

Corso NIS2 Advanced – La Direttiva NIS2

Marco Boz – Information Security Specialist – CSI Piemonte

Relatore

13 maggio 2026



Obiettivi del corso

- Comprendere i requisiti della Direttiva NIS2 e il relativo recepimento normativo in Italia.
- Analizzare le responsabilità operative in ambito tecnico e le misure da adottare per la gestione della sicurezza informatica.
- Approfondire le tecniche di monitoraggio, gestione delle vulnerabilità, sicurezza della supply chain e risposta agli incidenti.
- Comprendere come sviluppare un piano tecnico per garantire la resilienza dei sistemi IT in conformità alla normativa.



Il contesto odierno: Cyberspazio e Cybersecurity





Cyber: circa 60 gli attacchi informatici significativi al comparto trasporti nel 2024

Studio rileva un aumento annuo del 48%; nel settore aereo i danni possono superare i 580.000 Euro



Negli ultimi cinque anni il settore dei trasporti ha registrato un'escalation senza precedenti degli attacchi informatici. Secondo il nuovo report pubblicato dal Cyber Defense Center di Maticmind, nel 2024 si sono verificati quasi 60 attacchi significativi, rispetto ai 12 del 2020, con un tasso di crescita medio annuo del 48%. Il ransomware si conferma la minaccia principale (38% degli attacchi), seguito da DDoS (24%) e phishing (18%).

"Il settore dei trasporti sta vivendo un'escalation preoccupante di attacchi informatici. La digitalizzazione ha portato molti vantaggi, ma ha esposto il settore a rischi cyber anche di grandi portate. La protezione delle infrastrutture critiche richiede un cambio di paradigma: non basta più una difesa passiva, ma è essenziale adottare un approccio proattivo basato sul rischio e sull'adozione di soluzioni adeguate non solo per fronteggiare, ma per prevenire attacchi cyber,

investendo in modo significativo nella protezione dei dati, delle infrastrutture e nei sistemi di sicurezza", commenta Lorenzo Forina, ceo di Maticmind Group. "La cybersicurezza deve essere una priorità strategica fondamentale per la protezione dell'intero ecosistema aziendale"

Nel 2024, il 25% degli attacchi globali al settore trasporti ha avuto come obiettivo aziende italiane, che rappresentano da sole il 7,3% degli incidenti totali. Nonostante una crescita degli investimenti del 25% (contro il 15% della media nazionale), l'Italia resta fanalino di coda nel G7 per quota di spesa in cybersecurity rispetto al Pil (0,14%) e spende meno della media europea in percentuale sul budget IT (0,8% contro 1,5%). Il 53,8% delle aziende italiane del settore ha pianificato ulteriori investimenti nel biennio 2025-2026.

Quotidiano Nazionale • Tech • [Trasporti in tilt, internet do...](#)

Trasporti in tilt, internet down e persino l'acqua a rischio. Così gli Usa potrebbero crollare sotto un attacco informatico

Ecco l'avvertimento della ex consigliera della National Security Agency (NSA): troppi tagli e tecnologie obsolete. "Non dobbiamo chiederci se succederà, ma quando"



I pericoli di un attacco informatico negli Stati Uniti

Per continuare, goo
email e immagine de
[sulla privacy](#) e i [tern](#)

L'acqua potabile nel mirino dei cybercriminali russi, cinesi e iraniani

I criminali informatici attaccano sempre più i sistemi idrici degli Stati Uniti



NEWS RECENTI

per l'Italia ■ Un dipendente ha venduto le proprie credenziali per un colpo da 120 milioni di euro



NEWS

APPROFONDIMENTI

OPINIONI

TOP MALWARE

MINACCE

GUIDE ALLA SICUREZZA

PODCAST

ST...

Le reti elettriche sono armi potenti al servizio dei cybercriminali

Mar 03, 2025 Marina Londei Approfondimenti, Attacchi, Attacchi, Campagne malware, Hacking, In evidenza, News 0

Negli ultimi anni **gli attacchi contro le reti elettriche si sono moltiplicati**, ma non le misure di sicurezza per proteggerle: hackerare pannelli solari e le cosiddette "smart grid" non è affatto difficile, per lo più a causa di errori degli utenti.



Attacco informatico ai siti della Regione del Veneto. Presidente Zaia, "Seguiamo con attenzione l'evolversi della situazione. Nessuna violazione segnalata di dati sensibili"

GENOVA TODAY



CRONACA

Nuovo attacco degli hacker russi: preso di mira il sito della Regione

24 febbraio 2025 14:15



L'ente ha spiegato che i disservizi sono durati pochi minuti, nei giorni scorsi attacco al sito dell'Autorità Portuale del Mar Ligure Occidentale per il quale è stata aperta un'inchiesta



la di

3r

1e

stesso argomento



OPERA DEL GRUPPO FILORUSSO "NONAME057(16)"

Cybersicurezza, nuovo attacco hacker: nel mirino Comuni e Regione Puglia

LE SANZIONI

Attacco Regione Lazio, il Garante Privacy conferma i gravi errori

Home > Attacchi Hacker E Malware: Le Ultime News In Tempo Reale E Gli Approfondimenti > Ransomware



Arrivano le sanzioni del Garante per i fatti cyber accaduti in pieno periodo vaccinale anti Covid, a servizio sanitario di Regione Lazio. Un attacco ransomware dagli impatti gravi e importanti per i cittadini che trovarono indisponibilità delle strutture sensibili per giorni

INFORMATICA

Attacchi hacker: anche la Regione Emilia Romagna nel mirino dei filorussi

Gli hacker filorussi colpiscono il sito della Regione Emilia Romagna e altre istituzioni italiane con attacchi DDoS



ENZO VANNELLI

redazione@bolognacronaca.it

24 FEBBRAIO 2025 - 13:08





I casi ancora più gravi in sanità

SANITÀ SOTTO ATTACCO

Attacco all'Azienda Ospedaliera di Verona: dati in vendita, ma quelli sanitari sono una minima parte

RANSOMWARE

Attacco all'ASST Rhodense, online 1 TB di dati: c'è la rivendicazione del ransomware Cicada3301

Home > Attacchi Hacker E Malware: Le Ultime News In Tempo Reale E Gli Approfondimenti

f in X M E P

I dati personali dei pazienti dell'ASST Rhodense sono stati pubblicati online e sono ora liberamente scaricabili. La rivendicazione è del gruppo ransomware Cicada3301. Ecco le implicazioni e le misure che servono per impedire che attacchi del genere si verifichino di nuovo

Pubblicato il 21 giu 2024

SANITÀ SOTTO ATTACCO

Ransomware colpisce tre Asl di Modena: c'è la rivendicazione del gruppo Hunters, primi dati rubati online

MISURE D'URGENZA

Ospedali londinesi messi in ginocchio da un ransomware: cosa impariamo

Home > Attacchi Hacker E Malware: Le Ultime News In Tempo Reale E Gli Approfondimenti > Ransomv

f in X M E P

Sono diversi gli ospedali londinesi interessati dall'attacco ransomware in tutto, sono stati cancellati 800 interventi chirurgici. Notizie simili costringono a rivedere l'idea stessa di cyber security

Pubblicato il 4 lug 2024

RANSOMWARE

Attacco al sistema sanitario lucano: unità di crisi attivata su ASP Basilicata

Home > Attacchi Hacker E Malware: Le Ultime News In Tempo Reale E Gli Approfondimenti

f in X M E P

RANSOMWARE

ASL di Torino colpita da attacco informatico, molti disagi per i pazienti

Home > Malware E Attacchi Hacker: Come Affrontare La Sicurezza

f X in M E P

Sanità pubblica nuovamente sotto attacco informatico, si assiste alle difficoltà trascorse in questi giorni dalla Asl Città di Torino colpita da quello che potrebbe essere un tipico attacco ransomware. Computer degli ospedali bloccati, compare una nota di riscatto e le indagini proseguono

Pubblicato il 24 Ago 2022



L'evoluzione del perimetro DI SICUREZZA...

Fino a qualche anno fa il perimetro di difesa era circoscritto



Ora invece lo scenario di accesso ai dati è cambiato!!!



I nuovi rischi nel contesto Cyber

Cloud

L'utilizzo del cloud introduce rischi di violazioni dei dati, in particolare attraverso configurazioni errate e accessi non autorizzati. Inoltre, il cloud è vulnerabile ad attacchi DoS (Denial Of Service) e alla compromissione di credenziali da parte di cybercriminali.

Intelligenza Artificiale (AI)

L'AI (Artificial Intelligence) può essere manipolata tramite attacchi adversarial, che alterano i dati per influenzare i modelli. Altri rischi includono la compromissione dei dati sensibili utilizzati per l'addestramento e la diffusione di bias, tendenza a deviare la razionalità, nei sistemi decisionali.

Smart Working

Il lavoro remoto espone le reti aziendali a rischi di phishing, malware e accessi non autorizzati, soprattutto se i dispositivi personali non sono adeguatamente protetti o connessi a reti insicure.



I nuovi rischi nel contesto Cyber

Supply Chain

La supply chain è vulnerabile ad attacchi mirati contro fornitori terzi, che possono agire come punto di ingresso per malware. La mancanza di trasparenza nei processi aumenta i rischi di sabotaggi e compromissioni.

Internet of Things (IoT)

I dispositivi IoT sono spesso caratterizzati da scarsa sicurezza e sono bersagli facili per attacchi DDoS, manipolazione dei dati o violazione della privacy. La connessione a reti principali amplifica il rischio di infiltrazioni.

Social Network

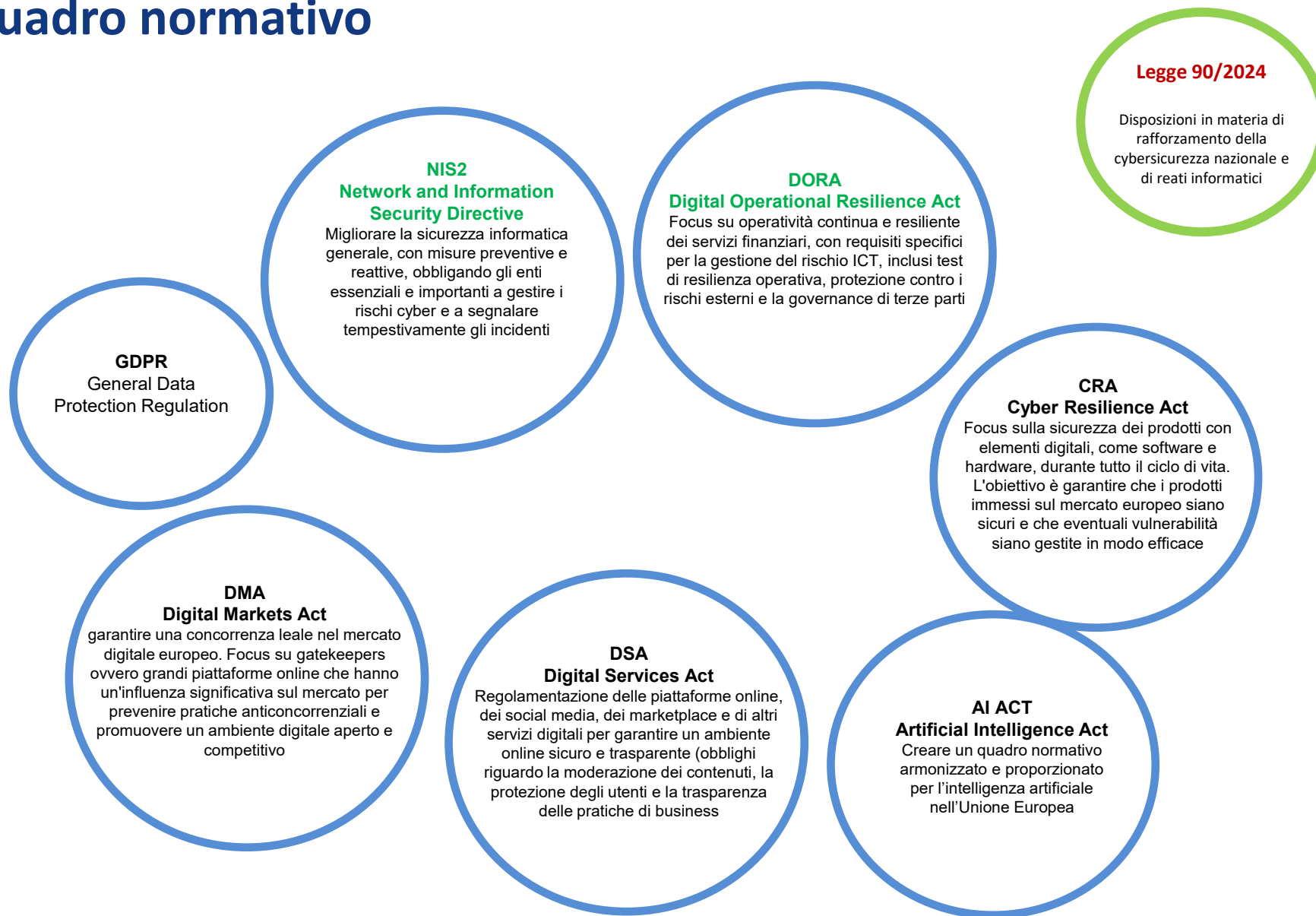
I social network sono un terreno fertile per attacchi di ingegneria sociale, furto di identità e diffusione di malware tramite link malevoli. Inoltre, la raccolta e l'uso improprio di dati personali rappresentano un rischio significativo.

