AIEA FOR NIS2: Network and Information System 2

Prima edizione: febbraio 2026

Autori

Margherita Masseroni, Stefano Tagliabue, Ambrogio Ferretti, Paolo Artuso, Samantha Andriamarohasy, Niccolò Colcerasa, Maggi Gabriele, Daniela Mazzarone, Giuseppe Alfonsetti, Antonella Caproni, Giancarlo Butti, Silvia Lombardi, Massimo Beghini, Marco Tomazzoni, Luciano Lambresa, Christian Bassi, Bruno Ceradelli, Leonardo Brunori, Fabrizio Nuzzo, Mauro Alovisio, Simone Rinaldi, Alice Bragagnolo, Francesco Fabbri, Claudia Confini, Cesare Gallotti, Serena Bedendo, Mauro Gris, Daniele Rusconi, Filippo Bianchini, Marco Gheri, Cagnoli Diego, Luigi Sbriz, Franco Vincenzo Ferrari, Elenio Dursi.

Coordinatori e autori

Giulia Palmarini, Internal Audit - Recordati.

Luca Savoia, Partner Forvis Mazars.

Arianna Pellati, Manager Forvis Mazars.

Luca Verdolini, Senior Forvis Mazars.

Claudio Telmon, Consigliere Clusit e Partner P4I.

Abstract

La Direttiva NIS2 (UE 2022/2555), recepita in Italia con il D.Lgs. 138/2024, introduce obblighi stringenti per la governance della cybersicurezza, imponendo alle organizzazioni essenziali e importanti l'adozione di misure tecniche, organizzative e procedurali proporzionate al rischio. Questo paper analizza un framework integrato per la conformità alla NIS2, articolato in tre macro-aree: modello di governance e management, gestione del rischio nella supply chain e incident management.

Viene proposto un modello organizzativo che integra principi di accountability, segregazione dei ruoli e miglioramento continuo, allineato a standard internazionali (ISO/IEC 27001, GDPR, Modello 231). Sono dettagliate le policy chiave per la sicurezza dei sistemi, la gestione del rischio, la continuità operativa, la sicurezza della catena di fornitura e la formazione del personale.

Il paper definisce processi di due diligence sui fornitori, clausole contrattuali per la resilienza della supply chain e metodologie di audit periodico. Viene presentato un modello di gestione degli incidenti conforme alle linee guida ACN ed ENISA, con procedure di notifica, piani di risposta e test di efficacia. L'approccio proposto consente di trasformare la compliance normativa in leva strategica, riducendo il rischio legale e reputazionale e rafforzando la resilienza operativa delle organizzazioni.

Sommario

Elenco delle Tabelle

Elenco delle Figure

Introduzione

La crescente complessità del panorama delle minacce informatiche e l'impatto sistemico degli incidenti di sicurezza hanno reso indispensabile un approccio normativo armonizzato a livello europeo. La Direttiva NIS2 (UE 2022/2555), recepita in Italia con il D.Lgs. 138/2024, rappresenta un punto di svolta nella governance della cybersicurezza, imponendo obblighi più stringenti per la gestione del rischio, la resilienza operativa e la protezione delle infrastrutture critiche.

Questo lavoro si propone di analizzare e proporre un framework integrato per la conformità alla NIS2, articolato in tre aree principali: modello di governance e management, gestione del rischio nella supply chain e incident management. L'obiettivo è fornire alle organizzazioni un approccio strutturato e proporzionato, capace di trasformare la compliance normativa in leva strategica, riducendo il rischio legale e reputazionale e rafforzando la resilienza operativa.

Il paper si basa su un'analisi comparativa delle best practice internazionali (ISO/IEC 27001, NIST Cybersecurity Framework), delle linee guida ENISA e delle determinazioni dell'Agenzia per la Cybersicurezza Nazionale (ACN), integrandole in un modello operativo scalabile e adattabile alle diverse realtà aziendali.

1. MANAGEMENT MODEL NIS2

1.1 Analisi Normative

Responsabilità organi di amministrazione e direttivi

L'articolo 23 del D.Lgs. 138/2024 stabilisce **obblighi per gli organi di amministrazione e direttivi** dei soggetti essenziali e importanti.

Con la locuzione "**organi di amministrazione**" e "**organi direttivi**" ci si riferisce a quegli organi che detengono il potere di direzione dell'Organizzazione, incluso, ove presente, il Consiglio di amministrazione dell'organizzazione. In ogni caso, il rappresentante legale è considerato tra i componenti degli organi di amministrazione e direttivi. (*FAQ NIS ACN – ref. ODA 5*)
I **dirigenti** che **non** fanno parte del Consiglio di amministrazione (o altro organo analogo) non sono considerati componenti degli organi di amministrazione e direttivi.

Nel nuovo framework normativo sulla cybersecurity la conoscenza e la vigilanza da parte dei vertici aziendali diventano obblighi non eludibili o integralmente derogabili. Il contesto attuale impone un cambiamento di prospettiva e mentalità: i leader devono assumere un ruolo attivo ed essere sempre allineati. È essenziale un modello di leadership che riconosca le minacce, valorizzi la resilienza digitale e trasformi la sicurezza in un vantaggio strategico.

Gli organi di amministrazione e direzione devono approvare e supervisionare le misure di gestione del rischio, garantire la notifica degli incidenti, aggiornare le informazioni richieste, promuovere la formazione in cybersecurity e nominare un responsabile della sicurezza, assumendo una **responsabilità diretta** per il rispetto di tutti questi obblighi e con conseguenti **sanzioni personali** in caso di inadempimento.

Macroaree di coinvolgimento dei CdA:

L'art. 23 del D.Lgs. 138/2024 prevede un dovere per gli organi di amministrazione di predisporre assetti organizzativi adeguati anche ai fini della gestione dei rischi di cybersecurity, secondo i principi generali dell'articolo 2381 c.c. (che disciplina il conferimento e la gestione delle deleghe da parte del Consiglio di amministrazione). In base a tale disposizione, si distingue un doppio livello di competenze all'interno dell'organo di amministrazione

- definizione della strategia complessiva e valutazione dei risultati di gestione per il plenum del consiglio;
- attuazione operativa per gli amministratori delegati.

La mancata, o la inadeguata, predisposizione di tali assetti comporta una responsabilità dell'organo di amministrazione, secondo le regole generali dell'art. 2392 c.c. (che regola la responsabilità solidale degli amministratori nei confronti della società).

Nello specifico, gli adempimenti a carico degli organi di amministrazione e direttivi ricadono nei tre ambiti seguenti:

1) Responsabilità e supervisione

- Devono approvare le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica.
- Sovrintendono all'implementazione degli obblighi di sicurezza informatica.
- Sono responsabili per eventuali violazioni del decreto.

2) Formazione in sicurezza informatica

- Devono seguire una formazione in materia di sicurezza informatica.
- Promuovono una formazione periodica coerente per i dipendenti, per garantire che acquisiscano conoscenze e competenze sufficienti per identificare e gestire i rischi per la sicurezza informatica.

3) Informazioni sugli incidenti

- Devono essere informati periodicamente o tempestivamente sugli incidenti e le notifiche rilevanti, come stabilito negli articoli 25 e 26.

Sanzioni previste per le persone fisiche

Rappresentante Legale	La persona fisica che, in base alla legge o allo statuto, ha il potere di rappresentare legalmente un'organizzazione (impresa, ente, società) nei confronti di terzi e delle autorità, assumendo la responsabilità per gli adempimenti previsti dalla normativa sulla cybersicurezza.	Il Rappresentante Legale di un soggetto essenziale **può essere ritenuto responsabile dell'inadempimento in caso di violazione del decreto** da parte del soggetto di cui ha la rappresentanza.**[Art 38 co.5]** In caso di inadempimento dei tempi previsti dalla diffida ad adempiere emessa dall'Autorità competente nell'ambito delle

		proprie attività di verifica e ispezione, l'Autorità competente medesima ha il potere di **applicare la sanzione amministrativa accessoria della incapacità a svolgere funzioni dirigenziali all'interno del soggetto. Tale sanzione è applicabile agli organi di amministrazione e direttivi, al legale rappresentante nonché a funzioni dirigenziali a livello di amministratore delegato. [Art 38 co.6]**

Membri di "organi di amministrazione" e "organi direttivi"	La persona fisica membro di organo/i che detengono il potere di direzione dell'Organizzazione, incluso, ove presente, il Consiglio di amministrazione dell'organizzazione o strutture analoghe. I dirigenti che non fanno parte del Consiglio di amministrazione (o altro organo analogo) non sono considerati componenti degli organi di amministrazione e direttivi. Non sono considerati organi direttivi figure come il CISO o il responsabile della sicurezza aziendale	In caso di inadempimento dei tempi previsti dalla diffida ad adempiere emessa dall'Autorità competente nell'ambito delle proprie attività di verifica e ispezione, l'Autorità competente medesima ha il potere di **applicare la sanzione amministrativa accessoria della incapacità a svolgere funzioni dirigenziali all'interno del soggetto. Tale sanzione è applicabile agli organi di amministrazione e direttivi, al legale rappresentante nonché a funzioni dirigenziali a livello di amministratore delegato. [Art 38 co.6]**

Tabella 1: Sanzioni previste per le persone fisiche

Il ruolo del Punto di Contatto

Il Punto di contatto è una persona fisica, che deve essere designata dai soggetti pubblici e privati che rientrano nel campo di applicazione della normativa NIS2 (nel seguito «Soggetti NIS»).

Il Punto di contatto NIS2 ha i seguenti compiti:

- curare l'attuazione delle disposizioni della normativa NIS2 per conto del Soggetto NIS che lo ha designato;
- effettuare la registrazione del soggetto NIS alla piattaforma online della ACN;
- interloquire con l'ACN per conto del Soggetto NIS.

Le funzioni di punto di contatto possono essere svolte:

- dal rappresentante legale del Soggetto NIS,
- da uno dei procuratori generali del Soggetto NIS,
- da un dipendente delegato dal rappresentante legale.

Qualora il Soggetto NIS sia parte di un gruppo di imprese, le funzioni di punto di contatto possono essere svolte da un dipendente di un'altra impresa del gruppo che rientra nell'ambito di applicazione della normativa NIS2.

Qualora il soggetto NIS sia una pubblica amministrazione, le funzioni di punto di contatto possono essere svolte da un dipendente di un'altra pubblica amministrazione che rientra nell'ambito di applicazione della normativa NIS2.

Il punto di contatto riferisce direttamente al vertice gerarchico, nonché agli organi di amministrazione e direttivi, per quanto attiene alla normativa NIS2. Resta ferma, in ogni caso, la responsabilità degli organi di amministrazione e direttivi del Soggetto NIS.

La designazione del Punto di contatto da parte dei soggetti di cui all'art. 1.1 della legge 90/2024 [*], che rientrano nell'ambito di applicazione della normativa NIS2, può soddisfare l'obbligo di nomina e comunicazione del referente per la cybersicurezza di cui all'art.8.2 della medesima legge.

[*] Le pubbliche amministrazioni centrali, le regioni e le province autonome di Trento e di Bolzano, le città metropolitane, i comuni con popolazione superiore a 100.000 abitanti e, comunque, i comuni capoluoghi di regione, le società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane e le aziende sanitarie locali, nonché le rispettive società in house che forniscono servizi informatici, servizi di trasporto, servizi di raccolta, smaltimento o trattamento di acque reflue o di gestione dei rifiuti.

Limiti deleghe interne

FAQ ACN n.ODA.8 e ODA.9: è ammesso delegare lo svolgimento delle attività finalizzate all'assolvimento degli obblighi previsti dall'art. 23, commi 1 e 2, del D.lgs. 138/2024. Tuttavia, tale possibilità **non esclude la responsabilità degli organi deleganti**.
In particolare, le suddette FAQ chiariscono che gli obblighi ex art.23 in capo ai membri del CdA permangono, pertanto loro dovranno:

1. approvare le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica di cui alla determinazione ACN 164179 del 14 aprile 2025 (comma 1, lett. a));
2. sovrintendere alla loro implementazione (comma 1, lett.b));
3. essere responsabili delle violazioni di cui al decreto nis (comma 1, lett. c));
4. seguire una formazione in materia di sicurezza informatica (comma 2, lett. a));

5. promuovere l'offerta periodica di formazione per i dipendenti coerente con quella seguita dagli organi di amministrazione e dagli organi direttivi (comma 2, lett. b)).

Pertanto, non può essere delegata complessivamente la Responsabilità ex art.23 e gli organi di amministrazione, direttivi e legale rappresentante sono soggetti alle sanzioni personali di cui all'art.38 co.5 e co.6. In caso di delega, ai fini delle responsabilità, per le società, resta fermo quanto previsto dagli artt. 2381 c.c. (" Presidente, comitato esecutivo e amministratori delegati") e 2392 c.c..("Responsabilità verso la società") circa le responsabilità in capo ai soggetti deleganti.

1.2 Modello Organizzativo per la Cybersecurity in ottica NIS2

Premessa

La Direttiva NIS2 e il D.Lgs. 138/2024 introducono un approccio strutturato e cogente alla governance della cybersicurezza. L'adozione di un **modello organizzativo interno** diventa condizione imprescindibile per garantire conformità normativa, continuità operativa e resilienza digitale.
Questo modello non deve essere considerato un semplice adempimento, ma un vero e proprio **framework di governo aziendale**, integrato con i sistemi già in essere (Modello 231, GDPR, ISO/IEC 27001, sistemi di Enterprise Risk Management) e capace di trasformare la sicurezza da costo a **leva strategica di business**.

Principi guida

Il modello si fonda su principi trasversali che orientano l'intera architettura organizzativa:

- **Accountability**: gli organi apicali sono direttamente responsabili della strategia e della vigilanza sulla cybersicurezza. Tale responsabilità si estende a decisioni, omissioni e alla supervisione delle funzioni delegate, con conseguenze anche personali in caso di inadempimento.
- **Segregazione dei ruoli**: la netta distinzione tra funzioni operative, di controllo e di assurance evita conflitti di interesse, garantisce indipendenza di giudizio e rafforza la credibilità del sistema.
- **Integrazione**: il modello di cybersicurezza non è un silo, ma parte di un ecosistema di governance integrato, che comprende risk management, compliance normativa, anticorruzione, privacy e sistemi di qualità.
- **Proporzionalità e adeguatezza**: le misure organizzative e di controllo devono essere commisurate al livello di rischio, alle dimensioni aziendali e al ruolo critico dei servizi erogati, evitando approcci "one size fits all".
- **Trasparenza e tracciabilità**: ogni decisione, escalation o reporting deve essere formalizzata, documentata e tracciata, a tutela dell'organizzazione e dei suoi amministratori.
- **Miglioramento continuo**: il modello non è statico, ma soggetto a riesame periodico, aggiornamenti post-incident e affinamento in base a nuove minacce o cambiamenti normativi.

Struttura organizzativa

L'assetto organizzativo prevede una distribuzione multilivello delle responsabilità, dal vertice fino alle funzioni operative:

Organi apicali

- **Consiglio di amministrazione (CdA)**: definisce le strategie di sicurezza, approva le policy aziendali, stabilisce il risk appetite e supervisiona l'attuazione delle misure. È destinatario di reporting sintetici e strategici (KPI, KRI, gap analysis).
- **Amministratore Delegato / Direzione Generale**: traduce gli indirizzi del CdA in obiettivi operativi, assegna risorse e responsabilità, nomina le figure chiave (CISO, Punto di Contatto NIS2) e presiede i comitati strategici (Cybersecurity & Risk Committee, Crisis Management Committee).

Funzioni chiave

- **Chief Information Security Officer (CISO)**:
  - Cuore operativo e strategico del modello.
  - Definisce framework e politiche di sicurezza, sovrintende a SOC, IRT e processi di risk management.
  - È referente privilegiato per il CdA e si coordina con Compliance, Risk Management, DPO e Audit.
  - Garantisce il ciclo di miglioramento continuo tramite monitoraggio, reporting e remediation.
- **Punto di Contatto NIS2**:
  - Unico canale formale di interlocuzione con ACN e CSIRT.
  - Assicura il rispetto delle tempistiche di notifica (24h, 72h, 30gg).

    - Riferisce direttamente alla Direzione Generale.
- **Funzione Compliance e Risk Management**:
    - Integra i rischi cyber nell'ERM aziendale.
    - Coordina le attività di compliance trasversali (GDPR, 231, standard ISO).
    - Monitora il rispetto delle policy interne e gestisce i piani di remediation.
- **Data Protection Officer (DPO)**:
    - Gestisce i rischi legati al trattamento dei dati personali.
    - Coopera con CISO e IRT in caso di data breach per garantire le co-notifiche al Garante e ad ACN.
- **Internal Audit**:
    - Funzione indipendente e terza.
    - Verifica periodicamente l'efficacia delle misure implementate.
    - Riporta direttamente al CdA e al Comitato Controllo e Rischi, con piena autonomia.

Struttura operativa

- **Security Operation Center (SOC)**: monitoraggio continuo, gestione eventi e analisi delle minacce.
- **Incident Response Team (IRT)**: gestione end-to-end degli incidenti (triage, contenimento, eradicazione, ripristino e lesson learned).
- **IT/OT Operations**: gestione tecnica di sistemi, patching, backup e infrastrutture critiche.
- **Security Engineering**: progettazione sicura, hardening, identity management, crittografia e vulnerability management.
- **Business Continuity & Disaster Recovery (BCM/DR)**: piani, test ed esercitazioni per la continuità dei servizi essenziali.
- **Procurement & Fornitori**: gestione dei rischi di supply chain, due diligence, contrattualistica NIS2, audit terze parti.

- **HR e Formazione**: verifica pre-employment, gestione accessi, formazione continua e campagne di awareness.
- **Ufficio Legale**: supporto contrattuale, gestione contenziosi, assistenza nelle comunicazioni con autorità.
- **Business Units**: responsabilità diretta sulla sicurezza dei servizi e degli asset sotto la propria gestione.

Strumenti di coordinamento

- **Comitato Cybersecurity & Risk**: forum direzionale che monitora indicatori, valuta rischi emergenti, definisce priorità e indirizza le strategie.
- **Comitato di Gestione Crisi**: attivato in caso di incidenti significativi, assicura decisioni rapide e coerenti a livello aziendale.
- **Processi di escalation**: definiscono in maniera chiara soglie, tempi e livelli decisionali da coinvolgere.
- **Flussi informativi multilivello**:
    - Report operativi (giornalieri/mensili per CISO e SOC).
    - Dashboard direzionali (trimestrali per CdA e comitati).
    - Report straordinari (incidenti significativi).

Integrazione con altri modelli

- **Modello 231**: presidio sui reati informatici; il CISO collabora con l'Organismo di Vigilanza, fornendo evidenze e audit trail.
- **GDPR**: gestione integrata di incidenti con impatti sui dati personali; coordinamento CISO-DPO; allineamento tra registro trattamenti e inventario asset critici.
- **ISO/IEC 27001**: utilizzo dell'ISMS come backbone organizzativo, con audit periodici e mapping delle misure di

sicurezza previste da Annex A/27002 come base di conformità.

Benefici attesi

Un modello organizzativo conforme alla NIS2 produce benefici tangibili:

- **Riduzione del rischio legale e reputazionale**: minimizzazione delle sanzioni e delle responsabilità personali degli organi apicali.
- **Maggiore resilienza operativa**: migliore capacità di resistere, rispondere e ripristinare i servizi in caso di attacco.
- **Trasparenza e accountability**: chiarezza nei flussi informativi e nella distribuzione delle responsabilità.
- **Vantaggio competitivo**: la cybersecurity diventa un asset di fiducia verso clienti, partner, investitori e autorità.

1.3 Policy

Executive Summary

Il presente report analizza in dettaglio le principali policy e procedure IT interne più diffuse e adottate nelle aziende italiane, in risposta alle nuove sfide di cybersecurity introdotte dalla Direttiva NIS2 (UE 2022/2555) e dal relativo decreto legislativo italiano 4 settembre 2024, n. 138. Queste normative impongono requisiti più stringenti in materia di gestione dei rischi informatici e richiedono un riesame delle policy IT esistenti. L'approccio metodologico adottato ha mirato a effettuare una mappatura delle policy esistenti e confrontarle con i requisiti della Direttiva NIS2, al fine di identificare eventuali gap, proporre aggiornamenti o nuove policy per garantire la compliance e definire i controlli coerentemente con il management model richiesto da NIS2.

Questo processo si è articolato in quattro fasi: Kick-off e Raccolta Documentale, Analisi dei Requisiti NIS2, Policy Mapping & Gap

Analysis e Proposte di Allineamento. Dall'analisi delle best practice di settore, sono state individuate circa policy in ambito sicurezza informatica, di cui circa documenti di indirizzo risultano necessari per garantire la compliance alla Direttiva NIS2.

Questi includono policy fondamentali come la sicurezza dei sistemi di rete e informazione , la politica di gestione del rischio , la gestione degli incidenti , la continuità operativa e gestione delle crisi , la sicurezza della catena di fornitura , la sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi di rete e informazione , le politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza , le pratiche di base di igiene informatica e formazione sulla sicurezza , la crittografia , la sicurezza delle risorse umane , il controllo degli accessi , la gestione degli asset e la sicurezza ambientale e fisica. Il report evidenzia per ciascuna di queste policy i requisiti chiave imposti dalla NIS2 e le azioni necessarie per una loro efficace implementazione.

Vengono altresì forniti dettagli sulle aspettative dell'Agenzia per la Cybersicurezza Nazionale (ACN) in termini di documentazione, approvazione da parte dell'alta direzione, comunicazione al personale e ai fornitori, e requisiti di aggiornamento e audit periodici. L'obiettivo finale è supportare le imprese nell'allineamento delle proprie policy IT con i nuovi obblighi normativi, rafforzando così la loro resilienza cibernetica.

Contesto di riferimento

Il panorama della cybersicurezza è in rapida evoluzione, caratterizzato da un aumento esponenziale del numero, della portata, della sofisticazione e dell'impatto degli incidenti informatici, che minacciano il funzionamento dei sistemi e delle reti, con gravi conseguenze economiche e sociali. In questo scenario, le imprese

italiane, incluse PMI, grandi aziende ed enti pubblici, si trovano ad affrontare nuove e più complesse sfide. A livello europeo, la Direttiva NIS2 (UE 2022/2555), entrata in vigore il 17 gennaio 2023 e recepita in Italia con il Decreto Legislativo 4 settembre 2024, n. 138, rappresenta un aggiornamento cruciale della legislazione sulla sicurezza delle reti e dei sistemi informativi. Questa direttiva sostituisce la precedente NIS (Direttiva (UE) 2016/1148) con l'obiettivo di stabilire un livello comune elevato di cybersicurezza nell'Unione Europea, migliorando il funzionamento del mercato interno e rafforzando le capacità di cybersicurezza degli Stati membri.

La NIS2 impone requisiti più stringenti in materia di gestione dei rischi informatici per una vasta gamma di entità pubbliche e private che operano in settori considerati essenziali e importanti. Tali requisiti includono, tra gli altri, politiche di analisi dei rischi, gestione degli incidenti, continuità operativa, sicurezza della catena di approvvigionamento, sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi e pratiche di igiene informatica e formazione. In questo contesto normativo rafforzato, il presente report si propone di analizzare in dettaglio le principali policy e procedure IT interne diffuse nelle aziende italiane.

L'obiettivo è duplice: individuare i requisiti e le azioni necessarie per implementare efficacemente i controlli richiesti dalla Direttiva NIS2, e supportare le organizzazioni nel riesame e nell'aggiornamento delle proprie policy esistenti. Attraverso una mappatura delle policy e un confronto con i requisiti della NIS2, miriamo a identificare i gap e a proporre aggiornamenti o nuove policy per garantire la piena compliance e rafforzare la resilienza cibernetica complessiva.

Metodologia

L’approccio metodologico utilizzato mira ad effettuare una **mappatura delle policy esistenti** e confrontarle con i **requisiti della Direttiva NIS2**, al fine di:

- Identificare eventuali **gap** rispetto ai nuovi obblighi;
- Proporre **aggiornamenti o nuove policy** per garantire la compliance;
- Definire i controlli coerentemente con il management model richiesto da NIS2.

Per raggiungere le finalità espresse è stato avviato un flusso operativo definito da quattro fasi come riportato nell'immagine di seguito:

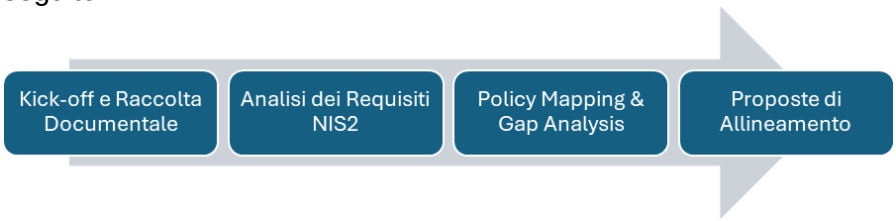


Figura 1: Metodologia

Ogni fase è stata caratterizzata dalle seguenti attività:

- **Kick-off e Raccolta Documentale**: identificazione del perimetro delle policy oggetto di analisi (es.: Incident Response, Supply Chain, Business Continuity, ecc.) e raccolta best practice;
- **Analisi dei Requisiti NIS2**: traduzione dei requisiti rilevanti della Direttiva NIS2 in controlli attesi e mappatura per area tematica;
- **Policy Mapping & Gap Analysis**: confronto di ciascuna policy individuata con i requisiti NIS2 mappati e identificazione delle pratiche per la soddisfazione dei requisiti;
- **Proposte di Allineamento**: elaborazione di proposte di aggiornamento per le policy esistenti o identificazione nuove policy da introdurre.

Mappatura Policy IT

Dall'analisi delle best practice di settore vengono individuate circa 36 policy in ambito sicurezza informatica che risultano maggiormente

diffuse, sintetizzata in tabella dell'Allegato 1. In risposta alla Direttiva, vengono individuate circa 16 documenti di indirizzo che risultano necessari al fine di garantire la compliance:

1. **Sicurezza dei Sistemi di Rete e Informazione;**
2. **Policy di Gestione del Rischio;**
3. **Gestione degli incidenti;**
4. **Continuità Operativa e Gestione delle Crisi;**
5. **Sicurezza della Catena di Fornitura;**
6. **Sicurezza nell'Acquisizione, nello Sviluppo e nella Manutenzione dei Sistemi di Rete e Informazione;**
7. **Politiche e procedure per Valutare l'Efficacia delle Misure di Gestione dei Rischi di Cybersicurezza;**
8. **Pratiche di Formazione sulla Sicurezza Informatica;**
9. **Crittografia;**
10. **Sicurezza delle Risorse Umane;**
11. **Controllo degli Accessi;**
12. **Gestione degli Asset;**
13. **Sicurezza Ambientale e Fisica.**

Sicurezza dei Sistemi di Rete e Informazione

La Direttiva NIS2 impone alle organizzazioni di **definire una politica chiara** per la sicurezza dei sistemi di rete e informazione, che deve coprire tutti i sistemi, gli asset e le procedure rilevanti. Questa policy, che funge da quadro di riferimento generale per la gestione della cybersecurity, deve essere **formalmente approvata dall'alta direzione**, **comunicata a tutto il personale interessato** e, se del caso, a fornitori e partner esterni, e **aggiornata almeno annualmente**. Secondo le specifiche dell'Agenzia per la Cybersicurezza Nazionale (ACN), ogni soggetto NIS deve **adottare e documentare politiche di sicurezza informatica** che includano ambiti quali la gestione del rischio, ruoli e responsabilità, sicurezza delle risorse umane, conformità e audit, sicurezza della catena di fornitura, gestione degli asset, gestione delle vulnerabilità, continuità operativa e gestione delle crisi, gestione delle identità e controllo degli accessi, sicurezza fisica, formazione e consapevolezza, sicurezza dei

dati, sviluppo e manutenzione dei sistemi, protezione di reti e comunicazioni, monitoraggio degli eventi di sicurezza, e risposta agli incidenti e ripristino. Per l'implementazione, l'ente deve **formalizzare questa politica in un documento approvato dal top management**, che dovrebbe specificare scopo, obiettivi, principi (come l'approccio basato sul rischio), e la struttura di governance. È fondamentale che la politica sia **comunicata efficacemente**, spesso richiedendo ai dipendenti e terze parti di **attestare la presa visione e accettazione delle regole di sicurezza**. Gli **audit verificheranno l'esistenza di questo documento aggiornato**, le firme di approvazione del management, i **registri di lettura da parte del personale** e le **comunicazioni ai fornitori**. È inoltre cruciale che la politica sia **riesaminata almeno una volta all'anno o in seguito a incidenti gravi o cambiamenti significativi nel rischio**, con **evidenze documentate di tale revisione**.

