Giuseppe Serafini
Avvocato
G. S.
L. F.

White Paper

La Gestione degli Incidenti nell'Era NIS 2

Metodologie, Criteri di Significatività e Metriche per la Notifica Obbligatoria

Ns. Rif. G.S.:
15102025073000

Via S. Antonio n. 7 - 06012 - Città di Castello (PG).
Tel. 075.4652093 - Fax. 178 2213120
giuseppe.serafini@ordineavvocati.perugia.it – giuseppe.serafini@avvocatiperugiapec.it
P. IVA. 01929710547 - C. F. SRF GPP 71 L 20 B963 W

Via S. Antonio n. 7 - 06012 - Città di Castello (PG).
Tel. 075.4652093 - Fax. 178 2213120
giuseppe.serafini@ordineavvocati.perugia.it – giuseppe.serafini@avvocatiperugiapec.it
P. IVA. 01929710547 - C. F. SRF GPP 71 L 20 B963 W

Introduzione: La Resilienza Cibernetica

Il Cambio di Paradigma

L'entrata in vigore della Direttiva (UE) 2022/2555, nota come Direttiva NIS 2, segna un punto di svolta irrevocabile nella concezione della sicurezza cibernetica a livello europeo.

Superando l'impostazione della precedente Direttiva NIS del 2016, il nuovo quadro normativo abbandona un approccio basato prevalentemente sulla conformità formale per abbracciare una filosofia incentrata sulla gestione proattiva del rischio e sulla resilienza operativa.

La NIS 2 non rappresenta un mero aggiornamento, ma una vera e propria rifondazione della strategia di cybersicurezza dell'Unione, spinta dalla crescente interconnessione delle economie digitali e dalla constatazione che il numero, la portata, la sofisticazione e l'impatto degli incidenti informatici sono in costante aumento, rappresentando una grave minaccia per il funzionamento del mercato interno.

La Centralità della Gestione degli Incidenti

In questo rinnovato contesto, la gestione e la notifica degli incidenti di sicurezza informatica, disciplinate in particolare dagli articoli 21 e 23 della Direttiva, emergono come i pilastri fondamentali su cui poggia l'intero edificio normativo.

La capacità di un'organizzazione non solo di prevenire e proteggersi, ma anche di rilevare, gestire e comunicare efficacemente una crisi informatica, diventa la metrica principale per valutarne la maturità, la responsabilità e, in ultima analisi, l'affidabilità.

L'obbligo di notifica, con le sue tempistiche stringenti, cessa di essere un mero adempimento burocratico per trasformarsi in un meccanismo di condivisione delle informazioni essenziale per la difesa collettiva e la comprensione del panorama delle minacce a livello nazionale ed europeo.

Obiettivo del Saggio

Il presente saggio si propone di fornire una guida strategica e operativa per i soggetti designati come "essenziali" o "importanti" dalla nuova normativa.

L'analisi si concentrerà sulla decodifica del concetto di "incidente significativo", che funge da fattore scatenante per gli obblighi di notifica. Verranno esaminate le metodologie e i framework internazionali per la gestione degli incidenti, per poi tradurre i criteri normativi, spesso qualitativi, in un insieme di metriche e indicatori concreti e applicabili.

Via S. Antonio n. 7 - 06012 - Città di Castello (PG).
Tel. 075.4652093 - Fax. 178 2213120
giuseppe.serafini@ordineavvocati.perugia.it – giuseppe.serafini@avvocatiperugiapec.it
P. IVA. 01929710547 - C. F. SRF GPP 71 L 20 B963 W

L'obiettivo finale è quello di dotare i responsabili della sicurezza, della conformità e della gestione del rischio degli strumenti necessari per costruire una capacità di risposta agli incidenti che sia non solo conforme alla lettera della legge, ma anche efficace nel proteggere l'organizzazione e contribuire alla resilienza dell'ecosistema digitale in cui opera.

Capitolo 1: Il Contesto Normativo di Riferimento.

La comprensione degli obblighi in materia di gestione e notifica degli incidenti richiede la navigazione di un'architettura normativa strutturata su tre livelli gerarchici:

I. la Direttiva europea, che stabilisce i principi;
II. il decreto legislativo di recepimento nazionale, che li adatta al contesto italiano e assegna le responsabilità;
III. e le misure tecniche dell'autorità competente, che ne definiscono i dettagli operativi.

1.1. Livello 1 - La Direttiva (UE) 2022/2555 (NIS 2).

Al vertice della piramide normativa si colloca la Direttiva NIS 2, entrata in vigore nel gennaio 2023 che stabilisce i principi cardine che guidano l'azione degli Stati membri.

Un elemento di rottura rispetto al passato è l'ampliamento dell'ambito di applicazione poichè la Direttiva supera la vecchia distinzione tra Operatori di Servizi Essenziali (OSE) e Fornitori di Servizi Digitali (FSD), introducendo le nuove categorie di **Soggetti Essenziali (SE)** e **Soggetti Importanti (SI)**.

Questa classificazione, basata sulla criticità del settore e sulle dimensioni dell'entità, comporta un regime differenziato di vigilanza (più stringente per i SE) e sanzionatorio, ma uniforma gli obblighi fondamentali in materia di gestione del rischio e notifica degli incidenti.