NIS2: Introduzione





Il quadro normativo





Plasmare il futuro digitale dell'Europa

Homepage

Politiche

Attività

Notizie

Biblioteca

Finanziamenti

Calendario

Consultazioni

AI Office

Homepage > ... > Politiche in materia di cibersicurezza > Direttiva NIS 2: nuove norme sulla cibersicurezza delle reti e dei sistemi info

Il parlamento italiano
ha recepito la direttiva
e dal 17 ottobre 2024
ha preso il via il piano di
adeguamento nazionale

Direttiva NIS 2: nuove norme sulla cibersicurezza delle reti e dei sistemi informativi

La direttiva NIS2 istituisce un quadro giuridico unificato per sostenere la cibersicurezza in 18 settori critici in tutta l'UE. Invita inoltre gli Stati membri a definire strategie nazionali di cibersicurezza e a collaborare con l'UE per la reazione e l'applicazione transfrontaliere.

La sicurezza informatica comporta la protezione delle **reti e dei sistemi informativi** (NIS), dei loro utenti e di altre persone interessate da incidenti e minacce informatiche. Per rispondere alla maggiore esposizione dell'Europa alle minacce informatiche, la [direttiva 2022/2555](#), nota anche come NIS2, ha

Condividi

Direttiva NIS 2 (direttiva (UE)
2022/2555) [↗](#)

Domande & risposte [↗](#)



Direttiva NIS2: introduzione

La nuova direttiva impone ai soggetti in perimetro di essere **proattivi nella gestione dei rischi** e di adottare **misure di sicurezza idonee** al proprio **contesto** e alle **capacità di spesa**.

L'adeguatezza delle misure di sicurezza si basa su alcuni pilastri essenziali, tra cui:

- l'**individuazione e la valutazione dei rischi**
- le **procedure proattive** per la **gestione degli incidenti**,
- il **monitoraggio e il miglioramento continuo** della sicurezza e la continuità operativa, garantita dalla qualità dell'erogazione dei servizi.



Direttiva NIS2: Differenze tra NIS1 e NIS2

- NIS2 introduce **requisiti più stringenti** rispetto a NIS1, includendo **nuovi settori** e **aumentando le sanzioni** per non conformità.
- NIS2 **enfatizza la cooperazione tra gli Stati membri** e la **condivisione delle informazioni**.



Direttiva NIS2: Differenze tra NIS1 e NIS2

Ambito di applicazione esteso



Aggiunta di più settori

Obblighi cybersecurity



Armonizzazione degli obblighi cyber e maggior specifiche

Supervisione autorità



Poteri di vigilanza ex-ante e ex-post

Sanzioni ed *enforcement*



Regime sanzionatorio specifico



NIS2: gli ambiti



**Mercati
online**



**Infrastrutture
digitali**



**Gestione
dei rifiuti**



**Prodotti
chimici
e medici**



**Settore
bancario**



**Motori di
ricerca online**



**Servizi postali
e di spedizione**



**Infrastrutture
mercato
finanziario**



**Assistenza
Sanitaria**



Utilities



Trasporti



**Prodotti
alimentari**



**Macchine e
attrezzature**



**Computer ed
elettronica**



**Veicoli
a motori**



**Servizi
di cloud
computing**



1

Ambito di applicazione esteso*

La novità principale della Direttiva NIS2 è il suo ambito di applicazione. Le nuove disposizioni normative oltre ad essere applicabili ai settori originariamente previsti dalla Direttiva NIS1 saranno applicabili anche ad un novero di società prima non incluse



Servizi Essenziali

- Settore energetico: elettrico, *oil and gas*, riscaldamento, idrogeno
- Settore sanitario: produttori di dispositivi medicali, laboratori, R&D, settore farmaceutico
- Trasporti: aereo, nautico, ferroviario e stradale
- Acque e acque di scarico
- Infrastrutture digitali
- Settore spaziale
- Pubblica amministrazione



Servizi Importanti

- Settore postale e più in generale di spedizione
- Gestione/Trattamento dei rifiuti
- Settore chimico: produzione e distribuzione
- Settore alimentare: approvvigionamento, inclusa anche la grande distribuzione
- Industrie tecnologiche e ingegneristiche
- Servizi digitali: social network e servizi di data center
- Ricerca scientifica



I fornitori e service provider dei Servizi Essenziali e Importanti



Ambito di applicazione nella PA

Nell'ambito della Pubblica amministrazione i Settori individuati includono:

1. **pubbliche amministrazioni centrali** incluse nell'elenco annuale ISTAT delle PA, previsto dall'art. 1, c. 3, della L. 196/2009
2. **regioni e province autonome di Trento e di Bolzano**
3. **città metropolitane**
4. **comuni con popolazione superiore a 100.000 abitanti e comunque i comuni capoluoghi di regione**
5. società di **trasporto pubblico urbano** con bacino di utenza non inferiore a 100.000 abitanti
6. società di **trasporto pubblico extraurbano** operanti nell'ambito delle città metropolitane
7. **aziende sanitarie locali**
8. **società in house degli enti richiamati che siano fornitrici di servizi informatici**, dei servizi di trasporto sopra indicati, dei servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali ovvero servizi di gestione dei rifiuti.



Il ruolo di ACN



Agenzia per la Cybersicurezza Nazionale

<https://www.acn.gov.it/>

L'**Agenzia per la Cybersicurezza Nazionale (ACN)** svolge un ruolo centrale e strategico nell'attuazione della Direttiva NIS2 in Italia, in quanto **autorità nazionale competente per la cybersicurezza**. La sua funzione è definita dal **Decreto Legislativo 4 settembre 2024, n. 138**, che ha recepito la Direttiva (UE) 2022/2555 (NIS2) nell'ordinamento italiano.



Il ruolo di ACN



Agenzia per la Cybersicurezza Nazionale

<https://www.acn.gov.it/>



Autorità Competente

Coordina l'attuazione della NIS2 a livello nazionale



Registro dei Soggetti

Classifica le entità essenziali e importanti



Vigilanza e Controlli

Conduce audit, ispezioni e verifica la conformità



Gestione degli Incidenti

Riceve e coordina le segnalazioni di incidenti cyber



Linee Guida Tecniche

Definisce standard minimi e buone pratiche



Cooperazione UE

Rappresenta l'Italia nei gruppi europei di cybersicurezza



Sensibilizzazione

Promuove formazione e cultura della sicurezza informatica

NIS2 – Supervisione autorità e sanzioni





Direttiva NIS2: Governance

ART. 23

(Organi di amministrazione e direttivi)



- Gli **organi di amministrazione** e gli organi direttivi dei soggetti essenziali e importanti:
 - a) **approvano le modalità di implementazione** delle misure di gestione dei rischi per la sicurezza informatica adottate da tali soggetti ai sensi dell'articolo 24;
 - b) **sovrintendono all'implementazione** degli obblighi di cui al presente capo e di cui all'articolo 7;
 - c) **sono responsabili delle violazioni** di cui al presente decreto
 - d) sono tenuti a **seguire una formazione** in materia di sicurezza informatica;
 - e) promuovono l'offerta periodica di una **formazione coerente** a quella di cui alla lettera a) **ai loro dipendenti**, per favorire l'acquisizione di conoscenze e competenze sufficienti al fine di **individuare i rischi e valutare le pratiche di gestione dei rischi** per la sicurezza informatica e **il loro impatto** sulle attività del soggetto e sui servizi



Direttiva NIS2: sanzioni

Categoria	Tipologia di Violazione	Sanzione prevista
 Entità essenziali	Violazioni gravi o sistemiche	Fino a 10 milioni € o 2% fatturato mondiale (se applicabile)
 Entità importanti	Violazioni significative	Fino a 7 milioni € o 1,4% fatturato mondiale
 Notifica incidenti	Mancata o ritardata notifica entro 24 ore	Sanzione pecuniaria + obbligo di notifica entro termine fissato
 Misure di sicurezza	Mancata adozione misure tecniche e organizzative adeguate	Sanzione + obbligo di adeguamento
 Obblighi documentali	Omessa valutazione rischio o mancata cooperazione con ACN	Sanzione + eventuale ispezione
 Reiterazione o inadempienza	Violazioni gravi reiterate o ostruzione dei controlli	Sospensione temporanea dei dirigenti o commissariamento funzionale
 Trasparenza	Grave negligenza o mancata risposta a prescrizioni	Pubblicazione della sanzione sul sito dell'ACN



Direttiva NIS2: sanzioni

Sono previste **sanzioni specifiche** per:

- **mancata registrazione** sulla piattaforma dell'Agenzia per la Cybersicurezza Nazionale (ACN)
- **mancata registrazione, comunicazione o aggiornamento** delle informazioni richieste
la sanzione amministrativa pecuniaria per le **PA** va **da 10.000 a 50.000 €** ed allo **0,1% del fatturato per soggetti essenziali**
- **violazione degli obblighi in materia di sicurezza informatica**
la sanzione amministrativa pecuniaria per le **PA amministrazioni** va **da 25.000 a 125.000 €**



Direttiva NIS2: sanzioni accessorie

Il decreto di recepimento della Direttiva NIS2 introduce sanzioni accessorie anche per:

- **organi di amministrazione**
- **persone fisiche responsabili** di un soggetto essenziale o che agisca in qualità di suo rappresentante legale con l'autorità di rappresentarlo, di prendere decisioni per suo conto o di esercitare un controllo sul soggetto stesso
- **amministratore delegato**
- **legali rappresentanti** del soggetto essenziale o importante



Questi soggetti non potranno svolgere funzioni dirigenziali all'interno dell'ente, finché lo stesso non avrà adottato le misure necessarie a porre rimedio alle carenze riscontrate dall'Agenzia per la Cybersicurezza Nazionale, o finché non si sarà conformato alle prescrizioni indicate dalla stessa



