CYBERNEXUS

NIS 2

Compliance, Rischio e Continuità Operativa

Sommario

Introduzione

L'entrata in vigore del **Decreto Legislativo n. 138/2024**, in attuazione della Direttiva (UE) 2022/2555 (**NIS2**), determina un'evoluzione strutturale per il sistema produttivo e amministrativo nazionale. La sicurezza delle reti e dei sistemi informativi trascende la dimensione esclusivamente tecnica per configurarsi come una responsabilità primaria di *Governance*, centrale per la continuità operativa dell'organizzazione.

Il nuovo assetto normativo non si limita a un aggiornamento dei requisiti preesistenti, ma sancisce la transizione verso il modello della *Cyber-Resilienza*, intesa come la capacità dell'organizzazione non solo di prevenire gli incidenti, ma di resistere, assorbire gli impatti e ripristinare tempestivamente l'operatività a fronte di minacce complesse.

Il legislatore impone l'adozione di un approccio sistemico e proattivo, fondato sul principio *Multi-Rischio*, che supera la distinzione tra sicurezza fisica e logica per tutelare il patrimonio informativo e infrastrutturale nella sua interezza. In tale scenario, la responsabilità in materia di sicurezza assume carattere diretto, inalienabile e non delegabile in capo agli organi di vertice, chiamati a integrare le strategie di difesa nei processi decisionali di business.

Obiettivi del Documento

Il presente documento ha l'obiettivo di fornire un'analisi tecnica ed operativa del quadro normativo vigente. Attraverso l'esame dell'architettura istituzionale nazionale (*ACN*, *CSIRT*) e dei criteri di applicazione, viene delineato il percorso di conformità (*compliance*) per i soggetti obbligati, approfondendo:

- La metodologia per la gestione del rischio (*Risk Management*) in conformità al Framework Nazionale (FNCSDP).
- Il regime di responsabilità giuridica e il sistema sanzionatorio.
- Le capacità operative necessarie per garantire la continuità dei servizi essenziali.

La trattazione mira a supportare le organizzazioni nell'implementazione di processi strutturati di *Business Continuity*, *Disaster Recovery* e *Incident Response*, elementi indispensabili per garantire la resilienza del singolo ente e la tenuta del sistema Paese.

1. Network Information Security

Contesto Normativo e Principi Fondamentali

La disciplina relativa alla sicurezza delle reti e dei sistemi informativi in Europa è definita dalla Direttiva (UE) 2022/2555, nota come **NIS2**, la quale è subentrata, abrogando e sostituendo, la precedente Direttiva (UE) 2016/1148 (NIS1).

L'adozione della NIS2 a livello europeo è avvenuta il **14 dicembre 2022**. La direttiva è stata pubblicata sulla gazzetta ufficiale dell'unione europea ed è entrata in vigore il **16 gennaio 2023**. Il percorso normativo che ha portato alla NIS2 non è stato improvviso, ma è il risultato di un lungo processo di armonizzazione iniziato già nel 2013, per rispondere alle crescenti sfide del mondo cibernetico.

L'obiettivo primario della NIS2 è contribuire a rafforzare la sicurezza complessiva all'interno dell'unione europea e a garantire un elevato livello comune di sicurezza delle reti e dei sistemi informativi, favorendo in tal modo il buon funzionamento del mercato interno. La nuova direttiva introduce requisiti più stringenti rispetto alla versione precedente.

1.1 Natura Giuridica: Direttive e Regolamenti

Per comprendere l'attuazione della NIS2, è essenziale distinguere la sua natura giuridica:

- Un **regolamento**, come il GDPR[1], è immediatamente vincolante e direttamente applicabile in tutti i suoi elementi in ogni stato membro, senza necessità di una legge nazionale di recepimento;
- Una **direttiva**, come la NIS2, stabilisce un risultato o un obiettivo che gli stati membri devono raggiungere (in questo caso, un elevato livello comune di sicurezza) ma lascia agli stati la libertà di scegliere i mezzi e gli strumenti operativi più adatti per raggiungerlo.

Per tale ragione, la direttiva NIS2 ha richiesto una fase di recepimento nazionale, che in Italia è avvenuta sotto forma di decreto legislativo, atto a tradurre gli obiettivi europei in norme concrete e adattarle all'ordinamento giuridico e alle strutture amministrative nazionali.

[1] **GDPR (General Data Protection Regulation)**: regolamento europeo sulla protezione dei dati personali (Regolamento UE 2016/679), in vigore dal 25 maggio 2018. Stabilisce obblighi per titolari e responsabili del trattamento, diritti per gli interessati e principi per garantire la tutela dei dati personali, imponendo misure tecniche e organizzative adeguate, notifica dei data breach e responsabilizzazione delle organizzazioni.

1.2 Recepimento in Italia: Cronologia e Atto Normativo

Gli stati membri dell'unione europea avevano tempo fino al **17 ottobre 2024** per recepire la NIS2 nelle rispettive legislazioni nazionali:

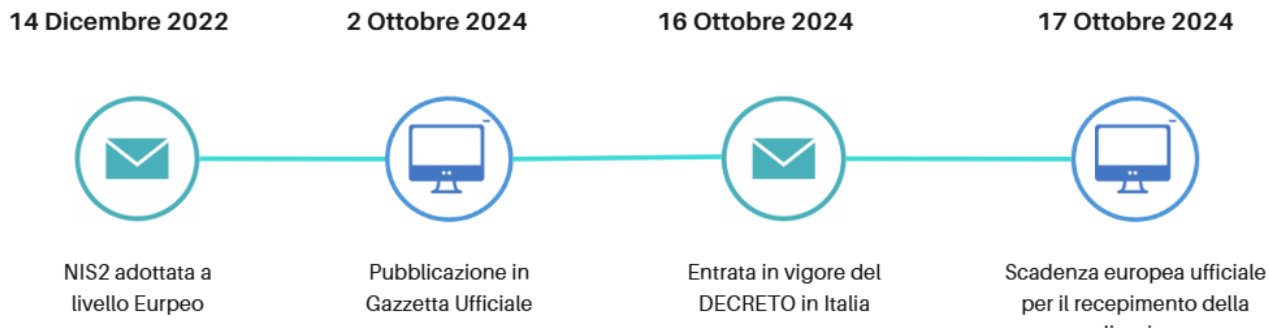
In Italia, la direttiva è stata recepita mediante l'emanazione del **Decreto Legislativo n. 138 del 4 settembre 2024**. Il percorso cronologico del recepimento nazionale è il seguente:

- **2 ottobre 2024:** Pubblicazione in gazzetta ufficiale (serie generale n. 230)
- **16 ottobre 2024:** Entrata in vigore del decreto in Italia
- **17 ottobre 2024:** Scadenza europea ufficiale per il recepimento della direttiva

L'entrata in vigore della norma nazionale ha avuto luogo il giorno precedente la scadenza fissata dall'unione europea, rispettando formalmente i termini. Contestualmente alla sua entrata in vigore, il d.lgs. n. 138/2024 ha abrogato il precedente Decreto Legislativo 18 maggio 2018, n. 65, che recepiva la NIS1. Il decreto mira a garantire l'aumento del livello di sicurezza del tessuto produttivo e delle pubbliche amministrazioni.

1.3 Approccio Strategico

La NIS2 introduce un approccio sistemico, proattivo e multirischio alla cybersicurezza, ampliando il perimetro di applicazione e rafforzando la governance[2].



La direttiva adotta un approccio basato sul rischio[3], richiedendo un monitoraggio costante delle minacce e l'implementazione di misure preventive e di mitigazione. Le misure devono essere adeguate e proporzionate alla gestione dei rischi specifici di ciascun soggetto.

[2] Insieme di processi, regole e strutture decisionali che guidano la gestione della sicurezza informatica in azienda, allineandola con la strategia aziendale.
[3] Approccio alla gestione dei rischi che considera contemporaneamente le minacce digitali (es. malware, phishing) e le minacce fisiche (es. furti, incendi, interruzioni di corrente elettrica), al fine di proteggere i sistemi informativi e il loro ambiente fisico.

Questo approccio si fonda su principi operativi e culturali definiti nel Framework Nazionale per la Cybersecurity e la Data Protection (FNCSDP[4]) che ricalca lo standard NIST[5]:

Integrazione Organizzativa (Governance)

La NIS2 non si limita agli aspetti strettamente tecnologici, ma introduce obblighi di natura organizzativa, gestionale e procedurale. Richiede l'integrazione della cybersecurity nella governance aziendale, elevando il rischio cibernetico a componente fondamentale dell'Enterprise Risk Management (ERM)[6], tramite il processo di Cyber Risk Governance[7].

L' obiettivo non è solo l'implementazione di controlli, ma anche la verifica che le decisioni di business siano prese con una consapevolezza chiara e strategica del rischio cyber.

Obiettivi Strategici della Cyber Risk Governance

- **Definizione delle Policy di Cybersicurezza:** Stabilire obiettivi chiari, misurabili e coerenti con la strategia aziendale per la sicurezza delle informazioni;

- **Chiarimento di Ruoli e Responsabilità:** Assegnare in modo esplicito le responsabilità del rischio cyber al Consiglio di amministrazione e ai dirigenti e definire le competenze necessarie per tutti i ruoli chiave;

- **Supervisione e Monitoraggio**: Implementare un quadro di sorveglianza (Oversight) e misurazione per garantire che il livello di rischio residuo sia sempre mantenuto entro la Risk Appetite[8] definita dall'organizzazione.

---

[4] Modello italiano per la gestione della sicurezza informatica e della protezione dei dati, sviluppato dal CINI (Consorzio Interuniversitario Nazionale per l'Informatica) in collaborazione con il Laboratorio Nazionale di Cybersecurity e con il supporto di istituzioni come ACN e il Garante Privacy. È di fatto la versione italiana del NIST Cybersecurity Framework, adattata alla normativa europea (GDPR, direttive UE), al contesto italiano e alle esigenze delle organizzazioni pubbliche e private.

[5] **National Institute of Standards and Technology**: ente federale statunitense che sviluppa standard, linee guida e best practice in ambito tecnologico e di cybersecurity. È autore del *NIST Cybersecurity Framework* (NIST CSF), uno dei riferimenti internazionali più adottati per la gestione del rischio cyber e per la strutturazione di controlli tecnici e organizzativi.

[6] Processo strutturato per identificare, valutare e gestire tutti i rischi di un'organizzazione. Integra rischi operativi, strategici e tecnologici per supportare decisioni aziendali consapevoli e allineate agli obiettivi strategici.

[7] Insieme di processi, responsabilità e strutture decisionali che integrano il rischio cyber nella governance aziendale. Comprende la definizione di strategie, policy, ruoli, metriche e meccanismi di supervisione necessari affinché organi direttivi e management valutino, controllino e gestiscano il rischio informatico come componente del più ampio Enterprise Risk Management (ERM). L'obiettivo è garantire che le decisioni di business tengano sempre conto dell'esposizione ai rischi cibernetici.

[8] Livello di rischio che un'infrastruttura è disposta ad accettare.

Normativa di Compliance e Documentazione

Un aspetto fondamentale della NIS2, che la accomuna al GDPR, è la sua natura di normativa di compliance[9]: l'adempimento richiede che ogni azione intrapresa (tecnica, organizzativa o procedurale) sia formalmente documentata.

Questa documentazione deve garantire la tracciabilità e la dimostrazione documentale di tutte le attività svolte, al fine di fornire prove concrete dell'effettivo rispetto degli obblighi previsti dalla normativa.

Cooperazione e Condivisione delle Informazioni

Il decreto stabilisce l'adozione di misure in materia di cooperazione e di condivisione delle informazioni: il fondamento della sicurezza europea è la condivisione e la cooperazione tra stati. La NIS2 prevede la partecipazione nazionale ai consessi e alle iniziative promosse a livello di unione europea, come il Gruppo di cooperazione NIS, per incrementare la fiducia e la collaborazione transfrontaliera, attraverso lo scambio tempestivo di informazioni, la fiducia reciproca e la possibilità di risposte coordinate.

1.4 Autorità Nazionale Competente NIS (ACN)

L'architettura di governance nazionale italiana identifica l'Agenzia per la Cybersicurezza Nazionale (**ACN**), istituita con il d.l. 14 giugno 2021, n. 82, come Autorità nazionale competente NIS.

[9] Necessità che ogni azione intrapresa sia formalmente documentata, in modo da fornire prove concrete e tracciabili dell'effettivo rispetto degli obblighi normativi

Funzioni e Compiti Istituzionali

L'ACN svolge un ruolo centrale, essendo l'autorità incaricata di:

- **Supervisione e attuazione normativa**: Garantisce la corretta applicazione del decreto e adotta tutti i provvedimenti attuativi necessari per renderlo pienamente operativo;
- **Attività regolatoria e di indirizzo**: Esercita funzioni di regolamentazione tecnica ed emana linee guida, raccomandazioni e orientamenti (anche di natura non vincolante) per guidare i soggetti nell'adeguamento;
- **Identificazione dei soggetti**: È responsabile dell'individuazione e del censimento dei soggetti che rientrano nel perimetro della direttiva, redigendo e aggiornando gli elenchi ufficiali dei soggetti essenziali e importanti;
- **Cooperazione internazionale**: Rappresenta l'Italia nel *Gruppo di cooperazione NIS*[10] e partecipa alle iniziative europee per coordinare l'applicazione della direttiva con gli altri Stati membri;
- **Vigilanza e supporto**: Svolge attività di monitoraggio e analisi sui livelli di sicurezza e fornisce supporto operativo ai soggetti essenziali e importanti per la gestione dei rischi.

Punto di Contatto Unico e Indipendenza

L'ACN assume inoltre la funzione strategica di **Punto di contatto unico NIS**. Tale ruolo è fondamentale per assicurare il coordinamento operativo a livello nazionale e garantire la cooperazione transfrontaliera con le istituzioni europee (Commissione UE ed ENISA[11]) e le autorità omologhe degli altri Stati membri.
Nello svolgimento delle proprie attività di vigilanza, l'Agenzia opera in regime di piena indipendenza. Questa autonomia è indispensabile per garantire l'imparzialità e la credibilità dei controlli, specialmente quando questi sono rivolti verso altre Pubbliche Amministrazioni.
Per sostenere l'operatività e l'attuazione delle funzioni previste dal decreto NIS2, è stato autorizzato uno stanziamento strutturale pari a **2 milioni di euro annui** a partire dall'anno 2025.

Per una trattazione esaustiva e tecnica riguardante i poteri specifici di vigilanza, le procedure ispettive e il dettaglio delle misure esecutive e sanzionatorie a carico dell'ACN, si rimanda all'approfondimento dedicato nel Capitolo 4.

[10] Organo dell'Unione Europea istituito con la Direttiva NIS e confermato dalla NIS2, con l'obiettivo di facilitare la cooperazione strategica tra gli Stati membri in materia di cybersicurezza. Riunisce rappresentanti degli Stati, della Commissione Europea, dell'ENISA e di altri enti competenti. Il gruppo elabora linee guida, raccomandazioni, best practice e coordina iniziative congiunte per l'attuazione armonizzata della direttiva.
[11] **European Union Agency for Cybersecurity**: Agenzia dell'UE per la cybersicurezza, supporta gli Stati membri nel coordinamento, nella gestione dei rischi e nell'attuazione tecnica della Direttiva NIS2.

2. NIS1 e NIS2 a confronto

La Direttiva NIS2 (UE 2022/2555) rappresenta un'evoluzione sostanziale rispetto alla precedente NIS1 (UE 2016/1148), la quale è stata formalmente abrogata con l'entrata in vigore del decreto di recepimento nazionale (D.lgs. n. 138/2024).
Mentre la normativa originaria si concentrava prevalentemente sulle grandi infrastrutture critiche, la nuova direttiva estende significativamente il perimetro d'azione per superare la frammentazione applicativa tra gli Stati membri.
L'obiettivo è istituire un quadro europeo uniforme e coordinato attraverso l'aggiornamento dei settori coinvolti e il potenziamento dei poteri di supervisione.

Inserendosi in un ecosistema normativo integrato con **GDPR** e **Regolamento DORA**[12], la NIS2 impone che le organizzazioni non si limitino alla prevenzione, ma dimostrino una concreta capacità di risposta e resilienza. Tale scenario richiede pertanto l'adozione di un approccio metodologico rigoroso e strutturato.

2.1 Principali Novità: NIS2 rispetto a NIS1

Le evoluzioni significative introdotte dalla NIS2 stabiliscono un salto qualitativo negli standard di *cyber-resilience*[13], con particolare enfasi sulla gestione del rischio e sulla responsabilità degli organi direttivi.

[12] Regolamento UE 2022/2554 sulla resilienza operativa digitale del settore finanziario; armonizza requisiti di sicurezza ICT, gestione incidenti, testing avanzato e risk management per banche, assicurazioni, fintech e fornitori ICT critici.
[13] Capacità di un'organizzazione di resistere, assorbire, rispondere e riprendersi da attacchi o guasti informatici garantendo continuità operativa, integrità dei servizi e rapidità di ripristino. Combina sicurezza, gestione del rischio, continuità operativa e capacità di adattamento.

