | Le reti e i servizi di rete sono monitorati per individuare eventi potenzialmente avversi. |
| DE.CM-03 | L'attività del personale e l'utilizzo della tecnologia sono monitorati per individuare eventi potenzialmente avversi. |
| DE.CM-06 | Le attività e i servizi dei fornitori di servizi esterni sono monitorati per individuare eventi potenzialmente avversi. |
| DE.CM-09 | L'hardware e il software di elaborazione, gli ambienti di *runtime* e i loro dati sono monitorati per individuare eventi potenzialmente avversi. |

[18] Sulla base del quale è stato definito il modello di processo di gestione degli incidenti qui presentato.

[19] Per le categorie e sottocategorie con priorità basse e media si può far riferimento alle tabelle 2 e 3 del documento del NIST.

| CODICE | DESCRIZIONE |
|---|---|
| DE.AE | Anomalie, indicatori di compromissione e altri eventi potenzialmente avversi sono analizzati per caratterizzare gli eventi e rilevare gli incidenti di cybersecurity. |
| DE.AE-02 | Gli eventi potenzialmente avversi sono analizzati per meglio comprenderne le attività associate. |
| DE.AE-03 | Le informazioni sono correlate da più fonti |
| DE.AE-04 | L'impatto e la portata stimati degli eventi avversi sono compresi. |
| DE.AE-06 | Le informazioni sugli eventi avversi sono fornite al personale e agli strumenti autorizzati. |
| DE.AE-07 | La cyber threat intelligence e le altre informazioni contestuali sono integrate nell'analisi |
| DE.AE-08 | Gli incidenti sono dichiarati quando gli eventi avversi soddisfano i criteri definiti per gli incidenti. |
| RS.MA | Le risposte agli incidenti di cybersecurity rilevati sono gestite. |
| RS.MA-01 | Il piano di risposta agli incidenti è eseguito in coordinamento con le terze parti interessate una volta dichiarato un incidente. |
| RS.MA-02 | I report sugli incidenti sono sottoposti a triage e convalidati. |
| RS.MA-03 | Gli incidenti sono categorizzati e prioritizzati |
| RS.MA-04 | Gli incidenti sono scalati (assegnati a meccanismi di risposta con risorse crescenti) o elevati (passati in gestione a un livello superiore) a seconda delle necessità. |
| RS.MA-05 | Sono applicati i criteri per l'avvio del ripristino dagli incidenti |
| RS.AN | Sono condotte indagini per garantire una risposta efficace e supportare le attività forensi e di ripristino. |
| RS.AN-03 | È eseguita un'analisi per stabilire cosa è avvenuto durante un incidente e la causa principale dell'incidente. |
| RS.AN-06 | Le azioni eseguite durante un'investigazione sono registrate e l'integrità e la provenienza delle registrazioni sono preservate. |
| RS.AN-07 | I dati e i metadati degli incidenti sono raccolti e la loro integrità e provenienza sono preservati |
| RS.AN-08 | La magnitudo di un incidente è stimata e convalidata. |
| RS.CO | Le attività di risposta sono coordinate con i portatori di interesse (stakeholder) interni ed esterni come richiesto da leggi, regolamenti o politiche. |
| RS.CO-02 | Gli stakeholder interni ed esterni sono informati degli incidenti. |
| RS.CO-03 | Le informazioni sono condivise con gli stakeholder interni ed esterni designati. |

| CODICE | DESCRIZIONE |
|---|---|
| RS.MI | Sono eseguite attività per prevenire l'espansione di un evento e mitigarne gli effetti. |
| RS.MI-01 | Gli incidenti vengono contenuti. |
| RS.MI-02 | Gli incidenti vengono eradicati. |
| RC.RP | Le attività di ripristino sono eseguite per garantire la disponibilità operativa dei sistemi e dei servizi interessati da incidenti di cybersecurity. |
| RC.RP-01 | La parte del piano di risposta agli incidenti relativa al rispristino viene eseguita una volta avviata dal processo di risposta agli incidenti. |
| RC.RP-02 | Le azioni di ripristino sono selezionate, contestualizzate, prioritizzate e eseguite |
| RC.RP-03 | L'integrità dei backup e delle altre risorse di ripristino è verificata prima che siano utilizzati per il ripristino. |
| RC.RP-04 | Le funzioni critiche per la mission dell'organizzazione e la gestione del rischio di cybersecurity sono considerate per stabilire le norme operative post-incidente. |
| RC.RP-05 | L'integrità degli asset ripristinati è verificata, i sistemi e i servizi sono ripristinati e lo stato operativo normale viene confermato. |
| RC.RP-06 | La conclusione del ripristino dell'incidente viene dichiarata sulla base di criteri definiti e la documentazione relativa all'incidente è completata. |
| RC.CO | Le attività di ripristino sono coordinate con le parti interne ed esterne. |
| RC.CO-03 | Le attività di ripristino e i progressi nel ripristino delle capacità operative sono comunicati agli stakeholder interni ed esterni designati. |
| RC.CO-04 | Gli aggiornamenti pubblici sul ripristino dagli incidenti sono condivisi utilizzando modalità e messaggi approvati. |

# Appendice B: elenco attività processo e procedure

Per ogni fase e sotto-fase del processo di gestione degli incidenti è di seguito riportato un elenco[20] delle attività (evidenziate in grassetto) e delle possibili procedure associate.