Direttiva NIS2: sanzioni – riassunto

Tipologia	Ambito	Riferimento normativo	Condotta sanzionata	Importi / Natura	Destinatari	Esempi di trigger
Sanzioni pecuniarie	Soggetti essenziali	Art. 38, co. 8, lett. a	Violazioni obblighi NIS2 o inottemperanza ordini ACN	Fino a €10.000.000 o 2% fatturato mondiale (min 1/20)	Organizzazione (persona giuridica)	Piano di gestione del rischio assente o inadeguato
Sanzioni pecuniarie	Soggetti importanti	Art. 38, co. 8, lett. b	Violazioni obblighi NIS2 o inottemperanza ordini ACN	Fino a €7.000.000 o 1,4% fatturato mondiale (min 1/30)	Organizzazione (persona giuridica)	Incident management non conforme
Sanzioni pecuniarie	Pubbliche Amministrazioni	Art. 38, co. 8, lett. c	Violazioni obblighi NIS2 o inottemperanza ordini ACN	€25.000 – €125.000	Ente pubblico (persona giuridica)	PA non implementa misure o ignora ordini ACN
Sanzioni pecuniarie	Mancata registrazione / Punto di contatto	Art. 38, co. 10–11	Omessa registrazione/designazione punto di contatto	Essenziali: 0,1% fatturato; Importanti: 0,07%; PA: €10.000 – €50.000	Organizzazione (impresa o PA)	Non registrazione entro 28 febbraio
Misure accessorie	Sospensione certificati/autorizzazioni	Art. 38, co. 4	Inadempienza persistente dopo diffida ACN	Sospensione temporanea certificati/autorizzazioni	Organizzazione (persona giuridica)	Non conformità non sanata
Misure accessorie	Interdizione funzioni direttive	Art. 38, co. 5–6	Responsabilità dei vertici nel mancato rispetto del decreto	Divieto temporaneo di svolgere funzioni direttive	Persone fisiche (top management)	Ripetute inottemperanze o violazioni gravi
Poteri esecutivi	Diffida e audit obbligatori	Art. 37	Assenza di evidenze o dubbi su conformità	Ordini di esibire dati e audit periodici	Organizzazione (impresa o PA)	Documentazione incompleta o misure non verificate



Direttiva NIS2: in sintesi

- registrazione e aggiornamento dei dati (art.7)
- **responsabilizzazione degli organi di amministrazione e direttivi** (art. 23)
- **obblighi in materia di misure di sicurezza informatica** (art. 24)
- **obblighi in materia di notifica di incidente** (art. 25)
- **obblighi in materia di banca dei dati** di registrazione dei nomi di dominio (articolo 29)
- categorizzazione delle attività e dei servizi (art.30)

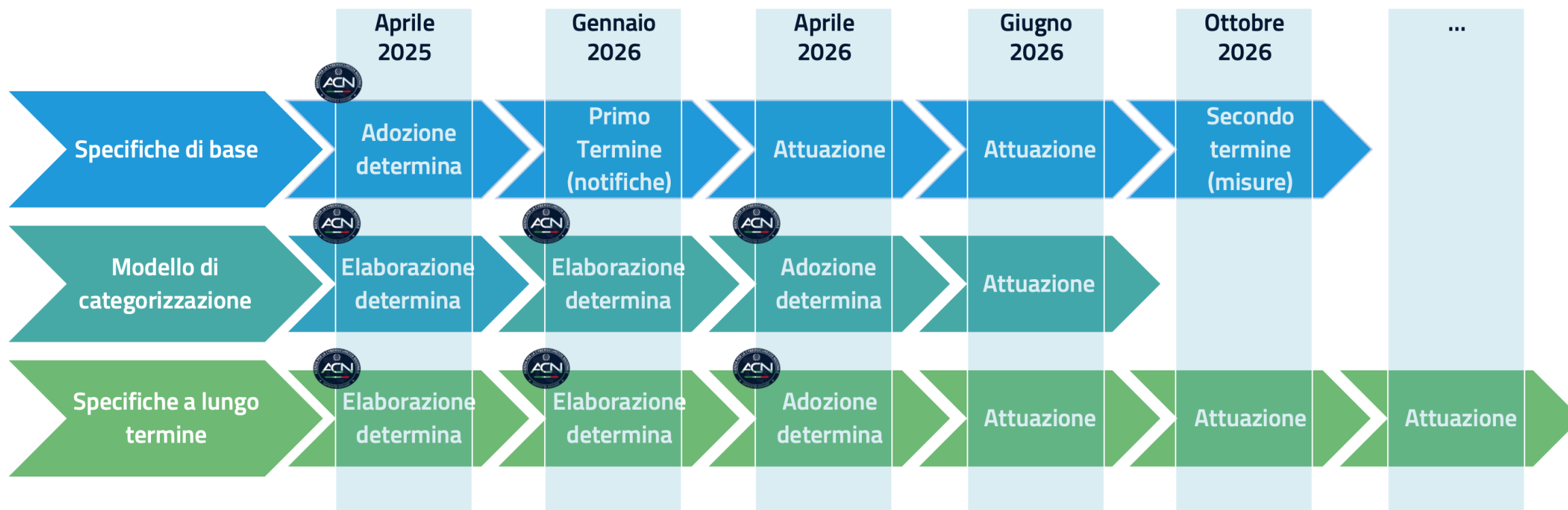


NIS2 – Timeline





Timeline Adozione NIS2



Specifiche di base

Specifiche degli obblighi, anche orizzontali, minimi per tutta l'infrastruttura con un orizzonte a breve termine.

Specifiche a lungo termine

Obblighi, anche settorializzati e potenzialmente ambiziosi, proporzionati in base alla categorizzazione e con scadenze a medio e lungo termine.



Timeline Adozione NIS2 - 2025

dal 1° gennaio al 28 febbraio 2025 le aziende hanno dovuto registrarsi o aggiornare la propria registrazione sulla piattaforma indicando il proprio settore di attività e un punto di contatto;

entro il 31 marzo 2025 l'Autorità Nazionale ha redatto l'elenco dei soggetti essenziali e importanti e lo ha comunicato agli stessi tramite la piattaforma (inserimento/permanenza/espunzione dall'elenco);

dal 15 aprile al 31 luglio 2025 i soggetti essenziali e importanti devono comunicare/aggiornare tramite la piattaforma alcune informazioni fondamentali per permettere i controlli;

dal 1° maggio al 30 giugno 2025 i soggetti comunicano/aggiornano tramite la piattaforma l'elenco delle proprie attività e dei propri servizi.

entro il 31 marzo 2025 l'Autorità Nazionale ha realizzato l'elenco dei soggetti essenziali e importanti e ha comunicato ad ogni singola azienda, tramite la piattaforma, la propria qualificazione, e di seguito si sono svolti gli altri passaggi.



Timeline Adozione NIS2 - 2026

A partire da gennaio 2026:

- Scatta l'[obbligo di notifica degli incidenti informatici](#). Le aziende dovranno segnalare ogni attacco significativo al CSIRT Italia.

Entro aprile 2026 ACN:

- Definizione del modello di categorizzazione delle attività e dei servizi.
- Pubblicazione degli obblighi a lungo termine, che stabiliranno gli standard operativi per i prossimi anni.

Questo periodo sarà caratterizzato da controlli e verifiche per valutare il grado di conformità delle aziende.



Timeline Adozione NIS2 – Aprile – Ottobre 2026

Questa fase segnerà l'inizio della piena operatività della NIS2, con un'attenzione particolare alla categorizzazione delle attività e alla definizione di obblighi avanzati:

- Applicazione integrale del modello di categorizzazione delle attività e dei servizi.
- **Entro settembre 2026** piena attuazione degli obblighi a lungo termine, con un rafforzamento continuo delle misure di sicurezza.

A questo punto, tutti i soggetti in ambito dovranno dimostrare di aver raggiunto un livello di cybersecurity adeguato e conforme alle direttive europee.

NIS2 – Obblighi cybersecurity





La Direttiva NIS2 – Focus D.LGS 138/2024

Art. 24

Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica

1. I soggetti essenziali e i soggetti importanti adottano misure tecniche, operative e organizzative adeguate e proporzionate, secondo le modalità e i termini di cui agli articoli 30, 31 e 32, alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi. Tali misure:

- a) assicurano un livello di sicurezza dei sistemi informativi e di rete adeguato ai rischi esistenti, tenuto conto delle conoscenze più aggiornate e dello stato dell'arte in materia e, ove applicabile, delle pertinenti norme nazionali, europee e internazionali, nonché dei costi di attuazione;
- b) sono proporzionate al grado di esposizione a rischi del soggetto, alle dimensioni del soggetto e alla probabilità che si verifichino incidenti, nonché alla loro gravità, compreso il loro impatto sociale ed economico.

Art. 25

Obblighi in materia di notifica di incidente

1. I soggetti essenziali e i soggetti importanti notificano, senza ingiustificato ritardo, al CSIRT Italia ogni incidente che, ai sensi del comma 4, ha un impatto significativo sulla fornitura dei loro servizi, secondo le modalità e i termini di cui agli articoli 30, 31 e 32.

Art. 31

Proporzionalità e gradualità degli obblighi

1. Ai fini di cui agli articoli 23, 24, 25, 27, 28 e 29 l'Autorità nazionale competente NIS stabilisce obblighi proporzionati tenuto debitamente conto del grado di esposizione dei soggetti ai rischi, delle dimensioni dei soggetti e della probabilità che si verifichino incidenti, nonché della loro gravità, compreso il loro impatto sociale ed economico.

Art. 40

Attuazione

5. Con una o più determinazioni dell'Agenzia per la cybersicurezza nazionale, sentito il Tavolo per l'attuazione della disciplina NIS:

l) sono stabiliti obblighi proporzionati e gradualità, a valenza multisettoriale e, ove opportuno, settoriale, di cui all'articolo 31, le modalità di applicazione dei medesimi obblighi per i soggetti che svolgono attività in più settori o sottosettori e per i soggetti di cui all'articolo 32, commi 1 e 2;

Art. 42

Fase di prima applicazione

1. In fase di prima applicazione:

- a) ai sensi dell'articolo 7, entro il 17 gennaio 2025, i fornitori di servizi di sistema dei nomi di dominio, i gestori di registri dei nomi di dominio di primo livello, i fornitori di servizi di registrazione dei nomi di dominio, i fornitori di servizi di cloud computing, fornitori di servizi di data center, fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network che rientrano nell'ambito di applicazione del presente decreto, si registrano sulla piattaforma digitale di cui all'articolo 7, comma 1;
- b) sino al 31 dicembre 2025, il Tavolo per l'attuazione della disciplina NIS di cui all'articolo 12 si riunisce almeno una volta ogni sessanta giorni;
- c) sino al 31 dicembre 2025, il termine per l'adempimento degli obblighi di cui all'articolo 25 è fissato in nove mesi dalla ricezione della comunicazione di cui all'articolo 7, comma 3, lettere a) e b), e il termine per l'adempimento degli obblighi di cui agli articoli 23, 24 e 29 è fissato in diciotto mesi dalla medesima comunicazione. Ai fini di cui al primo periodo, l'Autorità nazionale competente NIS può stabilire modalità e specifiche di base per assicurare la conformità dei soggetti essenziali e dei soggetti importanti.



La Direttiva NIS2 – Focus Misure di Sicurezza: Ambiti

a) Politiche di analisi dei rischi e di sicurezza dei sistemi informativi.

b) Gestione degli incidenti.

c) Continuità operativa, inclusa la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi.

d) Sicurezza catena di approvvigionamento, compresi aspetti relativi sicurezza rapporti con diretti fornitori o fornitori di servizi.

e) Sicurezza acquisizione, sviluppo e manutenzione sistemi informativi e di rete, ivi compresa gestione e divulgazione vulnerabilità.

f) Politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza.

g) Pratiche di igiene informatica di base e formazione in materia di cybersicurezza.

h) Politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura.

i) Sicurezza risorse umane, strategie di controllo dell'accesso e gestione degli assetti.

j) Uso di soluzioni di autenticazione a più fattori o di autenticazione continua e di sistemi di comunicazione protetti.