Di seguito le principali differenze strutturali:

- **Ampliamento del Perimetro di Applicazione**
  La NIS1 operava una distinzione tra Operatori di Servizi Essenziali (OSE)[14] e Fornitori di Servizi Digitali (FSD)[15], spesso identificati con criteri disomogenei dai singoli Stati.
  La direttiva NIS2 introduce una nuova architettura di classificazione basata sulla criticità, eliminando la discrezionalità precedente. Viene formalizzata per la prima volta la distinzione tra due macrocategorie di soggetti, a cui corrispondono regimi di supervisione e sanzionatori differenti:

  - **Soggetti Essenziali (S.E.)**: Sono i soggetti a maggiore criticità, operanti in settori vitali, la cui interruzione avrebbe un impatto massimo sul funzionamento dell'economia, della società e della sicurezza nazionale
  - **Soggetti Importanti (S.I.**): Sono i soggetti a minore criticità (rispetto agli essenziali), operanti in settori critici ma comunque fondamentali per la catena del valore e la fornitura di servizi

  Questa distinzione definisce un perimetro che ora coinvolge oltre 20.000 organizzazioni tra medie e grandi imprese in 18 settori, oltre a specifiche categorie di Pubbliche Amministrazioni;

- **Gestione del Rischio (Risk-Based Approach)**
  Se la NIS1 si focalizzava spesso su misure di sicurezza standard e reattive, la NIS2 impone un cambio di paradigma verso una gestione proattiva e globale: viene introdotto l'approccio multirischio. Tale modello richiede di considerare congiuntamente le minacce digitali e quelle fisiche (come incendi, guasti elettrici o accessi non autorizzati), integrando la cybersecurity nella governance aziendale attraverso obblighi organizzativi, gestionali e procedurali;

- **Responsabilità Diretta degli Organi di Gestione**
  Nella NIS1 la responsabilità della sicurezza era spesso delegata ai reparti tecnici (IT/Security), adesso è invece diventata una responsabilità diretta, inalienabile e non delegabile degli organi di amministrazione e direttivi (Governance). I vertici aziendali

[14] Organizzazione individuata dalla direttiva NIS1 come erogatore di servizi fondamentali per la società e l'economia (es. energia, trasporti, sanità). La loro interruzione avrebbe impatto significativo sulla continuità dei servizi critici.
[15] Soggetti previsti dalla NIS1 che offrono servizi digitali quali cloud computing, motori di ricerca o piattaforme e-commerce. Avevano obblighi di sicurezza meno stringenti rispetto agli OSE.

possono essere chiamati a rispondere personalmente delle inadempienze e sono obbligati a seguire percorsi di formazione specifici;

. **Risposta e Ripristino agli Incidenti**
La normativa precedente non definiva con la medesima granularità gli obblighi relativi alla pianificazione della risposta e al ripristino, lasciando spazio a procedure eterogenee. Con la NIS2 si introduce l'obbligo di implementare un piano strutturato di risposta agli incidenti (*Incident Response Plan*[16]). La gestione degli incidenti e la continuità operativa (*Business Continuity*[17]) diventano elementi obbligatori delle misure di gestione del rischio (Articolo 24). Tali requisiti sono allineati alla funzione *RESPOND*[18] del *Framework Nazionale per la Cybersecurity e la Data Protection* (FNCSDP), che struttura le attività di analisi, mitigazione e comunicazione per limitare gli impatti degli eventi di sicurezza;

. **Inasprimento delle Sanzioni**
Il regime sanzionatorio della NIS1 era frammentato e spesso poco incisivo, è stato quindi armonizzato per risultare più efficace, proporzionato alla gravità della violazione e dissuasivo, per scoraggiare comportamenti negligenti. Le sanzioni sono amministrative, irrogate dall'Agenzia per la Cybersicurezza Nazionale (ACN) e prevedono massimali distinti che riflettono la nuova classificazione dei soggetti:

- **Soggetti essenziali**: sanzioni massime fino a **10 milioni di euro** o il **2%** del fatturato annuo mondiale, se superiore;

- **Soggetti importanti**: sanzioni massime fino a **7 milioni di euro** o l'**1,4%** del fatturato annuo mondiale, se superiore;

- **Pubbliche amministrazioni**: sono previste sanzioni specifiche che variano da **25.000** a **125.000 euro** per i soggetti essenziali, con riduzioni previste per i soggetti importanti.

[16] Documento operativo che definisce ruoli, responsabilità, processi e procedure per rilevare, analizzare, contenere, mitigare e risolvere un incidente informatico. Garantisce una risposta coordinata, tempestiva e ripetibile, riducendo l'impatto dell'evento e supportando le attività di ripristino e comunicazione.
[17] Insieme di strategie, piani e procedure che garantiscono il mantenimento o il rapido ripristino delle attività aziendali essenziali durante e dopo un'interruzione significativa.
[18] Funzione del Framework Nazionale (e del NIST CSF) dedicata alla gestione della risposta agli incidenti. Include attività strutturate come la pianificazione della risposta, la comunicazione, l'analisi, il contenimento, la mitigazione e il miglioramento continuo. L'obiettivo è limitare gli impatti di un evento di sicurezza attraverso azioni tempestive, coordinate e documentate.

2.2 Obblighi Normativi Fondamentali

La Direttiva NIS2 introduce requisiti di governance e operativi sensibilmente più rigorosi rispetto al passato, fondati sull'**Articolo 24** del decreto e sul principio di proporzionalità. Mentre in passato l'analisi dei rischi poteva essere un adempimento formale, la NIS2 pone al centro l'obbligo di condurre un'Analisi dei Rischi (*Risk Assessment*[19]) strutturata e basata su criteri oggettivi. Questo processo sistematico, riconducibile alla funzione ***IDENTIFY***[20], deve mappare gli asset critici e valutare impatto e probabilità, imponendo ai Soggetti Essenziali requisiti specifici come l'esecuzione di penetration test[21] annuali.

Le organizzazioni sono tenute inoltre ad implementare strategie concrete di mitigazione (*Risk Treatment*[22]) per ridurre sia la probabilità che l'impatto di potenziali incidenti. Le misure obbligatorie comprendono:

- Adozione di politiche di sicurezza dei sistemi;
- Procedure di continuità operativa (inclusi backup e disaster recovery[23] e gestione crisi);
- Uso di soluzioni di autenticazione a più fattori (*MFA*[24]) e crittografia.

È rivolta un'attenzione particolare anche alla sicurezza della catena di approvvigionamento (*Supply-Chain Security*[25]) e alle pratiche di igiene informatica di base, affiancate dalla formazione continua del personale.

---

[19] Processo strutturato che identifica minacce, vulnerabilità e asset critici, valutando probabilità e impatto dei rischi. Fornisce la base decisionale per definire priorità, controlli e misure di mitigazione in modo oggettivo e ripetibile.

[20] Funzione del Framework Nazionale/NIST che comprende attività di mappatura degli asset, analisi del contesto, classificazione delle risorse critiche e valutazione dei rischi. Ha lo scopo di comprendere cosa l'organizzazione deve proteggere e contro quali minacce.

[21] Attività tecnica avanzata che simula un attacco reale per identificare vulnerabilità sfruttabili. Eseguita da professionisti qualificati, consente di valutare l'efficacia dei controlli di sicurezza e di ridurre i rischi prima che vengano sfruttati da attori malevoli.

[22] Processo di selezione e implementazione delle misure di mitigazione atte a ridurre la probabilità o l'impatto del rischio. Può includere controlli tecnici, procedure, trasferimento assicurativo, accettazione o evitamento del rischio.

[23] Insieme di strategie, tecnologie e procedure volte a ripristinare sistemi e servizi IT dopo eventi gravi o disastrosi. Include RTO, RPO, piani di ripristino e test periodici per garantire la continuità dei servizi critici.

[24] Meccanismo di sicurezza che richiede l'uso combinato di almeno due fattori di autenticazione (conoscenza, possesso, biometria). Riduce significativamente il rischio di compromissione delle credenziali e accessi non autorizzati.

[25] Gestione dei rischi derivanti da fornitori, partner e terze parti che trattano o supportano servizi IT critici. Include valutazioni di sicurezza, requisiti contrattuali, monitoraggio continuo e verifica delle vulnerabilità nella catena di approvvigionamento.

Protezione della Supply Chain

Con la NIS1 si dava importanza principalmente al perimetro interno dell'organizzazione. La nuova normativa riconosce che le minacce spesso provengono da fornitori terzi meno protetti.

Diventa obbligatoria la considerazione della sicurezza della catena di approvvigionamento (Supply Chain Security), in quanto le aziende devono:

- Valutare le vulnerabilità specifiche di ogni fornitore diretto
- Considerare la qualità dei prodotti di sicurezza e le pratiche di sviluppo sicuro adottate dai propri partner

Segnalazione degli Incidenti

Sotto la NIS1, le tempistiche e le modalità di notifica variavano tra gli Stati membri, creando ritardi nella risposta coordinata. Con la normativa attualmente in vigore si introduce un meccanismo di notifica rapido, formalizzato e uniforme a livello europeo, pensato per permettere alle autorità competenti di intervenire tempestivamente e limitare la propagazione delle minacce:

Per i Soggetti Essenziali e Importanti vige l'obbligo di notificare al CSIRT Italia[26] (approfondito nel Capitolo 5 dedicato) qualsiasi incidente che abbia un impatto significativo, ovvero che causi gravi perturbazioni operative, perdite finanziarie o danni rilevanti a terzi . L'obbligo formale decorre dal **1° gennaio 2026** e segue una tempistica sequenziale rigorosa definita dall'**Articolo 25**:

- **Pre-notifica** (Early Warning): entro **24 ore** dalla conoscenza dell'evento, deve essere inviata segnalazione che indichi se l'incidente sia di origine dolosa e se abbia un potenziale impatto transfrontaliero;

- **Notifica Iniziale** (Initial Notification): entro **72 ore** segue la notifica contenente una valutazione della gravità, dell'impatto e, ove disponibili, gli indicatori di compromissione (IoC)[27] ;

[26] Struttura nazionale responsabile della gestione degli incidenti di sicurezza informatica. Fornisce supporto tecnico, coordina la risposta agli incidenti significativi, emette avvisi, raccomandazioni e riceve le notifiche obbligatorie previste dalla NIS2.

[27] Segnali tecnici che indicano la possibile presenza di un attacco o compromissione (es. hash di malware, indirizzi IP malevoli, comportamenti anomali). Utilizzati per rilevare, analizzare e mitigare gli incidenti di sicurezza.

- **Relazione Intermedia:** su richiesta del CSIRT, potrebbe essere necessaria per fornire aggiornamenti pertinenti durante la gestione dell'evento;

- **Relazione finale:** entro **un mese** dalla notifica, si deve descrivere dettagliatamente l'accaduto, individuare la causa radice (*root cause*) e illustrare le misure di attenuazione adottate.

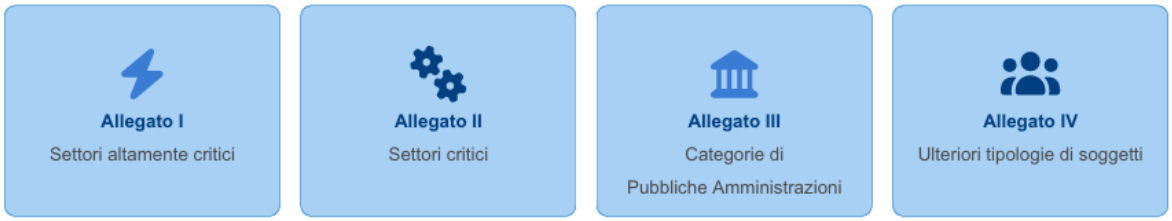
Collaborazione con le Autorità

Il rapporto con le istituzioni richiede una collaborazione attiva e bidirezionale, superando il concetto di semplice vigilanza. A fronte della segnalazione, il CSIRT Italia è tenuto a fornire un riscontro **entro 24 ore dalla pre-notifica**, offrendo orientamenti tecnici per la mitigazione. L'Agenzia per la Cybersicurezza Nazionale (ACN) esercita un ruolo di supervisione attiva: può impartire istruzioni vincolanti per gestire l'incidente e, qualora lo ritenga nell'interesse pubblico, ha la facoltà di informare la cittadinanza per prevenire ulteriori danni.

Comunicazione ACN / CSIRT Italia relativa agli obblighi di notifica

3. Ambiti di applicazione: Perimetro, Criteri di Classificazione e Individuazione dei Soggetti

Il Decreto Legislativo n. 138/2024 (recepimento NIS2) all'Articolo 3 indica con precisione, quali soggetti, sia pubblici che privati, rientrano nell'ambito di applicazione della direttiva. L'estensione dell'ambito di applicazione costituisce una delle novità più rilevanti, coinvolgendo un ecosistema vasto ed eterogeneo di oltre **20.000 organizzazioni identificate**. Tali soggetti sono individuati in base al ruolo strategico che svolgono nell'economia e nella società e sono raggruppati in **18 settori** di attività, che si dividono in **11 altamente critici** e **7 critici**.



3.1 Classificazione dei Soggetti Obbligati

La NIS2 introduce una classificazione binaria dei soggetti destinatari degli obblighi, basata sulla criticità del settore e sul loro impatto potenziale.

Categoria	Criticità	Riferimento Principale
Soggetti Essenziali	Maggiore criticità	Allegato I (Altamente Critici)
Soggetti Importanti	Minore criticità	Allegato II (Critici)

La distinzione tra Essenziali e Importanti è fondamentale, poiché determina un regime di obblighi e un livello di sanzioni differenziati. Sebbene entrambi debbano adottare misure di sicurezza di base, i Soggetti Essenziali hanno l'obbligo di implementare un numero maggiore di misure (43 misure e 116 requisiti totali) rispetto ai Soggetti Importanti (37 misure e 87 requisiti totali). Inoltre, i soggetti Essenziali sono sottoposti a un regime sanzionatorio più severo (Capitolo 2.1).

3.2 Individuazione dei Settori Coinvolti (Allegati I e II)

La collocazione di un'organizzazione negli Allegati del decreto rappresenta il primo passo per determinarne la criticità intrinseca.

Settori Altamente Critici: Comprendono gli ambiti fondamentali per la tenuta del sistema del Paese. I soggetti operanti in questi settori, qualora superino le soglie dimensionali, acquisiscono automaticamente lo status di Soggetti Essenziali.
L'elenco comprende in modo esaustivo :

- **Energia:** Include l'intera filiera dell'energia elettrica (produzione e distribuzione), il teleriscaldamento e teleraffrescamento, il settore petrolifero, il gas naturale e la produzione e distribuzione di idrogeno;
- **Trasporti:** Copre il trasporto aereo, ferroviario, marittimo e per vie d'acqua interne, nonché il trasporto su strada e la relativa logistica;
- **Settore Finanziario:** Include sia il settore bancario tradizionale sia le infrastrutture dei mercati finanziari;
- **Sanità:** Comprende i prestatori di assistenza sanitaria, i laboratori di riferimento dell'UE, la ricerca e fabbricazione di prodotti farmaceutici e le Aziende Sanitarie Locali;
- **Risorse Idriche:** Include la fornitura e distribuzione di acqua potabile e la gestione delle acque reflue urbane;
- **Infrastrutture Digitali:** Un comparto vasto che include fornitori di servizi di *cloud computing*[28], servizi di *data center*[29], reti di distribuzione dei contenuti (CDN)[30], prestatori di servizi fiduciari e reti pubbliche di comunicazione;
- **Spazio:** Operatori di infrastrutture terrestri che supportano i servizi spaziali.

[28] Modello di erogazione di servizi IT (es. server, storage, applicazioni) tramite infrastrutture remote accessibili via Internet, con elevata scalabilità, disponibilità e flessibilità operativa.
[29] Struttura fisica che ospita sistemi informatici, server e apparati di rete necessari per l'erogazione di servizi digitali, garantendo sicurezza fisica, ridondanza e continuità operativa.
[30] Rete distribuita di nodi e server progettata per fornire rapidamente contenuti digitali (es. siti web, video, file) agli utenti finali, migliorando prestazioni, resilienza e disponibilità.

Settori Critici: I soggetti operanti in questi ambiti, pur essendo fondamentali per l'economia, sono considerati a minore criticità relativa e vengono classificati come Soggetti Importanti (salvo eccezioni). L'elenco include :

- **Servizi Postali e Gestione Rifiuti:** Servizi di corriere, postali e operatori del trattamento e smaltimento rifiuti;
- **Chimica:** Fabbricazione, produzione e distribuzione di sostanze chimiche;
- **Agroalimentare:** Produzione, trasformazione e distribuzione di alimenti all'ingrosso;
- **Manifatturiero:** Fabbricazione di dispositivi medici (inclusi diagnostici in vitro), prodotti informatici, elettronici e ottici, apparecchiature elettriche, macchinari, autoveicoli, rimorchi e altri mezzi di trasporto;
- **Fornitori di Servizi Digitali:** Operatori di mercati online, motori di ricerca e piattaforme di *social networking*;
- **Ricerca:** Istituti di ricerca (con esclusione di quelli a fini didattici, salvo specifiche eccezioni).

3.3 Criteri di Applicazione in Base alla Dimensione (Size-Cap Rule)

L'applicazione della NIS2 è generalmente subordinata a un criterio di identificazione omogeneo basato sulla dimensione (*size-cap rule*[31]).

I soggetti dei settori Allegato I e Allegato II rientrano nel perimetro solo se superano i massimali stabiliti per le piccole imprese. l'organizzazione quindi deve:

- Occupare **più di 50 persone** (dipendenti)
- Realizzare un fatturato annuo **superiore a 10 milioni di euro**

Conseguentemente a ciò, sono interessate per di più le medie e grandi imprese, ma possono comunque esserci delle eccezioni in casi particolari

[31] Criterio dimensionale della Direttiva NIS2 che determina l'inclusione di un'organizzazione nel perimetro normativo quando supera i limiti delle piccole imprese, cioè più di 50 dipendenti e oltre 10 milioni di euro di fatturato annuo.

Indipendentemente dalle Dimensioni

Alcune categorie di soggetti sono infatti incluse nel perimetro della NIS2 a prescindere dalle loro dimensioni:

1. **Pubbliche Amministrazioni (PA):** Le categorie di PA elencate nell'Allegato III sono soggette alla NIS2, indipendentemente dal numero di dipendenti o dal fatturato. In particolare:
    - **Amministrazioni Centrali:** Organi costituzionali, Presidenza del Consiglio, Ministeri, Agenzie fiscali e Autorità amministrative indipendenti;
    - **Amministrazioni Regionali:** Regioni e Province autonome;
    - **Amministrazioni Locali specifiche:** Città metropolitane, Comuni con popolazione superiore a 100.000 abitanti, Comuni capoluoghi di regione e Aziende sanitarie locali.

2. **Soggetti Altamente Critici per la Rete:** Fornitori di reti pubbliche di comunicazione elettronica, prestatori di servizi fiduciari, gestori di registri di nomi di dominio di primo livello e fornitori di servizi DNS;

3. **Soggetti Già Identificati:** Soggetti già identificati come operatori di servizi essenziali (ose) ai sensi della precedente NIS1 o individuati come **soggetti critici** per ragioni di importanza nazionale o sistemica.

Sono previste anche ulteriori tipologie di soggetti nell'Allegato IV, che includono:

- istituti di istruzione che svolgono attività di ricerca;
- soggetti che forniscono servizi di trasporto pubblico locale;
- soggetti che svolgono attività di interesse culturale e le società *in house*[32] ;
- società partecipate[33] e società a controllo pubblico[34].

[32] Società partecipata o controllata da una Pubblica Amministrazione che opera come articolazione interna dell'ente pubblico e svolge attività di interesse generale per conto dell'amministrazione.
[33] Società in cui una Pubblica Amministrazione detiene una quota del capitale sociale, esercitando un'influenza più o meno significativa sulla gestione e sugli indirizzi strategici.
[34] Società in cui una o più Pubbliche Amministrazioni detengono la maggioranza dei voti esercitabili in assemblea o hanno il potere di nominare la maggioranza degli amministratori, esercitando quindi un controllo diretto sulla gestione.

3.4 Processo di Identificazione e Comunicazione Formale

I destinatari effettivi della normativa, si formalizzano attraverso un processo di censimento gestito dall'Agenzia per la Cybersicurezza Nazionale (ACN), articolato in fasi annuali precise:

1. **Registrazione Iniziale**: I soggetti potenzialmente interessati devono registrarsi o aggiornare la propria registrazione sulla piattaforma digitale ACN annualmente, nel periodo compreso tra il **1° gennaio** e il **28 febbraio** .
   Tale obbligo vige sia per chi si auto-identifica, sia per i soggetti che ricevono una specifica Notifica di Individuazione[35] da parte dell'Autorità, i quali sono tenuti a procedere al censimento a seguito della ricezione. Per effettuare l'iscrizione e accedere alla piattaforma, è necessario fare riferimento al portale ufficiale dei servizi ACN (https://www.acn.gov.it/portale/nis/registrazione) autenticandosi tramite identità digitale;
2. **Elaborazione dell'Elenco:** Entro il **31 marzo** di ogni anno, ACN in collaborazione con le Autorità di Settore NIS, redige l'elenco ufficiale dei soggetti essenziali e dei soggetti importanti. Le Autorità di Settore hanno un ruolo cruciale nel supportare ACN, anche nella verifica dell'elenco;
3. **Comunicazione Formale:** L'ACN comunica ai soggetti registrati l'esito del processo, che può consistere nell'*inserimento*, nella *permanenza* o nell'*espunzione* dall'elenco dei soggetti NIS . Ai soggetti inclusi viene comunicato un **codice identificativo univoco** per facilitare le interlocuzioni.