Gestione del Rischio

La Direttiva NIS2 richiede alle organizzazioni di **adottare una politica di gestione del rischio di cybersicurezza** che definisca processi e responsabilità per identificare, analizzare, valutare e mitigare i rischi cyber. Questo implica l'integrazione della sicurezza informatica nel sistema complessivo di gestione del rischio aziendale, adottando un **approccio basato sul rischio**, in cui le misure di sicurezza sono commisurate alla valutazione e alla tolleranza al rischio dell'organizzazione. Il Regolamento 2024/2690 specifica che devono esistere **processi per la gestione dei rischi derivanti da sistemi ICT critici, basati su risk assessment periodici**. L'ACN, in particolare, richiede che sia **definito, attuato, aggiornato e documentato un piano di gestione dei rischi per la sicurezza informatica**. La strategia di rischio deve inoltre **stabilire chiaramente priorità, vincoli, criteri di accettazione del rischio (risk appetite) e assunzioni** che supportino le decisioni in materia di

rischio, considerando anche i rischi derivanti dalla supply chain e dal contesto esterno. Per l'implementazione, l'ente dovrebbe **strutturare un processo continuo** che include: **identificazione degli asset critici, identificazione delle minacce e vulnerabilità, analisi degli impatti e probabilità, valutazione e trattamento dei rischi**, con **relativo monitoraggio nel tempo**. Un controllo chiave è la **redazione di un Risk Assessment periodico (annuale o più frequente)** sui sistemi informativi. L'output atteso è un **Registro dei rischi (risk register)** che documenti per ciascun rischio descrizione, punteggio, contromisure, azioni pianificate, proprietario e stato di trattamento. Gli auditor richiederanno **evidenze di questo processo**, inclusi: il **documento di Piano di gestione dei rischi informatici approvato**, i **report di valutazione del rischio eseguiti (con metodologia, criteri e risultati)**, e un **Risk Treatment Plan** che elenchi le misure correttive per i rischi intollerabili. È una best practice **allineare il risk management cyber con quello enterprise**, integrando il rischio cyber nel più ampio ERM aziendale, con il **coinvolgimento degli organi direttivi nella definizione del risk appetite e nell'approvazione dei criteri di valutazione**. Un indicatore di maturità è l'**istituzione di un Risk Committee** o organo simile che periodicamente riveda i principali rischi cyber e lo stato delle mitigazioni, riferendo al top management.

Gestione degli incidenti

La capacità di **gestire gli incidenti di sicurezza informatica** è un pilastro fondamentale della Direttiva NIS2. Agli enti viene richiesto di **predisporre procedure di gestione degli incidenti cyber**, che includano rilevamento, analisi, contenimento, ripristino e comunicazione, oltre all'obbligo di notifica agli organismi competenti (in Italia, CSIRT e ACN) entro tempistiche definite.La Direttiva NIS2 introduce **KPI temporali piuttosto stringenti** per la notifica degli incidenti significativi:

- **Notifica iniziale entro 24 ore dall'identificazione** di un incidente significativo, contenente almeno una prima valutazione sommaria e le misure prese.

- **Rapporto dettagliato entro 72 ore** dall'incidente, con un aggiornamento che include indicatori più precisi.
- **Report finale entro 1 mese** (a incidente gestito), con un'analisi ex-post.

Dal punto di vista operativo, l'ACN impone che ogni soggetto NIS disponga di un **Piano di gestione degli incidenti formalizzato**, **approvato dal management e riesaminato periodicamente**. Tale piano deve **definire ruoli** (es. team di risposta agli incidenti, referenti per notifica), **procedure passo-passo** per diverse tipologie di incidente, e **modulistica di reporting** interno ed esterno. Per l'implementazione, l'ente dovrebbe **istituire un vero e proprio Incident Response Plan (IRP)** che includa definizioni, flussi di escalation, fasi di gestione (identificazione, analisi forense, contenimento, eradicazione, ripristino, lezione appresa) e comunicazioni interne ed esterne. Gli auditor verificheranno l'**esistenza e la completezza del piano di incident response**, la sua copertura della comunicazione esterna obbligatoria, e, se possibile, ne **testeranno l'efficacia mediante evidenze**, come verbali di esercitazioni o simulazioni di incidente. **Evidenze chiave** includono il Piano di gestione incidenti **approvato dalla direzione**, l'**elenco dei membri del team di risposta**, i **registri di incidenti passati (incident log) con traccia delle azioni intraprese e notifiche inviate**, e la dimostrazione che i **dipendenti sanno come riconoscere e segnalare un incidente**. Si raccomanda inoltre di **integrare strumenti di monitoraggio e rilevamento** (SIEM, IDS/IPS) e di **condurre un post-mortem dopo ogni incidente maggiore** per aggiornare procedure e controlli.

Continuità Operativa e Gestione delle Crisi

La Direttiva NIS2 impone alle organizzazioni di **predisporre piani di Business Continuity (BCP) e Disaster Recovery (DR)** per assicurare la continuità operativa dei servizi essenziali e la **capacità**

di gestione della crisi in caso di eventi dirompenti. Un programma efficace inizia con un'**analisi d'impatto sul business (BIA)**, per identificare i processi e servizi critici, quantificare l'impatto di un'interruzione e **definire gli obiettivi di ripristino: Recovery Time Objective (RTO) e Recovery Point Objective (RPO)** per ciascun servizio/asset. Sulla base del BIA, si sviluppa un **Piano di Continuità Operativa** che indica come l'organizzazione reagirà a scenari di indisponibilità, prevedendo **soluzioni alternative** (es. attivazione di un sito secondario, uso di sistemi di backup, procedure manuali temporanee) e includendo i **contatti di emergenza** e i **canali comunicativi**. Parallelamente, un **Piano di Disaster Recovery IT** dettaglia le modalità tecniche per recuperare infrastrutture e dati, ad esempio tramite **ripristino da backup offline**. È fondamentale che tali **piani esistano in forma documentata** e, soprattutto, che siano **testati regolarmente**. Le **prove di test** (es. esercitazioni di simulazione, test di restore da backup, drill periodici) sono essenziali per dimostrare che il piano è praticabile e conosciuto dagli attori coinvolti. I controlli includono l'**esistenza di un BCP/DRP approvato**, **liste aggiornate dei sistemi critici e loro RTO/RPO**, l'**elenco dei team di crisi** (es. Crisis Management Team) con nominativi e contatti, **rapporti di test di continuità** e il **registro dei backup effettuati con verifica di restore periodici**. L'integrazione con la gestione crisi generale e la predisposizione di una **Crisis Committee** con procedure decisionali pre-definite sono inoltre raccomandate.

Sicurezza della Catena Logistica

La Direttiva NIS2 pone una forte enfasi sulla **resilienza** e la **sicurezza delle catene di approvvigionamento**, riconoscendole come potenziali vettori di **attacchi cyber** e punti critici per la continuità dei servizi essenziali e importanti. Le **policy** relative alla "Sicurezza della Catena Logistica" devono quindi essere progettate per **mitigare i rischi** intrinseci derivanti dalla dipendenza da **fornitori esterni** di prodotti e servizi ICT, hardware, software e servizi digitali. Questo implica l'adozione di un approccio **proattivo** che includa, ma non si limiti a, la **due diligence sui fornitori**, la definizione di **requisiti**

contrattuali stringenti in materia di sicurezza cyber, l'implementazione di meccanismi di **monitoraggio continuo** delle performance di sicurezza delle terze parti e la **gestione delle vulnerabilità** lungo l'intera **catena di fornitura**. È fondamentale che le organizzazioni identifichino i **fornitori critici**, valutino i loro **livelli di rischio** e adottino misure appropriate per garantire che i requisiti di sicurezza siano estesi e rispettati anche al di fuori dei confini aziendali, contribuendo così a un **ecosistema digitale più sicuro e affidabile**.

Sicurezza nell'Acquisizione, nello Sviluppo e nella Manutenzione dei Sistemi di Rete

La Direttiva NIS2 sottolinea l'importanza cruciale di integrare la sicurezza in ogni fase del **ciclo di vita dei sistemi di rete**, dall'**acquisizione** alla **manutenzione**. Le policy in questo ambito devono garantire che la **sicurezza informatica** sia un requisito fondamentale e non un'aggiunta successiva. In fase di acquisizione, ciò implica la **selezione di fornitori affidabili** e l'adozione di prodotti e servizi che incorporino il **security-by-design** e il **privacy-by-design**, con attenzione alla **valutazione delle vulnerabilità** e alla **conformità a standard di sicurezza riconosciuti**. Durante lo **sviluppo**, è essenziale implementare **pratiche di codifica sicura**, condurre **test di sicurezza rigorosi** (come penetration testing e vulnerability assessment) e gestire in modo proattivo le **dipendenze da componenti di terze parti**. Infine, nella fase di **manutenzione**, le policy devono prevedere l'applicazione tempestiva di **patch di sicurezza**, l'aggiornamento costante delle configurazioni, il **monitoraggio continuo** delle minacce e delle anomalie, e la gestione efficace degli **incidenti di sicurezza**. L'obiettivo è costruire e mantenere sistemi di rete robusti, **resilienti** e capaci di resistere a un panorama di minacce in continua evoluzione, garantendo la **disponibilità, integrità e riservatezza** dei dati e dei servizi.

Politiche e Procedure per Valutare l'Efficacia delle Misure di Gestione dei Rischi di Cybersicurezza

Nell'ambito della Direttiva NIS2, la mera implementazione di **misure di cybersicurezza** non è sufficiente; è imperativo che le organizzazioni definiscano **politiche e procedure** chiare per **valutare l'efficacia** di tali misure nel tempo. Questo processo continuo è fondamentale per assicurare che le difese adottate siano pertinenti, proporzionate e capaci di mitigare i **rischi cyber** in un panorama di minacce in evoluzione. Le policy dovrebbero delineare l'uso di **indicatori chiave di performance (KPI)** e **indicatori chiave di rischio (KRI)** per monitorare l'andamento della sicurezza, oltre a prevedere **audit di sicurezza** regolari, **valutazioni delle vulnerabilità** e **penetration testing** condotti da soggetti interni o esterni qualificati. È altresì essenziale stabilire meccanismi per la **raccolta e l'analisi dei dati** relativi agli incidenti di sicurezza, ai tentativi di intrusione e alle anomalie, al fine di identificare le aree di debolezza e le opportunità di miglioramento. I risultati di queste valutazioni devono essere documentati, comunicati ai livelli direttivi pertinenti e utilizzati per guidare il **processo decisionale** in merito agli **investimenti in sicurezza** e all'adattamento delle strategie di **gestione del rischio**, garantendo un approccio proattivo e basato sull'evidenza alla **resilienza cibernetica**.

Policy di Formazione sulla Sicurezza Informatica

La Direttiva NIS2 pone una forte enfasi sul **fattore umano** come elemento cruciale nella **gestione dei rischi di cybersicurezza**. Le **policy di formazione sulla sicurezza informatica** sono quindi essenziali per elevare la consapevolezza e le competenze di tutto il personale, che rappresenta spesso la prima linea di difesa contro gli attacchi cyber. Queste policy devono delineare un programma di **formazione continuo e obbligatorio** per tutti i dipendenti, a tutti i livelli, sin dall'assunzione. Il programma dovrebbe coprire argomenti fondamentali come l'identificazione e la prevenzione del **phishing** e dell'**ingegneria sociale**, la creazione e la gestione di **password**

robuste, l'uso dell'**autenticazione a più fattori (MFA)**, la gestione sicura dei dati e l'uso consapevole dei dispositivi aziendali e personali. È fondamentale che la formazione sia **regolarmente aggiornata** per riflettere l'evoluzione delle **minacce emergenti**, delle normative e delle **migliori pratiche** del settore. L'efficacia della formazione dovrebbe essere valutata attraverso **simulazioni di attacco** (es. campagne di phishing simulate) e test di conoscenza, i cui risultati devono essere utilizzati per affinare i contenuti formativi e identificare le aree che richiedono maggiore attenzione. L'obiettivo ultimo è promuovere una **cultura della sicurezza** radicata nell'organizzazione, in cui ogni individuo sia consapevole del proprio ruolo e delle proprie responsabilità nella protezione degli asset informatici, trasformando il personale da potenziale vulnerabilità in un elemento proattivo e resiliente della difesa cyber.

Crittografia

La **crittografia** è riconosciuta dalla Direttiva NIS2 (Articolo 21, comma 2, lettera h) come una delle **misure tecniche e organizzative** fondamentali per la **gestione dei rischi di cybersicurezza**. Le policy relative alla crittografia devono quindi definire in modo chiaro l'impiego appropriato di questa tecnologia per proteggere la **riservatezza, l'integrità e la disponibilità** delle informazioni e dei sistemi. Ciò include la crittografia dei **dati a riposo** (data at rest), come quelli archiviati su server, database e dispositivi endpoint, per prevenire accessi non autorizzati in caso di furto o compromissione fisica. Allo stesso modo, è essenziale l'applicazione della crittografia ai **dati in transito** (data in transit), utilizzando protocolli sicuri (es. TLS, IPsec, VPN) per proteggere le comunicazioni su reti pubbliche e private. Le organizzazioni devono stabilire procedure rigorose per la **gestione delle chiavi crittografiche**, inclusa la loro generazione, distribuzione, archiviazione sicura, revoca e distruzione, per garantirne l'efficacia nel tempo. L'adozione di soluzioni di **crittografia**

end-to-end per comunicazioni e scambi di dati sensibili è fortemente incoraggiata. L'obiettivo è sfruttare la crittografia come strumento proattivo per ridurre l'impatto potenziale di incidenti di sicurezza, rafforzando la **resilienza cibernetica** e la protezione degli asset critici.

Sicurezza delle Risorse Umane

La Direttiva NIS2 enfatizza che la **sicurezza informatica** non si limita agli aspetti tecnologici, ma include in modo fondamentale anche la **dimensione umana**. Le **policy** relative alla "Sicurezza delle Risorse Umane" devono quindi coprire l'intero **ciclo di vita del rapporto di lavoro**, dalla fase di pre-impiego fino alla cessazione, per mitigare i rischi derivanti dal fattore umano. Questo implica l'implementazione di **controlli di sicurezza** specifici per il personale, iniziando con un'adeguata **due diligence** e la verifica delle referenze durante il **reclutamento**. Durante l'impiego, è essenziale definire **ruoli e responsabilità** chiari in materia di sicurezza informatica per ogni posizione, prevedere un'**allocazione minima dei privilegi** (Least Privilege) e garantire che tutto il personale riceva una **formazione iniziale e continua** sulla sicurezza. Le policy devono inoltre stabilire procedure per la **gestione degli accessi** ai sistemi e alle informazioni, inclusa la rapida **revoca degli account** in caso di modifiche di ruolo o cessazione del rapporto. Particolare attenzione deve essere posta alla **sensibilizzazione** contro minacce come il social engineering e il phishing, e alla promozione di una **cultura della sicurezza** che incoraggi la segnalazione di potenziali incidenti. L'obiettivo è assicurare che il personale sia non solo consapevole dei rischi, ma anche equipaggiato e responsabilizzato per agire in modo sicuro, trasformando gli individui da potenziale vulnerabilità in un anello forte della **catena di difesa cibernetica**.

Controllo degli Accessi

Nell'ambito della Direttiva NIS2, il **controllo degli accessi** è una misura di **gestione del rischio di cybersicurezza** (come indicato

nell'Articolo 21, comma 2, lettera i) di primaria importanza per proteggere i **sistemi informatici** e i **dati sensibili** da accessi non autorizzati. Le policy in questo ambito devono stabilire **criteri rigorosi** per l'identificazione, l'autenticazione e l'autorizzazione di utenti, dispositivi e processi. Ciò include l'implementazione del principio del **"privilegio minimo" (Least Privilege)**, garantendo che gli utenti abbiano accesso solo alle risorse strettamente necessarie per svolgere le proprie funzioni. È essenziale adottare **soluzioni di autenticazione robusta**, preferibilmente l'**autenticazione a più fattori (MFA)**, per tutti gli accessi ai sistemi critici e ai dati sensibili, sia per il personale interno che per i fornitori esterni. Le policy devono inoltre definire procedure per la **gestione del ciclo di vita degli accessi**, dalla loro assegnazione iniziale, alle modifiche (es. in caso di cambio ruolo), fino alla **revoca tempestiva** in caso di cessazione del rapporto di lavoro o di ruolo. La **segregazione dei compiti (Separation of Duties)** e il **monitoraggio continuo** degli accessi e delle attività degli utenti sono altrettanto cruciali per rilevare comportamenti anomali o tentativi di accesso non autorizzati, contribuendo così a un robusto framework di **sicurezza perimetrale e interna** in linea con i requisiti di **resilienza cibernetica** della NIS2.

Gestione degli Asset

La Direttiva NIS2 riconosce la **gestione degli asset** come un pilastro fondamentale per un'efficace **postura di cybersicurezza**. Le policy in quest'area devono mirare a creare e mantenere una **visibilità completa** su tutti gli asset informativi e tecnologici che supportano i servizi essenziali e importanti dell'organizzazione. Questo include l'identificazione, la classificazione e l'inventario di **hardware, software, dati, servizi e informazioni critiche**. È essenziale che le policy definiscano procedure per l'**assegnazione della titolarità** degli asset, la **valutazione del loro valore** e l'identificazione dei **rischi associati** alla loro compromissione. Inoltre, devono essere stabiliti

meccanismi per il **monitoraggio continuo** dello stato degli asset, inclusa la configurazione, le patch di sicurezza e le vulnerabilità note. Le policy di gestione degli asset devono anche coprire il loro **intero ciclo di vita**, dall'acquisizione all'eliminazione sicura (disposal), garantendo che la sicurezza sia integrata in ogni fase. L'obiettivo è fornire alle organizzazioni una base solida per l'applicazione delle altre misure di sicurezza, facilitando la **gestione del rischio**, la **risposta agli incidenti** e la **continuità operativa**, e contribuendo così in modo significativo alla **resilienza cibernetica** richiesta dalla NIS2.

Sicurezza Ambientale e Fisica

La Direttiva NIS2 riconosce che la **sicurezza informatica** non può prescindere dalla protezione degli ambienti fisici e dalle condizioni ambientali in cui risiedono i sistemi e i dati critici. Le **policy** relative alla "Sicurezza Ambientale e Fisica" devono quindi concentrarsi sulla prevenzione di accessi non autorizzati, danni o interruzioni ai **datacenter, sale server, uffici e altre aree sensibili** che ospitano infrastrutture IT essenziali. Questo include l'implementazione di **controlli fisici rigorosi** come sistemi di controllo degli accessi (es. badge, biometrici), **videosorveglianza**, allarmi e pattugliamenti di sicurezza. È fondamentale proteggere le infrastrutture da minacce ambientali, come **incendi, allagamenti, sbalzi di corrente, temperature estreme e calamità naturali**, attraverso l'adozione di sistemi di rilevamento e spegnimento incendi, sistemi di climatizzazione, gruppi di continuità (UPS) e generatori. Le policy devono anche definire procedure per la **protezione delle apparecchiature** da furto o manomissione, inclusa la gestione sicura di dispositivi portatili e supporti di memorizzazione. L'obiettivo è garantire la **disponibilità, integrità e riservatezza** degli asset informatici, estendendo la protezione oltre il dominio digitale per contribuire a una **resilienza operativa** complessiva e minimizzare i rischi di interruzione dei servizi essenziali e importanti.

ALLEGATO 1

In collaborazione, la Cybersecurity Risk Foundation (CRF) e SANS hanno creato una libreria di modelli gratuiti per policy sulla cybersicurezza, pensati per aiutare le organizzazioni a definire, documentare e implementare rapidamente politiche chiave in questo ambito. L'intera gamma di misure di sicurezza, modelli di rischio e maturità alla base di questi modelli, è presente al link https://crfsecure.org.
L'elenco delle policy individuate, aggiornato al 15/05/2025 è sintetizzato nella tabella seguente, indicando il titolo della policy ed il rispettivo obiettivo di sicurezza.

TITOLO DELLA POLICY	DESCRIZIONE
Acceptable Encryption Standard	*Un approccio standardizzato per garantire l'uso di algoritmi di crittografia robusti e pubblicamente revisionati per proteggere i dati sensibili, assicurando la conformità alle migliori pratiche di sicurezza e ai requisiti normativi.*
Acceptable Use Standard	*Un insieme chiaro di linee guida per garantire che i dipendenti utilizzino le risorse aziendali in modo responsabile, sicuro e conforme alle politiche legali e organizzative.*
Access Management Policy	*Una strategia ben definita di gestione degli accessi per garantire che solo le persone autorizzate possano accedere a sistemi, dati e risorse critiche.*

Acquisition Assessment Standard	*Una valutazione strutturata degli acquisti per garantire che tutte le nuove tecnologie, software e servizi siano allineati con gli obiettivi di sicurezza, conformità e business prima dell'implementazione.*
Artificial Intelligence Acceptable Use Standard	*Un quadro di governance responsabile dell'IA per garantire un uso etico, sicuro e conforme nei processi e nelle decisioni basati sull'intelligenza artificiale.*
Asset Management Policy	*Una strategia completa per la gestione delle risorse tecnologiche e informative che garantisca sicurezza, conformità ed efficienza operativa durante tutto il loro ciclo di vita.*
Cloud Service Provider Management Policy	*Un approccio strutturato alla gestione dei fornitori di servizi cloud per garantire un'adozione sicura, la conformità e la mitigazione dei rischi negli ambienti cloud.*
Configuration Management Policy	*Una strategia strutturata di gestione della configurazione per garantire stabilità, sicurezza e conformità dei sistemi mantenendo la coerenza negli ambienti IT.*
Data Management Policy	*Un approccio strutturato alla gestione dei dati per garantire integrità, sicurezza e conformità normativa durante tutto il ciclo di vita delle informazioni dell'organizzazione.*

Database Credentials Standard	*Un approccio strutturato alla gestione delle credenziali dei database per garantire archiviazione sicura, autenticazione e controllo degli accessi per proteggere le informazioni sensibili.*
Education Management Policy	*Un approccio strutturato alla formazione sulla cybersicurezza per garantire che i dipendenti siano consapevoli delle politiche di sicurezza, delle minacce e delle migliori pratiche.*
Email Management Policy	*Una politica strutturata di gestione delle email per garantire comunicazioni sicure, filtraggio dello spam e protezione da phishing e malware.*
Identity Management Policy	*Una politica strutturata di gestione delle identità per garantire che le identità digitali siano create, mantenute e dismesse in modo sicuro ed efficiente.*
Internal Network Access Management Policy	*Una politica strutturata per controllare e monitorare l'accesso alle reti interne, garantendo che solo utenti e dispositivi autorizzati siano ammessi.*
Internet Acceptable Use Standard	*Un insieme chiaro di linee guida per l'uso responsabile e sicuro di Internet all'interno dell'organizzazione.*

Log Management Policy	*Una politica strutturata di gestione dei log per garantire che i log di sistema e di sicurezza siano raccolti, archiviati e analizzati per rilevare e rispondere agli incidenti.*
Mobile Device Management Policy	*Una politica strutturata di gestione dei dispositivi mobili per garantire l'uso sicuro di smartphone, tablet e altri dispositivi mobili sul posto di lavoro.*
Network Device Management Policy	*Una politica strutturata per la gestione di router, switch e altri dispositivi di rete per garantire configurazioni sicure e coerenti.*
Password Construction Standard	*Un approccio standardizzato alla creazione delle password per garantire password forti, complesse e sicure in tutta l'organizzazione.*
Perimeter Network Access Management Policy	*Una politica strutturata per gestire l'accesso alla rete perimetrale dell'organizzazione, inclusi firewall e DMZ.*
Physical Security Management Policy	*Una politica strutturata di sicurezza fisica per garantire che le strutture e l'hardware siano protetti da accessi non autorizzati e minacce ambientali.*
Privacy Management Policy	*Una politica strutturata di gestione della privacy per garantire la conformità alle normative sulla protezione dei dati e la salvaguardia delle informazioni personali.*

Privileged Account Management Policy	*Una politica strutturata per gestire e monitorare gli account privilegiati, riducendo il rischio di uso improprio o compromissione.*
Program Management Policy	*Una politica strutturata di gestione dei programmi per garantire che le iniziative di sicurezza siano allineate agli obiettivi aziendali e gestite in modo efficace.*
Resilience Management Policy	*Una politica strutturata di resilienza per garantire che l'organizzazione possa riprendersi rapidamente dalle interruzioni e mantenere le operazioni critiche.*
Risk Communication Management Policy	*Una politica strutturata per comunicare tempestivamente ed efficacemente i rischi di cybersicurezza agli stakeholder.*
Safeguard Implementation Management Policy	*Una politica strutturata per garantire che le misure di sicurezza siano implementate in modo coerente ed efficace in tutta l'organizzazione.*
Safeguard Selection Management Policy	*Una politica strutturata per guidare la selezione delle misure di sicurezza appropriate in base alle valutazioni dei rischi e alle esigenze aziendali.*

Safeguard Validation Management Policy	*Una politica strutturata per convalidare l'efficacia delle misure di sicurezza implementate attraverso test e valutazioni.*
Software Development Management Policy	*Una politica strutturata per garantire pratiche sicure di sviluppo software durante tutto il ciclo di vita del software.*
Software Development Vulnerability Management Policy	*Una politica strutturata per identificare, tracciare e correggere le vulnerabilità nei processi di sviluppo software.*
Software Management Policy	*Una politica strutturata per gestire in modo sicuro l'acquisizione, la distribuzione, la manutenzione e la dismissione del software.*
System Protection Management Policy	*Una politica strutturata per garantire che i sistemi siano protetti dalle minacce attraverso il rafforzamento, le patch e il monitoraggio.*
Technology Equipment Disposal Standard	*Un approccio standardizzato per smaltire in modo sicuro le apparecchiature tecnologiche obsolete o danneggiate, garantendo la distruzione dei dati.*
Third-Party Risk Management Policy	*Una politica strutturata per valutare e gestire i rischi associati a fornitori e prestatori di servizi terzi.*

Vulnerability Management Policy	*Una politica strutturata per identificare, valutare e correggere le vulnerabilità nei sistemi e nelle applicazioni.*

Tabella 2: Policy sulla sicurezza

1.4 Reporting

Il reporting rappresenta un elemento cardine del modello di governance richiesto dalla Direttiva NIS2 e dal D.Lgs. 138/2024, in quanto consente di garantire **trasparenza, controllo e accountability** sia verso il top management che verso le autorità competenti (ACN e CSIRT).

Un sistema di reporting efficace deve consentire:

- la disponibilità di informazioni tempestive e affidabili sullo stato della cybersecurity;
- la misurazione dei risultati delle misure di sicurezza implementate;
- la comunicazione chiara di incidenti, vulnerabilità e rischi emergenti;
- il supporto alle decisioni strategiche degli organi di amministrazione e direttivi;
- la dimostrazione di conformità in caso di verifiche ispettive e audit.

Flussi Informativi Interni

I flussi di reporting interni devono essere strutturati su più livelli, per garantire che le informazioni siano comunicate alle persone giuste, al momento giusto:

- **Report Operativi**: prodotti con frequenza settimanale o mensile dai team IT e di sicurezza, contengono dati su incidenti minori, vulnerabilità rilevate, attività di patching, test effettuati, log di

sicurezza. Destinatari: CISO, responsabili IT, responsabili di processo.

- **Cruscotti Direzionali (KPI e KRI)**: report sintetici e periodici (trimestrali o semestrali) indirizzati al Consiglio di Amministrazione e agli organi direttivi. Devono evidenziare trend, indicatori di rischio (KRI), indicatori di performance (KPI) e stato di avanzamento delle azioni correttive.
- **Report Straordinari**: comunicazioni immediate e ad hoc in caso di incidenti significativi, secondo i flussi di escalation definiti nell'Incident Response Plan.