L'**articolo 21** della Direttiva costituisce il fondamento della prevenzione e della preparazione. Esso impone ai soggetti SE e SI di adottare "misure tecniche, operative e organizzative adeguate e proporzionate" per gestire i rischi.

Queste misure devono basarsi su un approccio "onnicomprensivo" (*all-hazards*), che consideri non solo le minacce informatiche ma anche i rischi fisici e ambientali.

L'articolo elenca un catalogo minimo di misure obbligatorie, tra cui spiccano esplicitamente la "gestione degli incidenti" (*incident handling*) e la "continuità operativa", come la gestione dei backup e il ripristino in caso di disastro (*disaster recovery*).

Via S. Antonio n. 7 - 06012 - Città di Castello (PG).
Tel. 075.4652093 - Fax. 178 2213120
giuseppe.serafini@ordineavvocati.perugia.it – giuseppe.serafini@avvocatiperugiapec.it
P. IVA. 01929710547 - C. F. SRF GPP 71 L 20 B963 W

Il cuore della disciplina reattiva è invece l'**articolo 23**, che introduce l'obbligo di notifica per ogni "incidente significativo", ovvero un incidente che ha un impatto rilevante sulla fornitura dei servizi.

Questo articolo stabilisce i principi generali su "cosa" notificare (informazioni sull'impatto, sulla gravità, sulla causa probabile) e "quando" farlo, introducendo un processo a più fasi che mira a fornire alle autorità informazioni tempestive ma progressivamente più dettagliate.

1.2. Livello 2 - Il D.Lgs. 138/2024: Il Recepimento Nazionale

L'Italia ha recepito la Direttiva NIS 2 con il **Decreto Legislativo 4 settembre 2024, n. 138**, pubblicato in Gazzetta Ufficiale il 1° ottobre 2024 ed entrato in vigore il successivo 16 ottobre.

Questo atto normativo abroga il precedente D.Lgs. 65/2018 (di recepimento della NIS 1) e traspone le disposizioni europee nell'ordinamento giuridico italiano.

Il decreto conferma e rafforza il ruolo dell'**Agenzia per la Cybersicurezza Nazionale (ACN)** come Autorità nazionale competente NIS.

L'ACN assume una funzione di supervisione, regolamentazione e sanzione, agisce come Punto di contatto unico per la cooperazione transfrontaliera. All'interno di questa architettura, il **CSIRT Italia (Computer Security Incident Response Team)**, operante in seno all'ACN, è designato come il destinatario primario delle notifiche di incidente da parte dei soggetti obbligati.

L'**articolo 25 del D.Lgs. 138/2024**, intitolato "Obblighi in materia di notifica di incidente", è la norma chiave che recepisce l'articolo 23 della Direttiva. Esso formalizza il processo di notifica a più fasi, stabilendo scadenze perentorie e inderogabili:

I. **Pre-notifica (Early Warning):** I soggetti devono inviare un primo allarme al CSIRT Italia "senza ingiustificato ritardo e, in ogni caso, **entro 24 ore** dal momento in cui sono venuti a conoscenza dell'incidente significativo". Questa prima comunicazione deve indicare, se possibile, se si sospetta una causa dolosa o illegittima e se l'incidente potrebbe avere un impatto transfrontaliero.

II. **Notifica:** Successivamente, "senza ingiustificato ritardo e, in ogni caso, **entro 72 ore** dalla conoscenza dell'incidente", il soggetto deve inviare una notifica più completa. Questa deve aggiornare le informazioni della pre-notifica e includere una valutazione iniziale dell'incidente, la sua gravità, il suo impatto e, se disponibili, gli indicatori di compromissione (IoC).

Via S. Antonio n. 7 - 06012 - Città di Castello (PG).
Tel. 075.4652093 - Fax. 178 2213120
giuseppe.serafini@ordineavvocati.perugia.it – giuseppe.serafini@avvocatiperugiapec.it
P. IVA. 01929710547 - C. F. SRF GPP 71 L 20 B963 W

III. **Relazione Finale:** Su richiesta del CSIRT o dell'ACN, possono essere richiesti rapporti intermedi. In ogni caso, il soggetto è tenuto a presentare una relazione finale **entro un mese** dalla data della notifica di cui al punto precedente. Tale relazione deve contenere una descrizione dettagliata dell'incidente, la causa scatenante, le misure di mitigazione adottate e l'impatto transfrontaliero.

1.3. Livello 3 - Le Misure ACN: Le Specifiche Tecniche Operative

Il terzo e più operativo livello del quadro normativo è costituito dagli atti di attuazione dell'ACN. In particolare, la **Determina n. 164179/2025** e le annesse "Linee Guida NIS - Specifiche di base" rappresentano lo strumento che traduce gli obblighi di legge, spesso formulati in termini generali, in requisiti tecnici e tassonomie concrete.

Questi documenti sono strutturati attraverso una serie di allegati tecnici che distinguono nettamente tra:

I. **Misure di sicurezza di base (Allegati 1 e 2):** Dettagliano i requisiti minimi che i soggetti Importanti (Allegato 1) ed Essenziali (Allegato 2) devono implementare per adempiere agli obblighi di gestione del rischio di cui all'articolo 24 del decreto.