L'inserimento formale nell'elenco è la condizione che fa scattare l'obbligo di conformità. La NIS2 prevede inoltre la possibilità per l'ACN, di effettuare **verifiche di coerenza** a campione sulle informazioni fornite dai soggetti nella fase di registrazione, in collaborazione alle Autorità di settore.

[35] Comunicazione formale inviata dall'Agenzia per la Cybersicurezza Nazionale (ACN) con cui un soggetto viene identificato come potenzialmente rientrante nel perimetro NIS2 e invitato a procedere alla registrazione o all'aggiornamento dei propri dati ai fini del censimento ufficiale.

4. Autorità nazionale competente NIS: Ruolo, Poteri di Supervisione e Sanzionatori

Ferme restando le funzioni istituzionali e di governance già delineate nel Capitolo 1, il Decreto Legislativo n. 138/2024 attribuisce all'Agenzia per la Cybersicurezza Nazionale (ACN) poteri operativi per garantire l'effettiva applicazione della norma. L'attività di controllo dell'Autorità è sostanziale in quanto essa monitora e valuta il rispetto degli obblighi da parte dei soggetti essenziali e importanti, nonché i relativi effetti sulla sicurezza dei sistemi informativi e di rete. Tale azione di vigilanza deve essere esercitata nel rispetto di tre principi cardine che la rendano effettiva, proporzionata e dissuasiva.

4.1 Autonomia Operativa e Indipendenza

È fondamentale sottolineare che l'esercizio della vigilanza si fonda sulla garanzia di piena indipendenza. L'ACN deve poter svolgere i suoi controlli in modo autonomo, senza subire pressioni o influenze, nemmeno da parte delle stesse amministrazioni pubbliche che è chiamata a vigilare. Sebbene sia l'Autorità di controllo (ACN) che i soggetti controllati (PA) facciano parte dello Stato, l'Agenzia opera in regime di autonomia operativa. Tale indipendenza è ritenuta essenziale per garantire l'imparzialità e la credibilità del sistema sanzionatorio e di controllo*: il controllore non deve essere in alcun modo influenzato dal controllato* .

Poteri Ispettivi Specifici

Usufruendo della sua autonomia, l'Autorità può esercitare i seguenti poteri di:

- **Monitoraggio e Analisi**: Attività continuativa di controllo sui flussi informativi e sulle notifiche ricevute;
- **Audit e Scansioni:** L'Autorità può richiedere o effettuare direttamente scansioni di sicurezza sui sistemi e audit mirati per verificare la conformità tecnica;
- **Verifiche Ispettive**: Potere di accedere ai locali, ai documenti e ai dati dei soggetti vigilati per condurre ispezioni in loco o verifiche documentali a distanza.

4.2 Poteri di Esecuzione: Diffide e Istruzioni

Qualora vengano accertate irregolarità o il mancato rispetto degli obblighi, l'Autorità interviene con misure di esecuzione dirette[36]. Il principale strumento correttivo è la **Diffida Formale**: l'ACN intima al soggetto di porre fine alla violazione e di conformarsi alle disposizioni entro termini ragionevoli e proporzionati. Nella diffida, l'Autorità indica le modalità specifiche per l'adeguamento e richiede aggiornamenti costanti sullo stato di attuazione delle misure.

Prima dell'adozione di provvedimenti sanzionatori o restrittivi, è garantita una procedura tramite la quale ACN comunica le conclusioni preliminari al soggetto interessato, concedendo un termine non inferiore a **15 giorni** per presentare osservazioni difensive .

4.3Conseguenze Operative e Sospensione delle Attività

Per i soli Soggetti Essenziali, la normativa introduce conseguenze che vanno oltre la sanzione economica e possono impattare sulla continuità operativa del business. In caso di persistente inottemperanza alle diffide, l'Autorità ha il potere di intervenire in maniera incisiva, disponendo (o richiedendo agli organismi competenti) la sospensione temporanea di certificazioni o autorizzazioni relative ad una parte o alla totalità dei servizi e delle attività pertinenti svolti dal soggetto essenziale.

Questa sospensione rimane valida finché il soggetto non adotta le misure necessarie per correggere le carenze evidenziate nella diffida e conformarsi agli obblighi di sicurezza

4.4 Criteri di Valutazione del Regime Sanzionatorio

L'esercizio del potere sanzionatorio non è automatico ma ponderato sulla base di un rigoroso **Criterio di Proporzionalità**. L'Autorità valuta caso per caso la sanzione considerando parametri oggettivi e soggettivi, tra cui :

- Gravità e durata temporale della violazione;
- Eventuale negligenza e precedenti del soggetto;
- Danno materiale o immateriale causato (inclusi impatti economici o sui dati);
- Livello di collaborazione dimostrato con l'Autorità;
- Misure proattive adottate per attenuare il danno o l'adesione a codici di condotta certificati.

[36] Interventi applicati dall'Agenzia per la Cybersicurezza Nazionale (ACN) per imporre l'adempimento degli obblighi NIS2 in caso di violazioni accertate, comprendendo azioni correttive immediate come la diffida formale e ulteriori provvedimenti necessari a ripristinare la conformità (Art. 37).

È fondamentale notare che l'utilizzo dei poteri di esecuzione (come le diffide o le istruzioni vincolanti) non esclude l'accertamento delle violazioni e l'applicazione delle relative sanzioni amministrative pecuniarie: i due procedimenti possono infatti coesistere.

Reiterazione

In caso di violazioni ripetute (reiterazione specifica), la sanzione può raddoppiare. In caso di violazioni diverse (reiterazione non specifica), si applica la sanzione per la violazione più grave aumentata fino al triplo. Anche il ritardo o l'omissione nella registrazione comporta l'aumento al triplo della sanzione base.

Strumenti Deflattivi

Al fine di ridurre il contenzioso legale e favorire la rapida regolarizzazione, sono previste modalità semplificate come l'Invito a conformarsi (per infrazioni minori), l'estinzione del procedimento tramite pagamento ridotto e la possibilità di non procedere alla pubblicazione della sanzione.

5. CSIRT Italia e Gestione Operativa degli Incidenti

All'interno dell'architettura nazionale di cybersicurezza disegnata dalla NIS2, la gestione tecnica della crisi e la risposta operativa agli attacchi sono demandate al **CSIRT Italia** (Computer Security Incident Response Team). Istituito presso l'Agenzia per la Cybersicurezza Nazionale (ACN), il CSIRT rappresenta l'interfaccia tecnica unica per tutti i soggetti rientranti nel perimetro normativo, operando in conformità con quanto stabilito dall'Articolo 15 del decreto e dal quadro regolatorio precedente (D.Lgs. 65/2018 e DPCM 8 agosto 2019).

5.1 Compiti e Funzioni Operative

Il CSIRT Italia svolge funzioni cruciali per la resilienza complessiva del Paese, applicando un approccio basato sul rischio per stabilire le priorità di intervento.

Le sue attività non si limitano alla reazione, ma coprono l'intero spettro della sicurezza operativa:

- **Monitoraggio e Analisi Dinamica**: L'organo sorveglia costantemente il panorama delle minacce informatiche a livello nazionale. Non si limita alla raccolta dati, ma fornisce analisi dinamiche dei rischi e degli incidenti, elaborando una consapevolezza situazionale (*situational awareness*) che permette di anticipare le tendenze di attacco e comprendere lo stato di salute del cyberspazio nazionale;
- **Allerta e Divulgazione**: Emette preallarmi, allerte tecniche e bollettini di sicurezza verso i soggetti interessati. L'obiettivo è divulgare informazioni su vulnerabilità critiche e minacce in tempo "prossimo al reale", permettendo alle organizzazioni di elevare le difese preventivamente prima che una minaccia si concretizzi;
- **Supporto Tecnico e Risposta**: In caso di incidente significativo, il CSIRT fornisce assistenza attiva ai soggetti essenziali e importanti. Ciò include un riscontro tempestivo alla notifica e, su richiesta, la fornitura di orientamenti tecnici per l'attuazione delle misure di mitigazione. Il team ha inoltre la capacità di raccogliere e analizzare dati forensi per identificare le cause radice dell'attacco (*root cause*);
- **Infrastruttura Resiliente**: Per garantire l'operatività anche in scenari di crisi sistemica, il CSIRT dispone di locali sicuri e di sistemi informativi ridondanti, assicurando un alto livello di disponibilità dei canali di comunicazione per essere sempre contattabile dai soggetti vigilati.

5.2 Attività Proattive: Scansioni e Divulgazione Vulnerabilità

Oltre alla risposta reattiva, il CSIRT Italia esercita funzioni preventive fondamentali delineate dettagliatamente nel decreto.

Scansioni delle Reti

Il CSIRT ha la facoltà di effettuare due tipologie di controlli tecnici sui sistemi dei soggetti NIS:

- **Scansioni su richiesta**: Analisi approfondite dei sistemi informativi e di rete di un soggetto, eseguite su specifica istanza dell'interessato per rilevare vulnerabilità potenziali;
- **Scansioni non intrusive**: Verifiche d'ufficio sui sistemi accessibili al pubblico (es. siti web, IP esposti su internet) per individuare configurazioni insicure o vulnerabilità note. In questo caso, il CSIRT informa tempestivamente il soggetto interessato senza impattare sull'operatività dei servizi.

Divulgazione delle Vulnerabilità

Il CSIRT agisce come coordinatore nazionale per la Coordinated Vulnerability Disclosure[37] (CVD, Articolo 16). In questo ruolo, funge da "intermediario di fiducia" tra gli interessati e i produttori di software o fornitori di servizi ICT[38]. Il suo compito è facilitare l'interazione, negoziare i tempi di correzione e divulgazione pubblica della vulnerabilità e, qualora richiesto, garantire l'anonimato del segnalante.

5.3 Ciclo di Risposta e la Gestione delle Notifiche

La NIS2 impone l'adozione di un piano strutturato di risposta agli incidenti (allineato alla Funzione *RESPOND*[39] del *Framework Nazionale FNCSDP*), che si attiva formalmente con la notifica al CSIRT.
Questo ciclo è un processo sequenziale mirato a ridurre l'impatto e garantire la continuità operativa, articolandosi in fasi precise:

1. **Preparazione**: Definizione a freddo di ruoli, responsabilità e procedure di escalation;
2. **Identificazione**: Conferma dell'incidente e valutazione dell'impatto reale;
3. **Contenimento**: Isolamento dei sistemi compromessi per limitare i danni e acquisire evidenze digitali;
4. **Eradicazione e Ripristino**: Rimozione della minaccia (es. malware) e riattivazione sicura dei servizi;
5. **Lessons Learned**: Analisi post-incidente per migliorare le capacità future.

Classificazione degli Incidenti Significativi

L'obbligo di attivazione riguarda gli incidenti significativi, definiti come eventi che causano gravi perturbazioni operative, perdite finanziarie o danni rilevanti a terzi. La normativa introduce una distinzione cruciale per i soli Soggetti Essenziali, che sono tenuti a monitorare e notificare anche la quarta categoria di incidente, identificata con il **codice IS-4 (**Accesso non autorizzato o abuso dei privilegi concessi). Tale requisito impone l'implementazione di parametri di

[37] Procedura strutturata che consente di segnalare in modo sicuro e coordinato vulnerabilità di sicurezza ai produttori o ai gestori dei sistemi, garantendo tempi concordati per la correzione e una divulgazione responsabile per evitare abusi prima della risoluzione.
[38] Insieme di servizi relativi alle tecnologie dell'informazione e della comunicazione, comprendenti infrastrutture digitali, sistemi informativi, software, reti, piattaforme cloud e attività di supporto tecnico e gestionale.
[39] Funzione del *FNCSDP* che definisce le attività necessarie per gestire un incidente di sicurezza informatica, coordinando le azioni di risposta, contenimento, comunicazione e ripristino al fine di limitare gli impatti operativi e garantire la resilienza dei servizi.

detection avanzati per sorvegliare le attività interne (*insider threat*[40]), un onere non richiesto ai Soggetti Importanti.

Codice	Descrizione	Soggetti Importanti (S.I)	Soggetti Essenziali (S.E)
IS-1	Perdita di **Riservatezza** (con impatto verso l'esterno, di dati di proprietà o sotto controllo)	✓	✓
IS-2	Perdita di **Integrità** (con impatto verso l'esterno, di dati di proprietà o sotto controllo)	✓	✓
IS-3	Violazione dei **Livelli di Servizio** attesi (SLA)	✓	✓
IS-4	**Accesso non autorizzato** o abuso dei privilegi concessi (es. *insider threat*)	✗	✓

Il processo di notifica (obbligatorio dal **1° gennaio 2026**) segue una timeline rigida, pensata per consentire al CSIRT di attivare rapidamente le misure di contenimento nazionale (vedi Capitolo 2.2)

5.4 Notifiche Volontarie e Comunicazione Pubblica

Il decreto nell'Art. 26 incentiva la collaborazione attraverso le *Notifiche Volontarie*: i soggetti possono segnalare incidenti non significativi, minacce informatiche o "quasi-incidenti" (*near-miss*). Tali segnalazioni, pur non comportando obblighi aggiuntivi, vengono trattate dal CSIRT (con priorità subordinata a quelle obbligatorie) per arricchire la base di conoscenza comune.

Parallelamente, la gestione della crisi implica doveri di comunicazione verso l'esterno, in quanto i soggetti devono informare i destinatari dei servizi qualora un incidente impatti sulla fornitura, suggerendo eventuali azioni correttive. L'ACN si riserva inoltre il potere di informare il pubblico generale riguardo a un incidente in corso qualora ciò sia necessario per prevenire ulteriori danni o sia ritenuto di interesse pubblico, bilanciando la trasparenza con la tutela reputazionale dell'operatore.

[40] Rischio derivante da individui interni all'organizzazione (dipendenti, collaboratori, fornitori con accesso autorizzato) che, intenzionalmente o accidentalmente, compromettono la sicurezza dei sistemi informativi attraverso l'abuso dei privilegi concessi o comportamenti non conformi alle policy aziendali.

5.5 Referente CSIRT

Per rendere efficace il dialogo operativo, la Determinazione ACN n. 333017/2025 ha introdotto l'obbligo di designare una figura specifica: il **Referente CSIRT**. Questa figura deve essere nettamente distinta dal Punto di Contatto (che ha valenza amministrativa). Il Referente CSIRT è una persona fisica dotata di competenze tecniche in materia di sicurezza e gestione incidenti e di una profonda conoscenza dell'infrastruttura IT dell'organizzazione. Il suo compito esclusivo è gestire tecnicamente le notifiche e interagire con il CSIRT Italia durante le crisi. La designazione del Referente (e dei suoi sostituti per garantire continuità) deve avvenire tramite il Portale ACN in finestre temporali dedicate, previste tra il 20 novembre e il 31 dicembre dell'anno di riferimento.

Link al portale: https://www.acn.gov.it/portale/nis/registrazione

6. Il Punto di contatto

Nell'architettura di implementazione della NIS2, la comunicazione tra i soggetti obbligati e le istituzioni non è affidata a canali informali, ma viene strutturata attraverso una figura cardine: il **Punto di Contatto**. È necessario operare una distinzione preliminare: a livello nazionale l'ACN funge da *Punto di Contatto Unico* verso le istituzioni europee, a livello organizzativo ogni Soggetto Essenziale o Importante deve designare una specifica persona fisica che agisca da interfaccia ufficiale verso l'Autorità Nazionale. Tale figura rappresenta l'unico canale legittimato ad accedere al Portale ACN e ai Servizi NIS per curare l'attuazione delle disposizioni previste dal decreto, per conto del soggetto stesso. Punto di Contatto e Punto di Contatto Unico sono quindi due figure ben distinte.

6.1 Natura del Ruolo e Responsabilità

Le funzioni principali del Punto di Contatto sono prettamente operative: egli accede alla piattaforma, effettua la registrazione formale dell'ente e gestisce le interlocuzioni con l'ACN . È cruciale, tuttavia, delineare correttamente il perimetro delle sue responsabilità.

La normativa specifica che il Punto di Contatto **non eredita la responsabilità legale** per gli adempimenti o per le eventuali violazioni del decreto. Egli ha il compito di "curare" l'attuazione delle norme, agendo come braccio operativo, ma la responsabilità giuridica e sanzionatoria rimane agli Organi di Amministrazione, Direttivi e alle persone fisiche con poteri decisionali dell'organizzazione .

6.2 Distinzione tra Punto di Contatto e Referente CSIRT

Un aspetto critico per la corretta *compliance* è la distinzione tra il Punto di Contatto e il Referente CSIRT. Sebbene siano figure complementari nel flusso di gestione della sicurezza, i loro perimetri d'azione e le competenze richieste sono nettamente separati, come chiarito dalle linee guida operative ufficiali:

- **Il Punto di Contatto** è la figura responsabile dell'interlocuzione istituzionale con l'Autorità (ACN). Il suo compito è garantire il flusso informativo tra l'azienda e l'ACN, facilitare la conformità normativa e assicurare che le disposizioni della direttiva siano attuate correttamente verso i vertici aziendali. Operativamente, è il Punto di Contatto che si occupa della rilevazione degli eventi e delle vulnerabilità a livello organizzativo e ha la responsabilità diretta di designare il Referente CSIRT;
- **Il Referente CSIRT** è una figura tecnica, incaricata di interfacciarsi operativamente con il CSIRT Italia. A differenza del Punto di Contatto, il Referente CSIRT gestisce concretamente le notifiche degli incidenti di sicurezza secondo le tempistiche stringenti previste (ampiamente descritte nel Capitolo 2.2). Il suo ruolo è supportare l'analisi degli eventi, validare tecnicamente le segnalazioni, gestire le procedure *di Incident Response*[41] e curare l'aggiornamento costante dei processi di sicurezza.

In sintesi, il flusso di comunicazione amministrativa e la rilevazione iniziale sono in capo al Punto di Contatto, mentre la gestione tecnica operativa e la notifica di dettaglio al CSIRT Italia sono prerogativa del Referente CSIRT.