Flussi Informativi Esterni

La Direttiva NIS2 impone obblighi stringenti di notifica verso le autorità competenti. Il reporting esterno deve quindi seguire uno schema standardizzato, coordinato dal Punto di Contatto NIS2, e integrarsi nei processi di incident management:

- **Notifica iniziale**: entro 24 ore dall'identificazione di un incidente significativo, con una valutazione preliminare e le prime misure adottate.
- **Report intermedio**: entro 72 ore, con informazioni aggiornate e più dettagliate.
- **Report finale**: entro 1 mese, con analisi delle cause, impatti e misure correttive implementate.
- **Comunicazioni periodiche**: ove richiesto da ACN o CSIRT, relativamente a vulnerabilità note, stato di sicurezza o risultati delle valutazioni periodiche.

Indicatori di Reporting

Il sistema di reporting deve basarsi su indicatori chiari, misurabili e confrontabili nel tempo, tra cui:

- **KPI (Key Performance Indicators)**: percentuale di patch applicate entro SLA, tempo medio di rilevamento di incidenti,

tempo medio di risposta (MTTR), numero di esercitazioni di business continuity effettuate.

- **KRI (Key Risk Indicators)**: numero di vulnerabilità critiche aperte, percentuale di fornitori critici non conformi, deviazioni dai livelli di servizio di sicurezza.
- **Compliance Indicators**: stato di avanzamento delle azioni correttive da audit, livello di formazione del personale, aggiornamento delle policy.

Modelli e Strumenti

Per garantire coerenza e tracciabilità, è raccomandato l'utilizzo di modelli di reportistica standardizzati e strumenti digitali di governance, risk & compliance (GRC). Tra gli output attesi:

- **Cruscotti digitali** integrati con SIEM/SOC per la visualizzazione in tempo reale delle minacce e degli eventi di sicurezza;
- **Report periodici al management** (trimestrali e semestrali), con sintesi esecutiva, indicatori chiave e stato delle azioni;
- **Template standard per notifiche ACN/CSIRT**, allineati ai requisiti del Regolamento di esecuzione 2024/2690.

Accountability e Riesame

Gli organi di amministrazione e direttivi hanno la responsabilità di esaminare e approvare i report di sintesi ricevuti, documentando le decisioni e le misure adottate. È raccomandato che i report:

- siano discussi periodicamente in sede di Consiglio di Amministrazione o Comitato Rischi;
- siano utilizzati come input per il **riesame periodico delle misure di sicurezza** e per la pianificazione degli audit;

- costituiscano evidenza documentale in caso di verifiche da parte dell'Autorità competente.

1.5 Formazione

Studieremo come impostare percorsi di formazione mirati sulla sicurezza informatica e sulla NIS2, obbligatori e differenziati per ruolo: **percorsi tecnici per chi gestisce i sistemi**, **formazione strategica per i manager** e **sensibilizzazione per il personale**.

Introduzione

La formazione verrà erogata con l'approccio di seguito riportato:

- formazione obbligatoria da fruire una tantum (con eventuali successivi approfondimenti su specifiche tematiche)
- pillole formative con frequenza periodica rivolte a tutto il personale aziendale

Formazione obbligatoria (una tantum)

1) STRUTTURA DEL CORSO: FORMAZIONE SULLA CYBERSICUREZZA PER ORGANI DI AMMINISTRAZIONE E DIRETTIVI

Obiettivi del Corso:

- Comprendere e agire in conformità con i propri ruoli, responsabilità (anche in termini di sanzioni) e poteri in materia di cybersicurezza, come definiti dal Decreto NIS
- Approvare e supervisionare efficacemente l'attuazione delle misure di gestione dei rischi di cybersicurezza all'interno dell'organizzazione
- Promuovere una cultura organizzativa incentrata sulla sicurezza informatica, garantendo la consapevolezza e la formazione del personale
- Ottenere e utilizzare le informazioni necessarie per la sorveglianza e il miglioramento continuo della sicurezza dei sistemi informativi e di rete (in particolare per quelli critici)

Modulo 1: Il Contesto Normativo e il Ruolo Strategico della Cybersicurezza

- Introduzione al Quadro NIS2 e al Decreto NIS
- Importanza della Cybersicurezza per la Governance

Modulo 2: Gestione del Rischio e Pianificazione della Cybersicurezza

- Strategia di Gestione del Rischio
- Valutazione del Rischio

Modulo 3: Politiche di Sicurezza Informatica

- Elaborazione e Applicazione delle Politiche
- Revisione e Aggiornamento delle Politiche

Modulo 4: Gestione degli Incidenti e delle Crisi di Cybersicurezza

- Notifica degli Incidenti Significativi
- Pianificazione e Risposta agli Incidenti
- Continuità Operativa e Gestione delle Crisi

2) STRUTTURA CORSO PER DIPENDENTI

Obiettivi del Corso:

- Comprendere l'importanza della cybersicurezza e le minacce più comuni nel contesto lavorativo
- Identificare i propri ruoli e responsabilità individuali in materia di sicurezza informatica
- Applicare le pratiche di igiene informatica e le politiche interne per proteggere i sistemi e i dati aziendali
- Saper riconoscere e segnalare tempestivamente eventi o incidenti di sicurezza
- Contribuire attivamente al mantenimento e al miglioramento continuo della postura di sicurezza dell'organizzazione

Modulo 1: Introduzione alla Cybersicurezza e al Contesto NIS2

- 1.1 Cos'è la Cybersicurezza e perché è importante per noi?
- 1.2 Il Contesto Normativo: la Direttiva NIS2 e il Decreto NIS

Modulo 2: Le Tue Responsabilità Quotidiane: Igiene Informatica e Protezione dei Dati

- 2.1 Pratiche di Igiene Informatica di Base
- 2.2 Sicurezza dei Dati
- 2.3 Gestione degli Accessi e del Personale

Modulo 3: Riconoscere, Segnalare e Rispondere agli Incidenti

- 3.1 Riconoscere un Incidente
- 3.2 Il Tuo Ruolo nella Gestione degli Incidenti
- 3.3 Collaborazione e Comunicazione

Considerato che i percorsi formativi previsti saranno erogati con cadenza ciclica, si propone di prevedere l'integrazione progressiva di ulteriori tematiche all'interno delle varie sessioni, in coerenza con le specifiche responsabilità e funzioni ricoperte dal personale. Di seguito alcuni dei principali temi da considerare:

Modulo: Contribuire al Miglioramento Continuo della Sicurezza

- 4.1 La Sicurezza nella Catena di Approvvigionamento
- 4.2 Sviluppo e Manutenzione Sicura dei Sistemi

Modulo: Gestione della Catena di Approvvigionamento e Sicurezza degli Asset

- Sicurezza della Catena di Approvvigionamento
- Gestione degli Asset

3) LA GOVERNANCE DELLA CYBERSICUREZZA NIS2 - RUOLI E RESPONSABILITÀ STRATEGICHE DEGLI ORGANI DI AMMINISTRAZIONE E DIRETTIVI

Destinatari: Membri del Consiglio di Amministrazione, Dirigenti, C-Level Executives e altri Organi di Amministrazione e Direttivi dell'azienda.

Obiettivi del Corso:

- Comprendere la propria **responsabilità legale e strategica** nella gestione della cybersicurezza aziendale secondo la Direttiva NIS2 e il Decreto NIS
- Conoscere i **requisiti chiave della Direttiva NIS2** in relazione alla governance della cybersicurezza, alla gestione dei rischi e alla resilienza operativa
- Assicurare e supervisionare l'implementazione di **politiche e piani** di cybersicurezza essenziali

- Riconoscere e rispondere adeguatamente agli **incidenti significativi**, gestendo le comunicazioni interne ed esterne
- Promuovere una **cultura della cybersicurezza** che si estenda a tutti i livelli dell'organizzazione, inclusa la formazione del personale
- Contribuire al **miglioramento continuo** della postura di sicurezza informatica dell'azienda attraverso la supervisione di audit e riesami.

Modulo 1: Il Quadro Normativo NIS2 e la Responsabilità della Governance

- 1.1 Introduzione alla NIS2 e al Decreto NIS: Il Contesto della Responsabilità Dirigenziale
  1.2 Ruoli, Responsabilità e Organizzazione della Cybersicurezza a Livello Direttivo
- 1.3 Sviluppo di Competenze e Cultura della Cybersicurezza

Modulo 2: La Gestione del Rischio e le Politiche di Sicurezza

- 2.1 Politiche di Sicurezza: Approvazione e Revisione Strategica
- 2.2 Valutazione e Trattamento del Rischio: La Decisione Direttiva
- 2.3 La Sicurezza nella Catena di Approvvigionamento: Vigilanza sui Fornitori

Modulo 3: Gestione e Comunicazione degli Incidenti

- 3.1 Il Ruolo della Dirigenza nella Notifica degli Incidenti Significativi
- 3.2 Procedure di comunicazione e di escalation degli incidenti significativi
- 3.3 Piani di Continuità Operativa e Gestione delle Crisi: La Resilienza Direttiva
- 3.4 Monitoraggio della Conformità e Audit di Sicurezza

Formazione non obbligatoria (periodica)

4) PILLOLE DI CYBERSECURITY

Predisposizione di pillole conoscitive sintetiche su argomenti di cybersecurity da diffondere in azienda tramite newsletter e/o webinar in funzione di:

- reportistica prodotta, al fine di applicare il principio di lessons learned, il cui obiettivo è quello di creare una sintesi di quanto accaduto per agevolare la gestione delle future occorrenze similari e migliorare i punti di debolezza (es. imparare dagli incidenti)
- diffusione di nuove minacce informatiche (es. es. Threat Intelligence);
- utilizzo di nuove tecnologie (es. AI);
- pubblicazione di studi e linee guida ufficiali provenienti da fonti accreditate riconosciute (ACN, ENISA, etc.).

Le tematiche propinate di volta in volta potranno soggiacere a periodicità predeterminate (es. trimestrale o per specifiche occorrenze).

5) ESERCITAZIONI PRATICHE: SIMULAZIONE DELLA CRISI

Una volta ricevuta l'opportuna formazione e consolidati gli argomenti affrontati sono ipotizzabili degli scenari pratici di Simulazione della Crisi da affrontare attraverso esercitazioni.

1.6 Verifica controlli e Piano di Audit

Premessa:

La direttiva NIS2 e il decreto D.lgs. 138/2024 richiedono che le organizzazioni in perimetro impostino un sistema di verifica e controllo, organizzato e indipendente, che preveda piani di audit interni e esterni.

Piano di Audit Interno

Il piano di audit interno è fondamentale per dimostrare la conformità continua e per identificare aree di miglioramento.

Definizione degli Obiettivi dell'Audit:

- Verificare la conformità ai requisiti della NIS2 (e del D.Lgs. di recepimento).
- Valutare l'efficacia dei controlli di sicurezza implementati.
- Identificare vulnerabilità, carenze o non conformità.
- Fornire raccomandazioni per il miglioramento continuo.

Ambito dell'Audit:

- Definire chiaramente cosa verrà auditato (es. specifici sistemi, processi, dipartimenti, la gestione degli incidenti, la sicurezza della supply chain, ecc.). A rotazione il piano di audit dovrebbe coprire tutti i requisiti rilevanti della NIS2.

Frequenza e Tempistiche:

- Gli audit devono essere condotti **periodicamente**, con una frequenza definita in base al profilo di rischio dell'organizzazione e alla rilevanza dei sistemi/processi.
- Vanno previsti anche audit **ad-hoc** in caso di eventi significativi (es. incidenti gravi, modifiche sostanziali all'infrastruttura).

- Va definito un calendario annuale o pluriennale per gli audit.

Team di Audit (Ruoli e Responsabilità):

- **Auditor Interni:** Se si dispone di competenze interne, si può utilizzare un team di auditor qualificati e indipendenti dalle aree che saranno auditate.
- **Auditor Esterni:** Si può considerare il coinvolgimento di esperti esterni specializzati in NIS2 per garantire obiettività e competenze specifiche.
- **Responsabile dell'Audit:** È opportuno identificare una figura responsabile della pianificazione, esecuzione e rendicontazione degli audit. Nel caso sia presente un sistema Integrato Qualità, Ambiente, Sicurezza etc..la figura può anche essere la stessa già incaricata del sistema.

Team di Audit (Competenze)

I componenti del team di audit devono possedere le seguenti competenze tecniche, in conformità a quanto previsto dal D.Lgs. 138/2024, al fine di garantire la conduzione di audit interni esaustivi ed efficaci in materia di cybersicurezza:

- **Conoscenza normativa e regolatoria**:
  - Padronanza del D.Lgs. 138/2024 e della Direttiva (UE) 2022/2555 (NIS 2)
  - Familiarità con normative collegate

- **Sicurezza delle reti e dei sistemi informativi**:
  - Valutazione delle misure di sicurezza per reti, sistemi e infrastrutture critiche
  - Conoscenza di firewall, IDS/IPS, segmentazione di rete, VPN, crittografia

- Verifica dei sistemi di autenticazione, gestione degli accessi e privilegi

- **Gestione del rischio e resilienza operativa**:
  - Capacità di analizzare processi di risk assessment e risk management
  - Valutazione di Business Continuity Plan (BCP) e Disaster Recovery Plan (DRP)
  - Analisi dell'impatto (BIA) e delle misure di mitigazione adottate

- **Gestione degli incidenti di sicurezza**:
  - Verifica dell'esistenza di un piano di risposta agli incidenti (Incident Response Plan)
  - Capacità di valutare i processi di rilevamento, gestione e notifica degli incidenti
  - Conoscenza dei requisiti di notifica verso CSIRT e ACN entro i termini previsti

- **Governance della sicurezza**:
  - Valutazione della struttura organizzativa e dei ruoli (es. CISO, DPO, IT Security)
  - Verifica dell'adozione di politiche e procedure di sicurezza formalizzate
  - Controllo della formazione e sensibilizzazione del personale in materia di cybersecurity

- **Controlli tecnici e organizzativi**:
  - Verifica dell'implementazione di misure tecniche minime (es. patch management, hardening, logging)
  - Analisi dei controlli organizzativi: segregazione dei compiti, gestione dei fornitori, audit trail

- **Conformità e audit**:
  - Capacità di condurre audit interni secondo standard riconosciuti (es. ISO/IEC 27001, ISO 19011)

- Redazione di report di audit, raccolta evidenze, identificazione di non conformità
- Follow-up delle azioni correttive e monitoraggio continuo

- **Conoscenza dei settori critici**:
  - Comprensione delle specificità dei settori ad alta criticità (Allegato I) e critici (Allegato II) del decreto
  - Capacità di valutare l'impatto delle misure di sicurezza in contesti settoriali (es. energia, sanità, trasporti)

- **Competenze tecniche trasversali**:
  - Familiarità con strumenti di vulnerability assessment e penetration testing

Metodologia dell'Audit:

- **Pianificazione Dettagliata:** Un piano di audit dettagliato deve includere:
  - Aree specifiche da verificare.
  - Criteri di audit (requisiti NIS2, politiche interne, standard di settore).
  - Calendario e scadenze.
  - Risorse necessarie.
- **Raccolta di Informazioni:**
  - Revisione della documentazione (politiche, procedure, registri, report di analisi dei rischi, piani di incident response, log di sistema).
  - Interviste con il personale chiave (management, IT, compliance, utenti).
  - Valutazione tecnica delle misure di sicurezza (configurazioni, log, risultati di test di vulnerabilità).
- **Verifica e Test:**

        - Esecuzione di test a campione per valutare l'efficacia dei controlli (es. test di accesso, verifica delle procedure di backup/restore, simulazioni di incidenti).
    - **Analisi dei Risultati:** Confronto delle evidenze raccolte con i criteri di audit.

Reporting e Follow-up:

- **Rapporto di Audit:** Deve essere redatto un rapporto di audit chiaro e completo che includa:
    - Obiettivi e ambito dell'audit.
    - Metodologia adottata.
    - Risultati e evidenze.
    - Identificazione di non conformità, vulnerabilità e aree di miglioramento.
    - Raccomandazioni specifiche per la mitigazione dei rischi e il miglioramento dei controlli.
    - Un piano d'azione correttivo con responsabilità e scadenze definite.
- **Comunicazione:** Il risultato del rapporto va presentato agli organi direttivi, che, secondo la NIS2, hanno la responsabilità di approvare e supervisionare l'implementazione delle misure di gestione del rischio di cybersecurity.
- **Monitoraggio:** Va implementato un processo di monitoraggio continuo che assicuri che le azioni correttive siano implementate e che i miglioramenti siano sostenuti nel tempo. Programma verifiche di follow-up.

Gestione delle Non Conformità e Follow-up

- Le non conformità e le aree di miglioramento identificate durante l'audit vanno documentate e classificate per criticità.
- Deve essere sviluppato un Piano di Azioni Correttive che specifichi:
    - Descrizione della non conformità/raccomandazione.
    - Azioni correttive proposte.

- Responsabili dell'implementazione.
- Scadenze.

- Devono essere programmate verifiche di follow-up per assicurare che le azioni siano state completate e che i controlli siano efficaci.

Comunicazione e Reporting

- Kick-off Meeting: incontro iniziale con il management per presentare il piano di audit e gli obiettivi.
- Aggiornamenti Periodici: se necessario, aggiornamenti sullo stato di avanzamento dell'audit.
- Rapporto Finale di Audit: è necessario produrre un rapporto scritto che riassuma i risultati, le non conformità, le raccomandazioni e il Piano di Azioni Correttive.
- Presentazione al Management: il rapporto finale sarà presentato e discusso con l'Alta Direzione e gli organi di governance competenti per l'approvazione e la definizione delle priorità.
- Archiviazione: i documenti relativi all'audit saranno archiviati in conformità con le politiche interne.

PIANO DI AUDIT ANNUALE SU NIS2

L'obiettivo principale del piano di audit annuale è di valutare e confermare la conformità dell'organizzazione ai requisiti della Direttiva NIS2 e del relativo decreto legislativo di recepimento italiano (D.Lgs. 138/2024), identificando al contempo aree di miglioramento continuo nella gestione della sicurezza delle informazioni e della resilienza cibernetica.

Nello specifico, gli obiettivi includono:

- Verificare l'adeguatezza e l'efficacia delle misure tecniche, operative e organizzative implementate per la gestione dei rischi di cybersecurity.
- Assicurare la conformità con gli obblighi di notifica degli incidenti cibernetici.
- Valutare la robustezza dei piani di continuità operativa e di ripristino in caso di disastro.
- Esaminare la sicurezza della catena di approvvigionamento IT/ICT.
- Confermare che i processi di governance e le responsabilità in materia di cybersecurity siano chiaramente definiti e rispettati.
- Identificare eventuali gap rispetto ai requisiti NIS2 e fornire raccomandazioni per il miglioramento.

L'audit deve coprire tutti i domini e i requisiti della Direttiva NIS2 rilevanti per l'organizzazione, focalizzandosi su:

- Governance della Cybersecurity: Ruolo e responsabilità del management, politiche e strategie di sicurezza.
- Gestione del Rischio: Processi di identificazione, valutazione e trattamento dei rischi di cybersecurity.
- Gestione degli Incidenti: Preparazione, rilevamento, risposta e ripristino post-incidente, inclusi i processi di notifica.
- Continuità Operativa e Disaster Recovery: Piani, procedure e test di backup, ripristino e continuità dei servizi.
- Sicurezza della Catena di Approvvigionamento: Valutazione dei rischi dei fornitori terzi, clausole contrattuali, monitoraggio.
- Sicurezza Fisica e Ambientale: Controlli per la protezione fisica degli asset critici.
- Sicurezza delle Reti e dei Sistemi Informatici: Controlli tecnici (es. firewall, patch management, segmentazione di rete, crittografia).
- Gestione degli Accessi: Politiche e procedure di gestione degli accessi, autenticazione (inclusa MFA).
- Acquisizione, Sviluppo e Manutenzione dei Sistemi: Security by design, gestione delle vulnerabilità.

- Formazione e Consapevolezza: Programmi di formazione del personale e campagne di sensibilizzazione.
- Test e Valutazione: Risultati di vulnerability assessment, penetration test, audit di terze parti.

L'audit si baserà su:

- Direttiva NIS2 (UE 2022/2555) e il D.Lgs. 138/2024 (recepimento).
- Standard e best practice di cybersecurity applicabili (es. ISO 27001, Cybersecurity Framework ect.).
- Politiche, procedure e linee guida interne dell'organizzazione in materia di sicurezza delle informazioni.
- Legislazione nazionale e regolamenti di settori pertinenti.

Metodologia:

- Revisione Documentale: Analisi di politiche, procedure, registri, rapporti di valutazione del rischio, piani di risposta agli incidenti, contratti con fornitori, report di audit precedenti.
- Interviste: Colloqui con personale chiave (management, responsabili IT, responsabili della sicurezza, HR, responsabili delle operazioni, fornitori se necessario).
- Esame Tecnico: Revisione di configurazioni di sistema, log di sicurezza, risultati di scansioni di vulnerabilità e penetration test, architetture di rete.
- Test a Campione: Verifica dell'implementazione e dell'efficacia dei controlli attraverso l'esecuzione di test specifici su un campione rappresentativo (es. verifica backup, simulazioni di attacco, test di ripristino).
- Osservazione diretta dei processi e delle procedure operative.

2. SUPPLY CHAIN RISK MANAGEMENT

2.1 Mappatura dei fornitori critici

Ci occuperemo di identificare quali fornitori sono effettivamente rilevanti per la continuità e la sicurezza dei servizi IT e business. Li classificheremo in base:

- alla criticità,
- al tipo di servizio offerto
- all'impatto potenziale su sistemi e processi.

Nella fase di mappatura della propria supply chain, le organizzazioni devono classificare i fornitori in base al loro **livello di criticità** per poter così identificare tutti i fornitori critici e documentare le dipendenze e le interconnessioni tra fornitori. Le organizzazioni devono inoltre mantenere un registro aggiornato di tutti i fornitori critici.

Un fornitore può essere, per quanto riguarda i servizi IT del tipo (da Implementing guidance di ENISA):

- fornitore di servizi informatici;
- produttore (manufacturer);
- fornitore di software;
- fornitore di hardware;
- fornitore di servizi gestiti (Managed Service Provider (MSP));

- fornitore di servizi di sicurezza gestiti (MSSP);
- utente.

Un fornitore di servizi ICT è critico se, ad esempio:

- Può compromettere **riservatezza/integrità/disponibilità** dei dati nel processo (soprattutto se si tratta di dati sensibili).
- **Non è facilmente rimpiazzabile/sostituibile** entro i tempi operativi accettabili.
- L'interruzione del suo servizio può **compromettere la continuità di operazioni/servizi di business** (quindi soprattutto se è a supporto di processi critici e importanti dell'azienda), la **solidità dell'organizzazione** e i **risultati finanziari** per mancati ricavi (direttamente per interruzione dei processi o indirettamente per danno d'immagine) o per extra costi (costi operativi, legali, penali, sanzioni) e danni reputazionali => risulta quindi importante individuare le funzioni/processi che sono critiche e importanti (FCI) per l'azienda (cioè la cui interruzione comprometterebbe i risultati finanziari della stessa o la solidità o la continuità dei suoi servizi e delle sue attività)
- L'interruzione del suo servizio può compromettere l'adempimento degli **obblighi previsti dalla normativa applicabile.**

Possibili dimensioni da considerare nelle valutazioni sulla criticità dei fornitori sono quindi: impatto sui processi aziendali, sostituibilità, tipo di servizio, sicurezza del fornitore stesso (data breach recenti ..), giurisdizione (il servizio fornito rientra all'interno dell'UE o se è fornito da un soggetto situato al di fuori di esso).

L’identificazione di una funzione di business come FCI può emergere dalle Business Impact Analysis (BIA) (costi e tempi di sostituzione, impatto operativo, danni reputazionali) o essere eseguita con una valutazione a sé stante.

Nell’esecuzione della BIA:

1. Si **mappano i processi aziendali**
2. Si identificano i **processi** (o funzioni) **critici e importanti** che contribuiscono direttamente alla produzione di ricavi (l'interruzione o compromissione di questi processi determina una sospensione o riduzione dei ricavi; quindi, comprometterebbe i risultati finanziari dell’azienda o la solidità o la continuità dei suoi servizi e delle sue attività). [identificare processi e sotto-processi di supporto, la loro interruzione determina l'interruzione del processo primario]
3. Si valuta in che misura il **tempo di interruzione di tali processi** determina mancati ricavi o gravi violazioni di compliance.
4. Si identificano e valutano i **fattori che determinano un aumento dei costi** (es sanzioni e costi per la gestione degli incidenti) e/o una perdita di posizioni di mercato
5. Per ogni processo si **mappano gli applicativi/servizi ICT** (service catalog) utilizzati per svolgere il processo critico e il **livello di importanza/criticità** che il business gli attribuisce per svolgere le attività collegate al processo critico [Indispensabile / Importante / Rinunciabile]

6. Per gli applicativi/servizi ICT acquistati, si mappano i **fornitori impiegati** [Nome Fornitore, estremi di contatto del Fornitore e tipologia di fornitura]

7. Si valuta la **dipendenza dei processi critici dai servizi ICT; quindi,** l'impatto che la mancanza di un servizio potrebbe avere sulla performance finanziaria, sulla continuità dei servizi e delle attività, e sul rispetto degli obblighi normativi. Il livello di dipendenza (o "reliance") da un servizio ICT può essere classificato in diverse categorie:

- **Non significativo**: In caso di interruzione del servizio, le funzioni supportate non subirebbero impatti significativi. Non ci sarebbero interruzioni o danni importanti, e qualsiasi problema potrebbe essere risolto rapidamente.
- **Bassa dipendenza (Low)**: Se si verifica un'interruzione, le funzioni supportate non sarebbero significativamente impattate. Non ci sarebbero interruzioni o danni importanti, e la situazione potrebbe essere risolta rapidamente con un impatto minimo.
- **Dipendenza materiale (Material)**: In caso di interruzione, le funzioni supportate sarebbero significativamente impattate se l'interruzione dura più di pochi minuti o ore. Potrebbero verificarsi danni, ma sarebbero comunque gestibili.
- **Dipendenza totale (Full)**: Se si verifica un'interruzione, le funzioni supportate sarebbero immediatamente e gravemente interrotte o danneggiate per un lungo periodo.

Post individuazione dei fornitori critici, è importante verificare/monitorare tali fornitori critici tramite:

- Risk assessment ante stipula contrattuale: per identificare minacce, vulnerabilità, probabilità e impatto, considerando accesso ai dati, integrazione con sistemi core e adesione a standard di sicurezza
- Continuous Monitoring à Dopo la classificazione, si attiva un monitoraggio costante: audit regolari, security ratings, alert in tempo reale su degradazione della postura.

Va poi definito un criterio chiaro per la classificazione della criticità dei fornitori [es BASSA, MEDIA e ALTA] per una gestione efficace della supply chain.

Ambito / Valori da attribuire ->	1 - BASSA	2 – MEDIA	3 – ALTA
Tipologia di dati personali trattati (anagrafica, dati particolari, dati particolari e sanitari, dati giudiziari, profilazione con elementi di intelligenza artificiale)	Anagrafiche per gestire il contratto (dati di contatto del fornitore).	Dati personali ulteriori a quelli necessari a gestire il contratto.	Dati particolari sanitari, dati giudiziari, profilazione con elementi di intelligenza artificiale.
Numerosità dei dati trattati	La numerosità dei dati trattati è esigua e relativa a meno di 50 persone fisiche.	La numerosità dei dati trattati è modesta e relativa ad un range tra 50 e 100 persone fisiche.	La numerosità dei dati trattati è relativa a più di cento persone fisiche.
Criticità dei dati trattati in termini di riservatezza e	I dati non presentano particolari requisiti di	La perdita di riservatezza, integrità o disponibilità	La perdita di riservatezza, integrità o disponibilità

Ambito / Valori da attribuire ->	1 - BASSA	2 – MEDIA	3 – ALTA
integrità e disponibilità	riservatezza (sono pubblici), non sono di tipo economico contabile, né la loro perdita o variazione ha impatto sulle persone, né la loro indisponibilità per lungo tempo comporta difficoltà per l'organizzazione. ESEMPI: anagrafiche	dei dati non ha elevati impatti sulle attività dell'organizzazione, sul suo personale, sugli utenti (solo leggeri fastidi). La perdita di riservatezza, integrità o disponibilità non comporta gravi inadempienze relative alla normativa vigente. Un eventuale incidente su questi dati non	dei dati avrebbe elevati impatti sulle attività dell'organizzazione (perdite economiche, multe contrattuali), sul suo personale, sugli utenti (anche in termini di stigmatizzazione, perdita di serenità). La perdita di riservatezza, integrità o disponibilità comporta gravi inadempienze

Ambito / Valori da attribuire ->	1 - BASSA	2 – MEDIA	3 – ALTA
		avrebbe gravi ripercussioni sull'immagine dell’organizzazione. I dati non sono di tipo economico contabile.	relative alla normativa vigente. Un eventuale incidente su questi dati avrebbe gravi ripercussioni sull'immagine dell’organizzazione. I dati sono di tipo economico contabile.
Integrazione con sistemi dell’organizzazione	Il prodotto o servizio non necessita di alcuna integrazione con i sistemi dell’organizzazione.	Il prodotto o servizio necessita di integrazioni limitate alle anagrafiche di accesso.	Il prodotto o servizio necessità di integrazione con sistemi dell’organizzazione.