II. **Incidenti significativi di base (Allegati 3 e 4):** Forniscono una tassonomia precisa delle tipologie di incidenti che sono considerati "significativi" e che, pertanto, fanno scattare l'obbligo di notifica per i soggetti Importanti (Allegato 3) ed Essenziali (Allegato 4).

Questa struttura normativa gerarchica (Direttiva, Decreto, Determina ACN) deve essere letta in modo integrato. La conformità non può prescindere dalla comprensione di tutti e tre i livelli. Tuttavia, è l'interazione tra questi livelli a generare implicazioni strategiche profonde.

La scadenza perentoria di 24 ore per la pre-notifica, stabilita a livello europeo e recepita a livello nazionale, non è un semplice adempimento amministrativo, ma un potente catalizzatore di cambiamento organizzativo.

Rispettare tale termine richiede un processo di valutazione e classificazione dell'incidente quasi istantaneo. Il momento della "conoscenza" non coincide con il semplice allarme di un sistema di monitoraggio, ma con il momento in cui l'organizzazione qualifica quell'evento come un potenziale incidente significativo.

Svolgere un'analisi tecnica e di impatto sul business da zero, sotto la pressione di una crisi in corso, in meno di 24 ore è un'impresa estremamente ardua e soggetta a errori.

Via S. Antonio n. 7 - 06012 - Città di Castello (PG).
Tel. 075.4652093 - Fax. 178 2213120
giuseppe.serafini@ordineavvocati.perugia.it – giuseppe.serafini@avvocatiperugiapec.it
P. IVA. 01929710547 - C. F. SRF GPP 71 L 20 B963 W

Ne consegue che l'unico approccio sostenibile consiste nell'aver pre-definito, in tempo di pace, cosa costituisce un "incidente significativo" per la propria specifica realtà operativa, in linea con le tassonomie dell'ACN, e nell'aver predisposto dei *playbook* di risposta che si attivano in modo semi-automatico al verificarsi di determinate condizioni.

L'obbligo di notifica rapida, quindi, impone una transizione culturale e operativa: dalla gestione reattiva e improvvisata degli incidenti alla preparazione proattiva, alla simulazione e alla definizione di processi decisionali rapidi e formalizzati.

Capitolo 2: Fondamenti Metodologici

2.1. Un Approccio Strutturato come Prerequisito per la Conformità

L'articolo 24 del D.Lgs. 138/2024, nel delineare le misure di gestione dei rischi, richiede esplicitamente ai soggetti di dotarsi di procedure per la "gestione degli incidenti".

La normativa non prescrive uno specifico modello da adottare, ma fa riferimento allo "stato dell'arte" e agli "standard europei e internazionali pertinenti", quindi l'adozione di un framework di *incident management* consolidato, pertanto, non è una mera scelta di *best practice*, ma una necessità operativa per strutturare la propria capacità di risposta in modo efficace, ripetibile e, soprattutto, documentabile e difendibile in sede di vigilanza.

2.2. Il Ciclo di Vita secondo il NIST (SP 800-61)

Il National Institute of Standards and Technology (NIST) degli Stati Uniti, con la sua Special Publication 800-61, offre uno dei framework più autorevoli e diffusi a livello globale ed articola la gestione degli incidenti in un ciclo di vita composto da quattro fasi principali, che forniscono un approccio strategico all'intera capacità di risposta:

I. **Preparation (Preparazione):** Questa fase proattiva si concentra sulla creazione e il mantenimento di una capacità di risposta efficace. Include la definizione di policy e procedure, la formazione di un team di risposta (CSIRT), l'acquisizione e la configurazione di strumenti tecnologici (es. SIEM, EDR) e la conduzione di esercitazioni periodiche.

II. **Detection & Analysis (Rilevamento e Analisi):** È la fase in cui un potenziale incidente viene identificato e investigato. Le attività includono il monitoraggio continuo, l'analisi dei log e degli allarmi, la validazione degli indicatori di compromissione (IoC) e la determinazione della portata e dell'impatto dell'evento.

Via S. Antonio n. 7 - 06012 - Città di Castello (PG).
Tel. 075.4652093 - Fax. 178 2213120
giuseppe.serafini@ordineavvocati.perugia.it – giuseppe.serafini@avvocatiperugiapec.it
P. IVA. 01929710547 - C. F. SRF GPP 71 L 20 B963 W

III. **Containment, Eradication, & Recovery (Contenimento, Eradicazione e Ripristino):** Questa fase rappresenta la risposta attiva all'incidente. Il *contenimento* mira a limitare i danni e a impedire la propagazione della minaccia. L'*eradicazione* consiste nella rimozione completa dell'attaccante e dei suoi artefatti dai sistemi. Il *ripristino* si occupa di riportare i sistemi alla normale operatività in modo sicuro.

IV. **Post-Incident Activity (Attività Post-Incidente):** Questa fase cruciale, spesso trascurata, si concentra sull'apprendimento. Attraverso riunioni di *lessons learned*, si analizza la gestione dell'incidente, si identificano i punti di forza e di debolezza e si definiscono azioni correttive per migliorare le difese, le policy e le procedure di risposta.