Passaggio	Punto di Contatto	Referente CSIRT
Rilevazione eventi e vulnerabilità	**SI**	Supporta se coinvolto
Flusso di comunicazione con ACN	**SI**	NO (solo operatività tecnica)
Designazione referente CSIRT	SI (responsabilità)	**NO**
Notifica e gestione incidenti con CSIRT Italia	NO (non operativo)	SI (notifica operativa)
Supporto operativo e validazione tecnica	**NO**	**SI**

[41] Processo strutturato che comprende le attività di rilevazione, analisi, contenimento, eradicazione e ripristino in seguito a un incidente di sicurezza, con l'obiettivo di limitarne l'impatto e garantire la continuità operativa.

6.3 Criteri di Designazione e Flessibilità

La normativa impone che il Punto di Contatto sia identificato necessariamente in una persona fisica; non è dunque possibile designare una funzione generica (es. "Ufficio IT"). Per assicurare la massima aderenza alla realtà operativa, il legislatore ha previsto criteri di eleggibilità flessibili. Le funzioni possono essere assunte da :

- Il Legale Rappresentante[42] del soggetto NIS;
- Un Procuratore Generale[43], purché censito nel registro delle imprese;
- Un Dipendente delegato formalmente dal Legale Rappresentante.

Deleghe Infragruppo e Pubblica Amministrazione

Per i gruppi societari complessi[44], è prevista una flessibilità organizzativa: il ruolo può essere ricoperto da un dipendente di un'altra impresa del gruppo, a condizione che anche quest'ultima rientri nel perimetro di applicazione della NIS2 e vi sia una delega esplicita da parte del Legale Rappresentante dell'impresa interessata. Analogamente, per le Pubbliche Amministrazioni, è ammessa la designazione di personale che presta servizio o è dipendente di un'altra PA soggetta al Decreto (es. in scenari di servizi condivisi[45]), previa autorizzazione formale dell'amministrazione di appartenenza.
In caso di avvicendamento della figura designata, gli organi direttivi hanno l'obbligo di provvedere senza ingiustificato ritardo alla nomina del nuovo titolare e al suo censimento sul portale.

6.4 Sostituto Punto di Contatto

Per garantire la continuità operativa e la reperibilità in ogni circostanza, la normativa introduce la figura del **Sostituto Punto di Contatto**. Si tratta di una persona fisica distinta dal titolare principale, designata con le medesime modalità, che ha il compito di supportare il Punto di Contatto e di vicariarlo in caso di necessità. Il Sostituto dispone di pieni poteri operativi sulla piattaforma digitale e può interloquire direttamente con ACN, con un'unica eccezione tecnica: non può effettuare la prima registrazione dell'ente (compito esclusivo del titolare) .

---

[42] Il soggetto che, per legge o statuto, ha il potere di rappresentare l'organizzazione verso terzi e assumere decisioni vincolanti, inclusa la responsabilità formale per gli adempimenti NIS2.
[43] Figura dotata di poteri di rappresentanza conferiti tramite procura e registrati nel Registro delle Imprese, abilitata a compiere atti giuridici per conto dell'organizzazione.
[44] Insieme di società collegate da rapporti di controllo o coordinamento che operano come gruppo integrato, con strutture organizzative e operative distribuite su più entità giuridiche.
[45] Modello organizzativo in cui più amministrazioni o società utilizzano strutture, personale o funzioni comuni per svolgere attività operative o gestionali, al fine di ottimizzare risorse e competenze.

Termini di Designazione ed Eccezioni

La nomina del Sostituto è soggetta a una scadenza tassativa, va fatta entro il **31 maggio** dell'anno in cui è avvenuto l'inserimento del soggetto nell'elenco NIS. L'unica deroga a tale obbligo è prevista per le organizzazioni in cui il Punto di Contatto coincide con l'unica persona fisica operante (es. imprese individuali o microstrutture), situazione in cui la nomina di un sostituto risulterebbe materialmente impossibile.

6.5 Procedure Operative di Registrazione e Convalida

L'operatività del Punto di Contatto si esplica attraverso il Portale dei Servizi ACN (attivo per l'autenticazione dal **1° dicembre 2024**). Il processo di accreditamento e dichiarazione segue un protocollo di verifica rigoroso e si articola nelle seguenti fasi tecniche:

1. **Autenticazione** e **Associazione:** L'accesso al portale avviene esclusivamente tramite identità digitale (SPID). Per associare il Punto di Contatto al soggetto è necessario indicare il Codice Fiscale o, per le Pubbliche Amministrazioni, il codice dell'Indice dei domicili digitali (IPA)[46]. Il sistema richiede di verificare la denominazione, l'indirizzo e i recapiti visualizzati.

2. **Caricamento del Titolo Giuridico:** Qualora il Punto di Contatto non coincida con il Legale Rappresentante o un Procuratore Generale già censito, il sistema richiede obbligatoriamente il caricamento del titolo giuridico (es. delega formale) che lo abilita ad operare per conto del soggetto nel contesto NIS.

3. **Compilazione della Dichiarazione**: Una volta accreditato, il Punto di Contatto deve compilare una dichiarazione dettagliata suddivisa in 4 sezioni fondamentali:
   - Contesto
   - Caratterizzazione
   - Tipologie di soggetto
   - Autovalutazione

4. **Convalida e Trasmissione:** Al termine della compilazione, dopo aver preso visione del riepilogo e accettato le clausole di responsabilità, il processo si conclude con l'invio di un link di richiesta di convalida al Domicilio Digitale (PEC) del soggetto stesso. Solo

[46] Identificativo univoco attribuito a ogni Pubblica Amministrazione all'interno dell'Indice dei domicili digitali della PA (IPA), il registro ufficiale nazionale che raccoglie indirizzi, contatti e domicili digitali delle amministrazioni italiane.

dopo questa conferma l'associazione è attiva e una copia della dichiarazione viene trasmessa alla PEC dell'ente .

6.6 Gestione delle Utenze: Operatori e Segreteria

Per le organizzazioni più strutturate, il Punto di Contatto ha la facoltà di delegare parte dell'operatività quotidiana invitando sulla piattaforma altri utenti con profili limitati:

- **Ruolo Operatore**: Utenti abilitati alla compilazione tecnica delle informazioni;
- **Ruolo Segreteria**: Utenti con funzioni di supporto per la gestione anagrafica.

È fondamentale sottolineare che tali figure di supporto non possono effettuare azioni che determinano la trasmissione di comunicazioni aventi valore legale (come il perfezionamento di adempimenti o l'invio di notifiche formali all'ACN), prerogativa che resta in capo al Punto di Contatto e al suo Sostituto. Il sistema garantisce infine autonomia nella gestione delle utenze in quanto tutti gli utenti possono:

- **Annullare** la propria associazione;
- **Disabilitare** l'utenza;
- **Ridurre** il proprio ruolo (es. da Punto di Contatto a semplice operatore) in base alle evoluzioni organizzative interne.

7. Governance e Responsabilità degli Organi di Vertice

Il recepimento della Direttiva NIS2 segna un punto di svolta storico nella gestione della sicurezza delle informazioni: la cybersicurezza cessa di essere una funzione prettamente tecnica delegata ai dipartimenti IT, diventando una responsabilità di *Governance* diretta, inalienabile e non delegabile. Gli organi di amministrazione e direttivi (OAD)[47] dei soggetti essenziali e importanti sono chiamati per legge ad assumere un ruolo attivo nella gestione del rischio, elevando la protezione degli asset digitali[48] a priorità strategica del Consiglio di Amministrazione[49].

[47] Strutture apicali che esercitano poteri decisionali e di supervisione sull'ente, comprendendo amministratori, direttori e componenti dei vertici responsabili della gestione strategica e del controllo.
[48] Risorse informative e tecnologiche di un'organizzazione, quali dati, applicazioni, infrastrutture, sistemi, reti e servizi digitali necessari al funzionamento operativo.
[49] Organo collegiale che esercita la funzione di governo strategico dell'organizzazione, definisce gli indirizzi generali e supervisiona l'operato della direzione esecutiva.

7.1 Ruolo Attivo: Approvazione e Supervisione

Il nuovo assetto normativo impone ai vertici aziendali di non limitarsi al sostegno finanziario della sicurezza, ma di guidare e controllare i processi (in linea con la funzione *GOVERN* del Framework Nazionale). Gli obblighi specifici in capo agli organi di vertice includono :

- **Approvazione delle Misure:** Gli organi di amministrazione devono approvare formalmente le modalità di implementazione delle misure di gestione dei rischi (tecniche, operative e organizzative) adottate dall'ente ai sensi dell'Articolo 24. Tale approvazione non è un visto formale, ma un'assunzione di responsabilità sulla loro adeguatezza rispetto al contesto di minaccia;
- **Supervisione Continua:** I vertici hanno il dovere di sovrintendere all'effettiva applicazione degli obblighi normativi, monitorando costantemente l'efficacia delle strategie difensive (*Oversight*)[50];
- **Responsabilità Diretta:** La norma stabilisce inequivocabilmente che gli organi di vertice sono responsabili per le violazioni del decreto, sancendo il passaggio definitivo della cybersecurity nell'ambito dell'*Enterprise Risk Management* (ERM).

7.2 Flusso Informativo

Affinché gli organi di vertice possano esercitare efficacemente il controllo, la normativa richiede l'istituzione di un flusso comunicativo costante, tempestivo e strutturato . Non si tratta di un adempimento burocratico, ma di uno strumento sostanziale: il *Punto di Contatto NIS* funge da interfaccia operativa e ha l'obbligo di riferire direttamente ai vertici aziendali.
Questo canale deve garantire che il Consiglio di Amministrazione sia informato:

- **Tempestivamente**, in caso di eventi critici, vulnerabilità gravi o perturbazioni operative, per permettere l'adozione di decisioni consapevoli e coordinate in emergenza;
- **Periodicamente**, attraverso reportistica sugli incidenti gestiti e sulle notifiche effettuate agli enti regolatori (Articoli 25 e 26).

Solo attraverso questa osmosi informativa i vertici possono valutare l'impatto dei rischi cyber sulla continuità del business.

[50] Attività di supervisione continuativa svolta dai vertici aziendali per verificare che i processi, le misure di sicurezza e gli obblighi normativi siano applicati correttamente e rimangano efficaci nel tempo.

7.3 Formazione Obbligatoria

La NIS2 individua una difesa primaria nel fattore umano e nella consapevolezza del rischio, per questo motivo, introduce due obblighi formativi distinti :

- **Formazione dei Vertici:** Gli organi di amministrazione e direttivi dei soggetti essenziali e importanti sono tenuti a seguire personalmente una formazione specifica in materia di sicurezza informatica. Lo scopo è fornire loro le competenze necessarie per comprendere le minacce, porre le domande corrette ai tecnici e valutare l'impatto dei rischi sulle attività aziendali;
- **Formazione del Personale:** I vertici devono promuovere e garantire l'offerta periodica di formazione a tutti i dipendenti, al fine di diffondere una "cultura della sicurezza" capillare che riduca la superficie di attacco legata all'errore umano.

7.4 Responsabilità Giuridica e Sanzioni Personali

L'aspetto più critico della riforma riguarda il regime di responsabilità. La *compliance* non è più solo un problema aziendale, ma investe direttamente le persone fisiche che ricoprono ruoli apicali:

Sanzioni Accessorie e Interdittive

Oltre alle sanzioni pecuniarie a carico dell'ente, il decreto introduce misure severe per i dirigenti: qualora un soggetto (essenziale o importante) non ottemperi a una diffida formale dell'ACN, l'Autorità ha il potere di intervenire sulle persone fisiche responsabili. Nello specifico, l'ACN può disporre la **sospensione temporanea dalle funzioni dirigenziali** (interdizione) per le persone fisiche che svolgono funzioni di amministrazione o direzione. Tale misura accessoria rimane in vigore finché l'organizzazione non adotta le misure correttive necessarie per sanare le carenze.

Sanzioni Pecuniarie per Violazioni di Governance

La mancata osservanza degli obblighi di governance (Art. 23), gestione del rischio (Art. 24) e notifica (Art. 25) costituisce la fattispecie di violazione più grave, punita con i massimali edittali più alti:

- **Soggetti Essenziali** (escluse PA): fino a **10.000.000 euro** o il **2%** del fatturato annuo mondiale.
- **Soggetti Importanti** (escluse PA): fino a **7.000.000 euro** o l'**1,4%** del fatturato annuo mondiale.

7.5 Censimento e Identificazione Formale

Per rendere operativa la responsabilità personale, l'ACN richiede un censimento puntuale dei membri del *board*[51].
Attraverso il servizio "*Aggiornamento annuale*" (disponibile sul portale ACN), il Punto di Contatto deve elencare i codici fiscali di tutte le persone fisiche che compongono gli organi di amministrazione e direttivi, indicando per ciascuno un indirizzo di Posta Elettronica Certificata (**PEC**) personale o professionale .

Procedura di Accettazione

Il processo non è unilaterale: per consolidare il ruolo di garanzia, le persone fisiche indicate ricevono una comunicazione formale via PEC contenente un link tramite il quale essi devono accedere al Portale ACN e completare una procedura di **accettazione esplicita** del ruolo. Solo con questa validazione si perfeziona l'identificazione delle "persone fisiche responsabili" ai sensi dell'articolo 38 del decreto.

8. Il Framework FNCSDP

L'implementazione operativa della Direttiva NIS2 in Italia non è lasciata all'improvvisazione ma è rigorosamente strutturata dal **Framework Nazionale per la Cybersecurity e la Data Protection (FNCSDP)**. Questo modello costituisce l'architettura di riferimento obbligatoria su cui si basano le misure tecniche e organizzative stabilite dall'Agenzia per la Cybersicurezza Nazionale (ACN), il cui ruolo di autorità regolatoria è approfondito al Capitolo 4.

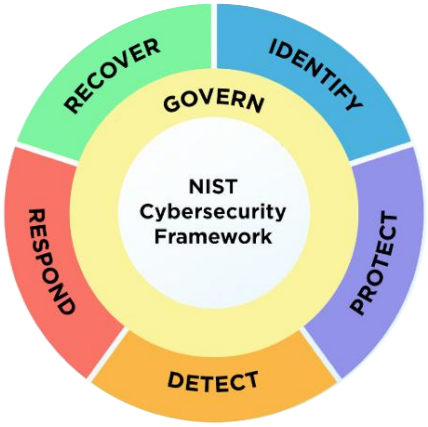
L'adozione del Framework risponde all'esigenza di fornire un linguaggio comune e standardizzato tra Pubbliche Amministrazioni, imprese e catena di fornitura. Essendo l'adattamento italiano del **NIST Cybersecurity Framework v.2**[52], garantisce la piena

[51] Insieme delle persone fisiche che compongono gli organi di amministrazione e direttivi di un ente, responsabili delle decisioni strategiche, della supervisione e della gestione complessiva dell'organizzazione.
[52] Modello internazionale di riferimento per la gestione del rischio cyber, sviluppato dal National Institute of Standards and Technology (NIST). La versione 2 introduce un'impostazione aggiornata e più orientata al governo del rischio, articolata in funzioni che guidano le organizzazioni nella definizione, implementazione e miglioramento continuo delle misure di sicurezza.

compatibilità internazionale e facilita i percorsi di certificazione (come la ISO 27001[53]), permettendo alle organizzazioni di elevare progressivamente il proprio livello di sicurezza partendo da una baseline reale .

8.1 Evoluzione Strutturale

Il FNCSDP (edizione 2025, v2) recepisce l'evoluzione sostanziale introdotta dal NIST 2. Rispetto alla versione precedente (v1), che si basava su 5 pilastri, il nuovo modello introduce una sesta funzione trasversale fondamentale: *GOVERN*. L'architettura attuale si articola dunque **in 6 Funzioni** logiche, suddivise in **23 Categorie** (obiettivi operativi) e **115 Sottocategorie** (controlli specifici). Questa granularità consente di trasformare il concetto astratto di *sicurezza* in un piano d'azione misurabile, eliminando i silos operativi[54] e favorendo la sinergia tra le diverse aree aziendali .



8.2 Funzioni Logiche

Le funzioni guidano l'intero ciclo di gestione del rischio (Cybersecurity Risk Management[55]), coprendo ogni fase dalla strategia al ripristino post-incidente. Di seguito la declinazione delle Categorie operative secondo l'edizione 2025 del Framework:

---

[53] Standard internazionale per i sistemi di gestione della sicurezza delle informazioni (ISMS). Definisce requisiti e controlli per proteggere riservatezza, integrità e disponibilità dei dati, fornendo un framework certificabile che attesta la conformità a pratiche di sicurezza riconosciute a livello globale.

[54] Condizione organizzativa in cui reparti o funzioni aziendali lavorano in modo isolato, senza adeguati flussi di comunicazione e coordinamento. Nei contesti di sicurezza informatica, i silos impediscono una visione integrata del rischio, ostacolano la condivisione tempestiva delle informazioni e generano inefficienze che compromettono la resilienza complessiva dell'organizzazione.

[55] Processo strutturato attraverso il quale un'organizzazione identifica, analizza, valuta e tratta i rischi legati alla sicurezza informatica. Comprende la definizione della strategia, l'adozione di controlli tecnici e organizzativi, il monitoraggio continuo delle minacce e la capacità di risposta e recupero in caso di incidente. È un ciclo continuo che garantisce coerenza tra obiettivi di business, governance e protezione degli asset digitali.

GOVERN (GV)

È la funzione centrale che stabilisce e monitora la strategia di gestione del rischio di cybersecurity, assicurando che gli obiettivi e le relative policy siano stabiliti, comunicati e monitorati.

- **Contesto organizzativo (GV.OC):** È compreso il contesto (missione, aspettative degli stakeholder, dipendenze e requisiti legali, normativi e contrattuali) che influisce sulle decisioni di gestione del rischio;
- **Strategia di gestione del rischio (GV.RM):** Le priorità, i vincoli, le dichiarazioni sulla tolleranza e la propensione al rischio (*Risk Appetite*) e le assunzioni dell'organizzazione, sono stabilite, comunicate e utilizzate per guidare le decisioni operative;
- **Ruoli, responsabilità e correlati poteri (GV.RR):** Sono stabiliti e comunicati i ruoli, le responsabilità e i correlati poteri in materia di cybersecurity per promuovere l'*accountability* e garantire che la governance non sia delegata esclusivamente ai reparti tecnici;
- **Politica (GV.PO):** La politica di cybersecurity dell'organizzazione (che deve coprire i 16 ambiti obbligatori) è stabilita, comunicata e applicata a tutto il personale;
- **Supervisione (GV.OV):** I risultati delle attività di gestione del rischio sono utilizzati per informare, migliorare e adeguare la strategia, garantendo una supervisione attiva da parte degli organi direttivi;
- **Gestione del rischio della catena di approvvigionamento (GV.SC):** I processi di gestione del rischio di cybersecurity della *Supply Chain* sono identificati, stabiliti, gestiti, monitorati e migliorati, vincolando i fornitori tramite contratti con clausole di sicurezza.

IDENTIFY (ID)

Questa funzione mira a comprendere i rischi attuali di cybersecurity per eliminare il *perimetro ignoto*.