Ambito / Valori da attribuire ->	1 - BASSA	2 – MEDIA	3 – ALTA
Tipo di fornitura (prodotti sviluppati ad hoc, prodotti a pacchetto, servizi, servizi cloud,…);	Prodotti o servizi che non trattano dati o informazioni dell'organizzazione (p.e. cancelleria). NB: in questo caso, il rischio è sempre molto basso.	Prodotti a pacchetto noti sul mercato. Servizi cloud noti sul mercato. Servizi noti sul mercato. ESEMPIO: prodotti Microsoft.	Prodotti informatici sviluppati ad hoc, prodotti a pacchetto di nicchia, servizi di nicchia, servizi cloud di nicchia, strumenti di intelligenza artificiale e profilazione.
L'ambiente in cui sarà usato il prodotto o servizio (disponibile solo internamente allo staff, al pubblico,…);	Staff	Staff	Tutti (staff, grande pubblico).
Complessità del prodotto o	Prodotto o servizio	Una delle seguenti:	Una delle seguenti:

Ambito / Valori da attribuire ->	1 - BASSA	2 – MEDIA	3 – ALTA
servizio e quindi anche la possibilità o meno di cambiare più o meno velocemente fornitore;	ampiamente diffuso sul mercato e facilmente sostituibile.	- prodotto o servizio ampiamente diffuso sul mercato ma non facilmente sostituibile; - prodotto o servizio mantenuto da una ampia comunità di sviluppato.	- prodotto o servizio ampiamente diffuso sul mercato ma non sostituibile (p.e. perché è usato un db particolare o non sono disponibili software di migrazione); - prodotto o servizio di nicchia per il quale non sono disponibili valide alternative; - prodotto o servizio mantenuto da una ridotta comunità di sviluppatori; - servizio

Ambito / Valori da attribuire ->	1 - BASSA	2 – MEDIA	3 – ALTA
			attivo sui server del fornitore che non ne consente la migrazione, né l'esportazione dei dati su db strutturati o comunque noti.
Eventuale necessità di un passaggio di consegne (rischio contingente e operativo).	Prodotto o servizio ampiamente diffuso sul mercato e con ampia disponibilità di competenze.	Prodotto o servizio diffuso sul mercato e con disponibilità (non ampia) di competenze.	Prodotto o servizio con poche persone e società competenti per mantenerlo (o proprietario).

Ambito / Valori da attribuire ->	1 - BASSA	2 – MEDIA	3 – ALTA
Dipendenze da misure tecniche di sicurezza (se la fornitura include misure tecniche di sicurezza con impatto su più prodotti e servizi);	Il servizio o prodotto non è di sicurezza.	Il servizio o prodotto è di sicurezza IT, ma soprattutto di monitoraggio o recupero.	Il servizio o prodotto è di sicurezza IT e di tipo preventivo (la sua compromissione permetterebbe numerosi e facili attacchi da parte di malintenzionati).
Fornitore italiano o estero (con diversità culturali).	Il fornitore è italiano	Il fornitore è estero (con diversità culturali) ma UE	Il fornitore è extra europeo
Fornitore con competenze nel settore dell'organizzazione	Il fornitore ha competenze ed esperienze nel settore dell'organizzazione.	Il fornitore ha competenze ed esperienze in settori simili a quello dell'organizzazione.	Il fornitore non ha competenze ed esperienze in settori simili a quello dell'organizzazione.

Tabella 3: Criteri per la classificazione della criticità dei fornitori

Due diligence e valutazione del rischio

Premessa

La **Direttiva NIS2** impone alle entità soggette di adottare misure di sicurezza tecniche, operative e organizzative che tengano conto anche dei rischi derivanti dalla catena di fornitura (*supply chain*). In particolare, l'articolo 21 stabilisce che le organizzazioni devono valutare il livello di rischio associato ai fornitori critici, in relazione sia alla sicurezza dei prodotti e servizi utilizzati, sia alla continuità operativa e resilienza dell'ecosistema digitale. Ciò significa che le aziende devono assicurarsi che i fornitori, soprattutto quelli che gestiscono dati sensibili o infrastrutture rilevanti, adottino misure minime di sicurezza come: security by design, procedure di gestione e notifica degli incidenti, e piani di business continuity e disaster recovery.
A livello operativo, la direttiva richiede di mantenere un registro costantemente aggiornato dei fornitori ritenuti critici, includendo per ciascuno una valutazione del rischio documentata.
È inoltre necessario implementare un sistema per riesaminare periodicamente tali valutazioni, e includere nella selezione dei fornitori criteri di sicurezza informatica misurabili.

L'obiettivo è ridurre la superficie d'attacco esterna, evitare effetti domino in caso di compromissioni a monte e garantire una governance robusta del rischio terze parti.

Obiettivi della due diligence

- Identificare e classificare i fornitori critici per la sicurezza della rete e dei sistemi informativi.
- Valutare il rischio cyber associato a ciascun fornitore.
- Garantire conformità alla normativa NIS2, in particolare in merito all’adozione di misure tecniche e organizzative adeguate.
- Definire obblighi contrattuali chiari sui requisiti di sicurezza.

Criteri di valutazione dei fornitori

1. **Criteri generali**
2. **Governance**
3. **Cybersecurity**
4. **Security monitoring**
5. **BC / DRP**
6. **Formazione e consapevolezza**

I criteri di valutazione, organizzati per dominio, possono essere trasformati in domande per il questionario o in metriche da valutare.

Nei successivi paragrafi vengono approfonditi i punti elencati e si fornisce il collegamento al relativo questionario.

Criteri generali

La direttiva **NIS2** richiede che le organizzazioni adottino un approccio strutturato alla gestione del rischio della supply chain, a partire da una valutazione dei **criteri generali di rischio dei fornitori**. Questo implica innanzitutto l'analisi della **natura del servizio fornito** e della sua **criticità per la continuità operativa**: i fornitori che erogano servizi essenziali, infrastrutturali o ICT strategici devono essere trattati come soggetti ad alto impatto.

Un secondo aspetto riguarda l'**accesso a dati personali, sensibili o a sistemi critici**: laddove il fornitore gestisca informazioni rilevanti o abbia accesso a componenti core dell'infrastruttura, è richiesta

un’attenta analisi del rischio e l’adozione di misure contrattuali e tecniche rafforzate.

La direttiva impone inoltre di considerare la **posizione geografica del fornitore**: in particolare, va valutato l’eventuale trattamento di dati o l’erogazione di servizi da Paesi extra-UE, con particolare attenzione a quelli con legislazioni non equivalenti in materia di protezione dei dati e sicurezza informatica.

Infine, la NIS2 introduce l’obbligo di considerare anche la **catena di subfornitura**: le organizzazioni devono accertarsi che i fornitori critici adottino a loro volta adeguate misure di sicurezza e gestiscano i propri fornitori secondo gli stessi principi di responsabilità e trasparenza.

Questo insieme di criteri generali rappresenta il primo passo per una corretta valutazione del rischio cyber connesso alla supply chain, come richiesto dalla direttiva.

In sintesi:

- Natura e criticità del servizio fornito.
- Accesso ai dati personali o ai sistemi critici.
- Posizione geografica (extra-UE? Paesi ad alto rischio?).
- Subfornitori coinvolti (supply chain).

È possibile usare il questionario allegato per categorizzare i propri fornitori nel rispetto dei Criteri Generali richiesti dalla Direttiva:

01 - Criteri generali e metriche di valutazione: questionario

Governance

La direttiva **NIS2** impone alle organizzazioni di valutare, nella selezione e nella gestione dei fornitori, anche gli aspetti legati alla **governance della sicurezza** e alla **conformità normativa**. In particolare, è richiesto che i fornitori, soprattutto quelli che erogano servizi critici o trattano dati sensibili, abbiano una **struttura organizzativa adeguata** per la gestione della sicurezza informatica, con **ruoli e responsabilità chiaramente definiti** (es. presenza di un CISO, DPO o equivalente).

La direttiva prevede inoltre che i fornitori rispettino le principali normative e standard di riferimento, come **ISO/IEC 27001**, **GDPR**, **NIS2 stessa**, **SOC 2** e, se applicabile, **PCI-DSS**, con disponibilità di documentazione comprovante la conformità.

L'adozione di **policy formalizzate** (es. gestione accessi, sicurezza fisica e logica, backup, gestione incidenti) e di **processi di controllo interno**, come audit periodici e valutazioni del rischio, è un altro elemento centrale richiesto dalla direttiva.

L'organizzazione committente ha la responsabilità di verificare tali aspetti, anche attraverso clausole contrattuali e audit, per garantire che i fornitori mantengano un livello di sicurezza coerente con i requisiti della NIS2, contribuendo così alla **resilienza complessiva della supply chain**.

In sintesi:

- Esistenza di un Responsabile Sicurezza, IT o DPO.

- Aderenza a normative: ISO 27001, GDPR, SOC 2, altri.
- Politiche documentate di sicurezza, backup, business continuity.

È possibile usare il questionario allegato per categorizzare i propri fornitori nel rispetto della Governance richiesto dalla DIrettiva:

02 - Governance e compliance del fornitore: questionario

Cybersecurity

La direttiva **NIS2** impone alle organizzazioni di valutare la **robustezza delle misure tecniche di sicurezza** adottate dai fornitori, soprattutto se coinvolti in processi critici, trattamento di dati sensibili o integrazione nei sistemi aziendali. L'obiettivo è garantire che i fornitori implementino **controlli tecnici adeguati** per prevenire, rilevare e mitigare gli attacchi informatici, proteggendo la riservatezza, integrità e disponibilità dei dati e dei sistemi.

Le organizzazioni devono accertarsi che i fornitori adottino **misure concrete** come:

- la cifratura dei dati a riposo e in transito,
- identity e access management (IAM),
- l'autenticazione a più fattori (MFA),
- la segmentazione della rete,
- il patch management regolare,
- la protezione da malware,
- sistemi di monitoraggio, logging e gestione delle vulnerabilità

- i controlli per la gestione degli accessi privilegiati,
- il controllo delle configurazioni,
- la segregazione degli ambienti (es. produzione/test),
- l'adozione di strumenti EDR, SIEM o sistemi di alerting automatico

Tutti questi sono elementi fondamentali per valutare la maturità tecnica del fornitore.

La **NIS2 richiede anche che tali misure siano documentate, testate e mantenute** nel tempo, con evidenza di aggiornamenti periodici. La valutazione tecnica deve essere proporzionata alla criticità del servizio fornito, ma sempre documentata come parte del processo di gestione del rischio della supply chain.

È possibile usare il questionario allegato per categorizzare i propri fornitori nel rispetto delle misure tecniche di sicurezza richieste dalla Direttiva:

03 - Cybersecurity: questionario

Security monitoring

La direttiva **NIS2** impone ai soggetti critici e importanti — e quindi anche ai loro fornitori rilevanti — di adottare **misure continue di monitoraggio della sicurezza** per garantire la capacità di **prevenire, rilevare e rispondere efficacemente agli incidenti informatici**. In particolare, i fornitori devono disporre di sistemi di logging centralizzato, soluzioni SIEM (Security Information and Event Management) per la raccolta e correlazione degli eventi, e

possibilmente di tecnologie avanzate come EDR/XDR (Endpoint Detection and Response) per il rilevamento di minacce sui dispositivi. La Direttiva richiede inoltre che vengano eseguiti con regolarità **test di sicurezza** — come vulnerability assessment e penetration test — per identificare e correggere vulnerabilità note o nuove. Altro elemento essenziale è la capacità del fornitore di **gestire gli incidenti** con un processo strutturato, che comprenda:

- il **monitoraggio continuo degli eventi**,
- l'**analisi tempestiva delle anomalie**,
- la **comunicazione interna ed esterna** degli incidenti rilevanti, e
- la **notifica rapida** al cliente o all'autorità competente, ove applicabile.

La conformità alla Direttiva NIS2 implica anche che i fornitori mantengano **evidenza documentale** delle attività di monitoraggio e risposta, e che siano in grado di dimostrare la loro efficacia operativa.

È possibile usare il questionario allegato per categorizzare i propri fornitori nel rispetto delle misure di monitoraggio della sicurezza richieste dalla Direttiva:

04 - Security Monitoring: questionario

Continuità Operativa e Disaster Recovery del Fornitore

La direttiva **NIS2** richiede che le organizzazioni critiche e i loro fornitori adottino misure adeguate per garantire **la continuità operativa e il ripristino tempestivo delle attività** in caso di incidente o disservizio rilevante.
In quest'ottica, ogni fornitore rilevante deve disporre di un **piano di**

Business Continuity (BCP) e di un **piano di Disaster Recovery (DRP)** formalizzati, aggiornati e coerenti con la criticità dei servizi forniti.
Tali piani devono coprire scenari di malfunzionamento IT, perdita di dati, indisponibilità di sistemi o personale chiave, e devono includere la definizione dei **Recovery Time Objective (RTO)** e dei **Recovery Point Objective (RPO)**.

La NIS2 richiede inoltre che questi piani siano **testati periodicamente**, che ne sia documentata l'efficacia, e che il fornitore sia in grado di garantire la **ripresa operativa senza impatti critici** sulla sicurezza o sulla disponibilità dei servizi.
Ai fini della conformità alla Direttiva, è essenziale anche la presenza di **procedure di comunicazione d'emergenza**, di **backup protetti e isolati**, e la designazione di un **team responsabile per la gestione delle crisi**. Durante la valutazione dei fornitori, è necessario verificare non solo l'esistenza di tali piani, ma anche la loro **attuabilità concreta e il livello di maturità**.

È possibile usare il questionario allegato per categorizzare i propri fornitori nel rispetto delle misure di monitoraggio della sicurezza richieste dalla Direttiva:

05 - Continuità Operativa e Disaster Recovery: questionario

Formazione e consapevolezza

La direttiva **NIS2** riconosce la **preparazione e la consapevolezza del personale** come un elemento essenziale per la sicurezza informatica e la resilienza operativa delle organizzazioni, incluse quelle della supply chain.

I fornitori devono garantire che i propri dipendenti — in particolare coloro che operano su sistemi IT, trattano dati sensibili o svolgono attività critiche — siano **adeguatamente formati sui temi della sicurezza informatica**, delle minacce attuali (per es. phishing, social engineering, ransomware) e delle politiche interne di sicurezza. La formazione deve essere **regolare, documentata, tracciabile e proporzionata al ruolo** svolto, includendo anche elementi pratici (esercitazioni, simulazioni di attacco, campagne di phishing simulato).

La Direttiva richiede inoltre che i fornitori promuovano una **cultura della sicurezza**, incoraggiando comportamenti responsabili, la segnalazione tempestiva di eventi sospetti e la comprensione delle procedure in caso di incidente.
Il coinvolgimento attivo del personale nella difesa dell'organizzazione è considerato un **fattore chiave di conformità e maturità cyber**, da valutare attentamente nella selezione dei fornitori.

In fase di due diligence, è quindi necessario verificare l'esistenza di **programmi di security awareness**, la **frequenza e l'efficacia delle attività formative**, e la disponibilità di **evidenze documentali** a supporto.

È possibile usare il questionario allegato per categorizzare i propri fornitori nel rispetto delle misure di monitoraggio della sicurezza richieste dalla Direttiva:

06 - Formazione e consapevolezza: questionario

Implementazione

Riassumendo, per garantire la conformità alla Direttiva NIS2 in materia di gestione del rischio nella supply chain, è fondamentale strutturare un processo di implementazione graduale e sistematico.

Il primo passo consiste nel segmentare i fornitori in base al livello di criticità, dando priorità a quelli che trattano dati sensibili, accedono a sistemi critici o dispongono di privilegi amministrativi. Questa classificazione permette di concentrare le risorse di controllo dove il rischio è più elevato.

La due diligence di sicurezza deve essere integrata nel ciclo di onboarding, includendo valutazioni iniziali e verifiche dei requisiti di sicurezza informatica prima della firma dei contratti. Analogamente, deve essere ripetuta in fase di rinnovo contrattuale per tenere conto di eventuali cambiamenti nel rischio o nei servizi forniti. È inoltre necessario formalizzare un processo di escalation: quando una valutazione di rischio evidenzia livelli superiori alla soglia accettabile, l'organizzazione deve attivare azioni correttive documentate (remediation), fino alla sospensione o sostituzione del fornitore in caso di non conformità persistente.

Infine, la NIS2 richiede l'attuazione di audit periodici, anche avvalendosi di terze parti indipendenti, per verificare il rispetto effettivo dei requisiti di sicurezza dichiarati dal fornitore, inclusi i controlli tecnici, le policy organizzative e la capacità di risposta agli incidenti. Solo con questo approccio iterativo e documentato è

possibile garantire una reale governance del rischio esterno in linea con gli obblighi della Direttiva.

In sintesi:

- Segmentare i fornitori per criticità, partendo da quelli che trattano dati sensibili o hanno accessi privilegiati.
- Integrare la due diligence nel ciclo di onboarding e di rinnovo contrattuale.
- Formalizzare processi di escalation e remediation se il rischio supera una soglia accettabile.
- Eseguire audit periodici, anche tramite terze parti, per verificare il rispetto dei requisiti NIS2.

Scoring

Utilizzare una scheda di scoring come riferimento per attribuire punteggi e note ai propri fornitori nella supply chain.

Un esempio di scheda di questo tipo si trova al seguente link: **Scheda Supply Chain NIS2 - esempio**

2.2 Clausole Contrattuali per la Sicurezza nella Supply Chain: Indicazioni per l'Adeguamento alla Direttiva NIS 2

Introduzione

Uno degli elementi fondamentali per garantire la resilienza della supply chain, secondo la Direttiva NIS 2, è l'integrazione di requisiti di sicurezza nei contratti con i fornitori. Le clausole contrattuali rappresentano lo strumento principale per formalizzare obblighi, controlli e responsabilità condivise in materia di cybersecurity. Di seguito vengono presentati i principali elementi da includere nei contratti, insieme alle criticità riscontrate nella loro applicazione e le relative proposte di mitigazione.

Clausole Raccomandate

1. **Obblighi di sicurezza**

   I fornitori devono adottare misure di sicurezza equivalenti a quelle richieste al soggetto NIS. Le aree chiave da formalizzare includono:

   - **Controllo accessi e identità** (es. MFA, minimum priviledge).
   - **Protezione dei dati** (cifratura, backup sicuri).
   - **Gestione delle vulnerabilità** (patching tempestivo, vulnerability management).

- **Monitoraggio e logging** (log centralizzati, monitoraggio continuo).
- **Continuità operativa e recovery** (BCP/DRP documentati e condivisi).

2. **Notifica degli incidenti**

   Clausole che obblighino il fornitore a notificare rapidamente incidenti di sicurezza, con indicazione chiara di tempi, modalità e responsabilità.

3. **Audit e verifica**

   Il soggetto NIS deve poter:

   - Condurre audit on-site o da remoto.
   - Richiedere evidenze documentali (es: audit di terza parte /enti certificatori, certificazioni).
   - Verificare la conformità contrattuale in qualsiasi momento.

4. **Gestione dei subfornitori**

   Obbligo per il fornitore di:

   - Notificare e ottenere approvazione per il coinvolgimento di terze parti.
   - Estendere a essi gli stessi obblighi di sicurezza.

5. **Formazione e consapevolezza**

   Il personale del fornitore deve essere adeguatamente formato in materia di sicurezza e consapevole delle responsabilità connesse ai servizi erogati.

Ostacoli Ricorrenti e Misure di Mitigazione

L'inserimento di clausole contrattuali che impongano requisiti di cybersecurity coerenti con la Direttiva NIS 2 può incontrare resistenze di diversa natura, a seconda del profilo e della maturità del fornitore. Di seguito si analizzano i principali ostacoli riscontrati, accompagnati da esempi concreti di misure di mitigazione.

1. Limitazioni da parte di fornitori di grandi dimensioni o hyperscaler

Ostacolo: I fornitori globali (come Microsoft, AWS, SAP, Google Cloud) spesso rifiutano clausole contrattuali che prevedano audit diretti da parte dei clienti o responsabilità contrattuali personalizzate. Questo è dovuto alla loro esigenza di mantenere contratti standardizzati e di evitare un eccessivo onere amministrativo e legale.

Esempi di mitigazione:

- Accettazione di certificazioni riconosciute: integrare nei contratti clausole che riconoscano certificazioni come ISO/IEC 27001, SOC 2 Type II o CSA STAR come prova di conformità ai requisiti di sicurezza richiesti.
- Richiesta di report di audit indipendenti: prevedere che il fornitore metta a disposizione, con cadenza almeno annuale,

summary report di audit condotti da terze parti indipendenti (es. SOC 2 report, Penetration Test su piattaforme SaaS).

- Uso di questionari standardizzati: inserire l'obbligo di compilazione periodica di questionari di sicurezza standard (es. Cloud Security Alliance CAIQ), che facilitano il confronto tra fornitori.
- Clausole di escalation e responsabilità residuale: quando l'audit diretto non è possibile, si possono inserire clausole che obblighino il fornitore a collaborare in caso di incidente o richiesta delle autorità, limitando l'impunità contrattuale.

2. Bassa maturità di sicurezza in fornitori di piccole dimensioni o startup

Ostacolo: Piccole aziende o startup, pur essendo innovative e competitive, spesso non dispongono delle risorse tecniche, organizzative o economiche per adottare le misure richieste dalla NIS 2 (es. backup offline, business continuity plan, logging avanzato).

Esempi di mitigazione:

- Approccio proporzionale: applicare un modello basato sulla classificazione del rischio del fornitore. Per fornitori non critici, richiedere un set minimo di requisiti (es. MFA, antivirus aggiornato); per fornitori critici, mantenere i requisiti completi.
- Piani di adeguamento progressivo: introdurre nei contratti roadmap di adeguamento con milestone temporali (es. "entro sei mesi il fornitore dovrà dotarsi di un piano di disaster recovery testato annualmente").

- Supporto o formazione: offrire materiale formativo o consulenza per aiutare il fornitore a migliorare la propria postura di sicurezza. Alcune organizzazioni prevedono anche fondi o crediti formativi come incentivo.
- Misure compensative: prevedere l'uso di compensazioni temporanee (es. segregazione di rete, limitazione dei privilegi, accessi VPN monitorati) in attesa della piena conformità.

3. Resistenze legali o commerciali alla responsabilizzazione contrattuale

Ostacolo: Alcuni fornitori manifestano forte riluttanza a sottoscrivere clausole che comportino penali, obblighi di notifica, o responsabilità in caso di incidente, temendo impatti reputazionali, economici o legali.

Esempi di mitigazione:

- Coinvolgimento anticipato degli stakeholder interni: includere fin da subito gli uffici legale e procurement per definire clausole bilanciate e realistiche.
- Penali proporzionate e flessibili: inserire penali progressive, legate a parametri oggettivi (es. ritardi nella notifica, numero di incidenti) e proporzionate al danno potenziale.
- Meccanismi di escalation e conciliazione: prevedere fasi intermedie di gestione delle controversie (es. tavoli tecnici, mediazione) prima di attivare la risoluzione contrattuale.

- Clausole a tempo: introdurre clausole che scattano solo in determinate condizioni (es. “in caso di impatto superiore a X utenti o Y ore di disservizio”).

4. Difficoltà nel monitoraggio continuo delle misure di sicurezza dei fornitori

Ostacolo: L’organizzazione committente può non disporre degli strumenti o dei processi per monitorare con regolarità l’effettiva applicazione delle clausole di sicurezza da parte dei fornitori.

Esempi di mitigazione:

- Implementazione di soluzioni VRM/GRC: Adozione di piattaforme di Vendor Risk Management, integrate con il sistema informativo aziendale, per tracciare valutazioni, documentazione e KPI di sicurezza.
- Automazione della raccolta di evidenze: Richiedere che i fornitori utilizzino portali dedicati o API per caricare log, report, certificazioni con periodicità stabilita.
- Revisione periodica dei fornitori: Definire in contratto sessioni di review (es. trimestrali /semestrali o annuali, a seocnda della criticità del servizio erogato dal fornitore) con la presentazione dei KPI, gestione delle non conformità e aggiornamento dei piani di miglioramento.
- Dashboard di rischio per la governance: utilizzare dashboard integrate per monitorare lo stato di rischio della supply chain, classificare i fornitori e prioritizzare le azioni correttive.

Conclusioni

L'introduzione strutturata di clausole contrattuali specifiche è essenziale per trasferire i requisiti NIS 2 all'interno della catena di fornitura. L'efficacia di tali clausole dipende dalla capacità di bilanciare obblighi di sicurezza, sostenibilità operativa e limiti contrattuali. L'approccio raccomandato è scalabile, proporzionale al rischio e orientato alla collaborazione tra le parti.

NOTA: alternativamente a quanto scritto sopra, se occorre sintetizzare, si può proporre sotto formato tabellare tipo la bozza qui sotto (ancora da modificare e/o meglio, dettagliare)

Ostacolo	Descrizione	Esempi di misure di mitigazione
1. Fornitori di grandi dimensioni	Rifiuto di audit diretti e clausole personalizzate	- Accettazione certificazioni (ISO 27001, SOC 2) - Accesso a report di audit indipendenti - Questionari standard (es. CAIQ) - Clausole alternative e penali eque
2. Fornitori piccoli o startup	Bassa maturità o capacità di implementazione	- Approccio proporzionale al rischio - Piani di adeguamento graduali

Ostacolo	Descrizione	Esempi di misure di mitigazione
		- Supporto formativo e misure compensative
3. Resistenza commerciale/legale	Rifiuto di responsabilità, penali o obblighi di notifica	- Coinvolgimento legale/procurement in fase iniziale - Penali proporzionate e graduali - Clausole con attivazione condizionata - Meccanismi di conciliazione/escalation
4. Difficoltà nel monitoraggio continuo	Mancanza di strumenti e risorse per controlli periodici	- Adozione piattaforme VRM/GRC - Automazione raccolta KPI (API/portali) - Revisioni semestrali/annuali - Dashboard di rischio e indicatori per la governance

Tabella 4: Esempi misure di mitigazione

2.3 Monitoraggio continuo e verifica periodica

Premessa

Il presente documento definisce l'approccio per la qualifica dei fornitori, con l'obiettivo di garantire che i servizi e i prodotti esternalizzati siano selezionati, valutati e monitorati in maniera coerente con le esigenze di sicurezza, qualità e conformità normativa dell'organizzazione.

Le linee guida qui riportate consentono di:

- classificare la criticità dei servizi da esternalizzare,
- valutare in modo strutturato i fornitori e le loro offerte,
- valutare il prodotto o servizio attraverso aspetti funzionali, tecnici e di sicurezza informatica
- assicurare un monitoraggio continuo delle performance e dei rischi associati ai fornitori.