2.3. Il Modello Tattico SANS PICERL

Il SANS Institute, leader mondiale nella formazione sulla sicurezza informatica, propone un modello in sei fasi, noto con l'acronimo PICERL. Questo framework è più granulare e orientato all'azione tattica durante la gestione di un incidente, rendendolo particolarmente utile per la formazione dei team operativi:

I. **Preparation (Preparazione):** Analoga alla fase NIST, si focalizza sulla preparazione di persone, processi e tecnologie.

II. **Identification (Identificazione):** Corrisponde al rilevamento e all'analisi, con l'obiettivo di confermare che un evento di sicurezza è effettivamente un incidente.

III. **Containment (Contenimento):** Fase dedicata a isolare i sistemi compromessi per prevenire ulteriori danni.

IV. **Eradication (Eradicazione):** Rimozione della causa radice dell'incidente (es. malware, account compromessi).

V. **Recovery (Recupero):** Ripristino dei sistemi e validazione della loro integrità prima di rimetterli in produzione.

VI. **Lessons Learned (Lezioni Apprese):** Analisi post-incidente per il miglioramento continuo, che si conclude tipicamente con un report dettagliato.

2.4. Lo Standard ISO/IEC 27035: Integrazione nel Sistema di Gestione

La serie di standard ISO/IEC 27035 è specificamente dedicata alla gestione degli incidenti di sicurezza delle informazioni.

Via S. Antonio n. 7 - 06012 - Città di Castello (PG).
Tel. 075.4652093 - Fax. 178 2213120
giuseppe.serafini@ordineavvocati.perugia.it – giuseppe.serafini@avvocatiperugiapec.it
P. IVA. 01929710547 - C. F. SRF GPP 71 L 20 B963 W

Il suo principale punto di forza è la sua progettazione per integrarsi nativamente con un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) conforme allo standard ISO/IEC 27001.

Il processo descritto è suddiviso in cinque fasi principali:

I. **Plan and Prepare (Pianificare e Preparare):** Sviluppo di policy, piani, procedure e creazione del team di risposta.

II. **Detect and Report (Rilevare e Segnalare):** Identificazione e segnalazione interna degli eventi di sicurezza.

III. **Assess and Decide (Valutare e Decidere):** Analisi degli eventi per determinare se costituiscono un incidente e decidere le azioni da intraprendere.

IV. **Respond (Rispondere):** Esecuzione delle attività di contenimento, eradicazione e ripristino.

V. **Learn Lessons (Imparare le Lezioni):** Analisi post-incidente e implementazione di miglioramenti.

2.5. Le Linee Guida Tecniche di ENISA

L'Agenzia dell'Unione Europea per la Cybersicurezza (ENISA) ha pubblicato delle "Technical implementation guidance on cybersecurity risk management measures" che traducono direttamente i requisiti dell'articolo 21 della NIS 2 in raccomandazioni operative.

La sezione 3, "Incident Handling", è di particolare rilevanza, in quanto fornisce indicazioni concrete su come strutturare la policy di gestione degli incidenti, le attività di monitoraggio e logging, le procedure di risposta e le revisioni post-incidente, in piena conformità con lo spirito della direttiva.

Un'analisi comparativa rivela che, al di là delle differenze terminologiche e del livello di granularità, tutti i principali framework internazionali condividono una struttura logica e ciclica comune, basata sulla sequenza preparazione-azione-post-analisi.

La scelta del framework più adatto dipende quindi dal contesto specifico dell'organizzazione. Il modello NIST è eccellente per un approccio strategico e integrato con la gestione del rischio complessiva.

Il modello SANS è ideale per la formazione e l'operatività quotidiana dei team di risposta. Lo standard ISO/IEC 27035 è la scelta naturale per le organizzazioni che hanno già adottato o intendono adottare un SGSI basato su ISO 27001.

Via S. Antonio n. 7 - 06012 - Città di Castello (PG).
Tel. 075.4652093 - Fax. 178 2213120
giuseppe.serafini@ordineavvocati.perugia.it – giuseppe.serafini@avvocatiperugiapec.it
P. IVA. 01929710547 - C. F. SRF GPP 71 L 20 B963 W

In questo scenario, le linee guida di ENISA non si configurano come un framework alternativo, ma piuttosto come una "chiave di lettura" o un "livello di traduzione".

Esse permettono alle organizzazioni di mappare i controlli e le procedure implementate secondo il framework prescelto (NIST, SANS, ISO o altro) rispetto agli obblighi specifici della Direttiva NIS 2.

In pratica, le organizzazioni non devono "reinventare la ruota", ma possono e devono adottare uno standard riconosciuto a livello internazionale e, successivamente, utilizzare le linee guida ENISA e le specifiche ACN come una "checklist di conformità" per assicurarsi che la loro implementazione sia completa, adeguata e allineata al nuovo contesto normativo.