- **Gestione degli asset (ID.AM):** Gli asset (dati, hardware, software, sistemi, persone) che consentono all'organizzazione di raggiungere gli obiettivi di business sono identificati e gestiti in coerenza con la loro importanza. Per il software, è fondamentale tracciare versioni e licenze;
- **Valutazione del rischio (*Risk Assessment*) (ID.RA):** È compreso il rischio di cybersecurity al quale l'organizzazione, gli asset e le persone sono esposti, attraverso una metodologia strutturata e ripetibile (con rivalutazione almeno biennale);
- **Data Management (DP-ID.DM):** I dati personali sono trattati attraverso processi definiti, in coerenza con le normative di riferimento (GDPR) e le esigenze di tutela della privacy;

- **Miglioramento (ID.IM):** I miglioramenti ai processi, alle procedure e alle attività di gestione del rischio sono identificati in tutte le funzioni del framework, assicurando un ciclo di evoluzione continuo.

PROTECT (PR)

Riguarda l'adozione di misure di protezione per gestire i rischi e contenere l'impatto di potenziali eventi.

- **Gestione delle identità, autenticazione e controllo degli accessi (PR.AA):** L'accesso agli asset fisici e logici è limitato agli utenti autorizzati, applicando il principio del minimo privilegio e l'obbligo di autenticazione a più fattori (MFA);
- **Sicurezza dei dati (PR.DS):** I dati sono gestiti in modo coerente con la strategia sul rischio per proteggere la riservatezza, l'integrità e la disponibilità delle informazioni (es. tramite cifratura e backup, incluso il *backup offline* per i Soggetti Essenziali);
- **Sicurezza delle piattaforme (PR.PS):** L'hardware e il software delle piattaforme fisiche e virtuali sono gestiti e configurati in modo sicuro (*Hardening*[56]) e aggiornati tempestivamente (*Patching*[57]);
- **Resilienza dell'infrastruttura tecnologica (PR.IR):** Le architetture di sicurezza sono gestite per proteggere la disponibilità degli asset e garantire la resilienza organizzativa.
- **Consapevolezza e formazione (PR.AT):** Il personale è sensibilizzato e formato sulla cybersecurity (formazione base per tutti e avanzata per i tecnici) in modo da poter svolgere i propri compiti in sicurezza.

DETECT (DE)

Si concentra sulla capacità di rilevare e analizzare possibili attacchi e compromissioni.

- **Monitoraggio continuo (DE.CM):** Gli asset sono monitorati costantemente per individuare anomalie, indicatori di compromissione (IoC) e altri eventi potenzialmente avversi. Ciò richiede log centralizzati e protetti da manomissione, conservati per almeno 6 mesi;

[56] Processo di rafforzamento della sicurezza di sistemi hardware e software attraverso la rimozione di componenti superflui, la disabilitazione di servizi non necessari e l'applicazione di configurazioni sicure che riducono la superficie di attacco.
[57] Attività di aggiornamento che consiste nell'applicare patch correttive ai sistemi per risolvere vulnerabilità, errori o criticità note, mantenendo l'infrastruttura protetta rispetto alle minacce più recenti.

- **Analisi degli eventi avversi (DE.AE):** Anomalie e indicatori di compromissione sono analizzati per caratterizzare gli eventi e rilevare gli incidenti di cybersecurity, supportati da fonti di *Threat Intelligence*[58] e soglie di allarme automatiche.

5. RESPOND (RS)

Gestisce le azioni intraprese in risposta a un incidente di cybersecurity rilevato.

- **Gestione degli incidenti (RS.MA):** Le risposte agli incidenti sono gestite attraverso un *Incident Response Plan*[59] chiaro e testato che definisca ruoli e procedure di *escalation*[60];
- **Analisi degli incidenti (RS.AN):** Sono condotte indagini per garantire una risposta efficace, supportare le attività forensi e comprendere la natura dell'attacco;
- **Mitigazione degli incidenti (RS.MI):** Sono eseguite attività operative per prevenire l'espansione di un evento e mitigarne gli effetti;
- **Segnalazione e comunicazione della risposta agli incidenti (RS.CO):** Le attività di risposta sono coordinate con gli stakeholder interni ed esterni (es. notifiche al CSIRT Italia) come richiesto da leggi, regolamenti o politiche.

6. RECOVER (RC)

Mira al ripristino degli asset e delle operazioni interessati da un incidente.

- **Esecuzione del piano di ripristino dagli incidenti (RC.RP):** Le attività di ripristino sono eseguite per garantire la disponibilità operativa dei sistemi e dei servizi, seguendo le priorità di business definite (RTO/RPO)[61].
- **Comunicazione sul ripristino dagli incidenti (RC.CO):** Le attività di ripristino sono coordinate con le parti interne ed esterne. Durante il ripristino, una comunicazione chiara, trasparente e costante è fondamentale per gestire la reputazione e le aspettative.

  Nota: Ogni incidente deve generare miglioramenti (*Lessons Learned*), portando all'aggiornamento di piani e procedure e alla condivisione delle esperienze nel settore.

---

[58] Processo di raccolta, analisi e condivisione di informazioni sulle minacce informatiche, comprendente tecniche di attacco, vulnerabilità emergenti, indicatori di compromissione (IoC) e attività di gruppi ostili. Supporta il rilevamento tempestivo degli incidenti e l'adozione di misure difensive aggiornate.

[59] Documento operativo che definisce ruoli, responsabilità, procedure e flussi decisionali necessari per rilevare, analizzare, contenere ed eradicare un incidente di sicurezza, garantendo una risposta tempestiva e coordinata.

[60] Processo formale che stabilisce quando e come un evento deve essere segnalato ai livelli superiori di responsabilità, indicando tempi, soglie di gravità e destinatari per assicurare decisioni rapide e adeguate durante la gestione dell'incidente.

[61] Il **Recovery Time Objective (RTO)** indica il tempo massimo entro cui un sistema o servizio deve essere ripristinato dopo un incidente. Il **Recovery Point Objective (RPO)** rappresenta invece la quantità massima di dati che l'organizzazione può permettersi di perdere, definita come intervallo temporale tra l'ultimo backup valido e l'evento di interruzione.

8.3 Declinazione dei Requisiti

L'ACN ha tradotto le categorie del Framework in specifiche tecniche obbligatorie, modulando l'onere di compliance in base alla classificazione del soggetto (Capitolo 3.1). Dal Framework derivano due profili di applicazione:

- **Profilo Soggetti Essenziali**: Richiede l'implementazione di 43 misure di sicurezza e 116 requisiti totali.
- **Profilo Soggetti Importanti**: Richiede l'implementazione di 37 misure di sicurezza e 87 requisiti totali.

Categoria Soggetto	Livello di Rischio	Misure di Sicurezza	Requisiti Totali
Soggetti Essenziali	Maggiore Criticità	43	116
Soggetti Importanti	Minore Criticità	37	87

Le differenze qualitative, derivanti principalmente dalle funzioni *PROTECT* e *IDENTIFY*, impongono ai Soggetti Essenziali controlli più onerosi quali l'esecuzione di penetration test annuali, l'implementazione di backup offline e procedure di patching accelerate. Tuttavia, l'ACN ha previsto clausole di flessibilità che permettono di modulare o derogare specifici requisiti (31 per gli Essenziali, 23 per gli Importanti) qualora sussistano vincoli tecnologici o di contesto, purché tale deroga sia rigorosamente motivata e documentata.

9. Cybersecurity Governance: Strategia, Metodologia e Pianificazione

Con la Direttiva NIS2 la cybersicurezza non è più una funzione tecnica accessoria, ma una responsabilità di Governance diretta. Nel Capitolo 7 sono stati analizzati gli aspetti di responsabilità giuridica e sanzionatoria in capo agli organi di vertice, in questa sezione si approfondisce la **metodologia strategica** necessaria per integrare la sicurezza nei processi decisionali aziendali. La *Cybersecurity Governance* è l'insieme di regole, processi e strutture che allineano la sicurezza informatica agli obiettivi di business, trasformandola da centro di costo a fattore competitivo in grado di abilitare l'innovazione sostenibile e ridurre i rischi reputazionali .

9.1 Analisi del Contesto

Per costruire una strategia di difesa efficace e su misura, il primo passo obbligatorio è la *Valutazione del Contesto*: l'analisi deve rispondere a domande cruciali su chi sono gli attori, quali sono gli asset critici e quali minacce sono realistiche .

Analisi del Contesto Esterno

Riguarda i fattori non controllabili dall'azienda, che devono essere monitorati costantemente :

- **Quadro Normativo:** Identificazione puntuale di tutte le leggi applicabili (NIS2, GDPR, DORA) per evitare sanzioni;
- **Panorama delle Minacce:** Mappatura degli attori malevoli (cybercriminali, attivisti, stati-nazione) e analisi delle loro Tattiche, Tecniche e Procedure (TTP);
- **Supply Chain:** La catena di fornitura è un'estensione del perimetro di rischio, in quanto un fornitore compromesso rappresenta un vettore di attacco critico;
- **Fattori Geopolitici:** Le tensioni internazionali e l'instabilità sociale possono tradursi in attacchi mirati o danni collaterali.

Analisi del Contesto Interno

Riguarda le caratteristiche intrinseche dell'organizzazione :

- **Obiettivi di Business:** La sicurezza deve fungere da abilitatore, se l'obiettivo è l'innovazione rapida, la sicurezza deve essere agile; se è l'affidabilità, deve essere rigorosa;
- **Asset Critici:** Identificazione dei dati potenzialmente interessanti (IP, dati sensibili, sistemi di produzione) la cui compromissione bloccherebbe l'operatività;
- **Cultura Organizzativa:** Il fattore umano è spesso la vulnerabilità maggiore, una cultura matura e consapevole è la prima linea di difesa;
- **Propensione al Rischio (*Risk Appetite*):** Il livello di rischio che il management è disposto ad accettare per perseguire i propri obiettivi.

9.2 Definizione degli Obiettivi e Stakeholder

Parte integrante e imprescindibile dell'analisi del contesto è l'identificazione puntuale degli *Stakeholder*. Con questo termine si definiscono tutte le parti interessate, sia interne che esterne al perimetro aziendale, che detengono un interesse legittimo nelle performance di sicurezza dell'organizzazione o che ne subiscono gli effetti. La governance efficace richiede la comprensione profonda delle loro aspettative, poiché queste influenzano direttamente i requisiti di sicurezza. La mappa degli stakeholder include :

- **Autorità di Regolamentazione:** Enti come l'ACN che impongono requisiti di conformità.
- **Top Management:** Che definisce il budget e la strategia aziendale;
- **Dipendenti:** Utenti dei sistemi e prima linea di difesa;
- **Partner e Fornitori:** Soggetti interconnessi alla catena del valore;
- **Clienti:** Che si aspettano la tutela dei propri dati e la continuità del servizio.

Sulla base del contesto e delle aspettative degli stakeholder, i vertici devono definire obiettivi strategici che seguano la logica **SMART** (Specifici, Misurabili, Raggiungibili, Rilevanti, Temporizzati). Esempi concreti di obiettivi SMART includono: *"Ridurre la superficie d'attacco del 20% entro 18 mesi"*, *"Abbassare il tempo medio di rilevamento a meno di 4 ore"* o "*Raggiungere il 90% di completamento del training entro l'anno"* .

9.3 Metodologia Operativa: Gap Analysis e Roadmap

Per raggiungere la conformità NIS2 e gli obiettivi prefissati, è necessario adottare un approccio metodologico strutturato che colmi la distanza tra la situazione attuale e quella desiderata.

Fase 1: Gap Analysis

Questa fase confronta lo stato attuale dei controlli (*As-Is*) con lo stato desiderato (*To-Be*) definito dal *Framework Nazionale (FNCSDP)* o dagli standard scelti (*NIST, ISO 27001*). L'analisi del divario identifica le mancanze specifiche.

Esempio pratico*:* Se il framework richiede log centralizzati con retention di 12 mesi e l'azienda ha solo log locali di 30 giorni, il Gap è la differenza tra quello che ha ora l'azienda (1 mese) e

quello che dovrebbe avere (12 mesi); il rischio associato, quindi il problema per il quale esiste il gap, è l'impossibilità di fare analisi forense. L'intervento richiesto è l'implementazione di nuove policy di retention a 12 mesi.

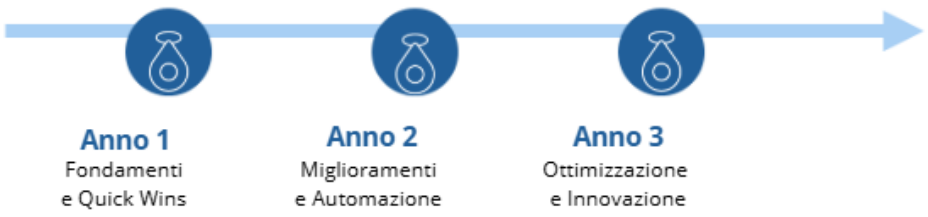
Fase 2: Prioritizzazione e "Quick Wins"

Non è possibile colmare tutti i gap simultaneamente, per questo gli interventi devono essere prioritizzati basandosi su:

- **Livello di Rischio:** Priorità alla mitigazione dei rischi con impatto/probabilità maggiori;
- **Analisi Costi-Benefici:** Miglior rapporto tra investimento e riduzione del rischio;
- **Compliance Obbligatoria:** Scadenze imposte dalla legge (es. le date di notifica NIS2);
- **Quick Wins:** Interventi ad alto impatto e basso sforzo (es. attivare l'MFA su tutti gli account, applicare patch critiche) che devono essere eseguiti subito per ottenere risultati tangibili.

Fase 3: Roadmap Pluriennale

L'output finale è la **Roadmap di Cybersicurezza**, un piano operativo (1-3 anni) che visualizza la sequenza degli interventi. Per ogni iniziativa, la roadmap deve specificare obiettivi, tempistiche, responsabilità, risorse necessarie (budget/personale) e KPI[62] di successo. È uno strumento dinamico che deve essere rivisto periodicamente.



9.4 Ruoli Chiave nella Governance (CISO e CRM)

L'ACN e il framework europeo delle competenze individuano due figure cardine per l'esecuzione della governance:

[62] Indicatori quantitativi o qualitativi utilizzati per misurare l'efficacia di un processo, progetto o controllo di sicurezza. Nel contesto della cybersecurity, servono a valutare i progressi della roadmap (es. tempo medio di applicazione patch, riduzione degli incidenti, percentuale di sistemi monitorati) e a fornire ai vertici un quadro oggettivo delle performance e delle aree da migliorare.

- **Chief Information Security Officer (CISO):** È il dirigente apicale responsabile della strategia. Agisce da raccordo tra business e tecnologia, riportando direttamente al Consiglio di Amministrazione. I suoi compiti includono lo sviluppo del programma di sicurezza a lungo termine, la garanzia della conformità normativa e il reporting regolare agli stakeholder sullo stato del rischio;
- **Cyber Risk Manager (CRM):** È il garante dell'approccio basato sul rischio, responsabile operativo dell'analisi del rischio (*Risk Assessment*), valuta minacce e vulnerabilità su sistemi e supply chain, propone i controlli di sicurezza giustificandoli con analisi costi-benefici e monitora il livello di rischio residuo nel tempo.

9.5 Manutenzione, Flessibilità e Miglioramento

La NIS2 è una normativa di *compliance* che richiede la dimostrazione documentale delle attività (evidenze). Tuttavia, la resilienza non è un progetto *una tantum*, è anzi obbligatoria una **revisione periodica** dei rischi (almeno biennale o post-incidente) e l'approvazione formale dei documenti chiave da parte del management.

Va infine notato che l'ACN, nelle sue Determinazioni, ha previsto clausole di **flessibilità proporzionale** (come già visto in diversi paragrafi): i soggetti possono motivare la non applicazione di specifici requisiti tecnici se il contesto o l'analisi del rischio lo giustificano, purché tale deroga sia documentata e compensata, garantendo che l'onere sia sempre sostenibile e proporzionato alla reale criticità.

10. Gestione dei Rischi: Approccio Proattivo e Multi-Rischio

La gestione dei rischi (*Risk Management*) rappresenta una parte fondamentale della Direttiva NIS2 e costituisce l'obbligo sostanziale primario per tutti i soggetti essenziali e importanti. Non si tratta di una semplice *checklist* di controlli, ma di un processo sistematico e iterativo volto a identificare, analizzare, trattare e monitorare il rischio informatico nel tempo. L'obiettivo del ***Risk Management (RM)*** non è l'eliminazione totale del rischio (operazione tecnicamente impossibile ed economicamente non sostenibile) bensì la sua gestione entro un livello di tolleranza accettabile (*Risk Appetite*) per l'organizzazione, garantendo la continuità dei servizi essenziali. Tale processo deve essere integrato organicamente nel più ampio *Enterprise Risk Management* (ERM) aziendale, concetto ampliamente discusso nei capitoli riguardanti *Governance*.

10.1 Approccio Multi-Rischio

La NIS2 impone un cambio fondamentale introducendo l'obbligo di un approccio **Multi-Rischio** (Capitolo 1.3). La sicurezza dei sistemi informativi e di rete non può più limitarsi solo alla sfera logica , ma deve considerare in modo olistico anche l'ambiente fisico in cui tali sistemi operano. L'analisi dei rischi deve pertanto valutare congiuntamente :

- **Minacce Digitali:** Rischi derivanti da vettori di attacco informatici, quali *malware*[63], *ransomware*[64], *phishing*[65], interruzioni di rete, furto di credenziali e accessi logici non autorizzati;
- **Minacce Fisiche:** Rischi derivanti dal contesto ambientale e infrastrutturale che possono compromettere la disponibilità, l'integrità o la riservatezza dei dati. Questi includono furti di hardware, incendi, allagamenti, guasti ai sistemi di raffreddamento, blackout elettrici, disastri naturali e accessi fisici non autorizzati ai locali server o data center.

10.2 Misure di Sicurezza Obbligatorie

I soggetti devono adottare misure tecniche, operative e organizzative adeguate e proporzionate al rischio specifico. Non esistono misure uniche, esse devono essere calibrate sulla base dell'esposizione al rischio e della criticità del soggetto. L'elenco minimo delle misure obbligatorie comprende :

- **Politiche di Analisi dei Rischi:** Adozione di procedure formali per la valutazione della sicurezza dei sistemi;
- **Gestione degli Incidenti:** Implementazione di capacità di *Incident Response* dettagli operativi trattati nel Capitolo 5);
- **Continuità Operativa:** Strategie di *Business Continuity*, gestione delle crisi e *Disaster Recovery* (inclusi backup sicuri);
- **Sicurezza della Supply Chain:** Gestione dei rischi derivanti dalle relazioni con fornitori e partner;
- **Sicurezza nello Sviluppo:** Adozione di politiche per la sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi;

[63] Software malevolo progettato per danneggiare sistemi, rubare dati o compromettere l'operatività di un dispositivo o di una rete, spesso diffuso tramite file infetti, siti compromessi o tecniche di ingegneria sociale.
[64] Tipologia di malware che cifra i dati o blocca i sistemi di un'organizzazione e richiede un riscatto per il loro ripristino. È uno dei vettori di attacco più critici per la continuità operativa.
[65] Tecnica di attacco basata sull'inganno, in cui l'aggressore induce l'utente a rivelare informazioni sensibili (come credenziali) o a compiere azioni dannose tramite email, messaggi o siti che imitano fonti legittime.