**Elementi obblighi in materia di misure di gestione dei rischi per la sicurezza informatica
(art. 24, c. 2 d.lgs. 138/2024)**



La Direttiva NIS2 – Focus Misure di Sicurezza D.LGS 138/2024

Art. 24 – Obblighi in materia di misure di sicurezza informatica

I **soggetti essenziali** e i soggetti importanti **adottano misure tecniche, operative e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete** [...] per prevenire o ridurre al minimo l'impatto degli incidenti. Tali misure sono basate su un **approccio multi-rischio**, [...] e comprendono almeno i seguenti elementi:

- Politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete;
- Gestione degli incidenti, ivi incluse le procedure e gli strumenti per eseguire le notifiche;
- Continuità operativa, ivi inclusa la gestione di backup, il ripristino in caso di disastro, ove possibile, e la gestione delle crisi;
- Sicurezza della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;



La Direttiva NIS2 – Focus Misure di Sicurezza D.LGS 138/2024

Art. 24 – Obblighi in materia di misure di sicurezza informatica

- Sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità;
- Politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi per la sicurezza informatica;
- Pratiche di igiene di base e di formazione in materia di sicurezza informatica;
- Politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura
- Sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli asset;
- Uso di soluzioni di autenticazione a più fattori o di autenticazione continua;



La Direttiva NIS2 – F.N.C.S. 2025



Table 1. CSF 2.0 Core Function and Category names and identifiers

Function	Category	Category Identifier
<u>Govern (GV)</u>	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
<u>Identify (ID)</u>	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
<u>Protect (PR)</u>	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
<u>Detect (DE)</u>	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
<u>Respond (RS)</u>	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
<u>Recover (RC)</u>	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO



La Direttiva NIS2 – F.N.C.S. 2025

FNCS: Framework Nazionale per la Cybersecurity e la Data Protection

Le misure sono organizzate secondo il modello del **NIST Cybersecurity Framework**, in:

1. Funzioni (es. Identificare, Proteggere, Rilevare, Rispondere, Ripristinare)
2. Categorie
3. Sottocategorie
4. Requisiti (operativi e tecnici)



Table 1. CSF 2.0 Core Function and Category names and identifiers

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
Detect (DE)	Technology Infrastructure Resilience	PR.IR
	Continuous Monitoring	DE.CM
Respond (RS)	Adverse Event Analysis	DE.AE
	Incident Management	RS.MA
	Incident Analysis	RS.AN
Recover (RC)	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Ogni misura ha un codice identificativo, una descrizione e uno o più requisiti da soddisfare.



La Direttiva NIS2 – F.N.C.S. 2025

Framework Core

Funzioni	Categorie	Sottocategorie	Informative References
GOVERNO (GV)			
IDENTIFICAZIONE (ID)			
PROTEZIONE (PR)			
RILEVAMENTO (DE)			
RISPOSTA (RS)			
RIPRISTINO (RC)			

Framework contestualizzato

Funzioni	Categorie	Sottocategorie	Informative References
GOVERNO (GV)			
IDENTIFICAZIONE (ID)			
PROTEZIONE (PR)			
RILEVAMENTO (DE)			
RISPOSTA (RS)			
RIPRISTINO (RC)			

43 sottocategorie

Misure di sicurezza

ALLEGATO 2

Misure di sicurezza di base per i soggetti essenziali

1. GOVERNO (GOVERN)

1.1. **Contesto organizzativo (GV.OC):** Il contesto – missione, aspettative degli stakeholder, dipendenze e requisiti legali, normativi e contrattuali – che influisce sulle decisioni di gestione del rischio di cybersecurity dell'organizzazione è compreso¹.

1.1.1. **GV.OC-4:** Gli obiettivi, le capacità e i servizi critici dai quali gli stakeholder dipendono o che si aspettano dall'organizzazione sono compresi e comunicati.

1. È mantenuto un elenco aggiornato dei sistemi informativi e di rete rilevanti.

1.2. **Strategia di gestione del rischio (GV.RM):** Le priorità, i vincoli, le dichiarazioni sulla tolleranza e la propensione al rischio, e le assunzioni dell'organizzazione sono stabilite, comunicate e utilizzate per supportare le decisioni sul rischio operativo.

1.2.1. **GV.RM-03:** Le attività e gli esiti della gestione del rischio di cybersecurity sono parte integrante dei processi di gestione del rischio dell'organizzazione.

1. Nell'ambito dei processi di gestione del rischio del soggetto NIS e nel rispetto delle politiche di cui alla misura GV.PO-01, è definito, attuato, aggiornato e documentato un piano di gestione dei rischi per la sicurezza informatica per identificare, analizzare, valutare, trattare e monitorare i rischi.

116 requisiti

Selezione
sottocategorie

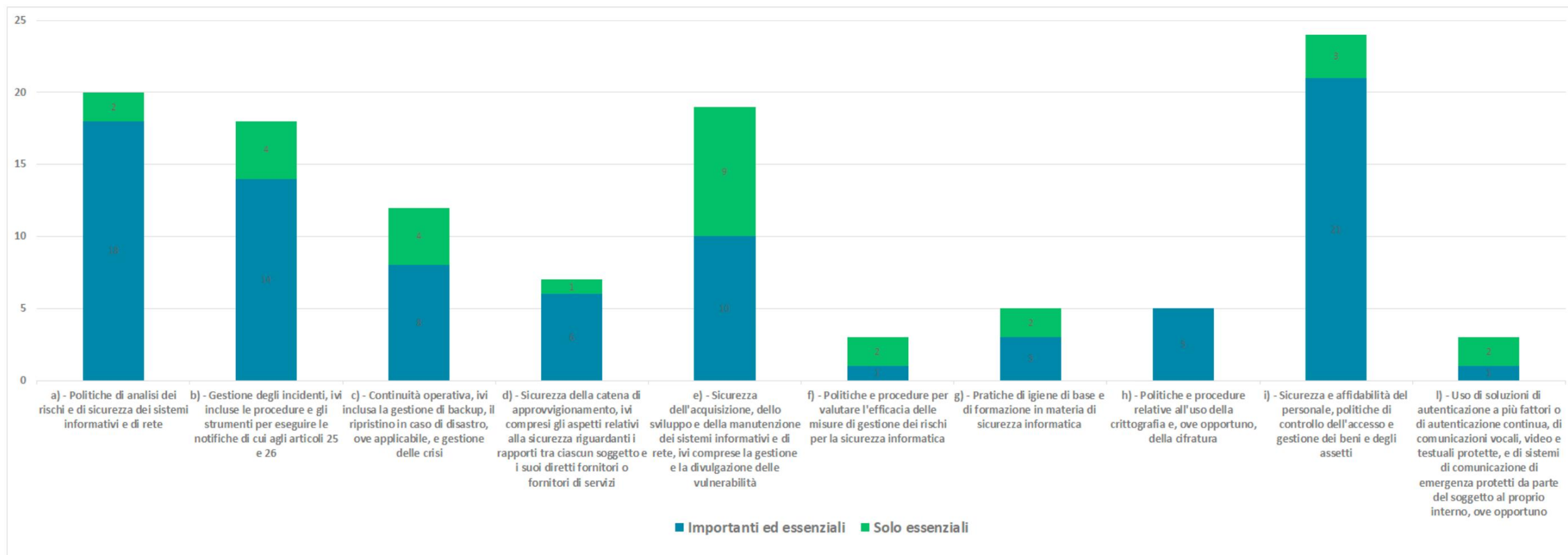
Definizione
requisiti

Previsioni
D.Lgs. 138/2024

Best practices

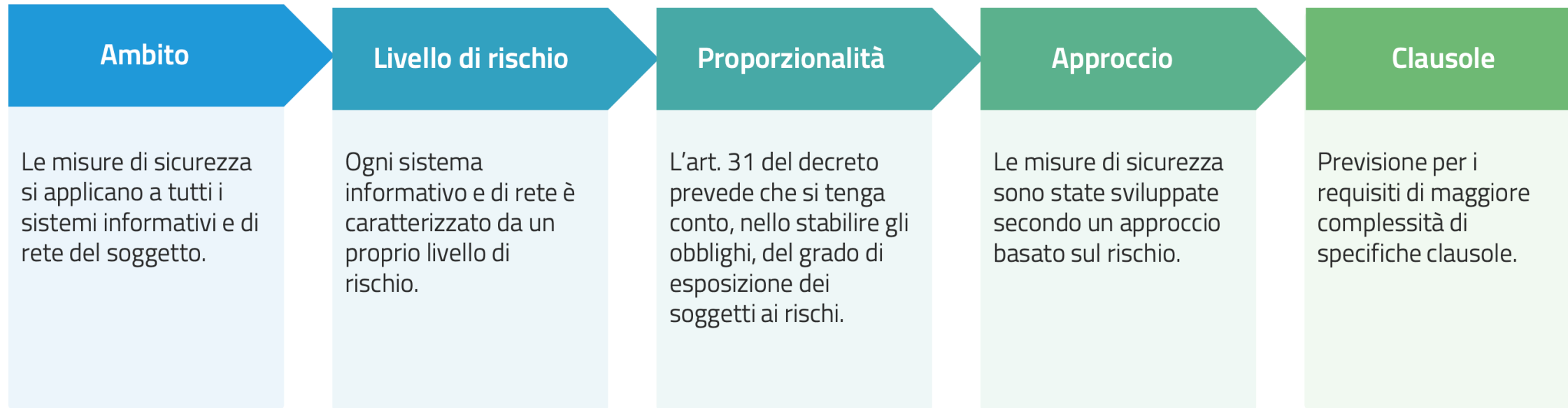


La Direttiva NIS2 – Mappatura Requisiti art. 24





La Direttiva NIS2 – Approccio basato sul rischio





La Direttiva NIS2 – Approccio basato sul rischio

14 requisiti per i soggetti importanti
e **19** per i soggetti essenziali

6 requisiti per i soggetti importanti
e **9** per i soggetti essenziali

Facoltà di limitare l'ambito di applicazione per specifici requisiti ai sistemi informativi di rete la cui compromissione determina un impatto significativo su R, I, D delle attività e servizi per i quali il soggetto rientra nell'ambito di applicazione del decreto NIS.

“ **... per almeno i sistemi informativi e di rete rilevanti ...** ”

“ **... in accordo agli esiti della valutazione del rischio di cui alla misura ...** ”

Possibilità di adattare le modalità di attuazione di specifici requisiti sulla base degli esiti della valutazione del rischio.

Deroga all'applicazione del requisito se sussistono vincoli normativi (ad esempio, leggi o regolamenti) o tecnici (ad esempio, limiti tecnologici o operativi) che non ne permettano l'implementazione.

“ **... fatte salve motivate e documentate ragioni normative o tecniche ...** ”

“ **... forniture con potenziali impatti sulla sicurezza ...** ”

Sono considerate le forniture la cui eventuale compromissione può determinare effetti sulla sicurezza dei sistemi informativi e di rete.

8 requisiti per i soggetti importanti
e **10** per i soggetti essenziali

3 requisiti per i soggetti importanti
e per i soggetti essenziali



Sistemi Informativi e di Rete «RILEVANTI»

PR.DS-11

I backup dei dati sono creati, protetti, mantenuti e verificati.

PUNTO	REQUISITO	S_I	S_E
1	In accordo alle esigenze di continuità operativa e di ripristino in caso di disastro individuate nei piani di cui alla misura ID.IM-04, sono effettuati periodicamente i backup dei dati e delle configurazioni e, per almeno i sistemi informativi e di rete rilevanti, sono anche conservate copie di backup offline.	●	●
2	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 1.	●	●
3	Per almeno i sistemi informativi e di rete rilevanti, è assicurata la riservatezza e l'integrità delle informazioni contenute nei backup mediante adeguata protezione fisica dei supporti ovvero mediante cifratura.		●
4	Per almeno i sistemi informativi e di rete rilevanti, in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, è verificata periodicamente l'utilizzabilità dei backup effettuati mediante test di ripristino.		●
5	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 3 e 4.		●



In accordo a esiti valutazione rischio

PR.AA-01

Le identità e le credenziali degli utenti, dei servizi e dell'hardware autorizzati sono gestite dall'organizzazione.