Tabella 1: Framework di Incident Management

Fase Concettuale	NIST SP 800-61	SANS PICERL	ISO/IEC 27035
Preparazione e Prevenzione	Preparation	Preparation	Plan and Prepare
Rilevamento e Analisi	Detection & Analysis	Identification	Detect and Report; Assess and Decide
Contenimento	Containment, Eradication, & Recovery (parte di)	Containment	Respond (parte di)
Eradicazione	Containment, Eradication, & Recovery (parte di)	Eradication	Respond (parte di)
Ripristino e Recupero	Containment, Eradication, & Recovery (parte di)	Recovery	Respond (parte di)
Apprendimento e Miglioramento	Post-Incident Activity	Lessons Learned	Learn Lessons

Questa tabella dimostra visivamente la convergenza dei principi fondamentali, consentendo alle organizzazioni di integrare approcci diversi in base alle proprie esigenze specifiche, con la certezza di coprire tutte le fasi cruciali del ciclo di vita della gestione degli incidenti.

Via S. Antonio n. 7 - 06012 - Città di Castello (PG).
Tel. 075.4652093 - Fax. 178 2213120
giuseppe.serafini@ordineavvocati.perugia.it – giuseppe.serafini@avvocatiperugiapec.it
P. IVA. 01929710547 - C. F. SRF GPP 71 L 20 B963 W

Capitolo 3: Criteri e Metriche per l'Incidente "Significativo"

La determinazione di quando un incidente di sicurezza diventa "significativo" è il fulcro del meccanismo di notifica previsto dalla NIS 2.

Questa valutazione, tuttavia, non può essere lasciata all'improvvisazione durante una crisi ma richiede un processo strutturato che traduca i principi legali qualitativi in soglie e metriche operative, possibilmente quantitative, definite in anticipo.

3.1. I Principi Guida della Direttiva NIS 2 e del D.Lgs. 138/2024

Sia l'articolo 23 della Direttiva che l'articolo 25 del decreto di recepimento definiscono un incidente come significativo quando soddisfa almeno uno dei seguenti due criteri di alto livello:

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

- b) Ha provocato o può provocare ripercussioni su altre persone fisiche o giuridiche, causando perdite materiali o immateriali considerevoli.

La sfida operativa risiede nell'interpretazione di termini volutamente ampi come "grave" e "considerevoli".

Questi aggettivi implicano una valutazione contestuale che deve tenere conto della natura del servizio, delle dimensioni dell'organizzazione e dell'impatto potenziale sull'economia e sulla società.

Lasciare questa interpretazione al momento dell'incidente espone l'organizzazione a decisioni affrettate, incoerenti e difficilmente difendibili.

3.2. La Tassonomia Operativa dell'ACN

È qui che intervengono le specifiche di base dell'ACN, in particolare gli Allegati 3 e 4 della Determina n. 164179/2025.

Questi documenti forniscono una tassonomia concreta degli "incidenti significativi di base", che fungono da *trigger* tecnici per l'obbligo di notifica. Essi rappresentano la traduzione operativa dei principi legali visti sopra.

La tassonomia prevede:

I. **IS-1: Perdita di riservatezza.** Si verifica quando il soggetto ha evidenza della perdita di riservatezza, verso l'esterno, di dati digitali di sua proprietà o sotto il suo controllo.

Via S. Antonio n. 7 - 06012 - Città di Castello (PG).
Tel. 075.4652093 - Fax. 178 2213120
giuseppe.serafini@ordineavvocati.perugia.it – giuseppe.serafini@avvocatiperugiapec.it
P. IVA. 01929710547 - C. F. SRF GPP 71 L 20 B963 W

II. **IS-2: Perdita di integrità.** Si verifica quando il soggetto ha evidenza della perdita di integrità, con impatto verso l'esterno, di dati di sua proprietà o sotto il suo controllo.

III. **IS-3: Perdita di disponibilità.** Si verifica quando il soggetto ha evidenza della violazione dei livelli di servizio attesi dei suoi servizi e/o delle sue attività.

IV. **IS-4 (solo per Soggetti Essenziali): Accesso non autorizzato o con abuso di privilegi.** Si verifica quando il soggetto essenziale ha evidenza di un accesso illecito o di un abuso di privilegi concessi a dati digitali di sua proprietà o sotto il suo controllo.

Un concetto fondamentale introdotto dall'ACN è quello di "**evidenza**" in base al quale l'obbligo di notifica non scatta sulla base di un semplice sospetto, ma quando l'organizzazione "dispone di elementi oggettivi dai quali si evince che si è verificato un incidente di sicurezza informatica" riconducibile a una delle categorie sopra elencate.

3.3. Dalla Qualità alla Quantità: Sviluppare Metriche di Impatto

La tassonomia dell'ACN definisce il "cosa" cercare, ma non stabilisce soglie quantitative per il "quanto". Per applicare in modo coerente e difendibile i criteri di "gravità" e "considerevolezza" della Direttiva, ogni organizzazione deve sviluppare un proprio sistema di metriche e soglie interne.

Metriche di Impatto Operativo (per IS-3)

Per valutare una "grave perturbazione operativa", è necessario misurare la deviazione rispetto al funzionamento normale. Le metriche pertinenti includono:

I. **Numero di utenti/clienti impattati:** Sia in valore assoluto che in percentuale sul totale.

II. **Numero di sistemi/servizi critici coinvolti:** Basato su una classificazione interna della criticità degli asset.

III. **Durata dell'interruzione:** Misurata in minuti o ore e confrontata con i Service Level Agreement (SLA) o Service Level Objective (SLO) contrattuali o interni. La misura ACN **DE.CM-01** richiede esplicitamente la definizione di tali livelli di servizio attesi, che diventano quindi il benchmark per la valutazione.