- **Valutazione dell'Efficacia:** Procedure per testare e misurare periodicamente le misure adottate;
- **Igiene Informatica e Formazione:** Pratiche di *Cyber Hygiene* (es. aggiornamenti software) e formazione obbligatoria del personale;
- **Crittografia e Cifratura:** Uso di tecnologie crittografiche per la protezione dei dati a riposo e in transito;
- **Sicurezza del Personale:** Politiche di controllo accessi, gestione degli asset e sicurezza delle risorse umane;
- **Autenticazione Forte:** Adozione obbligatoria di soluzioni di Autenticazione a Più Fattori (MFA) o autenticazione continua per l'accesso a reti e servizi.

10.3 Il Processo di Risk Assessment (Valutazione del Rischio)

Il cuore operativo del *Risk Management* è la Valutazione del Rischio (*Risk Assessment*), un'attività che rientra nella funzione *IDENTIFY* del *Framework Nazionale (FNCSDP)*. Il rischio cyber è calcolato combinando due variabili: la **Probabilità** (*Likelihood*) che una minaccia sfrutti una vulnerabilità e l'**Impatto** (*Impact*) che ne deriverebbe (economico, operativo, reputazionale).

Il processo si articola in tre fasi sequenziali:

1. **Identificazione (*Risk Identification*):** È la fase di mappatura, l'organizzazione deve censire tutti gli asset (hardware, software, dati) per eliminare le *zone d'ombra*. In questa fase si identificano le minacce pertinenti (usando fonti di *Threat Intelligence*) e le vulnerabilità tecniche. Per i Soggetti Essenziali, questa fase deve essere supportata da attività tecniche come *Vulnerability Assessment* e *Penetration Test* prima della messa in esercizio di nuovi sistemi critici.

2. **Analisi (*Risk Analysis*):** Si stima il livello di rischio associato a ogni scenario identificato. L'analisi può essere qualitativa (basata su scale di valore: Alto/Medio/Basso), quantitativa (basata su stime finanziarie del danno atteso) o mista. In questa fase si valuta anche la differenza tra *incidente* (evento con impatto reale) e *quasi-Incidente* (*Near-miss*), ovvero quegli eventi che avrebbero potuto causare un danno ma sono stati evitati (preziosi per prevenire incidenti futuri).

3. **Valutazione (*Risk Evaluation*):** Il livello di rischio emerso viene confrontato con i criteri di accettabilità dell'azienda (*Risk Appetite*). Questa fase determina quali rischi richiedono un intervento prioritario. La valutazione deve essere riesaminata almeno ogni due anni e obbligatoriamente dopo ogni incidente significativo o modifica strutturale dell'organizzazione.

10.4 Strategie di Trattamento del Rischio (*Risk Treatment*)

Qualora il rischio valutato superi la soglia di tolleranza, l'organizzazione deve scegliere una tra quattro strategie principali, con cui agire:

- **Mitigazione (Riduzione):** Consiste nell'applicare controlli di sicurezza (tecnici, fisici o organizzativi) per ridurre la probabilità dell'evento o limitarne l'impatto (es. installare firewall, formare il personale, segmentare la rete).
- **Accettazione:** Il management decide consapevolmente di non intervenire, accettando il rischio residuo. Questa scelta è ammissibile solo se il rischio è basso o se il costo della mitigazione supera il valore dell'asset da proteggere, e deve essere formalmente documentata.
- **Trasferimento:** La responsabilità finanziaria del rischio viene spostata su terze parti, tipicamente attraverso polizze assicurative o clausole contrattuali (*SLA*[66]) con i fornitori di servizi gestiti.
- **Evitamento:** Si decide di eliminare alla radice la causa del rischio, ad esempio dismettendo un processo obsoleto, un servizio non sicuro o una tecnologia non più supportata.

10.5 Sicurezza della Catena di Approvvigionamento (*Supply Chain Security*)

La NIS2 pone un'enfasi senza precedenti sulla sicurezza della *Supply Chain*. Il perimetro di rischio si estende oltre i confini aziendali, riconoscendo che i fornitori (specialmente di servizi ICT e software) possono rappresentare il vettore di attacco ideale per compromettere l'organizzazione cliente. I soggetti NIS sono tenuti a valutare e monitorare:

- Le **vulnerabilità** specifiche di ogni fornitore diretto;
- La **qualità** e le pratiche di sicurezza dei prodotti e servizi acquistati;
- Le **procedure** di sviluppo sicuro (*Secure Coding*) adottate dai fornitori di software .

Questa attività, riconducibile alla categoria **GV.SC** del Framework Nazionale, richiede di classificare i fornitori in base alla criticità (Standard, Importanti, Critici) e di vincolarli

[66] **Service Level Agreement**: accordo contrattuale tra un'organizzazione e un fornitore di servizi che definisce livelli di servizio misurabili, responsabilità, tempi di risposta e di ripristino, nonché eventuali penali. Nel contesto della gestione del rischio, può trasferire parte delle responsabilità operative o finanziarie al fornitore.

contrattualmente al rispetto di specifici requisiti di sicurezza, verificandone l'applicazione tramite audit periodici.

Focus

Applicazione Pratica: Modello di Gestione Integrata Per tradurre i concetti teorici in operatività aziendale, si propone la seguente matrice applicativa che illustra come le diverse componenti del Risk Management cooperino per gestire uno scenario di minaccia concreto (es. rischio di attacco Ransomware veicolato tramite Supply Chain).

Componente NIS2	Azione Operativa Concreta (Esempio Aziendale)	Obiettivo di Gestione del Rischio
Threat Intelligence	Ricezione di un bollettino CSIRT su una nuova vulnerabilità critica che colpisce i sistemi ERP.	Anticipazione: Rilevare la minaccia prima che colpisca il perimetro.
Risk Analysis	Stima dell'impatto economico derivante dal fermo del sistema ERP per 48 ore (mancata fatturazione, blocco logistica).	Quantificazione: Definire la priorità di intervento basata sul danno potenziale.
Mitigazione (Risk Treatment)	Implementazione di Segmentazione di Rete, Patching immediato e attivazione MFA per gli amministratori.	Protezione: Ridurre la probabilità di successo dell'attacco e limitarne la diffusione (Containment).
Supply Chain Security	Audit di sicurezza sul fornitore del software ERP e verifica delle clausole contrattuali sui tempi di ripristino (SLA).	Estensione del Perimetro: Evitare che la vulnerabilità di un terzo comprometta l'azienda.
Continuità Operativa (BC/DR)	Attivazione del piano di Backup Offline immutabile per garantire il ripristino dei dati senza pagare il riscatto.	Resilienza: Garantire la sopravvivenza del business anche in caso di incidente riuscito.
Risk Transfer	Attivazione di una polizza Cyber Insurance per coprire i costi legali e di notifica post-incidente.	Gestione Finanziaria: Mitigare l'impatto economico residuo non gestibile tecnicamente.

11. Cyber Risk Management: Strategia, Capacità e Ciclo di Miglioramento

Il **Cyber Risk Management (CRM)** rappresenta il dominio operativo che traduce la governance in azione. Non si tratta di un semplice adempimento burocratico, ma di un insieme strutturato di pratiche e capacità (*capabilities*) volte a gestire il rischio informatico in modo sistematico.

L'obiettivo primario del CRM (introdotto nel Capitolo 10) non è l'eliminazione completa del rischio, bensì la sua gestione entro un livello sostenibile per l'organizzazione, allineato agli obiettivi strategici di business e integrato nel più ampio *Enterprise Risk Management* (ERM) .

11.1 L'Impossibilità del "Rischio Zero" e l'Analisi Costi-Benefici

Il rischio cyber è funzione di due variabili: la *Probabilità* che una minaccia sfrutti una vulnerabilità e l'*Impatto* che ne consegue. La gestione di questa equazione si scontra con tre fattori che rendono impossibile l'azzeramento del rischio :

1. **Necessità Operativa:** L'apertura dei sistemi è necessaria per il business; ogni attività genera inevitabilmente punti di esposizione;
2. **Mutevolezza del Contesto:** Le tecniche di attacco evolvono più rapidamente delle difese statiche;
3. **Limitatezza delle Risorse:** Le misure di sicurezza hanno un costo economico e operativo.

Di conseguenza, le decisioni di sicurezza devono essere guidate da una rigorosa *analisi costi-benefici*: si implementano controlli solo quando il beneficio in termini di riduzione del rischio supera il costo dell'investimento e l'impatto sull'operatività (rallentamento dei processi). L'obiettivo è mantenere il *Rischio Residuo*[67] entro la soglia di *Risk Appetite* definita dal management .

11.2 Competenze Fondamentali

Per gestire il rischio in modo coeso e scalabile, l'organizzazione deve sviluppare quattro competenze chiave (*Capability*) che operano in sinergia :

1. **Risk Assessment:** È la capacità di identificare e analizzare i rischi. Si può adottare un approccio basato sulle minacce (partendo dagli scenari di attacco, es. intrusione) o basato sugli asset (partendo dalla criticità dei beni da proteggere). L'analisi può essere

[67] Livello di rischio che permane dopo l'applicazione delle misure di mitigazione, comprendendo la probabilità e l'impatto ancora presenti nonostante i controlli implementati. Rappresenta il rischio che l'organizzazione accetta consapevolmente entro la propria soglia di tolleranza (Risk Appetite).

Qualitativa (basata su giudizio esperto, es. Alto/Medio/Basso), *Quantitativa* (valore monetario) o *Mista*;

2. **Risk Treatment:** È la capacità di selezionare e applicare le misure per modificare il profilo di rischio. Le strategie di trattamento (Capitolo 10.4) si concretizzano attraverso tre tipologie di controlli:

   - **Controlli Tecnici:** Strumenti hardware/software (es. EDR, backup immutabili, firewall);
   - **Controlli Organizzativi:** Policy, procedure, *patch management*;
   - **Controlli Formativi:** Training di *awareness*, simulazioni di phishing. In questa fase si formalizzano anche le decisioni di trasferimento (es. assicurazioni cyber che coprono costi legali e sanzioni) e di accettazione consapevole del rischio.

3. **Communication:** La comunicazione è un processo trasversale essenziale che deve avvenire su tre livelli:

   - **Strategico:** Definizione del *Risk Appetite* e allocazione budget (verso il CdA);
   - **Tattico:** Traduzione degli obiettivi in processi e policy (verso il Management);
   - **Operativo:** Monitoraggio quotidiano e gestione dei controlli (verso i tecnici).

4. **Third-Party Management:** Data la criticità della *Supply Chain*, questa capability richiede un processo strutturato in quattro fasi operative per gestire i rischi esterni:

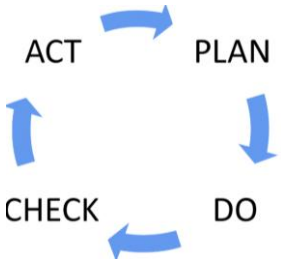
   - **Definire i Requisiti:** Stabilire a priori gli standard di sicurezza richiesti (es. certificazione ISO 27001, crittografia);
   - **Selezionare il Fornitore:** Eseguire una *due diligence*[68] preventiva per verificare il rispetto dei requisiti;
   - **Contrattualizzare:** Inserire clausole vincolanti, SLA di sicurezza e penali nel contratto;
   - **Monitorare:** Eseguire audit periodici per verificare il mantenimento degli standard nel tempo.

[68] Valutazione preventiva e approfondita delle capacità, dell'affidabilità e del livello di sicurezza di un fornitore, effettuata prima di instaurare il rapporto contrattuale. Include verifiche su controlli tecnici, organizzativi, conformità normativa e rischi potenziali legati alla terza parte.

11.3 Ciclo di Miglioramento (PDCA)

Il CRM non è statico ma adotta il **Ciclo di Deming (PDCA)**[69] per adattarsi in tempo reale alle nuove minacce :

- ***PLAN* (Pianificare):** Definizione della strategia, identificazione dei rischi e determinazione del *Risk Appetite*. Si stabiliscono obiettivi misurabili e budget;
- ***DO* (Eseguire):** Implementazione concreta, si installano tecnologie, si redigono policy operative e si eroga la formazione al personale;
- ***CHECK* (Verificare):** Fase di misurazione, si monitorano KPI e KRI[70], si eseguono *vulnerability assessment* e *penetration test* per verificare l'efficacia delle misure rispetto agli obiettivi;
- ***ACT* (Agire):** Fase correttiva, si colmano gap emersi durante la verifica e si aggiornano le strategie basandosi sulle lezioni apprese, rialimentando il ciclo.



11.4 Misurare il Successo: Metriche e KPI

Un sistema di gestione è efficace solo se misurabile, l'utilizzo di indicatori chiave (*Key Performance Indicators* - KPI e *Key Risk Indicators* - KRI) è infatti fondamentale per dimostrare il valore della sicurezza al business.

Le metriche principali includono :

- **Rischi High-Open:** Numero di rischi critici non ancora trattati;
- **Tempo di Chiusura:** Tempo medio necessario per risolvere una vulnerabilità;
- ***Dwell Time*:** Tempo di permanenza di un attaccante nella rete prima di essere rilevato;
- **Copertura Formazione:** Percentuale di dipendenti che hanno completato il training;
- **Costo Rischio Residuo:** Stima economica del rischio che l'azienda sta accettando.

---

[69] Modello di miglioramento continuo articolato in quattro fasi (Plan, Do, Check e Act) utilizzato per pianificare, implementare, verificare e correggere processi organizzativi. Nel contesto della cybersecurity consente di adattare costantemente le misure di protezione all'evoluzione delle minacce e ai risultati delle verifiche.

[70] **Key Risk Indicators**: Indicatori che misurano l'esposizione al rischio e segnalano variazioni o criticità potenziali prima che si manifesti un incidente. Forniscono ai vertici un quadro oggettivo dell'andamento dei rischi e supportano decisioni tempestive di mitigazione.

12. Cyber Hygiene: Best Practices e Manutenzione

La Direttiva NIS2 formalizza il concetto di Igiene Cibernetica (*Cyber Hygiene*), infatti proprio negli Articoli 24 del Decreto Legislativo e 21 della direttiva europea, la Cyber Hygiene non è descritta come un intervento straordinario, ma definita come un insieme ordinato e ripetitivo di pratiche tecniche, organizzative e comportamentali che forniscono le basi essenziali per proteggere la sicurezza delle infrastrutture di rete, dei sistemi informatici, dell'hardware e del software.

L'obiettivo statistico di queste pratiche di base è prevenire fino all'**80% degli incidenti comuni**, riducendo drasticamente la superficie di attacco e garantendo che l'ambiente digitale rimanga "pulito", controllato e misurabile nel tempo.

12.1 Gestione degli Asset e Riduzione del *Perimetro Ignoto*

Il presupposto di ogni strategia difensiva è la conoscenza puntuale del proprio perimetro. Le organizzazioni hanno l'obbligo di eliminare le *zone d'ombra* attraverso un Asset Management dinamico (Capitolo 8.2). È richiesto il mantenimento di inventari completi, aggiornati e dettagliati che coprano :

- **Hardware:** Censimento di tutti i dispositivi fisici connessi alla rete.
- **Software:** Mappatura delle applicazioni, inclusi dettagli su versioni, patch level[71] e scadenze delle licenze.
- **Servizi Cloud e Terze Parti:** Elenco dei servizi esterni e dei fornitori connessi all'infrastruttura.

Per garantire l'aderenza alla realtà operativa, l'inventario degli asset critici non può essere un documento statico, ma deve essere oggetto di revisione formale almeno **semestrale**. Solo attraverso questa mappatura è possibile velocizzare le attività di risposta agli incidenti (isolando rapidamente i sistemi colpiti) e dimostrare la conformità in sede di verifica.

[71] Livello di aggiornamento di un software, determinato dal numero e dal tipo di patch applicate. Indica lo stato di correzione delle vulnerabilità note e il grado di protezione del sistema rispetto alle minacce correnti.

12.2 Gestione delle Vulnerabilità e Sicurezza dei Sistemi

La gestione tecnica delle vulnerabilità abbandona la discrezionalità per diventare un processo procedurale rigoroso, basato su due pilastri:

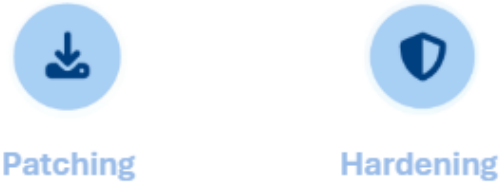
Patching Tempestivo e Documentato

È obbligatoria l'installazione degli aggiornamenti di sicurezza rilasciati dai produttori (*software* e *hardware*) senza ingiustificato ritardo, le organizzazioni devono infatti definire e contrattualizzare il *Time-to-Fix* (tempo massimo per l'applicazione della patch). Un aspetto cruciale per la *compliance* è la tracciabilità: le evidenze dell'avvenuta installazione e dei test di funzionamento devono essere conservate in archivi sicuri per almeno **24 mesi**, al fine di consentire ispezioni e analisi post-incidente.

Per i soli Soggetti Essenziali, i requisiti sono ancora più stringenti, imponendo scadenze accelerate per la mitigazione delle vulnerabilità critiche .

Hardening e Configurazione Sicura

Oltre all'aggiornamento, è richiesta anche l'applicazione di una *baseline* di configurazione[72] sicura documentata (*Hardening*[73]). Ciò include la gestione delle nuove installazioni, la disabilitazione dei servizi non necessari, la chiusura delle porte di rete inutilizzate e la modifica delle password di default, riducendone le opportunità di sfruttamento da parte degli attaccanti.



12.3 Gestione Identità e Accessi

Il controllo degli accessi deve evolvere verso modelli "*Zero Trust*", abbandonando la fiducia implicita. Le misure obbligatorie includono:

[72] Insieme di impostazioni tecniche standard e documentate che definiscono il livello minimo di sicurezza richiesto per sistemi, software e dispositivi, da applicare come configurazione iniziale e di riferimento.
[73] Processo di rafforzamento della sicurezza di un sistema attraverso la rimozione di componenti superflui, la disabilitazione di servizi non necessari, l'applicazione di configurazioni sicure e la riduzione delle superfici attaccabili.

- **Gestione Centralizzata:** Le identità digitali devono essere gestite centralmente, implementando meccanismi di *provisioning* (creazione)[74] e *deprovisioning* (revoca)[75] automatico. Questo è fondamentale per evitare la permanenza di *utenze orfane* (ad esempio di ex dipendenti o collaboratori) che rappresentano un'importante fonte di rischio.
- **Autenticazione Forte (MFA):** L'adozione dell'autenticazione a più fattori è tassativa per tutti gli accessi remoti (VPN, Cloud) e per gli account con privilegi di amministratore.
- **Minimo Privilegio e Revisione:** L'organizzazione deve applicare rigorosamente il principio del *Need-to-Know*[76] e della separazione dei compiti (*Segregation of Duties*)[77]. È inoltre prescritta una revisione periodica, con cadenza almeno **trimestrale**, di tutti gli account privilegiati per verificare la legittimità dei permessi attivi.