L'approccio adottato è in linea con le best practice internazionali e con quanto previsto dalla normativa vigente (es. D.Lgs. 138/2024, NIS2), ed è finalizzato a supportare decisioni consapevoli ed efficaci nella gestione della supply chain aziendale

Valutazione iniziale del servizio/processo da esternalizzare

Obiettivo: **capire quanto è critico per l'azienda il servizio che si desidera esternalizzare.**

Per arrivare a questo obiettivo riteniamo utile coinvolgere almeno i seguenti ruoli aziendali:

- Business Owner – responsabile strategico del risultato di business che un prodotto, servizio o processo deve generare. Definisce le esigenze, le priorità e i requisiti in termini di valore per il business.
- Service Owner – Responsabile da un punto di vista tecnico-operativo
- Cyber Security – Responsabile della protezione dei sistemi, dati e servizi digitali da accessi non autorizzati, incidenti o minacce

1. Descrivere il servizio/processo che si intende esternalizzare:

- Creare una RACI del processo
- Definire gli attori coinvolti
- Definire a quale area/funzione aziendale serve questo servizio?
- Descrivere il servizio
- Il servizio esiste già o è nuovo?
- Se esiste, è gestito internamente o da un altro fornitore?
- Motivare l'esternalizzazione
- Definire la frequenza e continuità del servizio richiesto
- Budget o valore stimato annuo del servizio

1. Creare un questionario di 8/10 domande per valutare l'impatto sul core business del servizio/processo (Service Impact

Assessment) assegnando un grado di criticità ad ogni domanda su una scala da 1 a 5 (5 molto critico/1 nessuna criticità):

- Il servizio ha un impatto diretto sulla continuità operativa aziendale (Business Continuity)?
- Il servizio influenza direttamente la qualità del prodotto o del servizio finale offerto al cliente?
- Qual è l'impatto operativo in caso di interruzione del servizio?
- Il servizio tratta dati personali, sensibili o riservati?
- Il servizio comporta attività che, se non eseguite correttamente, possono causare danni a persone, cose o reputazione aziendale?
- Il servizio è soggetto a monitoraggio da parte di autorità esterne o enti regolatori?
- La mancata esecuzione del servizio può comportare sanzioni legali, penali o economiche per l'azienda?
- Il servizio è parte integrante di una catena di fornitura estesa (supply chain) che impatta su altri fornitori o clienti?
- Il servizio necessita di continuità temporale (h24, giorni festivi, SLA stringenti)?
- Il servizio richiede un livello elevato di specializzazione o certificazioni tecniche per essere erogato?

Matrice RACI per i punti a) e b) della valutazione 1

	Business Owner	Service Owner	Cyber Security
Descrizione del servizio	A	R	C
Compilazione SIA	C	AR	C

Tabella 5: Matrice RACI

2. In base al risultato, viene assegnato un livello di criticità al servizio (Critical/Significant/Moderate/Minor)

Valutazione sul fornitore

Obiettivo**: valutare l'affidabilità, la qualità e l'idoneità di un fornitore. Una corretta valutazione permette di escludere determinati fornitori non adeguati, e creare una classificazione di fornitori. Definire in maniera approfondita il contratto ed eventuali clausole contrattuali, e quanto e cosa monitorare post-contratto.**

1. Creare una lista di domande di Assessment per il fornitore basandosi su diversi punti:

NB. Tra tutti gli elementi relativi alla valutazione del fornitore, noi ci concentriamo sulla valutazione dei livelli di sicurezza informatica.

GSI.01	Politica di alto livello che tratta la cybersecurity / sicurezza delle informazioni / sicurezza informatica

GSI.02	Politiche e procedure verticali collegate alla politica di alto livello
GSI.03	Piano per la gestione della continuità operativa
GSI.04	Continuità operativa dei sistemi ICT
GSI.05	Responsabilità in merito alla cybersecurity / sicurezza delle informazioni / sicurezza informatica
GSI.06	Responsabilità in merito alla protezione dei dati personali
GSI.07	Azioni di formazione e consapevolezza
GSI.10	Il rischio relativo alla cybersecurity / sicurezza delle informazioni
GSI.11	Verifica del livello di conformità della gestione della cybersecurity / sicurezza delle informazioni / sicurezza informatica
GSI.13	Budget per la cybersecurity / sicurezza delle informazioni / sicurezza informatica

GSI.16	Certificazioni relative alla sicurezza delle informazioni nell'ambito dell'oggetto della fornitura
SIT.01	Dispositivi di protezione del traffico di rete
SIT.03	Backup
SIT.09	Vulnerability assessment
SIT.10	Penetration test
SIT.11	Gestione dei log
SIT.18	Gestione degli incidenti relativi alla sicurezza delle informazioni / cybersecurity
SIT.19	Notifica degli incidenti
SIT.20	Cancellazione sicura dei dati
SIT.21	Trattamento dei dati personali
SIT.25	Architettura applicativa

GSI.08	Inventari dei beni aziendali utilizzati per il trattamento delle informazioni
GSI.09	Contratti stipulati con le terze parti
GSI.12	Processo per lo sviluppo sicuro del software
GSI.14	Servizi di Cloud Computing
GSI.15	Screening del personale
SIT.02	Reti wireless
SIT.04	Accessi logici degli utenti ai sistemi e alle principali applicazioni aziendali
SIT.05	Accessi logici degli amministratori ai sistemi, agli apparati di rete e alle principali applicazioni aziendali
SIT.06	Accessi logici da remoto ai sistemi aziendali
SIT.07	Utenti a livello di sistema operativo e, ove applicabile, di software applicativi

SIT.08	Patch di sicurezza pubblicate dai vendor
SIT.12	Dati memorizzati sui sistemi (data at rest)
SIT.13	Dati scambiati con i sistemi attraverso Internet (data in transit) e per l'accesso amministrativo (ivi incluse credenziali, token di sessione ed eventuali altri elementi analoghi)
SIT.14	Protezione degli endpoint aziendali (portatili, smartphone, tablet)
SIT.15	Sistemi di protezione locali
SIT.16	Sistemi di protezione di rete
SIT.17	Strumenti di elaborazione personale - BYOD (inclusi tablet e smartphone):
SIT.22	Cambiamenti ai sistemi informativi e ai software su di essi presenti
SIT.23	Configurazione di tutti i sistemi operativi e dei principali software installati sui sistemi informativi
SIT.24	Sistemi di monitoraggio

SIT.25	Architettura applicativa
SFA.01	Accesso al perimetro dell'organizzazione
SFA.02	Accesso ai locali che ospitano i server
SFA.03	Controllo di temperatura e umidità nei locali che ospitano i server
SFA.04	Continuità dell'alimentazione elettrica nei locali che ospitano i server
SFA.05	Protezione antincendio dei locali che ospitano i server
SFA.06	Archivi cartacei principali delle informazioni

Tabella 6: Assesment Fornitori

La lista è tratta dal questionario di valutazione fornitori clusit, scaricabile al sito:
https://clusit.it/blog/questionario-per-la-sicurezza-dei-fornitori/

2. Inviare il questionario a ciascun fornitore selezionato

3. Assegnare una scala di rilevanza ad ogni domanda (es. domanda da 1 punto, domanda da 3 punti, domanda da 5 punti)
4. Calcolare il punteggio finale del fornitore

Valutazione del prodotto/servizio

Obiettivo: **valutare se il prodotto o servizio specifico offerto dal fornitore rispetta i requisiti tecnici, di qualità, sicurezza e performance richiesti dall'azienda, in coerenza con la criticità del servizio esternalizzato e la sua integrazione nei processi aziendali.**

La valutazione tiene conto di aspetti funzionali, tecnici, normativi e di sicurezza informatica, con riferimento anche a quanto previsto dal D.Lgs. 138/2024, in particolare all'art. 24, comma 3, che impone di considerare le vulnerabilità specifiche di fornitori e la qualità dei loro prodotti, incluse le pratiche di sviluppo sicuro.

1. **Valutazione del prodotto/servizio offerto tenendo conto di questi elementi:**

- Aderenza ai requisiti funzionali e tecnici
- Documentazione tecnica e disponibilità di manuali
- Presenza di certificazioni tecniche e di cybersicurezza (es. schemi quali ISO/IEC 27001, EU Common Criteria)
- Presenza di vulnerabilità note
- Modalità di aggiornamento, patch management e supporto tecnico
- Qualità e usabilità del prodotto

Modalità di valutazione

- Verifica documentale
- Audit di sicurezza (interno o terza parte)
- Test tecnici (sandbox) su propria iniziativa o da parte di ACN (es. enti pubblici secondo DPR 54/2021)
- Griglie di valutazione con punteggio da 0 a 5

Incrocio delle valutazioni e definizione dell'idoneità complessiva

Obiettivo: **Una volta completate le valutazioni sul servizio, sul fornitore e sul prodotto offerto, si procede con l'integrazione delle tre valutazioni per determinare l'idoneità complessiva e supportare la decisione finale.**

a) Matrice di incrocio punteggi:

Per ogni fornitore viene costruita una matrice che incrocia:

- Il punteggio ottenuto nel Service Impact Assessment (valutazione della criticità del servizio)
- Il punteggio dell'Assessment del fornitore (affidabilità e sicurezza)
- Il punteggio ottenuto dalla valutazione del prodotto/servizio specifico (qualità, compliance, sicurezza, integrazione)

In base al livello di criticità del servizio (Critical, Significant, Moderate, Minor), vengono definiti punteggi minimi di accettabilità su ciascuna dimensione.

Esempio: un servizio classificato come "Critical" potrà essere affidato solo a fornitori con valutazione "Ottimo", che offrano un prodotto certificato e pienamente conforme agli standard di sicurezza e qualità richiesti.

b) Graduatoria dei fornitori idonei:

Viene generata una **graduatoria dei soli fornitori che risultano idonei**, in base all'incrocio delle valutazioni (fornitori/prodotti)

I fornitori non conformi in almeno una delle due valutazioni, (fornitore, prodotto) vengono esclusi

c) Matrice RACI per la decisione finale (go/no-go e contrattualizzazione) tenendo in considerazione i seguenti owner:

- Supplier Business Owner
- Service Owner
- Supplier

Valutazione continua del prodotto

Prevedere i seguenti obblighi contrattuali per il fornitore

- Comunicare entro 24-48 ore eventuali incidenti di sicurezza, perdita di certificazioni (sia di sistema di gestione che, specialmente, di prodotto), non conformità, minacce rivelanti
- Comunicare entro 24 ore(?) cambio del punto di contatto o persona di riferimento in caso di incidente

- Notificare entro 1 mese eventuali fusioni o cessioni di ramo d'azienda
- Notificare entro tre mesi eventuali acquisizioni societarie
- Segnalare ogni cambio significativo del prodotto (versione, architettura, tecnologia, logiche di sicurezza)

Frequenza delle rivalutazioni

- Almeno una volta l'anno, o più frequentemente se il servizio presenta alta vulnerabilità o criticità
- Ad ogni cambio significativo del prodotto
- A seguito di incidenti di sicurezza rilevanti
- Su richiesta a fronte di segnalazioni del CSIRT Italia o del Gruppo di Cooperazione

Monitoraggio continuo e riesame fornitore

Obiettivo: **garantire che le condizioni di sicurezza e qualità restino stabili nel tempo.**

Attivare un sistema di monitoraggio permanente del rischio fornitore, che includa:

- Indicatori di rischio e performance
- Alert automatici su eventi critici

- Verifiche periodiche basate su strumenti di audit e checklist
- Flussi di escalation

Periodicità delle verifiche:

- Annuale:
    - Riesame del rischio fornitore (GV.PO-02)
    - piano gestione incidenti (RS.MA-01)
- Biennale:
    - Valutazione del rischio legato ai fornitori (ID.RA-05)
    - Piani di risposta agli incidenti (ID.IM-04)
- Quadriennale:
    - Riesame completo del rischio ICT secondo NIS2, art. 12

2.4 Audit sui fornitori critici

L'obiettivo è progettare ed eseguire un programma di audit proporzionato alla criticità dei fornitori, verificando controlli di sicurezza, continuità operativa e adempimenti contrattuali.

Il perimetro include tutti i fornitori classificati ad alta criticità o con dipendenza "Material/Full" rispetto alle FCI. L'audit si svolge in due modalità: una prima fase documentale a distanza (policy, procedure, certificazioni come ISO/IEC 27001, SOC 2, CSA STAR, esiti di VA/PT, piani BC/DR e loro test), seguita da verifiche on-site o in sessione remota live con walkthrough dei processi, interviste e campionamenti tecnici.

Quando il fornitore è un hyperscaler, si accettano attestazioni di terza parte e si concentra la verifica sull'integrazione specifica e sulle responsabilità condivise.

La metodologia è risk-based: profondità e priorità derivano da criticità del servizio, esposizione dati, integrazioni core, giurisdizione e storico incidenti.

La griglia di controllo copre governance e ruoli, IAM/MFA e privilegi (incluso PAM), segregazione ambienti, patching e gestione vulnerabilità (con tracciamento KEV), protezioni endpoint/server/cloud, logging e SIEM, backup isolati e testati, gestione degli incidenti e delle notifiche, data protection (cifratura, DLP, cancellazione sicura), change e release management, subfornitori (inventario e flow-down) e sicurezza del prodotto/servizio (secure SDLC, SBOM, advisories).

Il campionamento è mirato: ticket di change, incident e accessi, almeno un sistema critico per dominio, ultime versioni rilasciate e una prova di restore.

Gli esiti sono classificati in non conformità maggiori, minori e osservazioni, con un report che riporta sintesi esecutiva, rating (conforme, parzialmente conforme, non conforme), evidenze, rischi residui e piano di remediation con owner, priorità e scadenze.

Il follow-up prevede verifiche a 30/60/90 giorni e, se necessario, re-audit dei punti maggiori, con escalation a Legal e Procurement oltre la soglia di rischio accettabile.

La frequenza è annuale per i fornitori ad alta criticità e biennale per quelli medi; sono previste verifiche straordinarie dopo incidenti o cambi significativi.

La responsabilità è del Vendor Risk/Cybersecurity per pianificazione ed esecuzione, del Supplier Business Owner per decisioni ed escalation, con il coinvolgimento di Legal e Procurement sugli aspetti contrattuali e del Service Owner sulle parti tecniche.

I principali indicatori di efficacia sono copertura dei fornitori critici auditati, chiusura delle major entro SLA, tempi medi di remediation, esito dei test BC/DR e copertura del logging sui servizi critici.

2.5 Gestione incidenti nella supply chain

La finalità è garantire una risposta coordinata, tempestiva e trasparente quando un incidente coinvolge un fornitore, minimizzando l'impatto su processi e servizi critici e assicurando le notifiche dovute.

L'approccio è "one-team": azienda e fornitore operano su playbook condivisi, con canali h24 e tempi di notifica contrattualmente definiti (più stringenti per gli eventi severi). Al rilevamento, l'Incident

Commander aziendale convoca una war-room con il referente del fornitore, Legal, DPO quando servono, Service Owner e comunicazione/PR se previsto.

L'identificazione della severità considera impatto sulle FCI, dati coinvolti, estensione e durata.

Le azioni seguono una sequenza chiara. Nella fase di contenimento si possono sospendere credenziali e integrazioni del fornitore, attivare "circuit breaker" sui flussi, applicare patch o rollback, rafforzare segmentazioni e regole temporanee di difesa.

L'eradicazione e il ripristino includono bonifica degli asset, validazione dell'integrità, restore da backup immutabili e riapertura controllata con test funzionali.

Le comunicazioni interne ed esterne avvengono secondo una matrice predefinita e tengono conto di NIS2/D.Lgs. 138/2024 e, se pertinente, GDPR.

Al termine si svolge una Post-Incident Review per definire cause radice, lezioni apprese e miglioramenti a controlli, playbook, clausole contrattuali e punteggio del fornitore; quando opportuno si pianifica un re-audit mirato.

La readiness è sostenuta da runbook specifici per tipologia di fornitura (SaaS, MSP/MSSP, software distribuito, on-prem gestito), da una forensic readiness adeguata (sincronizzazione oraria, retention log, catena di custodia), da canali di threat intelligence e advisories del vendor, SBOM per la valutazione rapida delle dipendenze e integrazione con gli strumenti aziendali di ticketing e SIEM/SOAR.

Sul fronte contrattuale sono essenziali i tempi e i contenuti minimi di notifica, la cooperazione durante l'indagine (compresa la messa a disposizione di log ed evidenze), l'obbligo di estendere le stesse regole ai subfornitori, l'esecuzione di esercitazioni congiunte e, quando necessario, penali o crediti di servizio.

È previsto un programma di esercitazioni: tabletop semestrali con i fornitori critici su scenari tipici di supply-chain, test annuali di continuità end-to-end e drill tecnici sulla revoca delle credenziali, rotazione chiavi, failover e ripristino.

Il successo operativo si misura con MTTD/MTTR, tempi di notifica, aderenza agli SLO per severità, completamento delle azioni post-incident e qualità delle evidenze forensi.

La responsabilità resta all'Incident Commander (accountability), con esecuzione congiunta tra il Cyber Incident Response Team e il referente del fornitore, e consultazione di Legal, DPO, Procurement e Service Owner; il top management e gli stakeholder vengono informati secondo quanto previsto dal piano di comunicazione.

3. INCIDENT MANAGEMENT

3.1 Modello di gestione degli incidenti

In questo documento è analizzato un processo completo per la gestione degli incidenti (incident handling): dalla rilevazione, alla comunicazione, al contenimento, fino alla risoluzione e alle lezioni apprese. Il modello vuole essere scalabile e applicabile a diversi scenari, prevedendo anche casi specifici e playbook operativi. La principale focalizzazione è comunque su quanto appropriato per un'azienda autonoma (quindi, non controllata da una capogruppo per quanto riguarda questi aspetti) che debba rispondere principalmente alla normativa italiana, alla quale faremo riferimento implicitamente quando non viene citata esplicitamente una norma. In particolare, faremo riferimento alla Direttiva NIS2 [Direttiva (EU) 2022/2555] (nel seguito, Direttiva NIS2), al Regolamento di esecuzione (EU) 2024/2690 (nel seguito, Regolamento 2690), e al D.Lgs. 138/2024 (el seguito, Decreto NIS), nonché alle pertinenti determinazioni di ACN, con particolare riferimento alla Determinazione 164179 del 2025 che definisce le "Modalità e specifiche di base" per l'adempimento degli obblighi di cui agli articoli 23, 24, e 25 del decreto NIS.

Nella Direttiva NIS2 la gestione degli incidenti è citata direttamente nell'elenco delle misure di sicurezza da adottare: fra le misure prescritte per i soggetti NIS2, sia essenziali che importanti, si prevede infatti che i soggetti si dotino di misure tecniche, operative ed organizzative per la gestione degli incidenti (Art. 21 Parr. 1 e 2). Non sono però specificate nel dettaglio tali misure, che devono essere proporzionate al grado di esposizione del soggetto ai rischi, alle dimensioni del soggetto e alla probabilità che si verifichino incidenti,

nonchè alla loro gravità, compreso il loro impatto sociale ed economico. Sono poi definiti all'art. 23 gli obblighi di segnalazione di incidenti significativi allo CSIRT Italia.

Qualche indicazione aggiuntiva su come predisporre un processo di gestione degli incidenti si trova nel Regolamento 2690 e nella relativa guida di ENISA "ENISA Technical Implemenation Guidance On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024". In Italia, però, il recepimento della Direttiva, ma soprattutto le determine di ACN, si sono un po' allontanate da questo approccio, preferendo basarsi sul Framework Nazionale per la Cybersecurity e la Data Protection (FNCDP), che a sua volta ricalca il Cyber Security Framework NIST. Ricaveremo perciò l'indirizzo per un processo di gestione degli incidenti, in primo luogo, dalla normativa italiana vigente e dalle specifiche di base finora adottate da ACN, appoggiandoci per completezza ad altri documenti e norme specifiche sull'argomento, quali le guide ENISA e le norme ISO/IEC 27035 e NIST SP 800-61r3.

Introduzione e Obiettivi

Un piano di risposta agli incidenti può aiutare un'organizzazione a reagire in modo più rapido, efficace ed economico a un incidente o a un evento di sicurezza ed a riprendersi da esso. Esso definisce chiaramente cosa deve essere fatto affinché il personale possa gestire la risposta agli incidenti in modo più efficace, efficiente e coerente e può aiutare il personale a ridurre al minimo la perdita o il furto di informazioni e le interruzioni del servizio.

- **Finalità:**
    - Fornire una risposta rapida, efficace e coordinata agli incidenti informatici, riducendo l'impatto e garantendo la continuità operativa.
- **Obiettivi principali**:
    - Ridurre tempi di identificazione e contenimento.
    - Ridurre l'impatto dell'incidente, sia dal punto di vista economico che rispetto ad altri parametri rilevanti per l'organizzazione; la NIS2 richiede esplicitamente di valutare anche gli impatti sociali ed economici dell'incidente, in una logica di doppia materialità
    - Ripristinare tempestivamente i servizi.
    - Comunicare efficacemente a livello interno ed esterno.
    - Migliorare la resilienza e la consapevolezza della sicurezza.

Ambito di Applicazione

- **Copertura:** Tutti i sistemi IT e OT, le reti, le applicazioni, i database e il personale coinvolto.
- **Tipologie di incidenti:** Violazioni dati, ransomware, DDoS, minacce interne, ecc.

Definizioni

- **Incidente informatico:** un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi [DL 4 settembre 2024 nr. 138 Art. 7].
- **IRT:** Incident Response Team, team di risposta agli incidenti informatici.
- **CSIRT:** Computer Security Incident Response Team, gruppo di persone che fornisce a un'organizzazione servizi e supporto relativi alla valutazione, alla gestione e alla prevenzione delle emergenze legate alla sicurezza informatica, nonché al coordinamento delle attività di risposta agli incidenti.
- **SOC:** Security Operations Center, è un'unità centralizzata che monitora e protegge l'infrastruttura IT di un'organizzazione dalle minacce informatiche, operando 24 ore su 24, 7 giorni su 7, per rilevare, analizzare e rispondere agli incidenti di sicurezza.
- **RTO:** Recovery Time Objective, cioè il periodo di tempo previsto e il livello di servizio entro il quale un processo aziendale deve essere ripristinato dopo un incidente, al fine di evitare conseguenze inaccettabili associate a un'interruzione della continuità operativa.
- **RPO:** Recovery Point Objective. È il periodo massimo previsto durante il quale potrebbero verificarsi perdite di dati da un servizio IT a causa di un incidente.

Fasi del Piano di Risposta

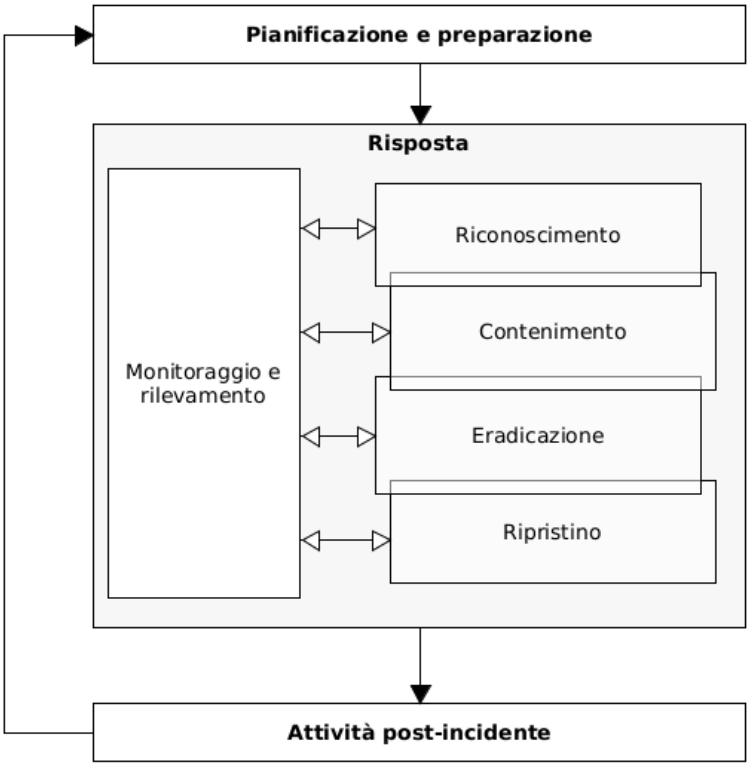


Figura 2: Fasi del Piano di Risposta

Lo schema con le fasi del piano di risposta agli incidenti informatici serve come orientamento, ma non deve essere considerato definitivo

ed intoccabile. Nella realtà, soprattutto nella realtà della gestione di un incidente in corso, le varie fasi spesso per necessità contingenti si sovrappongono, vengono eseguite in parallelo o non nella successione prevista. Il monitoraggio e rilevamento, per esempio, è un'attività che prosegue continuativamente; il ripristino può essere eseguito parzialmente in tempi diversi in settori distinti della attività, ecc. Nell'ambito di queste attività devono inoltre essere considerate le attività di escalation per allertare le diverse funzioni che possono dover svolgere attività correlate all'incidente, fra queste in particolare gli adempimenti di segnalazione alle diverse autorità competenti (ACN per gli incidenti significativi, Garante privacy per le violazioni di dati personali, ecc.).

Pianificazione e preparazione

Questa fase sarà esaminata più in dettaglio in altre parti del documento. Qui evidenziamo solo alcuni punti connessi con la vera e propria gestione dell'incidente.

Da notare che la responsabilità ultima dell'implementazione degli obblighi della Direttiva NIS2 ricade sempre, secondo il Decreto NIS, sugli "organi di amministrazione" (tipicamente, il Consiglio di Amministrazione). Ne consegue che il piano di risposta agli incidenti informatici deve essere approvato formalmente da queste funzioni, con allocazione di risorse e responsabilità chiare, e lo stesso dicasi per le attribuzioni di ruoli e responsabilità.

Definizione dei ruoli e delle responsabilità

Devono essere definiti i ruoli e le responsabilità di tutte le persone che intervengono nella gestione di un incidente informatico [vedi p.e. il Regolamento 2690, Allegato §1.2].

La normativa vigente non specifica nel dettaglio i ruoli da attribuire: il loro numero e gli incarichi ad essi assegnati variano in funzione della dimensione aziendale e dell'esposizione al rischio dell'azienda. Ciò significa che una analisi dei rischi, almeno a grandi linee, dovrebbe essere già stata effettuata prima. Delineiamo comunque di seguito alcune figure chiave per la sicurezza informatica.

Responsabile della sicurezza informatica

Se l'azienda non ne è già dotata, serve almeno una figura che coordini tutte le attività di sicurezza informatica e risponda alla direzione: un CISO, un Security Manager o titolo simile, che chiameremo per semplicità Responsabile della Sicurezza Informatica. È utile evidenziare che alcuni sistemi e reti possono essere gestiti da funzioni diverse dalla Direzione Sitstemi Informativi (ad esempio, le tecnologie OT di automazione nel facility management); questi sistemi e reti sono comunque nel perimetro di applicazione della Direttiva NIS, e il Responsabile della sicurezza informatica dovrà assicurare il presidio dei temi di sicurezza anche in questi ambiti.

Cyber Threat Specialist

Una o più persone dedicate ad esaminare i sistemi di difesa e fornire relazioni facendo riferimento ai risultati dei test di penetrazione, alle valutazioni di vulnerabilità e alle misure di conformità implementate.

Responsabile della risposta agli incidenti

La persona che si occuperà di dirigere e coordinare le operazioni di risposta in caso di rilevamento di un incidente. In organizzazioni non grandi può coincidere con il leader del team di risposta agli incidenti

o con lo stesso Responsabile della Sicurezza Informatica. Deve avere il potere di escalation di un incidente.

Team di risposta agli incidenti (IRT)

A seconda delle dimensioni e della struttura aziendale possono esistere uno o più Team di Risposta agli Incidenti (**IRT**, Incident Response Team).

La dimensione e la composizione di un IRT è variabile, secondo le necessità contingenti. Oltre ad un certo numero di membri fissi, che coprano le competenze generalmente richieste, vengono occasionalmente aggregati al team gli esperti adatti al tipo di minaccia che l'IRT è chiamato ad affrontare. È opportuno che ruoli e responsabilità all'interno del team siano ben definiti (es: team leader, analisti, specialisti ICT, responsabile della comunicazione, supporto legale, ecc.), per esempio come nella tabella seguente:

Ruolo	Compiti e responsabilità
IRT leader	Gestisce il IRT e coordina lo sviluppo e l'esecuzione del piano di risposta, assicurando che i vertici dell'organizzazione siano sempre informati sulla situazione. È richiesta un'elevata competenza tecnica, ma l'attenzione è focalizzata sul coordinamento della risposta complessiva, non solo sugli aspetti tecnici della gestione degli incidenti.
Capo tecnico	Dirige gli aspetti tecnici della risposta e coordina i fornitori e gli esperti tecnici di terze parti. È responsabile che il piano di

Ruolo	Compiti e responsabilità
	risposta soddisfi i problemi posti dall'incidente.
Tecnici interni	Implementano o controllano direttamente l'implementazione delle misure necessarie al trattamento dell'incidente.
Tecnici esterni	Se necessario partecipano all'azione tecnici esterni, per settori non coperti dalle competenze interne. Per esempio, potrebbero essere esperti di analisi forense.
DPO	Nel caso in cui siano coinvolti dati perdonali, deve essere interessato il Data Protection Officer (DPO).
Rappresentante reparto finanziario	Il rappresentante finanziario del team ha il compito di fornire consulenza sulla disponibilità dei fondi per l'intervento, sulle implicazioni finanziarie dell'intervento e, idealmente, sulla copertura assicurativa e sugli obblighi dell'organizzazione.
Rappresentante reparto risorse umane	È necessario coinvolgere un rappresentante delle Risorse umane qualora l'incidente possa avere ripercussioni sulle informazioni personali identificative del personale o qualora

Ruolo	Compiti e responsabilità
	sussistano preoccupazioni relative al benessere dei dipendenti.
Addetto comunicazioni	Ha il compito di effettuare le obbligatorie comunicazioni dell'incidente alle autorità competenti. Ha il compito di garantire che l'organizzazione sia in grado di spiegare chiaramente il problema, cosa è successo e cosa si sta facendo al riguardo, monitorando al contempo la risposta dell'opinione pubblica. È inoltre responsabile della gestione delle richieste di informazioni da parte della stampa e della preparazione dei portavoce e delle dichiarazioni da rilasciare. Per quanto riguarda i requisiti posti dal Decreto NIS, un ruolo specifico è attribuito al **punto di contatto**, il cui nominativo deve essere preventivamente comunicato ad ACN, e che l'ACN può contattare per eventuali richieste
Rappresentante reparto legale	È responsabile di fornire consulenza al IRT in merito alle responsabilità legali e normative dell'organizzazione e di sollevare eventuali questioni legali che potrebbero sorgere durante la pianificazione della risposta.