PUNTO	REQUISITO	S_I	S_E
1	Tutte le utenze, ivi incluse quelle con privilegi amministrativi e quelle utilizzate per l'accesso remoto, sono censite, approvate da attori interni al soggetto NIS e, fatte salve motivate e documentate ragioni tecniche, in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono individuali per gli utenti.	●	●
2	Le credenziali (ad esempio nome utente e password) relative alle utenze sono robuste e aggiornate in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05.	●	●
3	Per almeno i sistemi informativi e di rete rilevanti, sono verificate periodicamente le utenze e le relative autorizzazioni, aggiornandole/revocandole in caso di variazioni (ad esempio trasferimento o cessazione di personale).	●	●
4	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 1, 2 e 3.	●	●

PR.AA-03

Utenti, servizi e hardware sono autenticati

PUNTO	REQUISITO	S_I	S_E
1	Le modalità di autenticazione delle utenze per accedere ai sistemi informativi e di rete sono commisurate al rischio. A tal fine sono valutati almeno i rischi connessi: a) ai privilegi delle utenze; b) alla criticità dei sistemi informativi e di rete; c) alla tipologia di operazioni che le utenze possono effettuare sui sistemi informativi e di rete.	●	●
2	Per almeno i sistemi informativi e di rete rilevanti e in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono impiegate modalità di autenticazione multifattore.	●	●
3	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 1 e 2.	●	●



Fatte salve motivate e documentate ragioni

DE.CM-09

L'hardware e il software di elaborazione, gli ambienti di runtime e i loro dati sono monitorati per individuare eventi potenzialmente avversi.

PUNTO	REQUISITO	S_I	S_E
1	Fatte salve motivate e documentate ragioni normative o tecniche, sono presenti, aggiornati, mantenuti e configurati in modo adeguato, sistemi di protezione delle postazioni terminali per il rilevamento del codice malevolo.	●	●
2	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 1.	●	●



Forniture con potenziali impatti sulla sicurezza

GV.SC-01

Sono stabiliti e accettati dagli stakeholder dell'organizzazione il programma, la strategia, obiettivi, politiche e processi di gestione del rischio di cybersecurity della catena di approvvigionamento.

PUNTO	REQUISITO	S_I	S_E
1	In merito all'affidamento di forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete, anche mediante ricorso agli strumenti delle centrali di committenza di cui all'allegato I.1, articolo 1, comma 1, lettera i), del decreto legislativo 31 marzo 2023, n. 36, sono previsti: a) il coinvolgimento dell'organizzazione per la sicurezza informatica di cui alla misura GV.RR-02 nella definizione ed esecuzione dei processi di approvvigionamento a partire dalla fase di identificazione e progettazione della fornitura; b) in accordo agli esiti della valutazione del rischio associato alla fornitura di cui alla misura GV.SC-07, la definizione di requisiti di sicurezza sulla fornitura coerenti con le misure di sicurezza applicate dal soggetto NIS ai sistemi informativi e di rete.	●	●



Sistemi Informativi e di Rete «RILEVANTI»

In linea di principio, le misure di sicurezza si applicano a tutti i sistemi informativi e di rete del soggetto NIS (per la definizione di “**sistema informativo e di rete**” si faccia riferimento all’articolo 2, comma 1, lettera p) del decreto NIS). Ove, tuttavia, la disposizione di un requisito, o di parte di esso, contiene la dicitura **«per almeno i sistemi informativi e di rete rilevanti»**, il **soggetto NIS** ha la facoltà di **limitare l’ambito di applicazione della disposizione ai sistemi informativi e di rete la cui compromissione comporterebbe un impatto significativo sulla confidenzialità, integrità e disponibilità delle attività e servizi per i quali il soggetto NIS rientra nell’ambito di applicazione del decreto NIS.**



Sistemi Informativi e di Rete «RILEVANTI» Art. 2 Comma 1 Lett. P

"sistema informativo e di rete"

1) una rete di comunicazione elettronica ai sensi dell'articolo 2, comma 1, lettera vv), del [decreto legislativo 1° agosto 2003, n. 259](#);

*i **sistemi di trasmissione**, basati o meno su un'infrastruttura permanente o una capacità di amministrazione centralizzata e, se del caso, **le apparecchiature di commutazione o di instradamento** e altre risorse, inclusi gli **elementi di rete non attivi**, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti mobili e fisse (a commutazione di circuito e a commutazione di pacchetto, compresa internet), **i sistemi per il trasporto via cavo della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti utilizzate per la diffusione radiotelevisiva e le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato**;*

2) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali;

3) i dati digitali conservati, elaborati, estratti o trasmessi per mezzo di reti o dispositivi di cui ai numeri 1) e 2), per il loro funzionamento, uso, protezione e manutenzione;



Sistemi Informativi e di Rete «RILEVANTI»: esempi di valutazione

4. Criteri pratici per individuare i sistemi rilevanti

Criterio ACN	Domande da porsi	Esempi tipici
Impatto sul servizio	Se il sistema si ferma, il servizio NIS2 smette di funzionare?	Core-banking, portali anagrafici, sistemi SCADA
Dati trattati	Contiene o trasmette dati personali/sanitari/critici?	Database cittadini, repository referti medici
Interconnessioni	Serve da ponte tra reti interne ed esterne?	VPN, firewall, API gateway
External dependency	È un servizio cloud o di terza parte senza il quale l'ente non opera?	SaaS ERP, servizi DNS, CDN
Privilegi e identità	Gestisce autenticazione e autorizzazioni?	Active Directory, IdP, HSM



La Direttiva NIS2 – Focus Obblighi di base D.LGS 138/2024

Art. 25 – Obblighi in materia di notifica di incidente

Incidente Significativo se:

- ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;
- ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.





La Direttiva NIS2 – Focus Obblighi di base D.LGS 138/2024

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



Soggetti importanti ed essenziali
3 tipologie di incidenti



Solo soggetti essenziali
1 tipologia di incidente



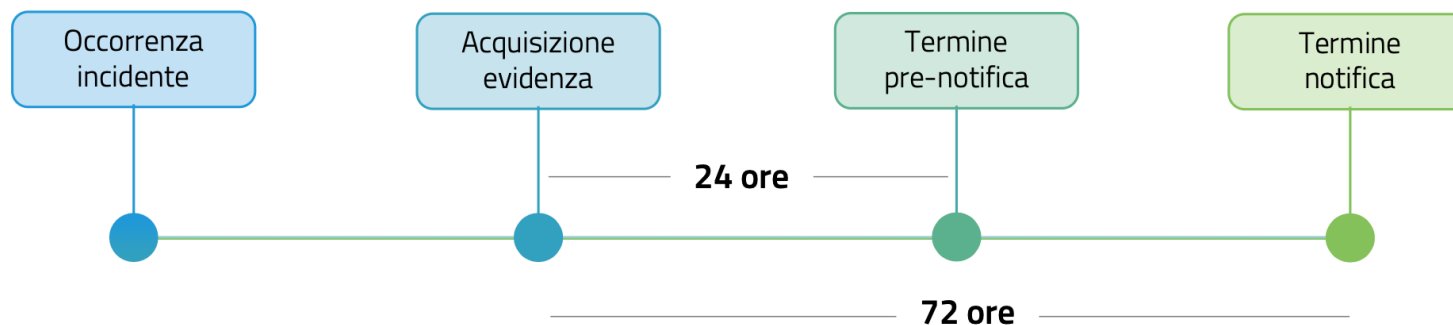


La Direttiva NIS2 – Focus Obblighi di base D.LGS 138/2024

Evidenza dell'incidente

Ai fini dell'adempimento dell'obbligo di notifica degli incidenti ciò che rileva è che il soggetto abbia evidenza (In tutte le tipologie di incidente previste negli allegati è infatti riportata la dicitura "Il soggetto NIS ha evidenza ...") del verificarsi di una delle tipologie di incidente indicate.

L'acquisizione dell'evidenza definisce il momento dal quale decorre il termine per l'obbligo di notifica.



Abuso dei privilegi concessi

Fattispecie in cui un operatore abbia l'autorizzazione tecnica (ossia la disponibilità di credenziali che sono configurate per accedere ai dati) per accedere a determinati dati ma tale accesso sia effettivamente illecito in quanto, ad esempio, effettuato in violazione delle politiche del soggetto o risultato strumentale al perseguimento di scopi estranei alle necessità funzionali di accesso..



La Direttiva NIS2 – Focus Catena di Fornitura D.LGS 138/2024

- **Valutazione e gestione del rischio nella catena di fornitura:** Le organizzazioni devono effettuare una valutazione approfondita dei rischi associati ai loro fornitori e subappaltatori. Questo implica l'analisi delle vulnerabilità specifiche che possono derivare dai rapporti con terze parti e l'adozione di misure adeguate per mitigare tali rischi.
- **Integrazione della sicurezza nei contratti con i fornitori:** È obbligatorio includere clausole contrattuali che impongano ai fornitori il rispetto di determinati standard di sicurezza informatica. Questo assicura che i fornitori adottino misure di sicurezza coerenti con quelle dell'organizzazione principale, garantendo una protezione uniforme lungo tutta la catena di approvvigionamento.





La Direttiva NIS2 – Focus Catena di Fornitura D.LGS 138/2024

- **Monitoraggio continuo e audit dei fornitori:** Le organizzazioni devono implementare processi per monitorare continuamente le pratiche di sicurezza dei loro fornitori. Questo può includere audit periodici e la richiesta di reportistica regolare per assicurarsi che i fornitori mantengano elevati standard di cybersecurity.
- **Piani di continuità operativa e gestione delle crisi:** È fondamentale che le organizzazioni sviluppino e mantengano piani di continuità operativa che considerino potenziali interruzioni derivanti dalla catena di fornitura. Questi piani devono includere procedure per il backup dei dati, il ripristino in caso di emergenza e la gestione delle crisi, garantendo la resilienza dell'intera filiera.





La Direttiva NIS2 – Focus Formazione D.LGS 138/2024

Art. 23: Gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti:

- a) sono tenuti a seguire una formazione in materia di sicurezza informatica;
- b) promuovono l'offerta periodica di una formazione coerente a quella di cui alla lettera a) ai loro dipendenti, per favorire l'acquisizione di conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi per la sicurezza informatica e il loro impatto sulle attività del soggetto e sui servizi offerti.

Art. 24 – Comma 2: Le misure di cui al comma 1 sono basate su un approccio multi-rischio, volto a proteggere i sistemi informativi e di rete nonché il loro ambiente fisico da incidenti, e comprendono almeno i seguenti elementi:

- g) pratiche di igiene di base e di formazione in materia di sicurezza informatica;





Acquisti: DPCM n. 102 del 5 maggio 2025

Regola l'acquisizione di beni e servizi informatici da parte delle pubbliche amministrazioni e degli enti pubblici, con particolare focus su quelli utilizzati **in ambiti sensibili per la sicurezza nazionale**.

L'obiettivo è garantire che tali acquisizioni rispettino elevati standard di sicurezza informatica, riducendo i rischi legati a vulnerabilità e minacce cibernetiche.





Acquisti: DPCM n. 102 del 5 maggio 2025

Principali elementi che disciplina il Decreto:

- ✓ gli **elementi essenziali di cybersicurezza** dei beni e dei servizi informatici (allegato 1), distinti fra:
 - requisiti relativi alle **proprietà** dei beni e dei servizi informatici
 - requisiti di **gestione delle vulnerabilità**
- ✓ le **specifiche categorie tecnologiche di beni e servizi informatici** per cui sono necessari elementi di cybersicurezza (allegato 2)
- ✓ i casi in cui, per la tutela della sicurezza nazionale, devono essere previsti **criteri di premialità** per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'UE o di Paesi aderenti all'Alleanza atlantica (NATO) o di Paesi terzi
- ✓ l'**elenco dei paesi terzi** tra quelli che sono parte di accordi di collaborazione sia con l'UE, sia con la NATO, in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione (allegato 3).

Misure di sicurezza





Tipologia di requisiti

Specifiche amministrative

Ad esempio:

- ✓ Adozione e approvazione politiche e procedure.
- ✓ Definizione di piani (ad es. risposta agli incidenti)
- ✓ Redazione documentazione.

Specifiche tecniche

Ad esempio:

- ✓ Cifratura dei dati.
- ✓ Aggiornamento del software.
- ✓ Modalità di autenticazione multifattore.



Evidenze documentali

Elenchi

Personale dell'organizzazione di sicurezza informatica, *configurazioni di riferimento*, sistemi ai quali è possibile accedere da remoto.