12.4 Crittografia e Protezione del Dato

Le politiche relative all'uso della crittografia costituiscono un elemento obbligatorio delle misure di gestione del rischio. Tutti i dati sensibili, sia quando sono archiviati (*Data at Rest*)[78] sia quando vengono trasmessi (*Data in Transit*)[79], devono essere protetti mediante tecniche crittografiche forti. La normativa pone un accento particolare sulla gestione sicura delle chiavi di cifratura, suggerendo l'adozione di soluzioni dedicate come gli *Hardware Security Module* (HSM)[80] per impedire la compromissione delle credenziali crittografiche, che renderebbe vana la protezione.



[74] Processo di creazione e assegnazione di un'identità digitale e dei relativi permessi di accesso a un utente, applicazione o dispositivo all'interno dei sistemi informativi.
[75] Processo di revoca e rimozione dei diritti di accesso di un utente, applicazione o dispositivo, incluso il blocco o l'eliminazione delle credenziali, per evitare la permanenza di utenze non autorizzate.
[76] Principio di sicurezza che limita l'accesso alle informazioni esclusivamente agli utenti che ne hanno necessità per svolgere le proprie mansioni, riducendo l'esposizione ai rischi interni.
[77] Principio organizzativo che prevede la separazione di attività e responsabilità critiche tra più persone, per evitare che un singolo individuo possa svolgere operazioni sensibili senza controlli incrociati.
[78] Dati conservati in forma statica su supporti o sistemi di archiviazione, come server, database o dispositivi locali, che devono essere protetti tramite crittografia e controlli di accesso.
[79] Dati trasmessi attraverso reti interne o esterne, inclusi Internet e VPN, che devono essere cifrati durante il trasferimento per impedirne l'intercettazione o la manipolazione.
[80] Dispositivo hardware dedicato alla generazione, protezione e gestione sicura delle chiavi crittografiche, progettato per prevenire accessi non autorizzati e garantire elevati livelli di sicurezza nelle operazioni crittografiche.

12.5 Resilienza Operativa: Backup e Test

La Cyber Hygiene trasforma il backup da semplice operazione di routine a strumento certificato di resilienza.

- **Verifica e Test:** Non è sufficiente eseguire le copie di sicurezza; è obbligatorio verificarne periodicamente la leggibilità e l'integrità. La norma impone l'esecuzione di *Test di Restore* (ripristino) con cadenza almeno **mensile**. Solo testando il ripristino è possibile validare concretamente i parametri di RPO e RTO definiti nel piano di continuità .
- **Backup Offline:** Come misura specifica di contrasto al *ransomware*, per i Soggetti Essenziali vige il requisito del backup disconnesso fisicamente o logicamente dalla rete (*air-gapped*[81]) o salvato su supporti *cloud* immutabili[82]. Questo garantisce che, anche in caso di compromissione totale della rete aziendale, esista una copia dei dati non cifrabile dall'attaccante.

12.6 Cultura della Sicurezza e Formazione

Riconoscendo che il fattore umano è spesso l'anello debole della catena difensiva, la NIS2 impone obblighi formativi strutturati per diffondere una cultura della sicurezza a tutti i livelli .

- **Formazione Generale:** Tutti i dipendenti devono seguire una formazione periodica in materia di sicurezza informatica con frequenza minima annuale. Tali corsi devono includere una verifica formale dell'apprendimento (test finale) per essere validi ai fini della *compliance* e dimostrare l'acquisizione delle competenze necessarie a riconoscere le minacce.
- **Formazione Specialistica:** È prevista una formazione tecnica avanzata riservata specificamente ai ruoli IT, agli amministratori di sistema e ai team di sicurezza, per mantenerli aggiornati sulle nuove tecniche di attacco e difesa.

---

[81] Soluzione di sicurezza in cui il sistema o il supporto di backup è fisicamente o logicamente isolato dalla rete, impedendo qualsiasi connessione che potrebbe consentire a malware o attaccanti di raggiungerlo.
[82] Sistemi di archiviazione in cloud configurati in modalità “immutabile”, cioè non modificabile né cancellabile per un periodo definito. Proteggono le copie di backup da manomissioni, sovrascritture o cifrature, anche in caso di compromissione dell’ambiente principale.

12.7 Il Ciclo di Manutenzione della Compliance

La Cyber Hygiene alimenta il ciclo di conformità fornendo le evidenze documentali (log, report di patching, registri di formazione) necessarie a dimostrare la *due diligence* in caso di ispezione. Un pilastro della manutenzione è l'aggiornamento dell'analisi dei rischi: sebbene il monitoraggio sia continuo, la normativa impone una revisione formale e completa del *Risk Assessment* almeno **ogni due anni**. Per i Soggetti Essenziali, tale obbligo di manutenzione include l'esecuzione mandataria di *Vulnerability Assessment* e *Penetration Test* prima della messa in esercizio di ogni nuovo sistema critico, per validarne la sicurezza *by design*[83].

13. Resilienza Operativa: IR, DR e BC

La Direttiva NIS2 e il Decreto Legislativo n. 138/2024 elevano la resilienza operativa a obbligo fondamentale del Risk Management. Il concetto di resilienza non si limita alla semplice difesa, ma si definisce come la capacità di un'organizzazione di resistere, assorbire, rispondere e riprendersi da attacchi o guasti, mantenendo l'operatività. Per attuare questo principio, è necessario un approccio integrato che orchestri tre discipline distinte ma interdipendenti:

- **Incident Response (IR):** La risposta operativa immediata all'emergenza;
- **Disaster Recovery (DR):** Il ripristino tecnologico dei sistemi e dei dati;
- **Business Continuity (BC):** La strategia di sopravvivenza dei processi di business;

[83] Principio secondo cui un sistema, servizio o applicazione deve essere progettato fin dall'origine integrando misure di sicurezza adeguate. Prevede che ogni componente sia sviluppato, configurato e testato per ridurre vulnerabilità, minimizzare la superficie d'attacco e garantire protezione preventiva, anziché applicare la sicurezza solo in fase successiva.

13.1 Incident Response (IR): Reazione Operativa Immediata

L'Incident Response non è una semplice procedura burocratica, ma la capacità reattiva e strutturata dell'organizzazione di gestire un evento avverso in tempo reale. La risposta è gestita da un team interno di Incident Response: una funzione multidisciplinare che coordina le attività tecniche e organizzative insieme al Referente CSIRT, che mantiene il raccordo operativo con il CSIRT Italia per le notifiche e le attività obbligatorie.

Il piano di IR deve allinearsi alla funzione *RESPOND* del Framework Nazionale (FNCSDP), trasformando la reazione da improvvisata a procedurale e distinguendo la natura dell'evento:

Evento di Sicurezza		Qualsiasi occorrenza osservabile (es. un login utente).
Allarme (*Alert*)		Evento segnalato come sospetto da uno strumento di sicurezza.
Incidente		Allarme verificato e confermato da un analista, indica una violazione in atto o imminente (es. infezione da codice malevolo o esfiltrazione dati)

Strumenti Tecnologici e Workflow

Per una risposta efficace, l'organizzazione deve dotarsi di un'attrezzatura adeguata a rilevare qualsiasi tipo di minaccia e di strumenti per automatizzare i flussi comunicativi:

- **SIEM (*Security Information and Event Management*):** Agisce come il *cervello* della sicurezza per la raccolta centralizzata, la normalizzazione e la correlazione dei log provenienti da diverse fonti, essenziale per distinguere i falsi positivi dagli incidenti reali;
- **EDR (*Endpoint Detection and Response*):** Funge da *sentinella* per il monitoraggio in tempo reale dei dispositivi periferici, capace di bloccare processi malevoli o isolare l'host.
- **Workflow Automatizzato:** È necessario mantenere un *sistema di ticketing*[84] o un workflow che automatizzi il flusso delle comunicazioni, garantendo la tracciabilità di ogni azione per le successive analisi forensi o legali .

[84] Piattaforma software utilizzata per registrare, assegnare, tracciare e gestire le attività operative e le segnalazioni di sicurezza. Garantisce tracciabilità, ordine cronologico e responsabilità chiare durante la gestione di un incidente.

Ciclo di Risposta

Il processo operativo segue fasi rigorose, dettagliate nelle procedure interne di gestione:

1. **Preparazione:** Definizione di ruoli, responsabilità, metodologie di intervento e procedure di *escalation*[85]. Questa fase include la predisposizione degli strumenti hardware/software necessari e la formazione specifica del personale che potrebbe ricevere le prime segnalazioni (es. Help Desk o uffici amministrativi);

2. **Identificazione e Analisi (Triage):** Questa è la fase critica in cui si valuta se un evento anomalo è un falso positivo o un incidente reale, la segnalazione può arrivare da sistemi automatici o da utenti. Una volta confermato l'incidente, si procede alla classificazione della gravità, basata su parametri quali la criticità dell'asset (definita dal BIA), il numero di utenti impattati, l'esposizione su internet e il tipo di danno (economico, reputazionale o normativo). Per la gestione interna, si adotta una **Matrice di Gravità** operativa:
    - **Gravità Alta:** Compromissione di sistemi che permettono accessi incontrollati a dati confidenziali, interruzione di servizi critici per oltre 30 minuti, frodi o danni reputazionali significativi. Richiede attivazione immediata del *Crisis Management Team*;
    - **Gravità Media:** Degrado delle prestazioni, funzionamento intermittente della rete, compromissione di server non critici o impatti circoscritti che non bloccano il core business[86].
    - **Gravità Bassa:** Interruzione limitata a poche postazioni, infezioni malware contenute automaticamente dagli antivirus, nessuna perdita di operatività significativa.

3. **Contenimento:** Le operazioni di contenimento hanno il duplice obiettivo di fermare la propagazione del danno e preservare le evidenze per l'analisi forense. Si dividono in due momenti tattici distinti :
    - **Contenimento a Breve Termine:** Azioni *chirurgiche* immediate per mettere in sicurezza i sistemi, ad esempio la creazione di regole firewall di blocco, la disabilitazione di account compromessi, il cambiamento di configurazioni DNS o la disconnessione fisica/logica dalla rete (*air-gap*)[87]. In questa fase è cruciale

[85] Sequenza strutturata di passaggi che definisce chi deve essere informato, in quali tempi e con quali responsabilità quando si verifica un evento di sicurezza, garantendo una risposta coordinata e tempestiva.
[86] Insieme delle attività principali da cui dipende la missione operativa e il valore economico dell'organizzazione; la loro interruzione comporta impatti significativi su servizi, operatività e redditività.
[87] Isolamento fisico o logico di un sistema o dispositivo dalla rete, per impedire che possa essere raggiunto da attaccanti o malware durante le attività di contenimento o protezione.

non spegnere brutalmente le macchine per non perdere i dati volatili nella RAM (vedi focus) e malevoli identificati. Queste azioni rendono il sistema "più sicuro" ma non ancora bonificato;

- **Contenimento a Lungo Termine:** Misure temporanee per mantenere l'operatività in attesa della bonifica, come l'applicazione di *patch* di emergenza[88], l'arresto di processi sospetti o la modifica delle configurazioni di sicurezza.

Focus

Conservazione delle Evidenze e Acquisizione Forense Prima di eseguire qualsiasi operazione potenzialmente distruttiva (come lo spegnimento, il riavvio o la formattazione del sistema) è fondamentale considerare che tali azioni causano la perdita definitiva dei dati volatili presenti in RAM, spesso essenziali per l'indagine (processi attivi, connessioni in corso, chiavi temporanee, artefatti di malware e tracce non ancora salvate su disco). In presenza, o anche solo in previsione, di un possibile risvolto legale, civile o penale, l'organizzazione deve procedere con una **acquisizione forense completa**, comprendente la copia dei dischi, il dump della memoria RAM e la raccolta dei log e delle configurazioni pertinenti. L'intera **catena di custodia** deve essere documentata con precisione, riportando persone coinvolte, date, strumenti e modalità utilizzate, per garantire l'integrità e l'opponibilità delle evidenze in sede giudiziaria.

4. **Rimozione:** Consiste nell'eliminazione definitiva della causa radice. Le attività possono includere l'aggiornamento dei sistemi, la rimozione di servizi vulnerabili (*hardening*) o, nel caso di infezioni profonde, la ricostruzione completa della macchina partendo da un'immagine sicura (*Gold Image*) o dai supporti di installazione originali. Questa fase può richiedere tempi lunghi per l'approvvigionamento di nuovo hardware o licenze;

5. **Ripristino:** È la fase di riattivazione dei sistemi in produzione, la decisione sul *quando* ripartire spetta al responsabile della sicurezza. Il ripristino deve avvenire solitamente in orari non lavorativi e richiede un monitoraggio rafforzato (*Hyper-care*) per verificare che l'attaccante non abbia mantenuto meccanismi di persistenza o che l'incidente non si ripresenti;

[88] Aggiornamento correttivo rilasciato in via straordinaria per risolvere rapidamente una vulnerabilità critica o un malfunzionamento grave che espone il sistema a rischi immediati. Viene applicata prima degli aggiornamenti ordinari per ridurre il tempo di esposizione all'attacco.

6. **Attività Post-Incidente (*Lessons Learned*):** Contestualmente alla chiusura formale della segnalazione, è mandatorio avviare una fase di analisi critica (*Post-Incident Review*) finalizzata a trasformare l'evento in valore strategico per la resilienza organizzativa. La metodologia di analisi deve seguire rigorosamente un approccio non colpevolizzante: l'indagine non deve mirare all'individuazione di responsabilità individuali (*human error*), bensì all'identificazione delle vulnerabilità sistemiche e delle lacune processuali che hanno reso possibile l'incidente . Gli esiti di tale attività devono essere formalizzati nel rapporto di incidente, il quale deve essere conservato in archivi sicuri per un periodo minimo di **5 anni** per finalità di *audit* e *compliance*. Il documento deve esaminare aspetti sistemici quali: l'accuratezza della classificazione iniziale della gravità, la tempestività dei flussi di comunicazione e l'adeguatezza degli strumenti tecnologici o delle competenze disponibili. Tali evidenze costituiscono il presupposto per la definizione di azioni correttive strutturali volte a implementare miglioramenti su persone, processi e tecnologie .

Data Breach e Gestione GDPR

È fondamentale distinguere operativamente tra "Incidente di Sicurezza" e "**Data Breach**". Mentre ogni Data Breach è un incidente di sicurezza, non è vero il contrario. Un Data Breach si configura specificamente quando la violazione comporta accidentalmente o illecitamente la distruzione, perdita, modifica, divulgazione o accesso non autorizzato a **dati personali**. Le tipologie di violazione GDPR sono tre:

1. **Violazione di Riservatezza:** Divulgazione o accesso non autorizzato.
2. **Violazione di Integrità:** Alterazione non autorizzata dei dati.
3. **Violazione di Disponibilità:** Perdita o distruzione accidentale .

Data Protection Officer (DPO)

La gestione di questo processo ruota attorno alla figura del **DPO** (*Data Protection Officer*). Si tratta di una funzione di garanzia obbligatoria in determinati contesti, incaricata di vigilare sulla conformità al regolamento privacy e di fungere da punto di contatto con l'Autorità Garante. Caratteristiche fondamentali del DPO sono la sua indipendenza e autonomia: non risponde gerarchicamente alla direzione per l'esecuzione dei suoi compiti, garantendo così un giudizio imparziale.

Valutazione del Rischio e Notifica

In caso di violazione, il DPO deve essere coinvolto immediatamente per esprimere un parere formale sulla gravità dell'accaduto. La valutazione deve determinare se la violazione presenta un rischio per i diritti e le libertà delle persone fisiche, basandosi su criteri oggettivi quali: la natura e il volume dei dati, la facilità di identificazione degli interessati e la gravità delle conseguenze (danni materiali o immateriali).

Se la valutazione evidenzia un rischio probabile, scatta l'obbligo di notifica al **Garante della Privacy**[89] entro **72 ore** dalla conoscenza dell'evento. La notifica deve obbligatoriamente contenere:

- La natura della violazione e le categorie di dati/interessati coinvolti;
- I dati di contatto del DPO;
- Le probabili conseguenze della violazione;
- Le misure adottate o proposte per porre rimedio alla violazione e attenuarne gli effetti negativi.

Se il rischio per gli interessati è valutato come elevato, è obbligatoria anche la comunicazione diretta agli interessati "senza ingiustificato ritardo". Tale comunicazione deve essere formulata con un linguaggio chiaro e semplice (evitando tecnicismi), per permettere agli utenti di comprendere la natura del rischio e adottare le necessarie contromisure.

13.2 Disaster Recovery (DR): Il Recupero Tecnologico e Infrastrutturale

Mentre l'Incident Response gestisce la reazione logica all'attacco, il Disaster Recovery (DR) si occupa della sopravvivenza fisica e tecnologica dell'infrastruttura. Si attiva esclusivamente in caso di *Disastro*, definito tecnicamente come un evento imprevisto e di ampia portata che causa un'interruzione prolungata delle operazioni IT, rendendo l'infrastruttura primaria inutilizzabile (es. incendio del Data Center, alluvione, attacco irreversibile).

Per attivare correttamente il DR, è necessario distinguere la gravità dell'evento sulla base della scala temporale e dell'impatto :

- **Incidente:** Durata di qualche ora, impatto limitato (es. un singolo server), gestito manualmente tramite *Incident Response*;
- **Crisi:** Durata di giorni, richiede interventi improvvisi e un controllo di alto livello manageriale;

[89] Autorità amministrativa indipendente (Autorità Garante per la Protezione dei Dati Personali) incaricata di vigilare sull'applicazione del GDPR in Italia, garantire la tutela dei dati personali e dei diritti degli interessati, ricevere le notifiche di violazione (data breach) ed emettere provvedimenti e sanzioni.

- **Disastro:** Durata di settimane, richiede interventi eccezionali e l'attivazione di siti alternativi;
- **Catastrofe:** Durata di mesi, potrebbe richiedere la ricostruzione totale dell'infrastruttura.

Le Metriche RTO e RPO

Il Disaster Recovery non si basa su stime approssimative, ma su due parametri matematici, che guidano ogni investimento tecnologico:

- **RTO (*Recovery Time Objective*)**: È il tempo massimo accettabile per ripristinare un servizio dopo un disastro.
  Risponde alla domanda: *"Quanto tempo possiamo permetterci di stare fermi?"*
  - *Esempio RTO Basso (1 ora):* Una piattaforma di e-commerce, dove ogni ora di fermo causa perdite dirette di fatturato.
  - *Esempio RTO Alto (24 ore):* Un server di test per sviluppatori, il cui impatto sul business è minimo. Un RTO basso non è necessario e richiederebbe tecnologie di replica sincrona o *clustering* ad alto costo.