IV. **Percentuale di degrado delle performance:** Per incidenti che non causano un'interruzione totale ma un rallentamento significativo.

Via S. Antonio n. 7 - 06012 - Città di Castello (PG).
Tel. 075.4652093 - Fax. 178 2213120
giuseppe.serafini@ordineavvocati.perugia.it – giuseppe.serafini@avvocatiperugiapec.it
P. IVA. 01929710547 - C. F. SRF GPP 71 L 20 B963 W

Metriche di Impatto Finanziario (per tutti gli IS)

La stima delle "perdite finanziarie" è complessa ma essenziale. Si possono distinguere due categorie di costi:

I. **Costi Diretti:** Facilmente quantificabili, includono i costi per il personale interno ed esterno dedicato alla risoluzione dell'incidente (remediation), le spese legali, i costi di notifica agli interessati (in caso di data breach GDPR), e le potenziali sanzioni normative.

II. **Costi Indiretti:** Più difficili da stimare, ma spesso più ingenti. Comprendono la perdita di fatturato dovuta al fermo delle operazioni, il danno reputazionale (che può essere stimato tramite analisi di mercato o impatto sul valore del marchio), la perdita di clienti (churn rate), e la potenziale diminuzione del valore azionario per le società quotate.[47] Per un approccio più strutturato alla quantificazione del rischio finanziario, le organizzazioni possono avvalersi di modelli come il **FAIR (Factor Analysis of Information Risk)**.

Metriche di Impatto su Dati (per IS-1, IS-2, IS-4)

La compromissione dei dati ha un impatto che va oltre quello puramente finanziario o operativo:

I. **Volume dei dati:** Numero di record o di soggetti interessati. Questa metrica è fondamentale anche per la valutazione di un data breach ai sensi del GDPR.

II. **Sensibilità dei dati:** L'impatto varia enormemente in base alla classificazione dei dati compromessi (es. dati personali comuni, dati sanitari, segreti commerciali, dati operativi critici di sistemi OT).

III. **Impatto sulla proprietà intellettuale:** Perdita di vantaggio competitivo a seguito del furto di brevetti, progetti o algoritmi.

Metriche di Impatto su Terzi e Sistemico

La NIS 2 pone grande enfasi sull'impatto a catena degli incidenti:

I. **Impatto sulla supply chain:** Numero di fornitori o clienti diretti che subiscono un'interruzione dei loro servizi a causa dell'incidente.

II. **Impatto transfrontaliero:** Valutazione del potenziale impatto su servizi o utenti in altri Stati membri dell'UE, un'informazione richiesta esplicitamente nella pre-notifica di 24 ore.

Via S. Antonio n. 7 - 06012 - Città di Castello (PG).
Tel. 075.4652093 - Fax. 178 2213120
giuseppe.serafini@ordineavvocati.perugia.it – giuseppe.serafini@avvocatiperugiapec.it
P. IVA. 01929710547 - C. F. SRF GPP 71 L 20 B963 W

III. **Rischio per la sicurezza o la salute pubblica:** Per i settori critici (sanità, energia, trasporti), la valutazione deve includere il potenziale danno a persone o alla collettività.

La definizione di queste metriche e delle relative soglie non può essere un esercizio confinato al dipartimento IT o di sicurezza ma deve essere un'attività strategica che coinvolge attivamente le funzioni di business, il legale, la compliance e il vertice aziendale.

Le soglie di "gravità" devono riflettere la propensione e la tolleranza al rischio dell'organizzazione.

Questo processo di definizione delle metriche diventa, di fatto, una componente essenziale dell'analisi del rischio richiesta dall'articolo 24 del Decreto.

L'ACN definisce *cosa* cercare (es. perdita di integrità, IS-2), ma è l'organizzazione che, attraverso un'analisi del rischio contestualizzata, deve stabilire *quando* quella perdita di integrità diventa "grave" per il proprio business.

Questo dialogo forzato tra IT e business è uno dei risultati più significativi della nuova normativa, in quanto promuove un allineamento strategico e rende la cybersecurity una funzione aziendale integrata, non più un silo tecnico.

Tabella 2: Matrice di Valutazione della Significatività dell'Incidente

Scenario di Incidente	Trigger ACN Primario	Esempi di Metriche da Raccogliere	Soglia di Gravità (Esempio)	Decisione di Notifica
Attacco Ransomware con crittografia server e-commerce e sospetta esfiltrazione dati	IS-3 (Disponibilità) IS-1 (Riservatezza)	- Durata downtime servizio > 1 ora - Numero record clienti nel DB > 10.000 - Perdita fatturato stimata > €50.000/ora	- Downtime > 4 ore - O: Evidenza di esfiltrazione di dati personali	**Sì**
Attacco DDoS su sito web istituzionale	IS-3 (Disponibilità)	- Durata interruzione > 30 min - Percentuale di richieste legittime bloccate > 90%	- Interruzione > 2 ore	**No** (se sotto soglia, monitorare)