Inventari

Apparati fisici, servizi, sistemi e applicazioni software, *flussi di rete*, servizi erogati dai fornitori, fornitori

Piani

Gestione del rischio, business continuity e disaster recovery, trattamento del rischio, gestione delle vulnerabilità, adeguamento, *valutazione dell'efficacia delle misure di gestione del rischio*, formazione in materia di sicurezza informatica, risposta agli incidenti

Politiche

definite per almeno i requisiti riportati nella tabella 1 in appendice all'Allegato 1, per i soggetti importanti, e all'allegato 2, per i soggetti essenziali, della determina 164179/2025

Procedure

In relazione agli specifici requisiti per i quali sono richieste.

Registri

Esiti del riesame delle politiche, attività formazione dei dipendenti, *manutenzioni effettuate*.



La Direttiva NIS2 – Linee Guida

L'implementazione di misure di sicurezza informatica è cruciale per garantire la resilienza dei sistemi critici

Tali misure devono essere definite tenendo conto delle risorse disponibili:

- Umane
- Tecnologiche
- Finanziarie.

All'interno di questo contesto opera il referente per la cybersicurezza, una figura designata sulla base di competenze specifiche e comprovate esperienze nel settore della sicurezza informatica.



Strumenti a supporto

Misure di sicurezza

Entro 18 mesi (ottobre 2026) dalla ricezione della comunicazione di inserimento nell'elenco nazionale NIS, i soggetti importanti sono tenuti ad adottare le misure di sicurezza riportate nell'allegato 1 della [determinazione ACN 164179 del 14 aprile 2025](#), mentre i soggetti essenziali sono tenuti ad adottare le misure di sicurezza riportate nell'allegato 2 della medesima determina.

Le misure di sicurezza sono sviluppate in accordo al [Framework nazionale per la Cybersecurity e la Data Protection](#)  (edizione 2025) e sono organizzate in funzioni, categorie, sottocategorie e requisiti.

Ogni misura è costituita da un codice identificativo e una descrizione e da uno o più requisiti. Il codice e la descrizione fanno riferimento alle sottocategorie del framework. I requisiti indicano ciò che è richiesto ai fini dell'implementazione della misura.

[Misure di sicurezza di base per i soggetti importanti](#)

[Misure di sicurezza di base per i soggetti essenziali](#)

[Misure di sicurezza di base per i soggetti importanti formato.xlsx](#)

[Misure di sicurezza di base per i soggetti essenziali formato.xlsx](#)



<https://www.acn.gov.it/portale/nis/modalita-specifiche-base>



La Direttiva NIS2 – Politiche e procedure di sicurezza



Questo ambito riguarda la definizione di un quadro strategico per la gestione della sicurezza informatica, che comprenda policy, standard e procedure operative coerenti e integrate.

In questo contesto si colloca la misura di sicurezza **GV.PO-01**, che richiede **l'elaborazione di politiche e processi di cybersecurity** applicabili a diversi ambiti organizzativi.

In particolare, la misura prevede la definizione di politiche e processi per:

- a) gestione del rischio;
- b) ruoli e responsabilità;
- c) affidabilità delle risorse umane;
- d) conformità e audit di sicurezza;
- e) gestione dei rischi per la sicurezza informatica della catena di approvvigionamento;
- f) gestione degli asset;
- g) gestione delle vulnerabilità;
- h) continuità operativa, ripristino in caso di disastro e gestione delle crisi;
- i) gestione dell'autenticazione, delle identità digitali e del controllo accessi;
- j) sicurezza fisica;
- k) formazione del personale e consapevolezza;
- l) sicurezza dei dati;
- m) sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete;
- n) protezione delle reti e delle comunicazioni;
- o) monitoraggio degli eventi di sicurezza;
- p) risposta agli incidenti e ripristino.



La Direttiva NIS2 – Analisi del Rischio (1/2)



Questa area è dedicata all'identificazione, analisi e valutazione dei rischi informatici, nonché alla definizione di piani strutturati per la loro gestione.

Diverse misure del Framework FNCS contribuiscono in modo determinante a una gestione efficace del rischio, tra cui:

GV.RM-03: Richiede la **definizione di un piano aggiornato per la gestione del rischio informatico**, che includa **linee guida, obiettivi e azioni operative** per identificare, valutare e trattare i rischi.

Un modello di riferimento utile è la norma ISO/IEC 27005, che fornisce un approccio strutturato alla gestione del rischio per la sicurezza delle informazioni.



La Direttiva NIS2 – Analisi del Rischio (2/2)



ID.RA-05: Prevede l'esecuzione di una **valutazione del rischio** che consideri **minacce interne ed esterne, vulnerabilità, probabilità di accadimento, impatti potenziali**.

La valutazione deve includere le fasi di identificazione, analisi e ponderazione del rischio.

ID.RA-06: Richiede l'identificazione e la prioritizzazione delle risposte al rischio, documentando le decisioni adottate per il trattamento di ciascun rischio e definendo il rischio residuo.

DE.CM-01 e **DE.CM-09:** Contribuiscono al monitoraggio continuo e alla rilevazione tempestiva di eventi che potrebbero indicare l'emergere di nuovi rischi o la materializzazione di minacce note.



La Direttiva NIS2 – Definizione di ruoli e responsabilità



Quest'ambito sottolinea l'importanza di assegnare ruoli e responsabilità specifiche in materia di cybersicurezza, garantendo una chiara struttura organizzativa.

La misura **GV.RR-02** risponde a questa esigenza, richiedendo la definizione e la comunicazione di ruoli e responsabilità.

Nello specifico, la misura prevede la **definizione di una struttura organizzativa per la cybersecurity**, con l'individuazione di una struttura dedicata che si occupi di attività come lo **sviluppo di politiche di sicurezza, la gestione del rischio, la pianificazione di interventi di sicurezza e il monitoraggio delle minacce**.

Inoltre, la misura richiede la **nomina di un referente per la cybersicurezza**, con specifiche competenze in materia, e la comunicazione del suo nominativo all'ACN.



La Direttiva NIS2 – Affidabilità risorse umane



Quest'ambito sottolinea l'importanza di **assegnare ruoli e responsabilità specifiche in materia di cybersicurezza**, garantendo una chiara struttura organizzativa.

La misura **GV.RR-04** risponde a questa esigenza di includere la cybersicurezza nelle pratiche delle risorse umane:

il personale autorizzato ad accedervi è individuato previa valutazione dell'esperienza, capacità e affidabilità e deve fornire idonea garanzia del pieno rispetto della normativa in materia di sicurezza informatica.



La Direttiva NIS2 – Piano programmatico per la sicurezza



Questa area si concentra **sull'elaborazione di un piano programmatico** che definisca in modo chiaro le **strategie**, gli **obiettivi** e le attività operative necessarie per garantire la protezione di dati, sistemi e infrastrutture critiche.

Un piano di sicurezza completo ed efficace si costruisce attraverso l'applicazione coordinata di diverse misure, tra cui:

PR.AA-01, PR.AA-03, PR.AA-05: per la gestione degli accessi e delle identità digitali;

PR.AT-01, PR.AT-02: per la formazione e la consapevolezza del personale;

PR.DS-01, PR.DS-02 : per la sicurezza dei dati;

PR.PS-02: per la manutenzione sicura dei sistemi;

PR.IR-01: per la protezione delle reti e delle comunicazioni.



La Direttiva NIS2 – Censimento delle risorse (1/2)



Questa area si concentra sulla creazione di un inventario completo che includa sistemi, apparati, piattaforme, applicazioni, flussi di dati, nonché fornitori e partner terzi coinvolti nella gestione dei sistemi informativi.

Le misure **ID.AM-01**, **ID.AM-02**, **ID.AM-03** e **ID.AM-04** sono fondamentali per garantire una **mappatura accurata e aggiornata delle risorse**.

ID.AM-01: Richiede il **censimento di tutti i sistemi e apparati fisici** utilizzati all'interno dell'organizzazione.

L'inventario deve includere informazioni su server, postazioni di lavoro, dispositivi mobili, apparati di rete e soluzioni di sicurezza.

L'accesso alla rete deve essere consentito solo ai dispositivi approvati.

ID.AM-02: Prevede il **censimento di tutte le piattaforme e applicazioni software installate**, con un inventario che comprenda sistemi operativi, software di produttività, database, ecc.

L'installazione deve essere limitata solo a software autorizzati.



La Direttiva NIS2 – Censimento delle risorse (2/2)



ID.AM-03: Richiede l'**identificazione e la documentazione dei flussi di dati** in ingresso e in uscita dai sistemi informativi.

L'inventario deve riportare sorgenti, destinatari e protocolli utilizzati.

Le comunicazioni devono essere consentite solo per i flussi approvati.

ID.AM-04: Prevede la creazione di un **inventario dei fornitori** e partner terzi che forniscono componenti, sistemi o servizi ICT.

L'inventario deve includere informazioni sui contratti attivi e sulle tipologie di fornitura.



La Direttiva NIS2 – Monitoraggio e aggiornamento (1/2)



Questa area è dedicata al monitoraggio costante delle minacce e delle vulnerabilità, con l'obiettivo di garantire un aggiornamento tempestivo ed efficace dei sistemi di sicurezza.

Le misure **ID.RA-01**, **ID.RA-05**, **PR.IP-01**, **RS.MA-01** sono fondamentali per assicurare un'attività di monitoraggio strutturata e reattiva.



La Direttiva NIS2 – Monitoraggio e aggiornamento (2/2)



ID.RA-01: Richiede l'**identificazione e la documentazione delle vulnerabilità presenti nei sistemi**.

Include la definizione di un piano per l'individuazione delle vulnerabilità e l'esecuzione periodica di attività come vulnerability assessment e penetration test.

PR.IP-01: Prevede lo sviluppo e l'attuazione di un piano di gestione delle vulnerabilità, che comprenda:

- la **risoluzione tempestiva delle vulnerabilità rilevate**,
- l'**adozione delle misure di sicurezza indicate dall'ACN**,
- la **definizione di politiche e processi per la gestione strutturata delle vulnerabilità**.

RS.MA-01: Richiede l'istituzione di **processi per ricevere, analizzare e rispondere** alle informazioni sulle **vulnerabilità provenienti** da fonti autorevoli, come CSIRT Italia, CERT e ISAC.

La misura prevede inoltre la definizione di procedure, ruoli e responsabilità per la gestione efficace di tali informazioni.



La Direttiva NIS2 – Risposta agli incidenti



La Direttiva richiede la predisposizione di un piano di risposta agli incidenti, che definisca in modo chiaro le unità organizzative responsabili, insieme alle loro competenze decisionali, tecniche e finanziarie.

La misura **RS.MA-01**, **RS.CO-02** è fondamentale per garantire una risposta tempestiva, coordinata ed efficace agli incidenti informatici.

RS.MA-01 : Richiede la redazione di un **piano di risposta agli incidenti**, che includa:

- l'individuazione delle strutture responsabili della gestione degli incidenti;
- le procedure per la notifica degli incidenti al CSIRT Italia;
- le modalità operative per la gestione degli incidenti all'interno dell'organizzazione.

RS.CO-02 : In accordo al piano per la gestione degli incidenti di cui alla misura **RS.MA-01**, sono documentate e adottate **procedure per comunicare senza ingiustificato ritardo**



La Direttiva NIS2 – Seconda Tappa NIS2 1 gennaio 2026

Ecco un estratto delle misure minime da implementare **entro dicembre 2025** (valide sia per soggetti essenziali che importanti) per ottemperare all'obbligo di segnalazione degli incidenti:

Funzione: Govern (GV) 1

Strategia di gestione del rischio
GV.RM-03

Gestione del rischio di cybersecurity della catena di approvvigionamento
GV.SC-01

Funzione: Identity (ID) 2

Valutazione del rischio
ID.RA-05

Funzione: Govern (GV) 3

Gestione del rischio di cybersecurity della catena di approvvigionamento
GV.SC-07
GV.SC-05

Ruoli, responsabilità e correlati poteri
GV.RR-02

Funzione: Respond (RS) 4

Gestione degli incidenti
RS.MA-01

Segnalazione e comunicazione della risposta agli incidenti
RS.CO-02

Queste misure rappresentano il livello minimo di conformità richiesto per dicembre 2025. **Entro settembre 2026, dovranno essere completate tutte le misure previste.**



La Direttiva NIS2 – Conclusioni

Le linee guida per il rafforzamento della resilienza pubblicate dall'ACN rappresentano uno strumento estremamente utile per tradurre in pratica i principi introdotti dalla Direttiva NIS2.