Tabella 7: IRT Ruoli e Responsabilità

In organizzazioni sufficientemente grandi e strutturate, o che operino in settori molto particolari, può esistere anche un Crisis Management Team, che entra in azione quando le conseguenze dell'incidente superano i limiti di capacità gestionale ordinaria e di conseguenza l'incidente viene scalato a "crisi".

Risorse

Elencare le risorse a disposizione del IRT ed in generale a disposizione di chi è coinvolto nel contenimento ed eradicazione di un incidente informatico.

Informazioni di contatto

Tabella con le informazioni di contatto rilevanti per la gestione di un incidente:

Ruolo	Contatti (nome, telefono, e-mail, ecc.)	Note (funzioni, reperibilità, ecc.)
IRT leader		
Capo tecnici		
DPO		
Autorità di Pubblica Sicurezza locali		

Ruolo	Contatti (nome, telefono, e-mail, ecc.)	Note (funzioni, reperibilità, ecc.)
Garante Privacy		
CSIRT nazionale		
...		

Tabella 8: Informazioni di contatto per la gestione degli incidenti

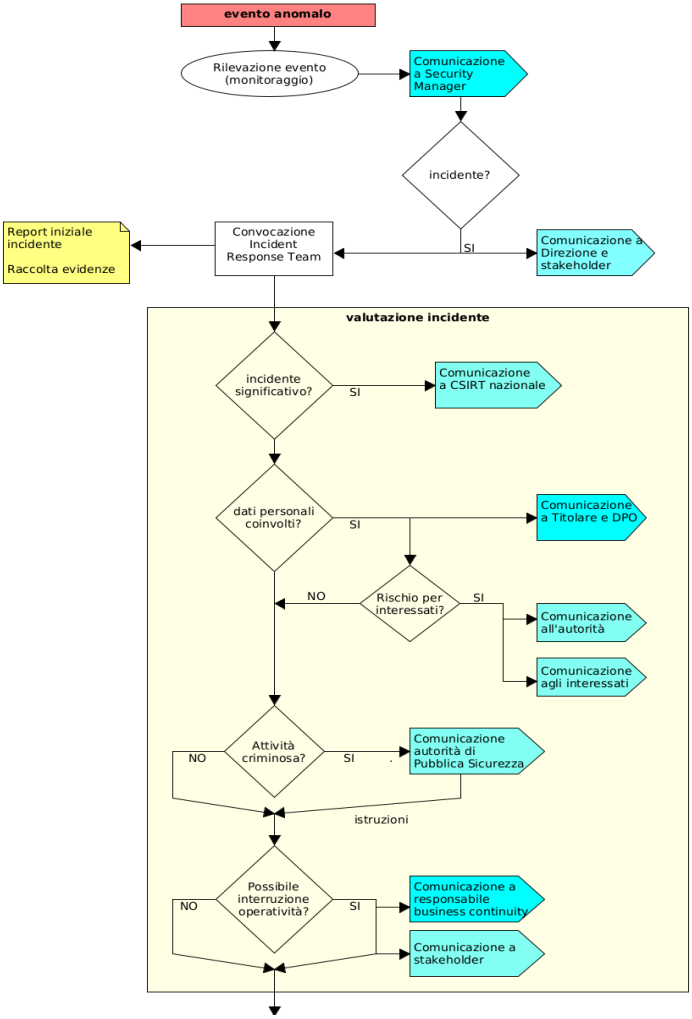
La rapidità nell'attivazione dei diversi ruoli e delle diverse attività gioca un ruolo sempre più critico, principalmente per due motivi:

- la capacità di contenere un incidente, e quindi di ridurne l'impatto, è sempre più legata alla rapidità di rilevazione ed all'attiviazione tempestiva di azioni di contenimento
- gli obblighi di segnalazione impongono tempi sempre più stringenti (24 ore e comunque senza indebito ritardo per un primo preallarme allo CSIRT Italia secondo il Decreto NIS, ma nell'ambito del Perimetro di Sicurezza Nazionale Cibernetica si scende fino a 1 ora)

Potrà inoltre essere necessario integrare con le informazioni di contatto di fornitori critici che debbano essere a vario titolo coinvolti nella gestione di un incidente: fornitori di servizi SOC, di manutenzione applicativa, si servizi specialistici come quelli di digital forensics, ecc.

Risposta

Schema semplificato di risposta ad un incidente informatico:



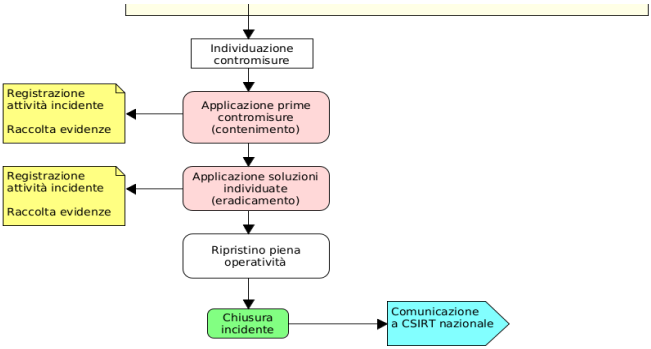


Figura 3: Schema di risposta ad un incidente informatico

Come per lo schema delle fasi del Piano di Risposta agli Incidenti, anche questo schema va considerato come indicativo: non necessariamente lo svolgimento delle attività riesce ad essere lineare come illustrato. Alcune attività, come per esempio la valutazione della gravità di un incidente, possono ricorrere più volte nel corso della gestione di un incidente, man mano che la natura e la gravità della situazione si fanno più chiare.

Monitoraggio e rilevamento

Monitoraggio

Analisi continua dei dati da rilevamento: elenco dei sistemi in uso per il monitoraggio dei sistemi critici.

Oggetto monitorato	Sistema di monitoraggio	Addetti responsabili

Le azioni di monitoraggio e rilevamento proseguono anche per tutta la durata della gestione dell'incidente.

Riconoscimento

Valutazione delle anomalie riscontrate

Ogni evento anomalo rilevato dal monitoraggio o segnalato in altro modo (da collaboratori, clienti, personale esterno, SOC, ecc.) va analizzata più rapidamente possibile.

Lo scopo dell'analisi è stabilire se si tratta o meno di un evento classificabile come incidente informatico, nel qual caso il responsabile deve dichiarare l'incidente e mettere in moto la procedura di risposta.

Chi effettua questa prima analisi in genere è il responsabile della sicurezza informatica, che è pure responsabile della decisione da prendere a seguito dell'analisi (avvio procedura risposta incidente o meno).

Classificazione degli incidenti rilevati in base al possibile impatto

Un incidente informatico rilevato va classificato il prima possibile in base alla sua pericolosità ed impatto, rilevati o previsti. L'operazione va fatta dal Team di Risposta agli Incidenti (IRT) unitamente al Responsabile della Sicurezza Informatica, sentita eventualmente la Direzione. Tale classificazione iniziale potrà essere rivista più volte nel corso dello sviluppo delle operazioni di contenimento ed eradicazione, man mano che il tipo e la portata dell'incidente si faranno più chiari.

Le modalità e la scala di classificazione di un incidente sono illustrati nel documento di politica di sicurezza informatica dell'organizzazione, unitamente alle considerazioni sul risk appetite dell'organizzazione stessa.

La prima operazione da fare è riconoscere se l'incidente è:

1. classificabile come significativo ai sensi del Decreto NIS, del Regolamento 2690 e/o della Determinazione ACN 164179;
2. se sono coinvolti dati personali;
3. è dovuto ad attività criminale;
4. può portare ad interruzioni della operatività.

Nei primi due casi sorgono obblighi di comunicazione, rispettivamente al CSIRT Italia (entro 24 ore dalla scoperta, Decreto NIS Art. 25) ed al Garante per la Privacy (entro 72 ore, Regolamento (EU) 2016/679 Art. 33).

In caso di attività criminale va allertata l'autorità di Pubblica Sicurezza competente.

Una definizione di incidente significativo è contenuta negli allegati 3 e 4 della Determina ACN 2025/164179. La riportiamo qui di seguito per comodità:

Codice	Descrizione
IS-1	Il soggetto NIS ha evidenza della perdita di riservatezza, verso l'esterno, di dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.
IS-2	Il soggetto NIS ha evidenza della perdita di integrità, con impatto verso l'esterno, di dati di sua proprietà o sui quali esercita il controllo, anche parziale.
IS-3	Il soggetto NIS ha evidenza della violazione dei livelli di servizio attesi dei suoi servizi e/o delle sue attività, sulla base dei livelli di servizio atteso (SL) definiti ai sensi della misura DE.CM-01.
IS-4	Il soggetto NIS ha evidenza, anche sulla base dei parametri quali-quantitativi definiti ai sensi della misura DE.CM-01, dell'accesso, non autorizzato o con abuso dei privilegi concessi, a dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.

Tabella 9: Definizione di incidente significativo - allegati 3 e 4 della Determina ACN 2025/164179

Se si prospettano interruzioni di attività, va attivato il piano di business continuity (vedi capitolo Business Continuity e Disaster Recovery).

È utile sottolineare che queste valutazioni richiederanno un'attività preparatoria. Ad esempio, la valutazione di impatto ai sensi del

Regolamento 2690, dove applicabile, richiede di valutare se l'impatto dell'incidente possa superare i 500.000 euro o il 5% del fatturato totale annuo. Nella maggior parte dei casi queste valutazioni non potranno essere fatte sul momento dall'IRT. Sarà quindi necessario identificare preventivamente quali sistemi e quali tipologie di incidente potranno superare quelle soglie, in modo da avere dei parametri oggettivi da utilizzare in fase di classificazione dell'incidente.

Azioni ad incidente rilevato

- **Attivazione IRT:** Attivazione del team di risposta agli incidenti. In caso di incidente di portata minore, può essere il caso di delegarne la soluzione ad un singolo o ad un piccolo gruppo di tecnici, senza attivazione del IRT.
- **Reporting:** Report iniziale dell'incidente, a scopo comunicazione.
- **Comunicazione interna:** Informazione a management, personale e stakeholder. Per maggiori dettagli sulle comunicazioni, vedi il capitolo Comunicazione.
- **Comunicazione esterna:** Segnalazione alle autorità competenti, clienti, fornitori secondo obblighi NIS2 e GDPR. Per maggiori dettagli sulle comunicazioni, vedi il capitolo Comunicazione.
- **Contatti:** Mantenimento di contatti con il CSIRT nazionale.

Contenimento

L’obbiettivo dell'attività di contenimento è interrompere la propagazione dell’incidente, stabilizzare i sistemi critici ed evitare escalation del rischio. Oltre a ciò, spece se si sospetta dolo

nell'incidente, preservare le evidenze per analisi forense e revisione post incidente. Anche le attività di contenimeto, eradicazione e ripistino richiedono delle attività di preparazione volte ad assicurare che in fase di gestione dell'incidente, attività svolta tipicamente in emergenza, con una forte pressione sul ripristino dei sistemi e spesso senza la disponibilità di tutto il personale, non si debbano improvvisare attività e prendere decisioni che potrebbero essere poco efficaci o addirittura dannose. Saranno quindi tipicamente predisposti dei playbook almeno per le tipologie di incidente più comuni o impattanti, nonché delle istrizioni operative per il corretto ripristino dei sistemi, anche in coordinamento con le attività di gestione della continuità operativa.

Prime contromisure

Sulla base delle prime informazioni raccolte e del report iniziale di incidente, il IRT stabilisce e provvede ad applicare le prime contromisure di contenimento dell'incidente. Idealmente dovrebbe essere prima stabilito e poi applicato un piano di intervento, ma non sempre l'urgenza della situazione lo permette.

Le misure da adottare naturalmente dipendono fortemente dal tipo di incidente occorso e dalla attività della organizzazione coinvolta. Tipicamente si potrà trattare di isolare il sistema compromesso, disconnettendo macchine e bloccando porte IP, bloccare account e sessioni sospette, revocare token o chiavi API, forzare cambio password, ecc.

Action log

Quanto fatto nella fase di contenimento va registrato con la maggiore accuratezza possibile. Documentare orari, decisioni prese, persone coinvolte. Nel caso l'incidente sia dovuto ad azione dolosa, si dovrà porre cura anche nel salvare tutte quelle informazioni che potrebbero servire per ricostruire gli accadimenti a posteriori. È utile sottolineare che il tracciamento delle attività svolte all'interno dell'action log porà servire anche a dimostrare, in caso di successive attività di verifica da parte delle autorità di controllo, che quanto effettuato sia stato effettivamente conforme ai requisiti normativi, in particolare in termini di tempestività delle azioni.

Eradicazione

Piano di eradicazione

Il IRT predispone un piano per l'eradicazione delle cause dell'incidente. Tipicamente queste ne saranno le fasi:

- Risanamento di tutti gli ambienti IT infetti (ad esempio, cloud, OT, ibridi, host e sistemi di rete).
- Reimaging dei sistemi interessati, ricostruzione dei sistemi da zero.
- Ricostruzione dell'hardware (necessaria quando l'incidente coinvolge rootkit).
- Sostituzione dei file compromessi con versioni pulite.
- Installazione di patch.
- Reimpostazione delle password sugli account compromessi.
- Monitoraggio di eventuali segni di risposta degli avversari alle attività di contenimento

- Attendere il tempo necessario per garantire che tutti i sistemi siano privi di ogni possibile meccanismo di persistenza delle minacce (backdoor, ecc.), poiché spesso gli avversari utilizzano più di un meccanismo.

Esecuzione piano

Il piano di eradicazione viene applicato.

Ripristino

L'obiettivo della fase di ripristino è di tornare alla normale operatività. Le principali operazioni di questa fase consistono nel confermare che la eradicazione abbia avuto successo, ricostruire i sistemi, ricollegare le reti, ripristinare le configurazioni e ricreare o correggere le informazioni. La disponibilità di backup completi, affidabili e recenti qui è fondamentale.

Test di funzionalità e rientro in produzione: per verificare che le operazioni normali siano riprese, prendere in considerazione l'esecuzione di un test indipendente o una revisione delle attività interessate alla compromissione/risposta.

Attività post-incidente

- **Reportistica**: relazione finale particolareggiata sull'incidente.
- **Analisi:** gli incidenti e tutta le relative attività di contenimento, comunicazione, eradicazione e ripristino vanno analizzati, per scoprire eventuali punti deboli sia nella struttura di sicurezza che nel processo di risposta che si è attuato.

- **Revisioni:** Il piano di risposta agli incidenti informatici va revisionato almeno annualmente, o comunque in presenza di significativi cambiamenti dell'organizzazione o del contesto in cui essa opera. Nella revisione vanno tenuti presenti i risultati delle analisi degli incidenti informatici occorsi.
- **Test:** Test annuali del piano, aggiornamento procedure in base alle lezioni apprese e alle nuove minacce.
- **Metriche:** Tracciamento degli gli indicatori chiave di prestazione (KPI) quali tempo di rilevamento, tempo di contenimento e tempo di ripristino.

3.2 Allineamento con ENISA e CSIRT

1. Finalità e Obiettivi

Questa sezione approfondisce il confronto tra le tassonomie di cybersicurezza sviluppate dall'Agenzia dell'Unione Europea per la Cybersicurezza (ENISA) e quelle adottate dall'Agenzia per la Cybersicurezza Nazionale (ACN) italiana. L'analisi condotta evidenzia che le due tassonomie si presentano come strumenti complementari, ognuno con specifici scopi e ambiti di applicazione.

La tassonomia di ENISA si posiziona come uno strumento fondamentale per la cooperazione volontaria a livello europeo. Il suo obiettivo primario è fornire un linguaggio comune e condiviso tra gli Stati membri, facilitando la comunicazione e la comprensione reciproca in materia di incidenti e minacce cibernetiche. Questo approccio basato sul consenso e sulla collaborazione è cruciale per costruire una resilienza cibernetica collettiva all'interno dell'Unione Europea, permettendo una risposta più coordinata ed efficace alle sfide transnazionali della cybersicurezza. L'ENISA mira a

standardizzare la terminologia e le classificazioni per migliorare lo scambio di informazioni e le migliori pratiche tra le diverse entità nazionali, senza imporre obblighi normativi stringenti.

D'altra parte, la tassonomia TC-ACN (Tassonomia degli Incidenti di Cybersicurezza dell'Agenzia per la Cybersicurezza Nazionale) è concepita come uno strumento normativo e prescrittivo specificamente per il contesto italiano. La sua funzione principale è quella di supportare la gestione degli incidenti di cybersicurezza e di garantire la conformità nazionale alle normative vigenti. La TC-ACN fornisce criteri dettagliati e obbligatori per la classificazione e la segnalazione degli incidenti, elementi essenziali per le organizzazioni pubbliche e private che operano in settori critici o che sono soggette a obblighi di notifica. Questo strumento è quindi orientato a fini regolatori, consentendo all'ACN di monitorare lo stato della sicurezza cibernetica a livello nazionale, di identificare pattern di attacco, e di coordinare le risposte a incidenti gravi, contribuendo attivamente alla protezione delle infrastrutture critiche e dei servizi essenziali in Italia.

In sintesi, mentre ENISA promuove un quadro di riferimento comune per la collaborazione transfrontaliera basata sulla volontarietà e sulla condivisione delle informazioni, la TC-ACN opera come un meccanismo normativo per l'applicazione delle leggi e la gestione operativa degli incidenti a livello nazionale. Entrambe le tassonomie sono indispensabili per un approccio olistico alla cybersicurezza, garantendo che le informazioni e le risposte siano coerenti sia a livello europeo che nazionale, pur rispettando le specificità normative e operative di ciascun contesto.

Aspetto	Tassonomia ENISA (eCSIRT.net)	Tassonomia ACN
Obiettivo principale	Facilitare lo scambio di informazioni tra CSIRT europei e migliorare la cooperazione con Law Enforcement.	Fornire un linguaggio comune per classificare e notificare eventi cyber in ambito nazionale.
Contesto di applicazione	Comunità CSIRT europea, interoperabilità e standardizzazione tra stati membri.	Perimetro di sicurezza nazionale cibernetica, PA e infrastrutture critiche.

Tabella 10: Quadro Sinottico Comparativo delle Tassonomie ENISA e ACN su obiettivi e contesto

2. Due strumenti a confronto

2.1 Il Mandato Sovranazionale – Finalità e Obiettivi delle Tassonomie ENISA

Le tassonomie sviluppate da ENISA sono strumenti fondamentali concepiti per creare coesione e interoperabilità all'interno del complesso e diversificato ecosistema della cybersicurezza europea. La loro finalità non è impositiva, ma abilitante: fornire un linguaggio comune, una "lingua franca", per facilitare la cooperazione volontaria e costruire una comprensione strategica condivisa del rischio tra Stati Membri, Computer Security Incident Response Team (CSIRT) e Law Enforcement Agencies (LEA).

Le principali tassonomie o schemi di classificazione sviluppati o a cui ENISA fa riferimento includono:

- **Reference Incident Classification Taxonomy (Tassonomia di Classificazione degli Incidenti di Riferimento):** Questa è una delle tassonomie più significative sviluppate da ENISA, spesso in collaborazione con CSIRT (Computer Security Incident Response Teams) e altre agenzie europee. L'obiettivo è fornire una classificazione comune per gli incidenti di cybersicurezza al fine di supportare i CSIRT europei nella gestione e nella comunicazione degli incidenti. Si propone di standardizzare il modo in cui gli incidenti vengono descritti e classificati.
- **ENISA Threat Taxonomy (Tassonomia delle Minacce di ENISA):** Utilizzata per strutturare le informazioni sulle minacce informatiche. Questa tassonomia aiuta a classificare e organizzare le diverse tipologie di minacce, agenti di minaccia e vettori di attacco. Viene spesso impiegata nella produzione di report come l'ENISA Threat Landscape (ETL), che fornisce una panoramica indipendente sulle minacce osservate.
- **Tassonomie relative a settori specifici o temi:** ENISA sviluppa anche tassonomie o guide di classificazione per aree di particolare interesse. Ad esempio, sono state create linee guida e schemi di classificazione per la cybersecurity nei veicoli connessi e autonomi, per la sicurezza dell'IoT (Internet of Things) e per la gestione della supply chain.
- **Framework per la valutazione delle capacità nazionali (National Capabilities Assessment Framework - NCAF):** Sebbene non sia una tassonomia nel senso stretto della

classificazione di eventi o minacce, il NCAF è un quadro che aiuta gli Stati membri a valutare il proprio livello di maturità in materia di cybersicurezza, strutturando gli obiettivi strategici in aree tematiche.

In particolare la Tassonomia delle Minacce di ENISA è definita come uno "strumento per strutturare le informazioni sulle minacce". Il suo obiettivo primario è quello di stabilire un punto di riferimento e una classificazione coerente delle tipologie di minacce a vari livelli di dettaglio, fornendo un quadro condiviso per la loro comprensione e categorizzazione a livello europeo.

La sua finalità strategica va oltre la semplice classificazione. È concepita come una "living structure", una struttura vivente che si evolve per mantenere una visione coerente e aggiornata delle minacce, consolidando le informazioni raccolte da una moltitudine di fonti. Nata come strumento interno di ENISA tra il 2012 e il 2015 per l'organizzazione delle informazioni, è stata successivamente resa pubblica per estenderne i benefici all'intera comunità della sicurezza. A livello pratico, la tassonomia permette di mappare le minacce direttamente agli asset informatici, esprimendo così la loro esposizione al rischio e collegando le vulnerabilità specifiche alle minacce che potrebbero sfruttarle. Questo processo è cruciale per le attività di gestione del rischio a livello strategico. La sua architettura gerarchica, suddivisa in "High level threats" (minacce di alto livello), "Threats" (minacce) e "Threats details" (dettagli delle minacce), è stata progettata per essere flessibile, consentendo di aggregare o dettagliare le informazioni a seconda del contesto di utilizzo.

Il mandato dell'agenzia è supportare gli Stati Membri e migliorare la resilienza delle infrastrutture europee in un contesto di minacce in continua evoluzione. Pertanto, la sua natura dinamica, alimentata dal

contributo della comunità e da un'analisi continua, è una finalità intrinseca: fornire uno strumento che rimanga nel tempo rilevante. Questa caratteristica la distingue da un quadro normativo come quello dell'ACN, che per sua natura richiede stabilità e processi formali di modifica per garantire la certezza del diritto.

L'obiettivo primario della Tassonomia di Riferimento per la Classificazione degli Incidenti è sviluppare un framework comune per semplificare e standardizzare la comunicazione e la cooperazione operativa tra i CSIRT e le LEA a livello europeo.

Questo strumento nasce da iniziative di collaborazione, come i workshop congiunti ENISA/EC3, e si fonda su tassonomie preesistenti e consolidate come eCSIRT.net. Questo approccio dal basso verso l'alto (bottom-up) ne sottolinea la natura collaborativa piuttosto che impositiva. La struttura è organizzata in categorie di alto livello volutamente ampie, come "Abusive Content" (Contenuto abusivo), "Malicious Code" (Codice malevolo), "Information Gathering" (Raccolta di informazioni) e "Availability" (Disponibilità), ciascuna con sottocategorie più specifiche. Questa architettura generica è progettata per essere facilmente mappabile con le classificazioni più dettagliate in uso a livello nazionale.

2.2 L'Imperativo Nazionale – Finalità e Obiettivi della Tassonomia ACN

La tassonomia sviluppata dall'Agenzia per la Cybersicurezza Nazionale (ACN) si posiziona su un piano radicalmente diverso da quello di ENISA. Non è una raccomandazione, ma un diretto strumento di politica pubblica e di legge. La TC-ACN è uno standard prescrittivo, granulare e giuridicamente vincolante, progettato per

rendere operative specifiche normative nazionali ed europee, abilitando la vigilanza regolamentare, l'applicazione della legge e l'analisi automatizzata dei dati a livello nazionale.

La TC-ACN è strutturata in quattro macrocategorie, che a loro volta si suddividono in 22 predicati e 144 valori, garantendo una caratterizzazione granulare degli eventi. Le macrocategorie sono:

- **BC – Baseline Characterization:** Descrive il tipo e la portata del danno. Include la causa radice, l'impatto e la gravità.
    - Esempi di valori: Compromissione account, Compromissione applicazione, Disponibilità, Esfiltrazione dati, Esposizione dati, Manipolazione dati, Nessun impatto, Compromissione sistema, Errore umano, Azioni malevole, Fenomeni naturali, Guasto del sistema, Guasto di terze parti.
- **TT – Threat Type:** Riguarda le modalità e le tecniche dell'attacco.
    - Esempi di valori: Ransomware, Phishing, Data exfiltration.
- **TA – Threat Actor:** Identifica l'identità e le motivazioni dell'attaccante.
- **AC – Additional Context:** Fornisce ulteriori informazioni contestuali, come la classificazione dei sistemi colpiti, correlazioni con incidenti passati, strumenti di difesa implementati e possibili scenari di escalation.

La base giuridica della TC-ACN è solida e inequivocabile. La Determina ACN del 3 gennaio 2023, pubblicata nella Gazzetta

Ufficiale della Repubblica Italiana, dà diretta attuazione all'articolo 1, comma 3-bis, del Decreto-Legge n. 105/2019, che ha istituito il Perimetro di Sicurezza Nazionale Cibernetica (PSNC). Questo atto conferisce alla tassonomia forza di legge, trasformandola in uno strumento normativo a tutti gli effetti.

Il suo obiettivo primario è la compliance. La tassonomia definisce in modo prescrittivo quali incidenti devono essere *obbligatoriamente* notificati al CSIRT Italia, l'organo operativo dell'ACN. Questo segna un passaggio fondamentale dal paradigma della condivisione volontaria, promosso da ENISA, a quello della notifica obbligatoria imposta dalla legge. Inoltre, la TC-ACN è stata esplicitamente progettata per allinearsi al contesto normativo nazionale e, allo stesso tempo, per armonizzarsi con le tassonomie internazionali e le nuove, più stringenti, disposizioni della Direttiva (UE) 2022/2555 (NIS2). L'obiettivo è creare un unico standard nazionale che soddisfi molteplici requisiti legali, fornendo chiarezza e certezza agli operatori.

Aspetto	**Tassonomia ENISA (eCSIRT.net)**	**Tassonomia ACN**
Numero di attributi	Undici categorie principali con esempi descrittivi di incidenti.	144 valori divisi in 22 predicati e 4 macro categorie.
Macrocategorie	- Abusive Content - Malicious Code	- Baseline Characterization

Aspetto	Tassonomia ENISA (eCSIRT.net)	Tassonomia ACN
	-Information Gathering - Intrusions - Availability - Fraud etc.	- Threat Type - Threat Actor - Additional Context
Esempio di granularità	Categoria “Malicious Code” include esempi come worm, trojan, spyware, ecc. senza ulteriori sottoattributi strutturati.	Predicato “Impact” distingue tra: account compromise, data exfiltration, data manipulation ecc.