L'elenco può essere utilizzato come *checklist* e riferimento pratico per la definizione dei processi e delle procedure per la gestione degli incidenti di sicurezza informatica.

## Preparazione – Governo

- ✓ **Definizione delle politiche di gestione degli incidenti:**
  - procedura per l'approvazione delle politiche;
  - procedura per la diffusione[21] delle politiche.
- ✓ **Assegnazione dei ruoli e delle responsabilità:**
  - procedura per l'approvazione dei ruoli e delle responsabilità;
  - procedura per la diffusione dei ruoli e delle responsabilità.

## Preparazione – Identificazione

- ✓ **Inventario dei sistemi informativi e di rete:**
  - procedura per il censimento dei sistemi informativi e di rete;
  - procedura per la categorizzazione dei sistemi informativi e di rete.
- ✓ **Individuazione di minacce e vulnerabilità:**
  - procedura per l'identificazione delle vulnerabilità;
  - procedura per la ricezione delle informazioni sulle vulnerabilità;

## Preparazione – Protezione

- ✓ **Predisposizione strumenti di sicurezza per il monitoraggio:**
  - procedura per l'installazione e la configurazione degli strumenti di monitoraggio;
  - procedura per la manutenzione e l'aggiornamento degli strumenti di monitoraggio.
- ✓ **Configurazione sistemi informativi e di rete per l'acquisizione dei log:**
  - procedura per la raccolta e centralizzazione dei log;
  - procedura per la verifica della sincronizzazione temporale dei sistemi di *logging*;
- ✓ **Pianificazione dei backup dei dati e delle configurazioni:**
  - procedura per l'esecuzione periodica dei backup;
  - procedura per il test di ripristino dei backup.

[20] L'elenco delle attività è delle procedure non ha carattere esaustivo.

[21] Con in termine *diffusione di...* si intende la comunicazione e divulgazione ai destinatari e alle parti interessate di determinati elementi (quali, ad esempio, le politiche o i ruoli e le responsabilità).

## Rilevamento

- ✓ **Monitoraggio degli eventi:**
  - procedura per la definizione delle logiche di rilevamento degli eventi rilevanti per la sicurezza;
  - procedura per la configurazione degli allarmi;
- ✓ **Analisi degli eventi rilevanti per la sicurezza:**
  - procedura per il *triage* degli eventi;
  - procedura per la dichiarazione di incidente.

## Risposta – Investigazione

- ✓ **Valutazione del perimetro compromesso:**
  - procedura per la caratterizzazione dell'incidente secondo tassonomie definite;
  - procedura per la documentazione dell'incidente;
- ✓ **Acquisizione evidenze:**
  - procedura per l'acquisizione forense delle evidenze digitali;
  - procedura per la conservazione delle evidenze.

## Risposta – Notifica

- ✓ **Notifica dell'incidente:**
  - procedura per la notifica dell'incidente al CSIRT Italia;
  - procedura per la comunicazione dell'incidente alle parti interne ed esterne interessate.

## Risposta – Contenimento

- ✓ **Contenimento dell'incidente:**
  - procedura per l'isolamento dei sistemi informativi e di rete compromessi;
  - procedura per la disattivazione/reset degli account compromessi.

## Risposta – Eradicazione

- ✓ **Eradicazione dell'indicente:**
  - procedura per la bonifica dei sistemi informativi e di rete compromessi;
  - procedura per l'aggiornamento dei sistemi e delle *patch* di sicurezza;
  - procedura per la disattivazione/reset degli account compromessi.

## Ripristino

- ✓ **Ripristino dell'incidente:**
  - procedura per la reinstallazione dei sistemi a partire da *golden/clean image*;
  - procedura per la validazione dell'integrità dei sistemi informativi e di rete ripristinati.

## Miglioramento

- ✓ **Attività di miglioramento:**
  - procedura per la revisione delle politiche;
  - procedura per la revisione del piano di gestione degli incidenti;
  - procedura per la revisione dei ruoli e delle responsabilità per la gestione degli incidenti;
  - procedura per la revisione dell'inventario;
  - procedura per la revisione delle logiche di rilevamento;
  - procedura per la revisione dei processi di notifica e comunicazione;
  - procedura per la revisione delle attività di contenimento;
  - procedura per la revisione delle attività di eradicazione;
  - procedura per la revisione delle attività di ripristino;
  - procedura per la formazione continua del personale anche sulla base delle *lesson learned*;

# Appendice C: playbook per la gestione degli incidenti

I *playbook* sono dei documenti operativi che forniscono istruzioni pratiche e contestualizzate per gestire specifiche categorie di incidenti. Contengono sia elementi di processo che di procedure. Esempi di *playbook* nell'ambito della gestione degli incidenti sono:

- *playbook* per la gestione di attacchi *ransomware*;
- *playbook* per la gestione di attacchi *DDOS*;
- *playbook* per la gestione di attacchi di tipo *Password Spray*;
- *playbook* per la gestione di mail di *spear-phishing*;
- *playbook* per la gestione di *webshell* rilevate sui *web server*;

I *playbook* sono strutturati secondo un formato standard che prevede la presenza di elementi ricorrenti quali ad esempio:

- **titolo e versione**: indica l'oggetto del *Playbook* e il suo numero di versione;
- **descrizione**: descrive sinteticamente le modalità dell'attacco;
- **condizioni di attivazione**: identifica gli eventi che determinano l'esecuzione del *playbook* e le relative logiche di rilevamento;
- **attività**: dettaglia, per le varie fasi del processo, le attività da implementare;
- **ruoli e responsabilità**: specifica le figure coinvolte e le relative responsabilità.

È possibile reperire su fonti aperte *playbook* per le vari tipologie di incidenti. A seguire è riportato, a titolo di esempio [22], un *playbook* per la gestione degli attacchi di tipo *Password Spray*.

## Titolo e versione

- Playbook per la gestione di attacchi di tipo *Password Spray*. V.1.0 – 01/10/2025.

## Descrizione

- In questo tipo di attacco un attore malevolo, con l'obiettivo di ottenere credenziali di utenti di un'organizzazione, prova ad autenticarsi su un elevato di numero di *account* relativi a un determinato servizio utilizzando *password* di uso comune, che presentano uno schema ritenuto comune o che risultano conosciute all'attaccante in quanto, ad esempio, già compromesse a seguito di un attacco di *phishing* su utenti dell'organizzazione stessa. Generalmente i tentativi di autenticazioni sono effettuati consecutivamente su tutte le utenze note all'attaccante.

## Condizioni di attivazione

- Tentativi di autenticazione falliti su molteplici *account* un medesimo *host* o indirizzo IP.

[22] Il *playbook* è presentato per l'appunto a titolo esemplificativo e non ha carattere esaustivo.

- Tentativi di autenticazione con successo da parte di *host* o indirizzi IP ritenuti malevoli (in quanto, ad esempio, hanno effettuato numerosi tentativi di autenticazione falliti su molteplici *account*.
- Allarmi da strumenti di sicurezza come, ad esempio, il SIEM o l'EDR su tentativi di autenticazione falliti.

## Attività

- **Preparazione**: configurazione logiche di rilevamento, accesso con minimi privilegi, formazione del personale.
- **Rilevamento**: identificazione di pattern di attacco, analisi dei log di autenticazione, degli indicatori di compromissione (IOC) e delle informazioni di *Cyber Threat Intelligence* (CTI).
- **Risposta**: contenimento degli indirizzi IP dai quali proviene l'attacco, disattivazione degli account, coinvolti nell'attacco, notifica all'autorità e raccolta delle evidenze.
- **Ripristino**: ripristino degli account, cambio password e altre misure *ad hoc*.
- **Miglioramento**: analisi *post-mortem* dell'incidente e miglioramento della postura di sicurezza (ad esempio, attraverso l'introduzione dell'autenticazione multifattore).

## Ruoli e responsabilità[23]

| Attività | OSI | RGI | IRT | SOC | IT | LEG | COM |
|---|---|---|---|---|---|---|---|
| *OSI: organizzazione sicurezza informatica, RGI: responsabile gestione incidenti, IRT: Incident Response Team, SOC: Security Operation Center, IT: Ufficio IT, LEG: ufficio legale, COM: ufficio comunicazione.* | | | | | | | |
| Configurazione logiche di rilevamento. | I | C | C | A/R | C | I | – |
| Accesso con minimi privilegi. | A | I | I | I | R | I | – |
| Formazione del personale. | A/R | C | C | C | C | C | C |
| Identificazione di pattern di attacco. | I | C | C | A/R | C | – | – |
| Analisi log autenticazione, IOC e CTI. | I | C | C | A/R | C | – | – |
| Contenimento indirizzi IP d'attacco. | C | A | C | C | R | I | I |
| Disattivazione account coinvolti nell'attacco. | A | C | C | I | R | C | – |
| Notifica all'autorità e raccolta delle evidenze. | C | R | R | C | R | A | C |
| Ripristino degli account. | A | C | C | C | R | C | I |
| Cambio password e altre misure *ad hoc.* | A | C | C | C | R | I | – |
| Analisi *post-mortem* dell'incidente. | I | A | R | C | C | C | I |
| Miglioramento della postura di sicurezza. | A/R | C | C | R | R | C | C |

[23] I ruoli riportati sono quelli indicati a titolo esemplificativo nel paragrafo Governo. I ruoli e le responsabilità assegnati sono a carattere puramente indicativo e dovranno essere effettivamente determinati dall'organizzazione sulla base del proprio contesto tecnico-organizzativo.