- **RPO (*Recovery Point Objective*)**: Definisce la quantità massima di dati (misurata in tempo) che l'organizzazione è disposta a perdere tra l'ultimo backup valido e l'evento disastroso.
  Risponde alla domanda: *"Quanti dati possiamo permetterci di perdere?"*
  - *Esempio RPO Basso (15 minuti):* Un database di transazioni finanziarie.
  - *Esempio RPO Alto (24 ore):* Un *file server* documentale interno. Questo parametro determina la frequenza tecnica dei backup o della replica dei dati.

Disaster Recovery Plan

Il piano di DR (DRP) non è un documento di *policy* astratto, ma una guida specifica che il personale tecnico deve seguire durante la crisi. Il DRP deve contenere tassativamente :

- **Inventario Dettagliato:** Lista aggiornata di hardware, software, licenze e configurazioni.
- **Catena di Comando:** Elenco dei contatti di emergenza, fornitori critici e responsabili decisionali.
- **Mappatura delle Priorità:** Identificazione delle applicazioni critiche associate ai loro specifici RTO/RPO.
- **Procedure di Ripristino:** Istruzioni tecniche sequenziali per riattivare ogni singolo sistema.

Strategie di Recovery: Il Trade-off Costi/Prestazioni

La selezione della strategia di *Disaster Recovery* non è una scelta tecnica isolata, ma il risultato di un compromesso diretto tra l'investimento sostenibile e la velocità di ripristino richiesta (RTO).

Le opzioni disponibili si ordinano per complessità e costi crescenti :

1. **Backup & Restore:** Rappresenta la soluzione più semplice e meno costosa. Consiste nel salvare copie dei dati su supporti esterni per poi ripristinarli su nuovo hardware in caso di incidente. Sebbene il costo sia contenuto, comporta un **RTO molto alto** (spesso giorni), poiché richiede il reperimento fisico delle macchine e tempi tecnici di *restore* lunghi.

2. **Cold Site:** Prevede la disponibilità di un sito alternativo predisposto con l'infrastruttura di base (elettricità, condizionamento, cablaggio di rete), ma privo di hardware attivo. Anche in questo caso i costi sono bassi, ma l'**RTO rimane alto**, in quanto è necessario attendere l'approvvigionamento e l'installazione fisica dei server prima di poter avviare il ripristino.

3. **Warm Site:** Si tratta di un sito già equipaggiato con hardware e connettività pronti all'uso, ma dove i dati non sono allineati in tempo reale (richiedono il caricamento dell'ultimo backup disponibile). Questa soluzione offre un buon compromesso, garantendo un **RTO e costi medi**.

4. **Hot Site:** È un clone speculare del data center primario, dotato di replica dei dati sincrona in tempo reale. In caso di disastro, il passaggio al sito secondario (*failover*) è

quasi istantaneo garantendo quindi un **RTO molto basso** (minuti), ma comporta costi infrastrutturali molto elevati dovendo mantenere doppia dotazione attiva.

5. **Cloud DR:** Rappresenta l'approccio più flessibile. Sfrutta le risorse di un *cloud provider*[90] per attivare la capacità di calcolo solo nel momento dell'emergenza. Grazie al modello *pay-per-use*[91], offre costi e tempi di ripristino (**RTO**) variabili e scalabili in base alle esigenze specifiche del momento.

Attività di Test

Un piano di DR non testato è solo un'ipotesi, un piano testato è una capacità reale. La normativa e le *best practice* impongono test periodici per validare l'efficacia delle procedure . Le tipologie di test si distinguono per impegno e frequenza :

. **Checklist Review:** Verifica documentale che il piano, i contatti e gli inventari siano aggiornati.
   - *Frequenza:* Alta (es. mensile/trimestrale)
   - *Impegno:* Basso

[90] Fornitore di servizi cloud che mette a disposizione infrastrutture, piattaforme o applicazioni accessibili via Internet, consentendo alle organizzazioni di utilizzare capacità di calcolo, archiviazione e rete senza possedere fisicamente l'hardware.
[91] Modello di tariffazione in cui i costi dipendono esclusivamente dalle risorse effettivamente utilizzate. Nel disaster recovery cloud permette di pagare solo l'infrastruttura attivata durante l'emergenza, evitando costi fissi continuativi.

. **Simulazione:** I membri del team discutono verbalmente le azioni da intraprendere in uno scenario di disastro specifico, verificando i processi decisionali.
    - *Frequenza:* Trimestrale
    - *Impegno:* Medio
. **Full Failover Test:** Attivazione reale del sito di Disaster Recovery con spostamento dei carichi di lavoro. È l'unico test che certifica il rispetto dei tempi RTO/RPO, ma comporta rischi operativi.
    - *Frequenza:* Annuale
    - *Impegno:* Alto

13.3 Business Continuity (BC)

La **Business Continuity (BC)** rappresenta il livello strategico apicale della resilienza. A differenza del Disaster Recovery, che si focalizza sul ripristino tecnologico, la BC è la capacità olistica di un'organizzazione di continuare a erogare prodotti e servizi a livelli predefiniti accettabili durante un'interruzione operativa. Non si tratta di un piano tecnico, ma di una strategia di business finalizzata a garantire la sopravvivenza dell'intera organizzazione, preservandone produttività, reputazione e valore.

Come stabilito dall'Articolo 24 del D.Lgs. 138/2024, la continuità operativa è un elemento obbligatorio della gestione del rischio. Secondo lo standard di riferimento **ISO/IEC 27031**, un piano efficace deve coprire tre aspetti (resilienza proattiva, recupero rapido e gestione dell'emergenza) e avvalersi di tre tipologie di misure :

. **Misure Preventive:** Per evitare che l'evento accada;
. **Misure Investigative:** Per rilevare l'evento indesiderato;
. **Misure Correttive:** Per ripristinare il sistema post-incidente/disastro.

Business Impact Analysis (BIA): Il Cuore della Strategia

Il fondamento di qualsiasi piano di continuità è la **Business Impact Analysis (BIA)**. Questo processo analitico sistematico risponde alla domanda cruciale: *"Cosa dobbiamo proteggere per primo e perché?"*. La BIA non si basa su supposizioni, ma analizza l'organizzazione attraverso tre pilastri fondamentali:

. **Funzioni di Business Critiche:** Identificazione dei processi vitali senza i quali l'azienda cesserebbe di esistere o subirebbe danni irreparabili (es. produzione, fatturazione);
. **Impatto dell'Interruzione:** Valutazione quantitativa e qualitativa del danno su scala temporale (es. impatto dopo 1 ora, 1 giorno, 1 settimana). L'analisi considera impatti

finanziari (perdita di fatturato), operativi (stop produzione), legali (violazione contratti/normative) e reputazionali (perdita di fiducia);

. **Dipendenze:** Mappatura delle risorse necessarie per sostenere le funzioni critiche, incluse risorse IT, personale chiave, fornitori essenziali e strutture fisiche.

Focus

I risultati della **Business Impact Analysis (BIA)** definiscono in modo diretto i requisiti tecnici del piano di *Disaster Recovery*. La BIA agisce come un "ponte" che traduce le esigenze astratte di business in parametri IT misurabili (*RTO* e *RPO*), garantendo che l'infrastruttura tecnologica sia dimensionata esattamente per supportare la continuità operativa richiesta.

Il processo segue una sequenza rigida in tre fasi:

1. **Esigenze di Business:** Si identifica la funzione critica e si quantifica il danno economico/operativo di un fermo.
2. **Parametri IT:** Si converte la tolleranza al danno in metriche temporali (RTO/RPO).
3. **Strategia DR:** Si sceglie la soluzione tecnologica capace di soddisfare quei parametri.

Analliziamo il caso di un sistema di fatturazione critico, dove ogni ora di fermo genera perdite significative:

Fase 1: Funzione Critica (Business)	
Processo	Fatturazione
Impatto	Perdita stimata di **€10.000/ora**
Tolleranza	L'azienda può reggere al massimo **4 ore** di fermo

Fase 2: Requisiti IT (Parametri)	
RTO (Tempo)	Il sistema *deve* ripartire entro **4 ore**
RPO (Dati)	La perdita massima di dati accettabile è **15 minuti.**

Fase 3: Strategia DR (Tecnologia)	
Soluzione	Adozione di un *Hot Site* o *DRaaS* (Disaster Recovery as a Service) con *Replica Continua* dei dati

(Nota: Un semplice backup notturno non sarebbe sufficiente perché violerebbe l'RPO di 15 minuti).

In sintesi: non è l'IT a decidere arbitrariamente di acquistare un sistema di replica costoso, ma è l'esigenza di business (evitare una perdita di 10.000€/ora) a imporre tecnicamente quella specifica strategia di Disaster Recovery.

Il Business Continuity Plan (BCP)

Il *BCP* è il **manuale operativo** che traduce l'analisi in procedure attuabili. Deve essere un documento dinamico, aggiornato regolarmente per riflettere i cambiamenti organizzativi (personale, tecnologie, processi). Le componenti essenziali del BCP includono:

- **Strategie di Continuità:** Procedure concrete per mantenere l'operatività in modalità degradata. Queste includono:
  - Siti Alternativi, identificazione di luoghi di lavoro di backup;
  - Lavoro da Remoto, protocolli per lo spostamento massivo della forza lavoro in smart working;
  - Procedure Manuali, istruzioni per operare temporaneamente in analogico (*carta e penna*) qualora i sistemi IT siano indisponibili.
- **Gestione della Supply Chain:** Identificazione dei fornitori critici e attivazione di piani alternativi per garantire l'approvvigionamento di beni o servizi essenziali qualora un partner primario sia bloccato, in linea con i requisiti di sicurezza della catena di approvvigionamento previsti dall'Art. 24.
- **Piani di Recupero e Reintegro:** Istruzioni per il ritorno graduale alla normalità, che prevedono il coordinamento del rientro del personale nelle sedi e la riattivazione sequenziale dei processi di business;
- **Testing e Manutenzione**: Un piano non testato è pressoché inutile, La resilienza richiede infatti un ciclo continuo di validazione attraverso simulazioni di spostamento in siti alternativi e test completi di *failover*[92]. Il piano deve essere aggiornato regolarmente per riflettere cambi di personale o tecnologie.

Governance della Crisi: La Doppia Catena di Comando

In caso di evento maggiore, la gestione efficace richiede l'attivazione di due strutture di comando distinte ma strettamente coordinate, per separare la gestione tecnica da quella decisionale:

- **CMT (Crisis Management Team):** È l'organo decisionale strategico, guidato dai vertici aziendali. Il suo obiettivo è la sopravvivenza del business: prende decisioni di alto livello (es. chiusura sedi, allocazione budget straordinari), gestisce la comunicazione istituzionale (interna ed esterna verso media/clienti) e coordina gli stakeholder per contenere il danno reputazionale;

[92] Verifiche operative che simulano l'interruzione dei sistemi principali per attivare l'infrastruttura di backup o il sito alternativo, con l'obiettivo di confermare che la continuità dei servizi possa essere garantita senza perdita di dati o malfunzionamenti.

. **CSIRT (Computer Security Incident Response Team):** È l'organo operativo tecnico, lavora per la risoluzione dell'incidente informatico: si occupa del contenimento, dell'analisi tecnica e dell'eradicazione della minaccia. (Approfondimento al Capitolo 5)

Focus

L'Ecosistema Integrato della Resilienza Per comprendere la reale portata della NIS2, è necessario superare la visione a compartimenti stagni: Business Continuity (BC), Disaster Recovery (DR) e Incident Response (IR) sono ingranaggi sincronizzati di un unico meccanismo di difesa. Per visualizzare questa sinergia, analizziamo lo scenario di un Incendio presso il Data Center Principale:

1. Attivazione Strategica (BC): È la prima a scattare. Il *Crisis Management Team* dichiara la crisi: vengono attivati il lavoro da remoto, la comunicazione di crisi ai clienti e le procedure manuali di emergenza. Si cerca di prendere tempo, mantenendo l'azienda operativa.
2. Ripristino Tecnologico (DR): In parallelo, il team IT attiva il piano di *Failover*. Poiché l'infrastruttura fisica è compromessa, i servizi vengono ripristinati su un sito secondario o in *cloud* seguendo le priorità di business (RTO). L'obiettivo del DR è restituire gli strumenti digitali per permettere alla BC di abbandonare le procedure di emergenza.
3. Supporto Operativo (Incident Response): Il team CSIRT interviene per gestire gli aspetti di sicurezza dei dati: in uno scenario fisico verifica l'eventuale esposizione di archivi o server; in uno scenario cyber (es. *ransomware*), l'IR lavorerebbe per contenere la minaccia e bonificare i sistemi prima che il DR li ripristini.

In sintesi: La BC garantisce la sopravvivenza del business, il DR ricostruisce l'infrastruttura abilitante e l'IR risolve la causa scatenante. Solo l'orchestrazione di questi tre livelli assicura la conformità e la tenuta del sistema.

16. Sicurezza della Supply Chain:

La **Supply Chain** (o catena di approvvigionamento) è definibile come l'ecosistema complesso di organizzazioni, persone, attività, informazioni e risorse coinvolte nel processo di creazione e distribuzione di un prodotto o servizio, dal reperimento delle materie prime fino al consumatore finale. Essa comprende, in un flusso continuo, le fasi di approvvigionamento, produzione, stoccaggio e distribuzione, con l'obiettivo di garantire che il prodotto raggiunga il cliente nel modo più efficiente e rapido possibile.

16.1 Vulnerabilità

Nel contesto economico attuale, molte imprese svolgono attività di importanza cruciale senza esserne pienamente consapevoli: i loro servizi, prodotti o componenti rappresentano spesso elementi indispensabili per l'operatività di organizzazioni di dimensioni maggiori o di rilevanza strategica nazionale. La società contemporanea è caratterizzata da una rete così fitta di interconnessioni economiche e tecnologiche che risulta sempre più arduo mappare in modo esaustivo tutti i legami di dipendenza reciproca lungo la filiera.

Un'interruzione anche minima in un servizio apparentemente marginale può innescare conseguenze imprevedibili su scala macroscopica. Questo fenomeno richiama il celebre "*effetto farfalla*": un malfunzionamento in una componente minore della catena (un software gestionale di nicchia, un modulo elettronico, un fornitore di servizi cloud ausiliario) può compromettere la funzionalità di intere filiere industriali o infrastrutture critiche, impattando sulla sicurezza nazionale e sulla continuità dei servizi essenziali.

16.2 Responsabilità Condivisa

Ogni organizzazione, indipendentemente dal proprio ruolo o dalle dimensioni, è oggi tenuta a farsi garante della sicurezza dei propri fornitori e partner, poiché da essi dipende la propria resilienza. In questa logica, i fornitori cessano di essere figure di supporto esterno e diventano invece *soggetti critici*. Il principio guida della Commissione Europea è la responsabilità condivisa: ogni componente deve assumersi la propria quota di responsabilità nella tutela della sicurezza collettiva. solo così è possibile costruire un sistema realmente resiliente, in cui la protezione della *Supply Chain* diventa un imperativo culturale prima ancora che normativo.

16.3 Criteri di Valutazione dell'Adeguatezza

Nel valutare l'adeguatezza delle misure verso la filiera, i soggetti obbligati devono tenere conto:

- Delle vulnerabilità specifiche di ogni fornitore diretto;
- Della qualità complessiva dei prodotti e delle pratiche di sicurezza adottate dai fornitori;
- Delle procedure di sviluppo sicuro implementate dai partner tecnologici;
- Dei risultati delle valutazioni coordinate dei rischi effettuate a livello europeo dal Gruppo di cooperazione NIS sulle catene di fornitura critiche.

Attraverso questa formulazione si estende il perimetro di responsabilità oltre i confini fisici dell'ente. Si riconosce che la vulnerabilità di un sistema non dipende solo dai controlli interni, ma anche dal livello di sicurezza dei soggetti esterni. Ne consegue che ogni organizzazione è chiamata a un ruolo proattivo di valutazione, selezione e monitoraggio dei fornitori, integrando la *Supply Chain Security* come dimensione strutturale del proprio *Risk Management*.

16.4 Integrazione nel Framework Nazionale e Linee Guida

Le Linee Guida NIS traducono l'obbligo di legge in azioni verificabili, mappando i requisiti normativi all'interno del Framework Nazionale per la Cybersecurity (FNCSDP).

Ruolo della Funzione GOVERN

La gestione della catena di fornitura non è un'attività tecnica isolata ma rientra nella funzione centrale di *GOVERN (GV)*, categoria **GV.SC** (*Gestione del rischio di cybersecurity della catena di approvvigionamento*). Questa collocazione conferma che la sicurezza dei fornitori è una questione di governance strategica.

Misure di Sicurezza Specifiche (Codici GV.SC)

Per garantire la conformità, le organizzazioni devono implementare i seguenti controlli specifici definiti dal Framework:

- **GV.SC-01 (Strategia):** Devono essere stabiliti e accettati dagli stakeholder il programma, la strategia, gli obiettivi e le politiche per la gestione del rischio di filiera;

- **GV.SC-02 (Ruoli):** I ruoli e le responsabilità di sicurezza per fornitori, clienti e partner devono essere definiti, comunicati e coordinati sia internamente che esternamente;
- **GV.SC-03 (Integrazione):** La gestione del rischio supply chain deve essere integrata nel *Risk Management* aziendale complessivo e nei processi di miglioramento continuo;
- **GV.SC-04 (Prioritizzazione):** I fornitori non sono tutti uguali, devono essere identificati e prioritizzati in base alla loro criticità per il business;
- **GV.SC-05 (Contrattualizzazione):** I requisiti di sicurezza devono essere stabiliti e formalmente integrati nei contratti e negli accordi di servizio con le terze parti;
- **GV.SC-07 (Monitoraggio):** I rischi posti dai fornitori e dai loro prodotti devono essere compresi, registrati e monitorati continuativamente per tutta la durata della relazione.

Conclusioni

L'analisi condotta nel presente documento evidenzia come l'attuazione della Direttiva NIS2 (D.Lgs. n. 138/2024) trascenda la natura di semplice adeguamento amministrativo, configurandosi come un imperativo strategico per la stabilità del sistema economico e sociale nazionale. Il passaggio da una logica di protezione perimetrale a una di *resilienza sistemica* impone alle organizzazioni una revisione strutturale dei propri modelli operativi. La sicurezza delle informazioni evolve da funzione tecnica di supporto ad asset strategico, elemento indispensabile per garantire la continuità operativa, la fiducia degli stakeholder e la competitività sul mercato.

Dall'esame dell'architettura normativa emerge con forza il principio della responsabilità diretta: gli organi di vertice non possono limitarsi a delegare la gestione del rischio, ma sono chiamati a governarlo, integrandolo nei processi decisionali e promuovendo una cultura della sicurezza che coinvolga l'intera organizzazione, dalla formazione del personale alla gestione della catena di approvvigionamento.

In definitiva, la conformità alla NIS2 non costituisce un punto di arrivo statico, bensì l'avvio di un **processo dinamico di miglioramento continuo**. L'integrazione di metodologie rigorose di *Risk Management* con le capacità operative di *Incident Response* e *Business Continuity* rappresenta l'unica garanzia per trasformare l'incertezza delle minacce attuali in una concreta capacità di reazione, adattamento e sviluppo in un ecosistema digitale sempre più complesso.