Tabella 11: Quadro Sinottico Comparativo delle Tassonomie ENISA e ACN su attributi e macrocategorie

La finalità primaria della TC-ACN è fornire un "linguaggio comune" e un "lessico comune" a livello *nazionale* per la notifica degli incidenti. In questo contesto, lo scopo non è solo facilitare la comprensione reciproca, ma garantire che le notifiche, avendo valore legale, siano coerenti, complete e prive di ambiguità. La Determina, attraverso le tabelle allegate che utilizzano codici identificativi come ICP-A e ICP-C, classifica in modo inequivocabile le tipologie di incidenti soggetti a notifica obbligatoria. Questo definisce con precisione il perimetro degli obblighi di legge per le organizzazioni soggette. Questo meccanismo serve a uno scopo di vigilanza. La raccolta standardizzata e obbligatoria di dati sugli incidenti permette all'ACN di costruire e mantenere un quadro della minaccia completo e aggiornato a livello nazionale. Questi dati sono essenziali per supportare gli obiettivi strategici delineati nella Strategia Nazionale di

Cybersicurezza 2022-2026, come la protezione degli asset strategici nazionali, l'anticipazione dell'evoluzione della minaccia e la gestione efficace delle crisi cibernetiche.

3. Convergenze e Divergenze Strategiche

Il confronto diretto tra i framework di ENISA e ACN rivela come le loro diverse finalità si traducono in architetture e approcci operativi fondamentalmente differenti. Sebbene entrambi mirino a migliorare la cybersicurezza, lo fanno con scopi, strumenti e logiche divergenti, che riflettono i loro rispettivi mandati: uno di armonizzazione sovranazionale, l'altro di regolamentazione nazionale.

La divergenza più netta risiede nella natura giuridica dei due framework. Le tassonomie di ENISA sono il prodotto di un centro di competenza che emana raccomandazioni e best practice. Non impongono un obbligo legale diretto, ma si propongono come standard di riferimento da adottare su base volontaria per migliorare l'interoperabilità. La loro forza risiede nella loro autorevolezza e utilità pratica. Al contrario, la TC-ACN è un atto amministrativo con forza di legge, emanato da un'autorità nazionale per dare attuazione a precisi obblighi normativi. La sua adozione non è una scelta, ma un dovere per i soggetti designati. Questo dualismo riflette una distinzione tra *soft power* (l'influenza e la persuasione di ENISA) e *hard power* (l'autorità regolamentare e sanzionatoria di ACN).

Caratteristica (Feature)	Tassonomia ENISA (Threat & Incident)	Tassonomia ACN (TC-ACN)
Finalità Primaria	Armonizzazione e interoperabilità a livello UE. Creare un linguaggio comune per la cooperazione volontaria.	Compliance normativa e vigilanza a livello nazionale. Standardizzare la notifica obbligatoria.
Base Giuridica	Raccomandazioni e best practice sviluppate da un'agenzia UE. Nessun obbligo legale diretto.	Determina ACN (atto con forza di legge) in attuazione di decreti legge nazionali (PSNC, NIS2).
Ambito di Applicazione	Pan-europeo, transfrontaliero.	Nazionale (Italia).
Destinatari Principali	CSIRT, Law Enforcement Agencies (LEA), Stati Membri, settore privato (su base volontaria).	Soggetti inclusi nel PSNC, operatori di servizi essenziali (OSE), fornitori di servizi digitali (FSD) e altre entità soggette a obblighi di notifica.
Livello di Obbligatorietà	Volontario. È un modello di riferimento ("reference").	Obbligatorio per le tipologie di incidenti definite dalla legge.
Struttura e Granularità	Gerarchica e concettuale. Categorie ampie per garantire	Granulare e codificata (144 attributi). Strutturata per

Caratteristica (Feature)	Tassonomia ENISA (Threat & Incident)	Tassonomia ACN (TC-ACN)
	flessibilità e mappabilità.	generare un "vettore di incidente" non ambiguo.
Obiettivo Operativo	Facilitare la comprensione e la cooperazione tra entità diverse. Funzionare come "pivot" o "traduttore".	Creare un report di incidente standardizzato, machine-readable, per l'analisi centralizzata da parte dell'autorità nazionale (ACN/CSIRT Italia).
Meccanismo di Aggiornamento	"Living document", evoluzione guidata dalla comunità e dall'analisi continua del threat landscape.	Processo formale guidato dall'autorità nazionale (ACN) in base all'evoluzione normativa e strategica.
Compatibilità con altre tassonomie	È usata come base per tassonomie derivate come CERT.PT e Common Taxonomy for LE/CSIRTs.	Integra elementi da ENISA, MISP, MITRE ATT&CK, NATO.
Machine-readability	Utilizzata anche in contesti MISP, ma	Pensata per essere compatibile con formati leggibili da macchina.

Caratteristica (Feature)	Tassonomia ENISA (Threat & Incident)	Tassonomia ACN (TC-ACN)
	meno strutturata in origine.	
Victim geography	assente	Rilevante per ambiti nazionali
Root cause (Errore umano, guasto, ecc.)	assente	Offerto più contesto causale

Tabella 12: Quadro Sinottico Comparativo delle Carattteristiche ENISA e ACN

4. Obiettivo Operativo: Facilitare la Cooperazione Transfrontaliera vs. Standardizzare la Notifica Nazionale

Gli obiettivi operativi sono una diretta conseguenza della natura giuridica. ENISA mira a risolvere un problema di comunicazione "molti-a-molti" (*many-to-many*) in un ambiente europeo eterogeneo, dove decine di CSIRT e LEA con sistemi diversi devono potersi scambiare informazioni. La sua tassonomia deve quindi essere flessibile, concettuale e facilmente mappabile per agire come un ponte. ACN, invece, affronta un problema di reporting "molti-a-uno" (*many-to-one*), dove migliaia di entità nazionali devono notificare incidenti a un'unica autorità centrale (il CSIRT Italia). In questo scenario, la priorità assoluta è la precisione, la coerenza e la non ambiguità del dato. La sua tassonomia deve essere rigida e prescrittiva per garantire che l'input ricevuto sia standardizzato e direttamente processabile.

Le filosofie di progettazione dei due sistemi sono agli antipodi, riflettendo i loro diversi obiettivi. Le categorie ampie e concettuali di

ENISA, come "Malicious Code" o "Intrusion Attempts", sono progettate per essere facilmente comprese dagli esseri umani e per includere un'ampia gamma di eventi specifici, facilitando la mappatura tra sistemi diversi. La tassonomia di ENISA è *human-centric*. Al contrario, i 144 attributi specifici e codificati di ACN, come BC:IM-AC per la compromissione di un account, sono progettati per la precisione e per eliminare l'interpretazione soggettiva in un contesto di notifica legale. Questa struttura è ottimizzata per essere processata da una macchina, non per essere discussa in una riunione. La tassonomia di ACN è *machine-centric*. Questa differenza fondamentale non è casuale, ma è la diretta conseguenza delle missioni divergenti: cooperazione facilitata dall'uomo da un lato, compliance verificata dalla macchina dall'altro.

Infine, le dinamiche di aggiornamento riflettono questa dualità. La definizione di "living document" per la tassonomia ENISA implica un'evoluzione agile, guidata dal basso, attraverso il feedback della comunità e l'analisi continua del panorama delle minacce. Questo le permette di adattarsi rapidamente a nuove tecniche di attacco o a nuove tipologie di minacce. La TC-ACN, essendo uno strumento con forza di legge, richiede un processo di modifica molto più formale e strutturato. Ogni aggiornamento significativo, per garantire la certezza del diritto, richiederebbe probabilmente una nuova determina dell'ACN, rendendo il processo meno agile ma garantendo stabilità e prevedibilità per i soggetti obbligati.

5. Implicazioni Strategiche e Raccomandazioni per gli Operatori Italiani

Per le organizzazioni italiane soggette agli obblighi di cybersicurezza, comprendere le finalità distinte dei framework ENISA e ACN non è un mero esercizio accademico, ma una necessità strategica. Tradurre questa comprensione in pratiche operative concrete è essenziale per garantire la compliance, ottimizzare i processi di sicurezza e rafforzare la propria postura difensiva. I due framework non si escludono a vicenda, ma operano a livelli diversi e dovrebbero essere integrati nei processi aziendali in modo complementare.

- **Raccomandazione 1:** Le organizzazioni dovrebbero utilizzare la **Tassonomia delle Minacce di ENISA** per le attività di alto livello. Questa è ideale per il *threat modeling*, la valutazione strategica del rischio, la stesura di report per il management e la comunicazione con partner e stakeholder a livello europeo. La sua natura concettuale la rende perfetta per descrivere il panorama dei rischi in modo comprensibile e strategico.

- **Raccomandazione 2:** La **TC-ACN** deve essere il framework di riferimento per la classificazione *operativa* degli incidenti all'interno dei processi di *incident management*. Essendo direttamente collegata agli obblighi di notifica, la sua adozione a livello operativo non è una scelta ma una necessità per garantire la compliance.

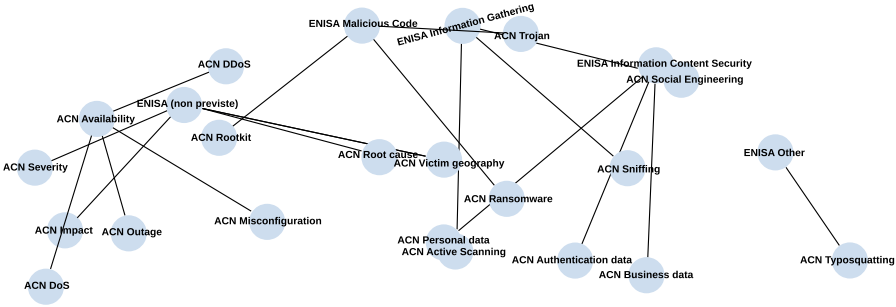
- **Raccomandazione 3:** I *playbook* di risposta agli incidenti devono essere aggiornati per includere passaggi specifici per la classificazione secondo la TC-ACN. Il team di risposta (CSIRT interno o provider esterno) deve ricevere una formazione adeguata per mappare correttamente e

tempestivamente gli eventi osservati ai 144 attributi definiti dall'ACN. Questo processo deve avvenire nelle prime fasi della gestione dell'incidente per rispettare le stringenti tempistiche di notifica.

- **Raccomandazione 4:** In fase di acquisto, implementazione o configurazione di strumenti tecnologici come SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation and Response) e piattaforme di ticketing (ITSM), è fondamentale assicurarsi che questi possano supportare la gestione del "vettore di incidente" ACN. Ciò significa poter aggiungere campi personalizzati, tag o integrazioni che permettano di registrare, tracciare e riportare gli incidenti utilizzando la sintassi codificata dell'ACN. Strumenti come il tool gratuito messo a disposizione da Utilia dimostrano la necessità di soluzioni ad hoc per facilitare questo processo.

Categoria	principale	Categoria ENISA/eCSIRT.net	Note
Availability	DoS	Availability	Corrispondenza diretta
Availability	DDoS	Availability	Corrispondenza diretta
Availability	Misconfiguration	Availability	Corrispondenza diretta
Availability	Outage	Availability	Corrispondenza diretta
Baseline Characterization	Impact	[non previsto]	ENISA non prevede classificazione dell'impatto
Baseline Characterization	Severity	[non previsto]	Assente categorizzazione per gravità
Baseline Characterization	Root cause	[non previsto]	ENISA non distingue cause (es. errore umano)
Baseline Characterization	Victim geography	[non previsto]	ENISA non considera la localizzazione geografica
Brand abuse	Brand abuse	Fraud / Other	ENISA non ha categoria dedicata
Brand abuse	Typosquatting	Other	Presente come esempio, non categoria
Command and Control	Command and Control	Bot	Parzialmente mappabile (botnet)
Command and Control	C2 beaconing	Bot	Implicito in botnet
Command and Control	C2 infrasructure	Bot	Implicito in botnet
Data Exposure / Integrity	Data exposure	Information Content Security	Corrispondenza diretta
Data Exposure / Integrity	Data manipulation	Information Content Security	Corrispondenza concettuale
Data Exposure / Integrity	Authentication data	Information Content Security	Corrispondenza diretta
Data Exposure / Integrity	Business data	Information Content Security	Corrispondenza diretta
Data Exposure / Integrity	Financial data	Information Content Security	Corrispondenza diretta
Data Exposure / Integrity	Personal data	Information Content Security	Corrispondenza diretta
Exploitation	Exploitation	Intrusion Attempts	Corrispondenza diretta
Exploitation	CVE-based exploit	Intrusion Attempts	Corrispondenza diretta
Exploitation	Custom exploit	Intrusion Attempts	Corrispondenza diretta
Fraud	Fraud	Fraud	Corrispondenza diretta
Fraud	Phishing	Fraud	Corrispondenza diretta
Fraud	Masquerade	Fraud	Corrispondenza diretta
Fraud	Impersonation	Fraud	Corrispondenza diretta
Fraud	Spam	Fraud	Corrispondenza diretta
Fraud	Resource misuse	Fraud	Corrispondenza diretta
Information Gathering	Active scanning	Information Gathering	Corrispondenza diretta
Information Gathering	Sniffing	Information Gathering	Corrispondenza diretta
Information Gathering	Social engineering	Information Gathering	Corrispondenza diretta
Information Gathering	Information gathering	Information Gathering	Categoria equivalente
Malicious Code	Malicious code	Malicious Code	Corrispondenza diretta
Malicious Code	Ransomware	Malicious Code	ACN più granulare
Malicious Code	Trojan	Malicious Code	Corrispondenza diretta
Malicious Code	Rootkit	Malicious Code	Corrispondenza diretta
Other	Other	(generica)	Categoria residuale in entrambe le tassonomie
Unauthorized Access / Intrusions	Intrusion	Intrusions	Corrispondenza diretta
Unauthorized Access / Intrusions	Account compromise	Intrusions	Corrispondenza diretta
Unauthorized Access / Intrusions	Application compromise	Intrusions	Corrispondenza diretta
Unauthorized Access / Intrusions	System compromise	Intrusions	Corrispondenza diretta
Unauthorized Access / Intrusions	Privilege escalation	Intrusions	Corrispondenza diretta

Figura 4: Mapping: ACN↔ ENISA/**eCSIRT.net**



Mapping dettagliato tra valori ACN e categorie ENISA

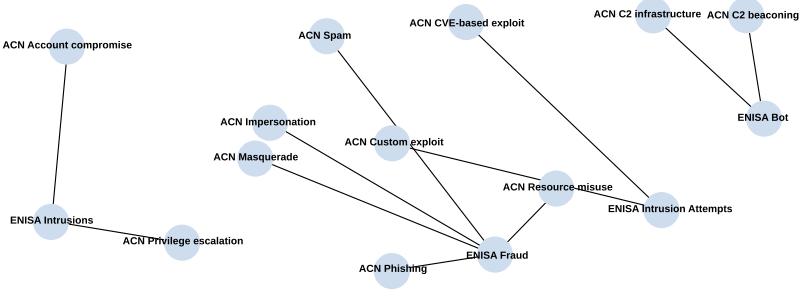


*Figura 5: Mapping: ACN↔ ENISA/**eCSIRT.net***

6. Verso una Compliance Efficace: Oltre la Semplice Notifica

Considerare la TC-ACN esclusivamente come un onere burocratico è un approccio riduttivo e un'opportunità mancata. La sua struttura granulare, sebbene imposta per legge, può essere trasformata in un potente strumento di analisi interna. L'obbligo di classificare ogni incidente significativo secondo lo schema ACN significa che

l'organizzazione sta, di fatto, già raccogliendo dati strutturati e di alta qualità su ogni evento di sicurezza.

Invece di considerare questi dati solo come un "output" da inviare all'autorità, l'organizzazione può trattarli come un "input" per i propri processi di analisi strategica. Analizzando i trend dei vettori di incidente nel tempo, un CISO o un responsabile della sicurezza può ottenere una visibilità senza precedenti sui pattern di attacco specifici che colpiscono l'azienda. Ad esempio, un aumento degli incidenti classificati con il predicato TT:AC-VU (Vulnerability Scanning) potrebbe indicare la necessità di rafforzare i programmi di vulnerability management e patch management. Un'alta frequenza di incidenti con il valore BC:RO-HU (Human Errors) potrebbe suggerire l'urgenza di investire in campagne di formazione e awareness per i dipendenti.

In questo modo, la TC-ACN può essere trasformata da un peso della compliance a un motore di *business intelligence* per la sicurezza. L'impegno richiesto per la conformità normativa viene così capitalizzato per guidare decisioni basate sui dati, ottimizzare l'allocazione delle risorse e migliorare proattivamente e continuamente la postura di sicurezza complessiva dell'organizzazione.

7. Conclusioni: Due Tassonomie, un Unico Ecosistema di Sicurezza

L'analisi comparativa dimostra in modo conclusivo che le tassonomie di ENISA e ACN non sono framework concorrenti, ma componenti funzionalmente distinti e complementari di una struttura di governance della cyber sicurezza multilivello. Questa architettura riflette la strategia europea, che combina l'armonizzazione a livello

continentale con l'implementazione e l'applicazione a livello nazionale.

ENISA fornisce il "linguaggio comune" strategico per l'Europa. Le sue tassonomie sono modelli di riferimento flessibili e concettuali, progettati per promuovere una comprensione condivisa del rischio e per abilitare la cooperazione volontaria in un ecosistema transfrontaliero complesso ed eterogeneo.

ACN, in qualità di autorità nazionale, fornisce il "dialetto" regolamentare, preciso e vincolante, per l'Italia. La TC-ACN è uno strumento normativo progettato per l'applicazione della legge, che traduce gli obblighi del PSNC e della Direttiva NIS2 in un protocollo di notifica standardizzato, granulare e ottimizzato per la vigilanza centralizzata e l'analisi automatizzata.

Per un operatore italiano, la comprensione delle finalità distinte di entrambi i framework è il presupposto indispensabile per navigare con successo nel complesso panorama della cybersicurezza. Padroneggiare la tassonomia di ENISA è cruciale per il posizionamento strategico e la cooperazione a livello europeo; implementare rigorosamente la tassonomia di ACN è un imperativo non negoziabile per la compliance operativa e la gestione efficace degli incidenti a livello nazionale. L'integrazione intelligente di entrambi i modelli consente di trasformare un doppio requisito in un doppio vantaggio: allineamento strategico europeo e rafforzamento della resilienza nazionale.

3.3 Business Continuity e Disaster Recovery

La norma di riferimento è la ISO 22301.

Un possibile indice degli argomenti potrebbe essere il seguente:

- definizione parametri principali in ambito BC (RPO, RTO, MTPD, MBCO) con esempi/casi esplicativi;
- definizione aspetti principali in ambito di continuità operativa (Business Impact Analysis, Business Continuity Plan);
- focus sul BCP/DRP con indicazioni:
    - definizione trigger di azione;
    - definzione procedure e azioni;
    - definizione team leader per varie azioni;
    - definizione obiettivi BC;
- focus su disaster recovery:
    - definizione esigenze di DR;
    - definizione caratteristiche siti e eventuali partner DR;

3.4 Gestione della crisi

Questa sezione delinea principi, ruoli, strutture e strumenti operativi da adottare per affrontare in modo efficace la gestione di una crisi, con particolare riferimento agli incidenti di cybersecurity e in linea con quanto richiesto dalla Direttiva NIS2, garantendo reattività, coordinamento e resilienza.

La crisi è una fase che si innesta nel ciclo di vita di un incidente quando l'evento supera la soglia di gestione ordinaria e compromette in modo significativo la continuità operativa; con effetti potenzialmente di lungo termine su persone, ambiente, operatività aziendale, reputazione. Nel contesto della Direttiva NIS2 e del

processo di gestione incidenti, la gestione della crisi è innescata principalmente da un'escalation legata ad un incidente di cybersecurity che possa portare ad una grave interruzione dell'operatività, come indicato nella sezione "Risposta" nel modello. Tuttavia, altre tipologie di incidenti potranno causare una crisi che potrà essere rilevata e gestita con tempi meno stringenti (es. l'esfiltrazione di dati riservati che possano causare un impatto elevato se pubblicati o ceduti a terzi).

Nel contesto della continuità operativa, **il fattore tempo è determinante**: intervenire tempestivamente può contenere danni, tutelare gli asset aziendali e accelerare il ritorno ad uno stato di nuova operatività.

Il processo di gestione della crisi è rappresentato come una sequenza temporale che inizia con un incidente (t1) e si articola attraverso:

- Golden Hour (t2): durante la quale è fondamentale attivare rapidamente il Crisis Management Team e le procedure di risposta; In questo intervallo (da pochi minuti a un paio d'ore dalla dichiarazione di crisi), è essenziale attivare prontamente i meccanismi decisionali e operativi previsti.
- il ripristino degli ambienti core (t3): consente il ritorno alle funzionalità critiche entro il Recovery Time Objective (RTO);
- fino al pieno ripristino della nuova operatività (t4): da conseguire entro il Maximum Tolerable Period of Disruption (MTPD).

Dichiarazione della Crisi

La crisi può essere dichiarata da una delle seguenti figure, in funzione della gravità e del contesto:

- **Il responsabile della continuità operativa**, in seguito alla valutazione dell'impatto sull'operatività e alla mancata efficacia delle contromisure standard;
- **il Responsabile della Sicurezza**, in presenza di incidenti di sicurezza gravi (es. compromissioni sistemiche, ransomware, attacchi APT);
- **Il Top Management** (componenti della Direzione), in caso di eventi che hanno impatti strategici, reputazionali o legali su scala aziendale;
- **Il Crisis Manager**, se nominato formalmente in una fase pre-incident, con delega operativa alla gestione delle emergenze.

L'attivazione formale della gestione della crisi deve essere comunicata in modo tempestivo, chiaro e tracciabile a tutti gli attori coinvolti.

Crisis Management Team

Il Crisis Management Team deve riflettere una **struttura multidisciplinare**, Essa è diretta dal Crisis Manager. In caso di sua assenza, la funzione sarà assunta da un altro membro designato. La sua composizione può dipendere dalla natura e/o tipologia dell'incidente.

Crisis Management Support Team

Il Crisis Management Support Team ha il compito di alleggerire il Crisis Management Team da attività amministrative e operative di supporto, consentendogli di concentrarsi esclusivamente sulle decisioni strategiche e gestionali.

Le sue funzioni includono:

- facilitare la logistica e il back-office;
- garantire il flusso informativo interno ed esterno;
- supportare nelle attività di comunicazione, procurement, e coordinamento tecnico-operativo.

Tra i membri del Support Team possono figurare: fornitori di sicurezza (es. MSSP o DFIR), l'ufficio acquisti, il team comunicazione, il team legale, il team IT e altri stakeholder interni o esterni.

Command Center

Il Crisis Management Team opera da una struttura fisica o virtuale denominata Command Center (Centro di Comando), che deve essere preventivamente identificata, allestita e testata per garantirne l'efficacia in fase di crisi.

Il Command Center può consistere in:

- una sala riunioni fisica dotata di strumenti ICT (es. connessioni sicure, lavagne digitali, videoconferenza).
- oppure in un ambiente virtuale sicuro e centralizzato, come ad esempio:

- Microsoft Teams con canali dedicati e file repository strutturati;
- Zoom con Zoom Rooms per la gestione di riunioni emergenziali;
- Google Workspace per la collaborazione documentale.

Il Command Center deve garantire le seguenti funzionalità operative:

- coordinamento e comunicazione centralizzata tra i membri del Crisis Management Team e gli stakeholder esterni;
- raccolta, archiviazione e tracciamento di tutta la documentazione rilevante alla gestione della crisi (log, verbali, decisioni, cronologia eventi, evidenze tecniche);
- gestione e schedulazione strutturata delle riunioni di crisi, con verbalizzazione automatica o assistita;
- monitoraggio in tempo reale delle attività in corso e aggiornamento continuo della situazione operativa.

Il corretto funzionamento del Command Center è condizione abilitante per la governance efficace della crisi, per cui la sua disponibilità e operatività devono essere periodicamente verificate nell'ambito delle esercitazioni o test di continuità.

Nota di resilienza

Per garantire la continuità operativa anche in caso di sede compromessa o sospette violazioni dei sistemi virtuali, è consigliabile predisporre una struttura di backup del Command Center, sia essa:

• una seconda piattaforma virtuale su infrastruttura separata e isolata (es. tenant secondario, backup su cloud differente), strumenti di comunicazione e collaborazione alternativi e non legati al sistema informativo potenzialmente compromesso

• oppure una location fisica alternativa in grado di subentrare rapidamente alle funzioni del Command Center principale.

Command Center Equipment

Il **Command Center**, per poter operare in modo efficace e supportare la gestione centralizzata della crisi, deve essere **dotato di attrezzature, piattaforme e strumenti specifici**, differenziati in base alla natura fisica o virtuale della struttura.

È responsabilità della funzione Business Continuity aziendale predisporre, attivare e rendere operativo l'equipment del Command Center, nel minor tempo possibile.

Le modalità più idonee per l'attivazione sono in carico al responsabile della sicurezza aziendale.

Risorsa	Descrizione	Quantità	Disponibilità
Piattaforma			
Ambiente sicuro per la gestione dell'incidente	Sistema predisposto o piano di attivazione di piattaforme quali Teams,	Sufficiente per dotare tutto il Crisis management Team e support team	Appena possibile

Risorsa	Descrizione	Quantità	Disponibilità
	Zoom o alternative.		
Documentazione in formato digitale o cartaceo			
Asset inventory, **schemi di rete e interconnessioni** **Business continuity plan,** **disaster recovery plan,** **Business Impact Analysis** **Lista Fornitori e riferimenti principali**	Questi documenti devono essere aggiornati e riflettere lo stato dell'organizzazione	N/A	Appena possibile
IT equipment			
Router WiFi + **Switch**	In presenza di una compromissione su larga scala o nel caso si sospetti una minaccia	Sufficiente per gestire efficacemente la connessione simultanea di tutto il Crisis management	Entro 1 ora

Risorsa	Descrizione	Quantità	Disponibilità
	avanzata persistente (APT), è necessario **assumere per default che i sistemi aziendali siano compromessi**.è necessario creare un ambiente airgapped tramite una LAN separata con possibilità di connettersi ad un exit node VPN sicuro.	Team e support team	
Laptop o workstation vergini in	In presenza di una compromissio	Sufficiente dotazione per tutto il Crisis	Entro 1 ora

Risorsa	Descrizione	Quantità	Disponibilità
alternativa predisposizione di distro live con boot da USB	ne su larga scala o nel caso si sospetti una minaccia avanzata persistente (APT), è necessario **assumere per default che i sistemi aziendali siano compromessi**.	management Team	
Canali di comunicazione			
Comunicazione su servizi di messaggistica alternativi/personali	In presenza di una compromissione su larga scala o nel caso si sospetti una minaccia avanzata persistente (APT), è		Appena possibile

Risorsa	Descrizione	Quantità	Disponibilità
	necessario **assumere per default che i sistemi aziendali siano compromessi**. In tali circostanze, l'attivazione del Crisis Management Team e della relativa piattaforma operativa deve avvenire privilegiando **canali di comunicazione alternativi e isolati**, preferibilmente esterni all'infrastruttura aziendale		

Risorsa	Descrizione	Quantità	Disponibilità
	(es. dispositivi personali, numerazioni mobili non registrate, account di emergenza).		

Tabella 13: Command Center Equipment

Processo Decisionale durante una situazione di Crisi

Nel contesto di una crisi, il processo decisionale si sviluppa attraverso sei fasi operative. Il tempo è un fattore critico, ma agire in fretta non significa agire in modo disordinato: ogni passaggio ha un ruolo preciso e si innesta su dinamiche interdipendenti.

Figura 6: Processo Decisionale durante una situazione di Crisi

Consapevolezza: È la capacità di riconoscere tempestivamente l'emergere di una situazione anomala o critica. Senza consapevolezza, non c'è risposta.

Valutazione: Analisi dei dati disponibili, verifica delle fonti, stima dell'impatto e dei possibili scenari. L'obiettivo è trasformare l'incertezza in informazione operativa. L'uso del pensiero critico e il confronto tra più punti di vista sono fondamentali in questa fase.

Decisione: Le decisioni in crisi non possono attendere la completezza dei dati. È quindi necessario prendere decisioni tempestive, anche parziali, basate su ciò che è noto in quel momento. La leadership deve emergere con chiarezza e determinazione.

Azione: Le azioni si articolano in tre sottocomponenti operative:

- Contenimento: Fermare la diffusione o l'aggravamento del danno.
- Recupero: Ripristinare rapidamente la funzionalità dei processi critici.
- Perfezionamento: Apportare miglioramenti immediati laddove possibile, riducendo la vulnerabilità residua.