Disporre di un **quadro chiaro delle misure di sicurezza da adottare**, con l'indicazione dei requisiti minimi attesi e delle modalità operative di implementazione, costituisce un supporto concreto per tutti gli attori coinvolti:

- **chi è responsabile della definizione delle modalità di applicazione** (governance, figure apicali);
- **chi è incaricato della messa in opera delle misure** (referenti e strutture operative dell'organizzazione, in coordinamento con struttura che governa la cybersecurity, supply chain);
- **chi ha il compito di verificare e vigilare sull'effettiva applicazione** (Direttori, Organi Amministrativi, CISO, etc.).



Gestione Vulnerabilità





Vulnerability Assessment

Il "vulnerability assessment" (valutazione delle vulnerabilità) è un processo cruciale nel campo della sicurezza informatica, finalizzato a **identificare, quantificare e prioritizzare (o classificare) le vulnerabilità in un sistema**





Analisi delle Vulnerabilità

Immaginiamo la nostra casa: porte, finestre, lucchetti, sono tutti **meccanismi di sicurezza** per proteggerci da intrusi.

Nel mondo digitale, i sistemi informatici (come i siti web, le applicazioni, le reti aziendali) hanno anch'essi "porte" e "finestre" che possono essere **vulnerabili ad attacchi**.

Il "vulnerability assessment" è come un controllo di sicurezza della casa, che **cerca punti deboli (vulnerabilità) che un intruso potrebbe sfruttare per entrare**.





Analisi delle Vulnerabilità

Obiettivi

Gli obiettivi principali del "vulnerability assessment" sono:

1. **Identificare** le vulnerabilità esistenti nei sistemi informatici.
2. **Quantificare** la gravità e il potenziale impatto di queste vulnerabilità.
3. **Prioritizzare** l'ordine di risoluzione basato sul rischio che ciascuna vulnerabilità rappresenta.





Analisi delle Vulnerabilità

Fasi

Il processo di "vulnerability assessment" può essere suddiviso in diverse fasi:

1. **Preparazione:** Definizione **degli obiettivi e delle risorse** (sistemi, applicazioni, reti) da valutare.
2. **Scansione:** Utilizzo di strumenti software per scansionare automaticamente i sistemi alla **ricerca di vulnerabilità note**.
3. **Analisi:** Valutazione dei risultati della scansione per identificare falsi positivi **e interpretare la gravità delle vulnerabilità trovate**.
4. **Rapporto:** Creazione di un rapporto dettagliato che elenca le vulnerabilità identificate, la loro gravità e le **raccomandazioni per mitigarle o risolverle**.
5. **Risoluzione:** Implementazione delle raccomandazioni per **correggere le vulnerabilità o ridurre il rischio**.
6. **Verifica:** Controllo post-risoluzione per assicurarsi che le **vulnerabilità siano state adeguatamente eliminate o mitigate**.





Analisi delle Vulnerabilità

Best Practices

È opportuno seguire queste indicazioni per ottenere un buon risultato su tutto il processo di Vulnerability Assessment

- **Frequenza delle scansioni:** è opportuno definire ogni quanto rieffettuare le scansioni, questo permetterà di ottenere una copertura sull'insorgere di nuove vulnerabilità
- **Integrazione con il ciclo di vita del software:** è consigliato farlo per ottenere una buona copertura in caso di cambiamenti del software
- **Formazione del personale:** è necessario formare il personale per essere in grado di interpretare i risultati ottenuti da un vulnerability assessment





Analisi delle Vulnerabilità

Diagramma di flusso





Analisi delle Vulnerabilità

Utilità

Il "vulnerability assessment" è fondamentale per mantenere la **sicurezza dei sistemi informatici**. I suoi benefici includono:

- **Prevenzione di Attacchi:** Identificare e correggere le vulnerabilità prima che gli aggressori possano sfruttarle.
- **Conformità Normativa:** Assicurare che i sistemi siano conformi agli standard di sicurezza richiesti da leggi e regolamenti.
- **Gestione del Rischio:** Aiutare le organizzazioni a comprendere e gestire meglio i rischi associati alle vulnerabilità dei loro sistemi.
- **Miglioramento Continuo:** Fornire un percorso chiaro per il miglioramento continuo delle pratiche di sicurezza.





Esempi pratici di Vulnerability Assessment nel settore sanitario

Dispositivi Medici Connessi (IoMT)

Scenario: Ospedale con dispositivi come pompe di infusione, monitor cardiaci e ventilatori collegati alla rete.

Attività: Scansione con strumenti specializzati (es. Medigate, Cynerio).

Vulnerabilità rilevate:

- Firmware obsoleto con CVE note
- Comunicazioni non cifrate (es. HTTP invece di HTTPS)
- Accesso remoto attivo senza autenticazione forte





Esempi pratici di Vulnerability Assessment nel settore sanitario

Laboratorio Analisi

Scenario: Sistema LIS (Laboratory Information System) connesso a strumenti diagnostici.

Attività: Vulnerability scan e analisi delle configurazioni.

Vulnerabilità rilevate:

- Database esposto su rete interna senza segmentazione
- Software con patch mancanti
- Account di default non disabilitati





Esempi pratici di Vulnerability Assessment nel settore sanitario

Cartelle Cliniche Elettroniche (EHR/EMR)

Scenario: Sistema EHR accessibile da medici e infermieri tramite web.

Attività: Scansione OWASP ZAP + analisi manuale.

Vulnerabilità rilevate:

- Cross-Site Scripting (XSS) nei campi di input
- Sessioni non invalidate dopo logout
- Mancanza di logging per accessi sensibili



Incident Response





Cos'è la Cybersecurity

La sicurezza NON E' un prodotto o un servizio

La sicurezza E' l'insieme di:

- Processi
- Regole - Procedure
- Servizi specializzati
- Risorse
- Organizzazione
- Cultura
- Strumenti
- Controlli

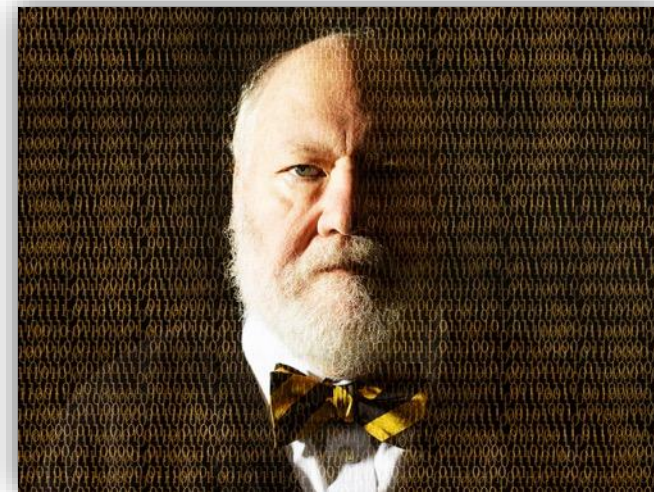




Cos'è la Cybersecurity

L'unico vero sistema sicuro è un sistema spento, chiuso in una gettata di cemento, sigillato in una stanza rivestita di piombo, protetta da guardie armate. Ma anche in questo caso ho i miei dubbi.

Questa frase è attribuita a Eugene Howard "Spaf" Spafford (1956), docente della Purdue University (USA) ed esperto nel settore dell'informatica e della sicurezza.





I principi fondamentali

RISERVATEZZA

- Avere la certezza che una determinata informazione possa essere conosciuta solo da chi ha il diritto di farlo

INTEGRITA'

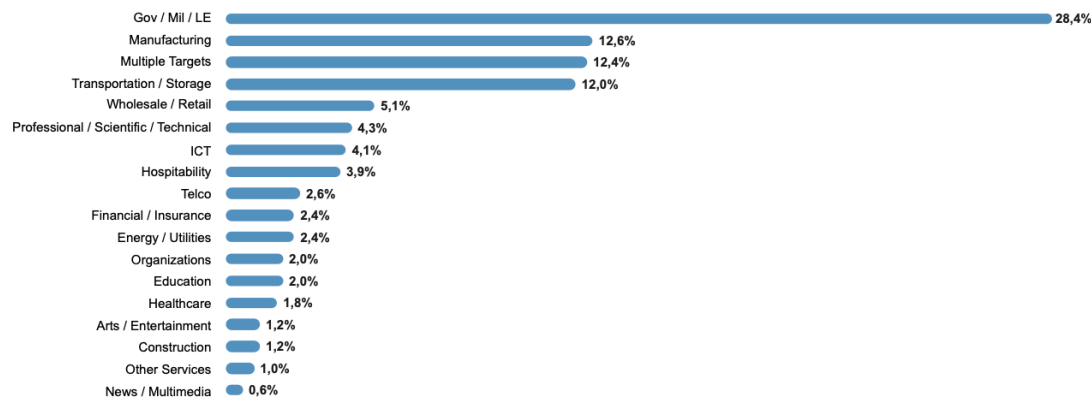
- Avere la certezza che una determinata informazione possa essere modificata solo da chi ha diritto di farlo e solo attraverso modalità note e verificabili

DISPONIBILITA'

- Avere la certezza che una determinata informazione possa essere prontamente reperita ed utilizzata tutte le volte che si ha necessità di farlo