Via S. Antonio n. 7 - 06012 - Città di Castello (PG).
Tel. 075.4652093 - Fax. 178 2213120
giuseppe.serafini@ordineavvocati.perugia.it – giuseppe.serafini@avvocatiperugiapec.it
P. IVA. 01929710547 - C. F. SRF GPP 71 L 20 B963 W

Compromissione credenziali di un amministratore di sistema	IS-4 (Accesso non autorizzato)	- Evidenza di accesso a sistemi critici - Evidenza di modifica configurazioni - Evidenza di accesso a dati sensibili	- Qualsiasi accesso a sistemi di Produzione Critica	**Sì** (per SE)
Data breach da database di marketing (dati non sensibili)	IS-1 (Riservatezza)	- Numero di record esposti > 50.000 - Tipologia dati: email, nomi	- Numero record > 1.000.000	**No** (ma notifica GDPR da valutare)
Sfruttamento vulnerabilità su un sistema SCADA in impianto produttivo	IS-2 (Integrità) IS-3 (Disponibilità)	- Evidenza di alterazione parametri di processo - Interruzione parziale della linea produttiva	- Qualsiasi alterazione non autorizzata dei parametri OT - O: Fermo linea > 1 ora	**Sì**

Questa matrice non è una soluzione universale, ma un *template* che guida le organizzazioni nel formalizzare il proprio processo decisionale poichè costringe a definire *prima* della crisi le soglie che fanno scattare l'obbligo di notifica, rendendo la risposta entro 24 ore un processo strutturato, rapido e difendibile.

Capitolo 4: Raccomandazioni Operative

La conformità alla Direttiva NIS 2 e al suo recepimento nazionale non si esaurisce nella comprensione della norma, ma richiede la sua traduzione in processi, procedure e capacità operative concrete.

Le seguenti raccomandazioni forniscono una roadmap per costruire una funzione di gestione degli incidenti robusta e allineata ai nuovi requisiti.

4.1. Costruire un Piano di Risposta agli Incidenti (IRP) Integrato

È imperativo che ogni organizzazione formalizzi un **Piano di Risposta agli Incidenti (IRP)**.

Questo documento non deve essere un esercizio teorico, ma una guida operativa viva. Si raccomanda di partire da un framework internazionale consolidato (come NIST, SANS o ISO/IEC 27035) per definire le fasi del ciclo di vita della risposta.

Via S. Antonio n. 7 - 06012 - Città di Castello (PG).
Tel. 075.4652093 - Fax. 178 2213120
giuseppe.serafini@ordineavvocati.perugia.it – giuseppe.serafini@avvocatiperugiapec.it
P. IVA. 01929710547 - C. F. SRF GPP 71 L 20 B963 W

Tuttavia, questo scheletro deve essere arricchito con sezioni specifiche dedicate alla conformità NIS 2, tra cui:

I. **Mappatura con la Tassonomia ACN:** Una sezione che colleghi esplicitamente gli scenari di incidente interni alla tassonomia degli incidenti significativi di base (IS-1, IS-2, IS-3, IS-4).

II. **Procedure di Notifica Dettagliate:** Descrizione passo-passo del processo di notifica al CSIRT Italia, specificando chi è responsabile della raccolta delle informazioni e dell'invio delle comunicazioni per le scadenze di 24 ore, 72 ore e un mese.

III. **Matrice di Comunicazione:** Un piano che definisca chi deve essere informato (internamente ed esternamente), quando e con quale messaggio, per ogni tipologia e livello di gravità dell'incidente.

4.2. Sviluppare "Playbook" Operativi

Mentre l'IRP fornisce la strategia generale, i **playbook** offrono la guida tattica. È necessario sviluppare documenti operativi passo-passo per gli scenari di incidente più probabili o a più alto impatto per l'organizzazione (es. attacco ransomware, compromissione di e-mail aziendale, data breach, attacco alla supply chain).

Ogni playbook dovrebbe includere:

I. Criteri di attivazione e di escalation.
II. Azioni tecniche immediate per l'analisi e il contenimento.
III. Checklist per la raccolta delle informazioni necessarie alla notifica.
IV. Punti di contatto interni ed esterni (es. legali, esperti di forensics).
L'esistenza di playbook predefiniti riduce drasticamente i tempi di reazione e il rischio di errori umani durante una crisi.

4.3. Definire Ruoli, Responsabilità e Formazione (Accountability)

Una risposta efficace agli incidenti richiede una chiara definizione di ruoli e responsabilità. L'utilizzo di una matrice **RACI (Responsible, Accountable, Consulted, Informed)** è una best practice consolidata.[32]

È cruciale che il team di risposta agli incidenti (CSIRT/SOC) non sia l'unico attore coinvolto.

La gestione di un incidente significativo richiede la collaborazione orchestrata di diverse funzioni aziendali: Legale e Compliance (per le implicazioni normative), Comunicazione (per la gestione della reputazione), Risorse Umane (in caso di coinvolgimento di dipendenti) e, soprattutto, il **vertice aziendale**.