Feedback: Ogni azione deve generare osservazioni utili per valutare l'efficacia delle decisioni prese. Il feedback permette di adattare la risposta in tempo reale e rappresenta il ponte tra azione e apprendimento.

Apprendimento (Learning): Al termine della crisi, è essenziale formalizzare quanto appreso: cosa ha funzionato, cosa, invece, no, e cosa va migliorato. È la base della resilienza organizzativa.

Durante la gestione della crisi è necessario tenere sempre in mente quattro parametri fondaemntali.

- **Flessibilità:** Capacità di cambiare approccio se le decisioni prese non portano ai risultati previsti.
- **Empatia:** La gestione della crisi è un processo umano non di business. Dimostrare effettiva empatia predispone le persone coinvolte nelle operazioni alla collaborazione.
- **Comunicazione:** Tutto il processo si basa sulla comunicazione: Chiara, diretta, bidirezionale. Essenziale per coordinare, motivare e ridurre l'incertezza su tutti i tavoli.
- **Leadership:** Presenza attiva, guida morale e operativa, capace di ispirare fiducia e determinazione.

3.5 Procedure e test

Obiettivo di questa sezione è approfondire gli aspetti di formalizzazione delle procedure di gestione incidenti, nonché le attività di verifica dell'efficacia attraverso diverse modalità di test.

Formalizzazione delle Procedure

Nel contesto della Direttiva NIS2, la formalizzazione delle procedure di gestione degli incidenti rappresenta un elemento imprescindibile per garantire un'efficace risposta alle minacce informatiche e una piena conformità normativa. Tuttavia, è essenziale chiarire che non è possibile – né auspicabile – definire un unico processo standardizzato valido per ogni organizzazione rientrante nel perimetro NIS2. Ogni soggetto obbligato dovrà necessariamente interpretare e adattare il

modello generale di gestione degli incidenti in funzione della propria struttura, settore di appartenenza, maturità tecnologica, esposizione al rischio e livello di complessità operativa. Il capitolo <Modello di gestione degli incidenti> fornisce un framework di riferimento, ispirato alle best practice internazionali (come il NIST SP 800-61), utile per identificare le fasi fondamentali che ogni processo di risposta agli incidenti dovrebbe prevedere: dalla preparazione, al rilevamento, all'analisi, fino al contenimento, al recupero e alla revisione post-incident. Tuttavia, questo modello deve essere inteso come struttura modulare, non prescrittiva, che ogni soggetto NIS2 è chiamato a declinare operativamente in coerenza con la propria realtà specifica.

La formalizzazione delle procedure di gestione incidenti ha anche un ulteriore obiettivo, più operativo. Dato che la gestione degli incidenti è un'attività svolta spesso in emergenza, con forti pressioni, disponibilità limitata di personale e al di fuori dei normali orari, si è dimostrato importante ridurre al minimo l'improvvisazione, fonte di indefficienze o di attività inefficaci o anche dannose. Questo, del resto, è valido per buona parte delle attività di gestione delle emergenze in generale, siano legate a temi di salute, protezione civile o altro (si pensi ad esempio alle esercitazioni antincendio). Per questo, la formalizzazione e il test aiutano ad assicurare la chiara definizione di ruoli e responsabilità, l'effettiva applicabilità di quanto definito, nonché ad individuare le azioni di miglioramento prima di dover provare le procedure in un vero incidente, dove le conseguenze di un errore potrebbero essere importanti.

Piano di Test Regolari

Il seguente capitolo si occupa di creare delle linee guida per tesate sotto diversi aspetti, per quanto possibile l'incident response plan e le sue procedure, per introdurre in maniera preventiva il concetto di

lesson learned e potenziare proattivamente il Piano di Risposta agli Incidenti Informatici.

Di seguito viene riportato in forma tabellare la frequenza di ogni tipologia di Test che il soggetto NIS2 dovrà effettuare:

Test Tecnico	Frequenza minima soggetti importanti	Frequenza minima soggetti essenziali
Test di Detection	---	Annuale
Test di Contenimento	---	Annuale
Penetration Test	Annuale	Semestrale
Ripristino Dati	Semestrale	Trimestrale
Ripristino Sistemi	Semestrale	Trimestrale
Simulazioni Red Teaming	---	Biennale

Tabella 14: frequenza di test soggetto NIS2

Tipologia Soggetto	Frequenza Minima Tabletop
Importante	Biennale
Essenziale	Annuale

Tabella 15: requenza Tabletop soggetto NIS2

Test Tecnici

Con l'ottica della resilienza operativa e la capacità effettiva nella gestione degli incidenti informatici, questa sezione copre la divisione per tipologia dei principali test di caratura tecnica, dunque da eseguire direttamente sui sistemi informativi del soggetto NIS2. QUesti test comprendono la predisposizione ed il miglioramento di istruzioni operative per le diverse attività. Ad esempio, istruzioni operative per il corretto ripristino di sistemi complessi, nonché per il corretto ordine di ripristino di sistemi e servizi.

Test di Detection

L'obiettivo dell'attività è verificare l'efficacia e la tempestività del rilevamento automatico di eventi sospetti o malevoli da parte dei sistemi e/o servizi di sicurezza. Per farlo, si parte da una fase di preparazione in cui viene definito il tipo di evento da simulare, come ad esempio un login anomalo, una scansione di rete o il rilascio di un malware.

Durante la fase esecutiva, si procede con la simulazione dell'evento scelto, che può consistere, ad esempio, in un accesso da un indirizzo IP non autorizzato, nella creazione di un file eseguibile sospetto o in un'elevazione di privilegi non autorizzata. L'attenzione si concentra quindi sul comportamento del sistema di rilevamento: si osserva se

vengono generati alert, se vi è una correlazione con altri eventi e se viene aperto automaticamente un ticket. Può comprendere anche la disattivazione di qualche sensore (es. la disconnessione di un sistema di IDS o di un componente del sistema di log management) per verificare che un tale evento venga rilevato, tipicamente dal SOC.

L'output atteso comprende la generazione di un alert coerente, la corretta classificazione dell'evento e la notifica al team SOC o IR. Infine, è fondamentale garantire l'auditabilità dell'intero processo, raccogliendo log dell'evento, alert generati, tempi di rilevamento (MTTD)

Test di Contenimento

L'attività prende avvio con la simulazione di un endpoint compromesso o di un malware in esecuzione, coinvolgendo attivamente sia il team tecnico che quello di sicurezza.

Durante la fase esecutiva, viene avviato un evento simulato, come ad esempio l'esecuzione di un payload, e si procede con l'attivazione di azioni specifiche, manualmente o tramite orchestrazione. Tra queste rientrano l'isolamento dell'host, l'interruzione del traffico di rete, il blocco dei processi malevoli e la revoca delle credenziali compromesse. Questo tipo di test può essere svolto inizialmente table top (vedi seguito), per verificare la corretta definizione di ruoli e responsabilità e la correttezza delle procedure, per poi passare a simulazioni su sistemi reali, in ambiente di test o di poduzione a seconda delle condizioni.

L'output atteso comprende la capacità dei sistemi e/o dei servizi di sicurezza nel contenere la minaccia su diversi livelli:

- Processo
- Sistema Operativo
- Rete
- Disabilitazione Utenze

Nella documentazione finale è importante mantenere traccia dei tempi di reazione (MTTC) producendo un report tecnico che descriva le attività svolte

Penetration Test

Il penetration test, da effettuare almeno una volta all'anno, ha lo scopo di identificare eventuali vulnerabilità tecniche sfruttabili sugli degli asset aziendali. L'attività inizia con una fase di preparazione in cui viene definito l'ambito del test, che può essere interno o esterno, e la modalità operativa, come ad esempio un approccio black-box o white-box.

Durante l'esecuzione, si procede con la scansione delle vulnerabilità e con tentativi controllati di exploit, finalizzati a verificare la reale esposizione dei sistemi. In questa fase vengono raccolte evidenze tecniche, come che permettono di valutare l'impatto potenziale delle vulnerabilità rilevate da parte di un potenziale attaccante.

L'output del documento deve essere corredato da un piano di remediation e dalla classificazione delle vulnerabilità riscontrate ed eventuali scenari d'attacco relalizzati.

Ripristino Dati

Ha come obiettivo la verifica dell'integrità e della disponibilità dei backup relativi ai dati critici aziendali. L'attività inizia con

l'identificazione di un dataset significativo, e con la selezione del punto di restore da utilizzare per la simulazione.

La fase esecutiva prevede il ripristino del dataset in un ambiente isolato o di test, dove vengono effettuate verifiche puntuali sull'integrità dei dati, sulla loro completezza e sull'assenza di corruzione. Questo consente di accertare che i backup dei file critici siano effettivamente utilizzabili in caso di necessità reale.

Sarà necessario produrre un verbale del test, raccogliere i log generati e confrontare gli hash dei dati originali con quelli ripristinati, così da fornire evidenze concrete e verificabili.

Ripristino Sistemi

Mira a valutare la capacità dell'organizzazione di riportare in funzione sistemi o ambienti critici a seguito di un incidente. L'attività prende avvio con la selezione di un sistema o ambiente rilevante (tipicamente sotto forma di macchina virtuale), come ad esempio un server Active Directory, simulandone l'indisponibilità totale come a seguito di un attacco ransomware.

La fase esecutiva prevede il ripristino del sistema partendo da un backup e seguendo le procedure di disaster recovery aziendali. Una volta ripristinato il sistema è importante verificarne il funzionamento relativamente ai servizi erogati come ad esempio l'accesso degli utenti o l'operatività delle applicazioni principali.

Sarà necessario produrre un verbale del test con eventuali dettagli tecnici di errore durante la procedura di ripristino e un dettaglio esecutivo utile a migliorare le procedure utilizzate.

Red Teaming

L'obiettivo di testare la resilienza dell'organizzazione rispetto a minacce reali come attacchi APT o ransomware, valutando al contempo la capacità di rilevamento e risposta in ambienti operativi reali. L'attività prevede il coinvolgimento di un team specializzato, interno o esterno, incaricato di condurre l'attacco simulato. Come per il penetration test è importante stabilire la modalità di erogazione, che preveda o meno la conoscenza del team difensivo del test in essere e definisca le modalità tecniche di erogazione, come ad esempio le tipologie di payload utilizzate.

L'output del report deve prevedere dettaglio utile al miglioramento delle tecnologie difensive ed eventuale ampliamento dell'asset tecnologico. Inoltre deve rendere conto delle eventuali falle o ritardi nei KPI definiti dal team di sicurezza informatica.

Esercitazioni Tabletop

Le esercitazioni tabletop rappresentano uno strumento strategico per valutare l'efficacia delle procedure di incident response in uno scenario simulato, senza impattare sugli ambienti produttivi. Queste simulazioni si svolgono in modalità teorica (non tecnica) e coinvolgono i principali stakeholder aziendali (IT, security, legal, compliance, comunicazione, HR, ecc.), stimolando la discussione su ruoli, decisioni, comunicazioni e azioni da intraprendere di fronte a un incidente ipotetico.

Principali obiettivi:

L'obiettivo principale è valutare il livello di preparazione e consapevolezza del personale coinvolto nella gestione degli incidenti, verificando al contempo l'efficacia delle procedure formali adottate, che si basano sul precedente capitolo <Modello di gestione degli

incidenti>. È fondamentale accertarsi che tali procedure siano corrette, chiare e realmente applicabili in contesti operativi concreti. Durante l'attività, si punta anche a individuare eventuali lacune operative, debolezze nei flussi decisionali e possibili ambiguità nei ruoli assegnati. Un altro aspetto rilevante è la simulazione delle dinamiche di reporting verso le autorità competenti, come ad esempio il CSIRT nazionale, l'ACN e le autorità di pubblica sicurezza, in linea con quanto previsto dalla direttiva NIS2.L'esercitazione rappresenta un'opportunità per allenare il team nella gestione della comunicazione, sia interna che esterna, tenendo conto degli impatti reputazionali e degli obblighi regolatori connessi a un incidente di sicurezza.

Modalità esercitazione:

Prevedendo le metodologie di test tecnici descritte nei precedenti paragrafi, il cui scopo in alcuni casi è quello di simulare un attacco informatico e la relativa risposta del soggetto, si definisce come metodologia di esercitazione Tabletop quella descirtta come Scripted Tabletop che prevede una simulazione "a tavolino" condotta su uno scenario di incidente predefinito, che si sviluppa in atti o fasi successive, secondo una sceneggiatura scritta in anticipo. I partecipanti reagiscono all'evoluzione dello scenario secondo i ruoli che ricoprono nel piano di gestione incidenti.

Tipologie e strutture scenari Tebletop

Visto l'affidabilità dell'ente CISA (**www.cisa.gov**) si sceglie di basarsi sull'utilizzo degli scenari messi a disposizione.

Le domande e le dinamiche proposte all'interno di ciascuno scenario sono attentamente progettate per riflettere le cinque funzioni fondamentali del NIST Cybersecurity Framework – Identify, Protect, Detect, Respond, Recover – framework sul quale è basato il seguente documento e sono pensate per coinvolgere attivamente i diversi attori aziendali secondo i rispettivi ruoli e responsabilità organizzative.

Questo approccio garantisce che le simulazioni non siano meri esercizi teorici, ma strumenti pratici per verificare la preparazione operativa e decisionale dell'intera struttura, mettendo in evidenza eventuali lacune nei processi, nella comunicazione o nella governance. L'allineamento tra contenuti, domande e framework consente inoltre di creare un ambiente di apprendimento efficace e multidisciplinare, in cui ogni figura – dal personale tecnico al management – può contribuire secondo le proprie competenze, migliorando allo stesso tempo la comprensione collettiva della gestione degli incidenti.

Di seguito il link a cui è possibile scaricare e accedere alle risorse:

https://www.cisa.gov/resources-tools/resources/cybersecurity-scenarios

Struttura Operativa delle Esercitazioni Tabletop:

Componente	Descrizione
Giocatori	Hanno un ruolo attivo durante l'esercitazione, discutendo o svolgendo i propri compiti principali. Sono chiamati a commentare o intraprendere azioni in risposta allo scenario proposto. Sono le figure indicate nelle procedure di risposta agli incidenti.

Componente	Descrizione
Osservatori	Sono incaricati di osservare e documentare le attività svolte durante l'esercitazione. Il loro compito principale è registrare le discussioni dei giocatori, verificando se e come queste siano coerenti con piani, politiche e procedure esistenti. non partecipano direttamente all'esercitazione. Possono essere figure terze all'azienda o meno.
Facilitatori	Forniscono aggiornamenti sullo scenario e moderano le discussioni. Offrono inoltre informazioni aggiuntive o chiarimenti quando necessario. Coordinano il tabletop e le sue fasi. Possono essere figure terze all'azienda o meno e eventualmente il loro ruolo può essere svolto dagli Osservatori stessi

Tabella 16: Struttura Operativa esercitazioni Tabletop

Linee Guida sullo svolgimento del tabletop:

L'esercitazione si svolge in un ambiente aperto e privo di colpe, dove è naturale che emergano punti di vista differenti. I partecipanti sono invitati a rispondere allo scenario facendo leva sulla propria conoscenza dei piani e delle capacità esistenti, integrando queste competenze con le esperienze e la formazione acquisite nel tempo. Le decisioni prese durante l'attività non sono vincolanti né rappresentano necessariamente la posizione definitiva dell'organizzazione su una determinata questione. Al contrario, l'esercitazione rappresenta un'opportunità per esplorare e discutere

diverse opzioni, soluzioni possibili e azioni suggerite per affrontare o mitigare un problema. Non ci sono secondi fini né domande trabocchetto: le risorse e i materiali forniti costituiscono la base per la discussione. Come in ogni esercitazione, alcune assunzioni e semplificazioni sono necessarie per rispettare i tempi previsti, raggiungere gli obiettivi formativi e gestire eventuali vincoli logistici. È importante che questi elementi non influenzino negativamente la partecipazione attiva dei presenti.

Al termine dell'esercitazione, il facilitatore guiderà una sessione di valutazione assieme ai partecipanti, con l'obiettivo di raccogliere idee, osservazioni e criticità emerse durante le discussioni. Questo momento conclusivo rappresenta un'opportunità per riflettere immediatamente su quanto accaduto, evidenziando sia i punti di forza sia le aree che necessitano miglioramento. La condivisione a caldo consente di consolidare l'apprendimento e di raccogliere spunti utili per ottimizzare le procedure e la risposta operativa in futuro con un punto di vista "dall'interno".

In maniera congiunta gli osservatori e facilitatori si occuperanno della creazione del report di attività, che descriverà a livello esecutivo quanto accaduto durante l'esercitazione e specificheranno nel dettaglio le aree di miglioramento dividendole per i punti identificati nello schema <Modello di gestione degli incidenti>:

- Pianificazione e preparazione
- Monitoraggio
- Riconoscimento
- Contenimento
- Eradicazione

- Ripristino
- Attività post-incidente

L’output del report deve inoltre contenere le seguenti informazioni:

- Sintesi dello scenario simulato.
- Mappa decisionale (chi ha fatto cosa e quando). Eventuale necessità di integrazione dei ruoli.
- Analisi degli scostamenti dalle procedure previste.
- Analisi procedure comunicazione interna
- Analisi procedure comunicazione esterna
- Metriche (tempo di rilevamento, escalation, comunicazione).
- Raccomandazioni operative
- Piano di remediation: aggiornamenti al piano IR, necessità formative, gap tecnologici.

Nota interna team "comunicazione": Prevedere anche la fase di test delle procedure di comunicazione (interne ed esterne)

3.6 Comunicazione

Definizione del ***Modello di Comunicazione*** per gli incidenti rilevanti ai sensi della direttiva NIS2, tra le parti interessate come di seguito

riportato:

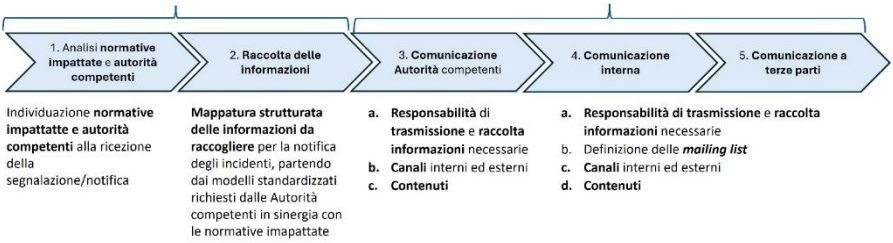


Figura 7: Modello di Comunicazione per incidenti rilevanti

Analisi normative impattate e autorità competenti

È un'attività preparatoria che prevede di valutare le normative impattate e i casi previsti di segnalazione/notifica degli eventi da indirizzare verso le relative Autorità competenti.

Raccolta delle informazioni necessarie

Consiste nella definizione di una mappatura strutturata delle informazioni da raccogliere per la notifica degli incidenti, partendo dai modelli standardizzati richiesti dalle Autorità competenti (es. CSIRT, Garante per la Privacy, ecc.). A supporto di questo processo, si propone – a titolo esemplificativo e non esaustivo – uno schema matriciale utile alle organizzazioni per individuare e reperire tempestivamente le informazioni necessarie alla comunicazione verso le Autorità. Dato che è necessario sempre più spesso comunicare a diverse autorità informazioni sugli incidenti, co diverse tempistiche, diverse informazioni, e spesso diverse definizioni di incidente, è necessario perarare la raccolta delle informazioni in modo strutturato, per assicurare di raccogliere tutte quelle necessarie e di comunicare tutte quelle richieste.

Normativa	Autorità competente	Data e ora rilevamento incident	Data e ora chiusura incident	Durata incident	Causa dell' incidente	Incidente significativo	Convocazione Incident Response	Altre Valutazioni interne
NIS2	**CSIRT**	X	X	X	X	X	X	…
Altre normative applicabili	**Altre Autorità**	X	X	X	X	…	…	…
….	**…**	…	…	…	…	…	…	…

Tabella 17: Raccolta Informazioni Necessarie

Oltre a definire le tipologie di informazioni richieste, è **fondamentale predisporre un elenco chiaro dei referenti e dei rispettivi ambiti di responsabilità (ownership)**, così da sapere a chi rivolgersi per ottenere tempestivamente i dati necessari. Questo approccio consente di garantire chiarezza e rapidità nell'accesso alle informazioni, facilitando il rispetto delle tempistiche di notifica imposte dalle diverse Autorità. In molti casi, inoltre, saranno specifici soggetti quelli deputati ad effettuare materialmente la comunicazione, a prescindere da chi l'abbia predisposta.

1. **Comunicazione verso Autorità Competente (CSIRT)**
    1. Responsabilità di trasmissione e raccolta informazioni necessarie
    2. Canali interni ed esterni
    3. Contenuti
2. **Comunicazioni interne**
    1. Responsabilità di trasmissione e raccolta informazioni necessarie
    2. Definizione delle mailing list
    3. Canali interni ed esterni
    4. Contenuti
3. **Comunicazioni verso terze parti**
    1. Responsabilità di trasmissione e raccolta informazioni necessarie
    2. Definizione delle mailing list
    3. Canali interni ed esterni
    4. Contenuti

Per le comunicazioni verranno predisposti template (a seconda del canale di comunicazione predefinito), di seguito alcuni esempi:

Comunicazioni interne

Template volto alla comunicazione dell'incidente a tutto personale interno al fine di fornire indicazioni circa accorgimenti/norme comportamentali da adottare. Di seguito si propone un template a titolo esemplificativo e non esaustivo:

- **Oggetto:** Avviso di incidente informatico e istruzioni operative;
- **Contesto:** È stato rilevato un incidente informatico che potrebbe influenzare l'operatività aziendale;
- **Azioni richieste:** non aprire mail sospette; cambiare la password aziendale; seguire le istruzioni del team IT;
- **Eventuali comunicazioni verso media/stampa:** cosa si può comunicare.

Comunicazioni verso terze parti

Template mail volto alla comunicazione dell'incidente alle Terze Parti (es. (clienti, fornitori, partner) al fine di fornire indicazioni ad alto livello circa l'incident. Di seguito si propone un template a titolo esemplificativo e non esaustivo:

- **Oggetto:** Comunicazione di incidente informatico che potrebbe coinvolgere dati o servizi;
- **Contesto:** nome dell'Organizzazione e servizi/processi coinvolti;
- **Descrizione dell'incidente:** desideriamo informarvi che in data [data] è stato rilevato un incidente informatico;

- **Impatto potenziale:** l'incidente potrebbe aver coinvolto dati o servizi a voi riferiti. Stiamo conducendo le opportune verifiche;
- **Misure adottate:** sono state attivate misure di contenimento e mitigazione. Vi terremo aggiornati sugli sviluppi;
- **Contatti:** Per ulteriori informazioni potete contattare: [email] - [telefono].

Procedure di Escalation

Predisposizione di un template per eventuale escaltion e della mailing list.

Canali sicuri di comunicazione

Destinatario	Canale consigliato	Note
CSIRT Italia	Portale dedicato dello CSIRT	Obbligatorio per la notifica formale degli incidenti
Personale interno	Intranet aziendale, email firmate, canali di workplace aziendali	Comunicazioni segmentate per ruolo, con autenticazione a più fattori
Terze parti	PEC, portali clienti, comunicati ufficiali	Solo se necessario, con supporto legale

Emergenze	Canali vocali	Per comunicazioni rapide e riservate in caso di crisi

Tabella 18: Canali sicuri di Comunicazione

Tipologia di comunicazioni al CSIRT e Tempistiche per la segnalazione

Link al documento "Guida alla notifica degli incidenti al CSIRT Italia":

https://www.acn.gov.it/portale/documents/20119/552690/ACN_Guida_Notifica_Incidenti_CLEAR.pdf/e7a1b3df-fac0-9b10-fb4d-c08be31061ad?t=1722593115655

Link al portale per la segnalazione: **https://segnalazioni.acn.gov.it/**

Secondo quanto previsto dall'articolo 25, comma 4 del D.Lgs. 138 del 2024, un incidente è considerato significativo se:

a) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;

b) ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

Si riportano di seguito le fasi di notifica al CSIRT, con indicazione della tipologia di segnalazione da inviare al CSIRT e le relative tempistiche (secondo quanto previsto dall'articolo 25, comma 5 del D.Lgs. 138 del 2024):

Invio di pre-notifica: senza ingiustificato ritardo, e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo,

che, ove possibile, indichi se l'incidente significativo possa ritenersi il risultato di atti illegittimi o malevoli o può avere un impatto transfrontaliero;

Invio di notifica: senza ingiustificato ritardo, e comunque entro 72 ore da quando sono venuti a conoscenza dell'incidente significativo, che, ove possibile, aggiorni le informazioni di cui alla pre-notifica e indichi una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione;

Invio di relazione intermedia (su richiesta del CSIRT Italia): una relazione su pertinenti aggiornamenti della situazione;

Invio di relazione finale: entro un mese dalla trasmissione della notifica dell'incidente, che comprenda:
1) una descrizione dettagliata dell'incidente, ivi inclusi la sua gravità e il suo impatto;

2) il tipo di minaccia o la causa originale (root cause) che ha probabilmente innescato l'incidente;

3) le misure di attenuazione adottate e in corso;

4) ove noto, l'impatto transfrontaliero dell'incidente;

Invio di relazioni mensili: in caso di incidente in corso al momento della trasmissione della relazione finale, relazione su progressi e una relazione finale entro un mese dalla conclusione della gestione dell'incidente.

Con riferimento alla segnalazione obbligatoria di un incidente, è necessario alimentare le seguenti sezioni:

- sezione A: soggetto che effettua la notifica;
- sezione B: dettagli dell'operatore/fornitore;
- sezione C: tipologia di incidente;
- sezione D: impatto dell'incidente;
- sezione E: da compilare solo in caso di incidenti transfrontalieri;
- sezione F: eventuali notifiche;
- sezione G: informazioni aggiuntive - incidenti cyber
- sezione H: informazioni aggiuntive - incidenti non cyber
- sezione I: ulteriori informazioni rilevanti

Nota interna team "Comunicazione": laddove necessario e/o ritenuto opportuno, abbiamo effettuato l'analisi del modulo per la segnalazione al CSIRT con evidenza dei campi (obbligatori e non) da compilare per ciascuna delle sezioni di cui sopra.

Nota interna team "comunicazione": nella sezione "Informazioni di contatto" inserire anche il riferimento alle eventuali mailing list interne create dalla società. Dettagliare nella fase di valutazione dell'incidente, eventuali driver per la classificazione di significatività dell'incidente ai fini NIS

Conclusioni

La Direttiva NIS2 e il relativo recepimento nazionale introducono un paradigma di sicurezza fondato su responsabilità diretta del management, misure proporzionate al rischio e obblighi di notifica stringenti. L'approccio proposto in questo paper dimostra come la compliance possa evolvere da mero adempimento normativo a strumento di governance strategica, capace di generare valore in termini di resilienza, trasparenza e vantaggio competitivo.

L'integrazione tra modelli organizzativi, policy di sicurezza, gestione della supply chain e processi di incident response consente di ridurre la superficie di attacco e di garantire continuità operativa anche in scenari di crisi. Tuttavia, la piena efficacia del framework richiede un impegno costante in termini di formazione, audit periodici e aggiornamento delle procedure in funzione dell'evoluzione delle minacce e delle normative.

Sviluppi futuri potranno includere l'adozione di strumenti di automazione per il monitoraggio della compliance, l'integrazione di soluzioni di intelligenza artificiale per il risk scoring e l'analisi predittiva, nonché la creazione di ecosistemi collaborativi tra imprese e autorità per la condivisione di informazioni e best practice.

Fonti

- Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione (NIS2).
- Decreto Legislativo 4 settembre 2024, n. 138, Attuazione della Direttiva (UE) 2022/2555.
- Agenzia per la Cybersicurezza Nazionale (ACN) - Determinazione n. 164179 del 14 aprile 2025, "Modalità e specifiche di base per l'adempimento degli obblighi NIS2".
- ENISA - "Technical Implementation Guidance on Commission Implementing Regulation (EU) 2024/2690".
- ISO/IEC 27001:2022 - Information Security Management Systems - Requirements.
- NIST SP 800-61r3 - Computer Security Incident Handling Guide.
- ENISA Threat Landscape Report - Latest edition.
- Framework Nazionale per la Cybersecurity e la Data Protection (FNCDP) - Versione aggiornata.
- eCSIRT.net – *Mapping dettagliato tra valori ACN e categorie ENISA.*