Via S. Antonio n. 7 - 06012 - Città di Castello (PG).
Tel. 075.4652093 - Fax. 178 2213120
giuseppe.serafini@ordineavvocati.perugia.it – giuseppe.serafini@avvocatiperugiapec.it
P. IVA. 01929710547 - C. F. SRF GPP 71 L 20 B963 W

La Direttiva NIS 2 e il D.Lgs. 138/2024 (art. 23) attribuiscono una responsabilità diretta e personale agli organi di amministrazione per l'approvazione e la supervisione delle misure di sicurezza, inclusa la gestione degli incidenti.

Questa accresciuta responsabilità del management deve essere supportata da un programma di formazione continua e da esercitazioni periodiche.

Simulazioni (*tabletop exercise*) che coinvolgano il top management sono essenziali per testare non solo le procedure tecniche, ma anche i processi decisionali e di comunicazione a livello strategico.

4.4. Integrazione con l'Ecosistema della Sicurezza

La gestione degli incidenti non è un processo isolato, ma un elemento di un ecosistema di sicurezza più ampio. Deve esistere un ciclo virtuoso di miglioramento continuo:

I. **Dall'Analisi del Rischio all'Incidente:** Le capacità di rilevamento e risposta devono essere progettate per mitigare i rischi identificati nell'analisi del rischio (richiesta dall'art. 24 del Decreto).

II. **Dall'Incidente all'Analisi del Rischio:** Le "lezioni apprese" da ogni incidente, significativo o meno, devono essere utilizzate per aggiornare l'analisi del rischio, identificare nuove vulnerabilità o minacce e migliorare le misure di sicurezza.

Un'attenzione particolare deve essere dedicata alla **sicurezza della catena di approvvigionamento**, uno dei pilastri dell'articolo 21 della Direttiva.

Un incidente di sicurezza che si verifica presso un fornitore critico (es. un provider di servizi cloud o un fornitore di software gestito) può avere un impatto diretto e significativo sui servizi del soggetto NIS.

Pertanto, i contratti con i fornitori devono includere clausole specifiche che obblighino alla notifica tempestiva degli incidenti, per consentire al soggetto NIS di valutare l'impatto sui propri servizi e, se necessario, attivare a sua volta il processo di notifica alle autorità.

Oltre la Compliance, Verso la Resilienza Strategica

Sintesi dei Punti Chiave

Il percorso delineato in questo saggio evidenzia una traiettoria chiara e ineludibile per le organizzazioni che rientrano nell'ambito di applicazione della Direttiva NIS 2.

Via S. Antonio n. 7 - 06012 - Città di Castello (PG).
Tel. 075.4652093 - Fax. 178 2213120
giuseppe.serafini@ordineavvocati.perugia.it – giuseppe.serafini@avvocatiperugiapec.it
P. IVA. 01929710547 - C. F. SRF GPP 71 L 20 B963 W

La normativa europea, recepita con il D.Lgs. 138/2024 e resa operativa dalle misure dell'ACN, impone obblighi stringenti e non delegabili in materia di gestione e notifica degli incidenti. Per far fronte a questa sfida, i framework internazionali come NIST, SANS e ISO/IEC 27035 forniscono la struttura metodologica necessaria.

Tuttavia, la chiave di volta per un'applicazione efficace e difendibile risiede nella capacità di ogni singola organizzazione di tradurre il concetto legale di "incidente significativo" in un insieme di metriche e soglie interne, definite attraverso un'analisi del rischio che coinvolga l'intera struttura aziendale.

La Gestione degli Incidenti come Funzione di Business

La Direttiva NIS 2 segna la fine dell'era in cui la cybersecurity poteva essere considerata una funzione puramente tecnica, relegata ai dipartimenti IT.

L'attribuzione di responsabilità dirette agli organi di amministrazione e le tempistiche di notifica aggressive elevano la gestione degli incidenti a un processo strategico di gestione del rischio d'impresa.

La capacità di rispondere a una crisi informatica diventa un indicatore della salute e della governance complessiva dell'organizzazione, con impatti diretti sulla continuità operativa, sulla reputazione e sulla fiducia del mercato.

Verso un Ecosistema Resiliente

In ultima analisi, l'obiettivo della Direttiva NIS 2 trascende la singola organizzazione. Il meccanismo di notifica obbligatoria, orchestrato a livello nazionale dall'ACN e a livello europeo da ENISA, non è concepito come un onere fine a se stesso, ma come un potente strumento di condivisione delle informazioni.

Ogni notifica contribuisce ad arricchire la conoscenza collettiva sulle minacce, sulle vulnerabilità e sulle tattiche degli avversari. Questa intelligenza condivisa è la base per costruire una difesa collettiva più forte e per migliorare la resilienza dell'intero mercato unico digitale.

Adeguarsi alla NIS 2, quindi, non significa solo proteggere la propria azienda, ma partecipare attivamente alla costruzione di un ecosistema digitale europeo più sicuro e resiliente per tutti.

Avv. Giuseppe Serafini

Via S. Antonio n. 7 - 06012 - Città di Castello (PG).
Tel. 075.4652093 - Fax. 178 2213120
giuseppe.serafini@ordineavvocati.perugia.it – giuseppe.serafini@avvocatiperugiapec.it
P. IVA. 01929710547 - C. F. SRF GPP 71 L 20 B963 W