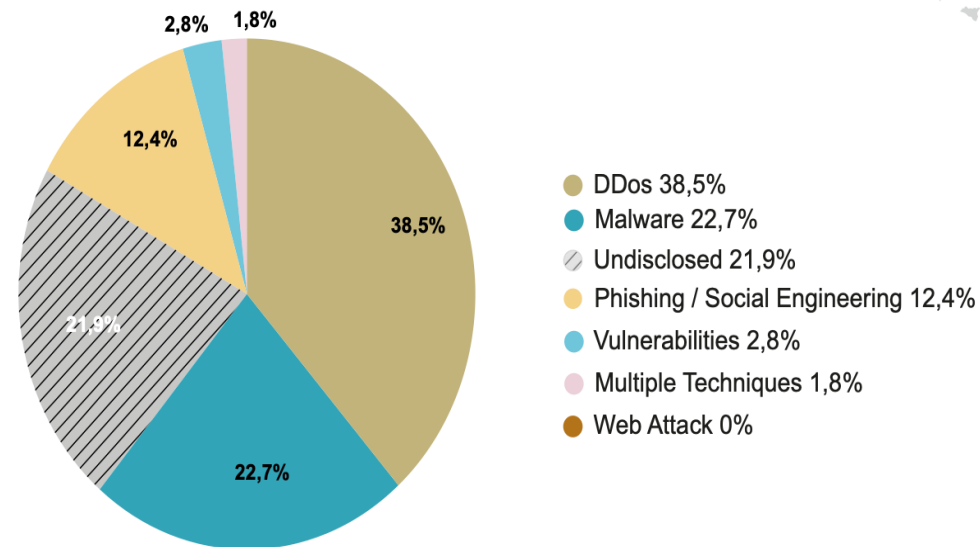
Vittime in Italia 2025



© Clusit - Rapporto 2026 sulla Cybersecurity

Fig. 29 - Distribuzione delle vittime in Italia nel 2025

Tecniche di attacco in Italia 2025



© Clusit - Rapporto 2026 sulla Cybersecurity

Fig. 31 - Tecniche di attacco in Italia nel 2025



Conosci il nemico

Vediamo come si sviluppa un Incidente e le cause





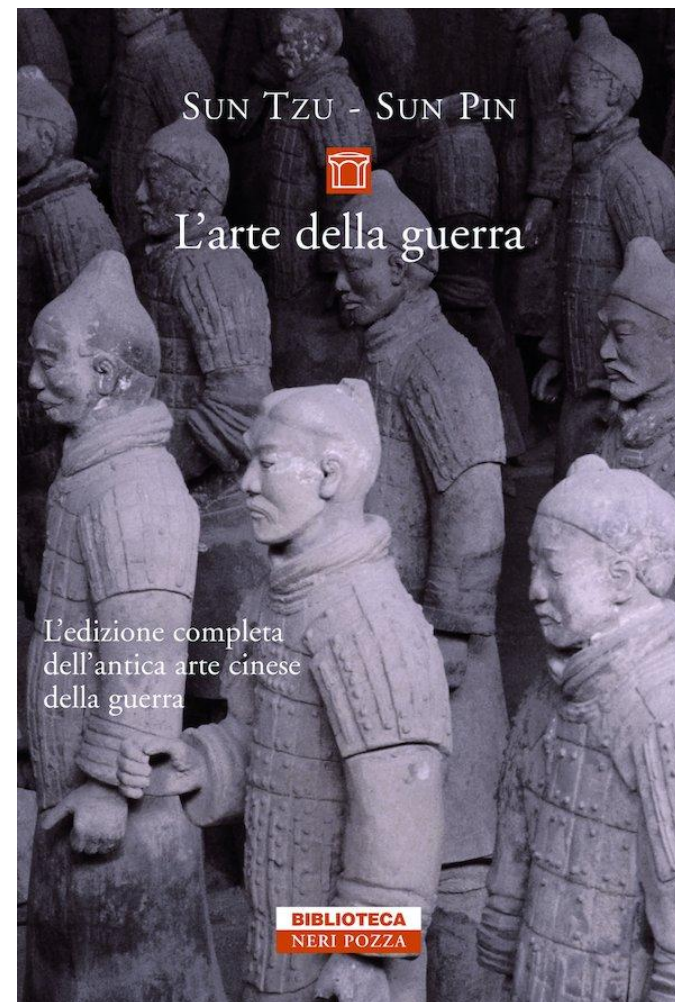
Conosci il nemico

«Se conosci il nemico e conosci te stesso, non devi temere il risultato di cento battaglie.

Se conosci te stesso ma non il nemico, per ogni vittoria ottenuta subirai anche una sconfitta.

Se non conosci né il nemico né te stesso, soccomberai in ogni battaglia»

Sun Tzu - "L'arte della guerra" VI secolo a.C.





Conosci il nemico

Le principali cause individuate da ACN:

1. **gestione decentralizzata dei sistemi IT**, con reparti che adottano soluzioni differenti senza una politica di sicurezza comune;
2. **obsolescenza delle tecnologie**, con dispositivi medicali non aggiornabili che rimangono vulnerabili;
3. **carenza di personale specializzato**, con la sicurezza informatica spesso affidata a personale IT non dedicato.

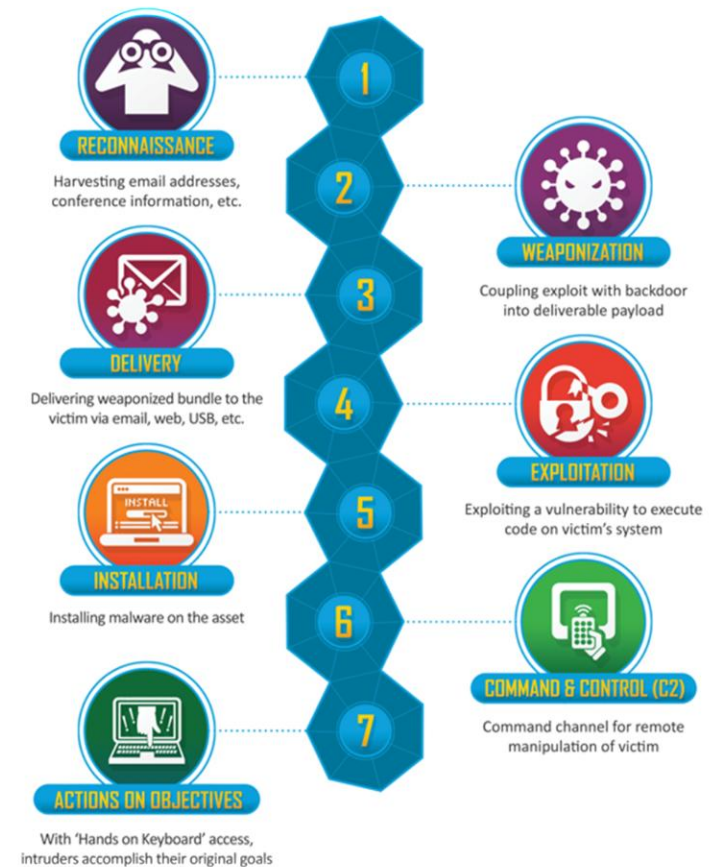


Conosci il nemico: la kill chain

La Cyber Kill Chain descrive i passaggi seguiti dagli hacker per effettuare un attacco informatico:

1. **Ricognizione:** Identificazione del bersaglio attraverso la raccolta di informazioni.
2. **Armamento:** Creazione di un malware specifico per il bersaglio.
3. **Consegna:** Trasmissione del malware al bersaglio, ad esempio tramite email.
4. **Sfruttamento:** Il malware sfrutta una vulnerabilità per entrare nel sistema.
5. **Installazione:** Il malware si installa consentendo l'accesso futuro.
6. **Comando e Controllo:** L'hacker comanda il malware da remoto.
7. **Azioni sugli Obiettivi:** L'hacker esegue azioni dannose, come furto di dati.

Ogni fase rappresenta un'opportunità per intercettare e bloccare l'attacco.





Riferire gli incidenti...

Non segnalo un incidente di sicurezza perché...

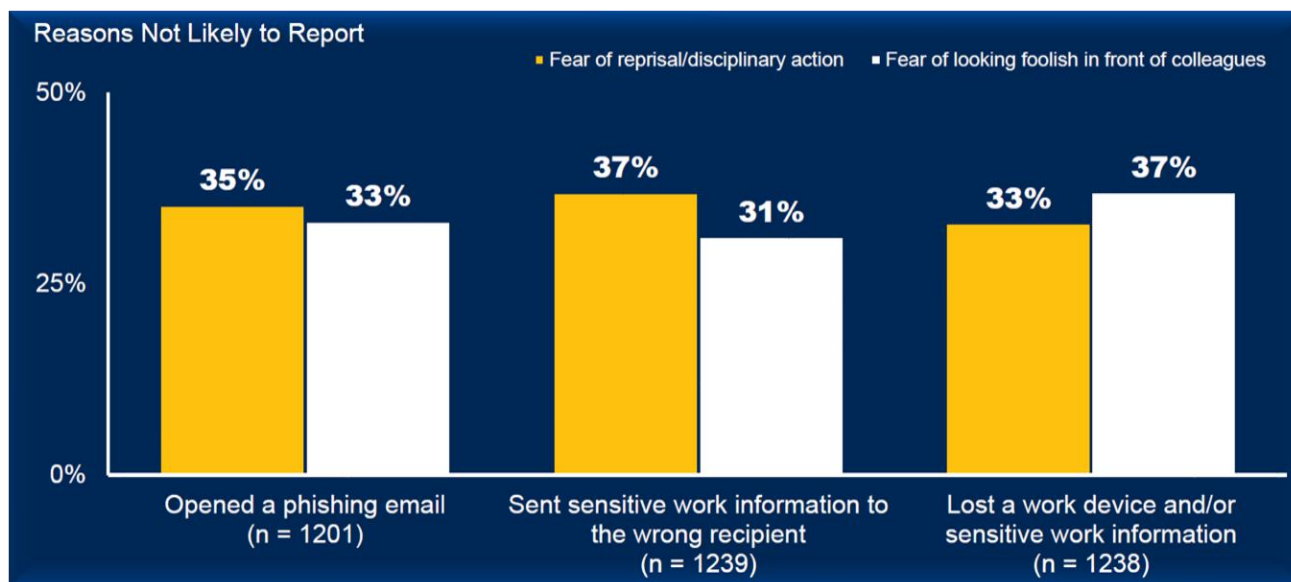
...sentirsi **VULNERABILI** ha un effetto
paralizzante sull'essere umano.





Riferire gli incidenti...

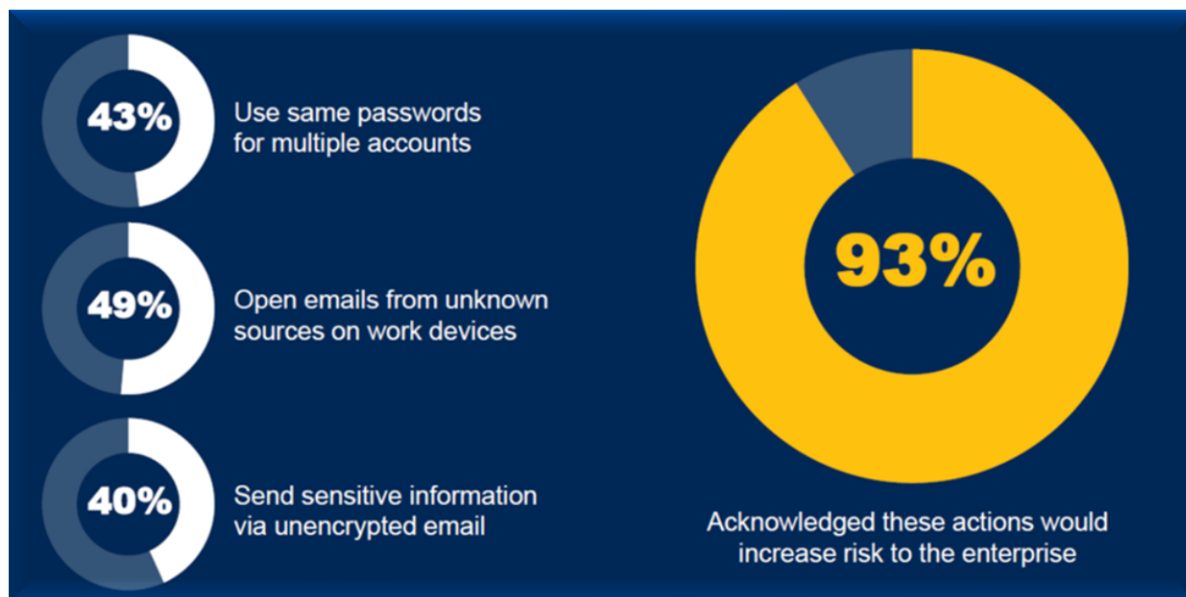
Non segnalo un incidente di sicurezza perché...





Riferire gli incidenti...

*So che **non si dovrebbe** fare ma...*

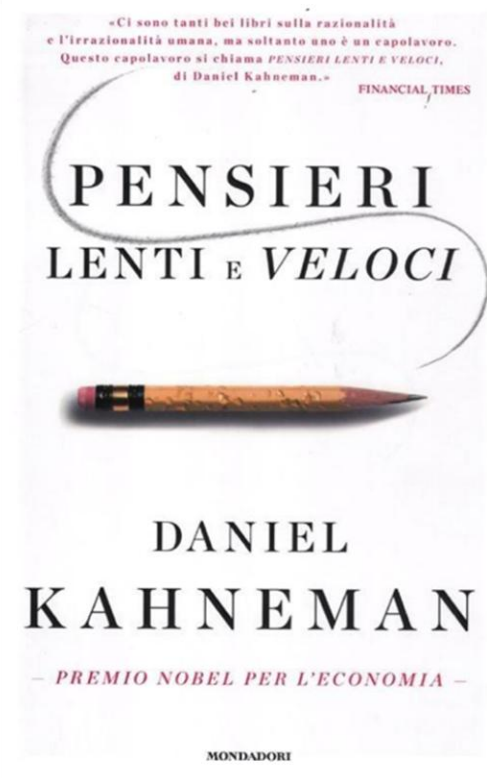




«Una generale **'legge del minimo sforzo'** si applica tanto all'esercizio cognitivo quanto a quello fisico...

...se ci sono diversi modi per raggiungere lo stesso obiettivo, le persone tenderanno a **scegliere l'azione meno impegnativa...**

La **pigrizia** è profondamente radicata nella nostra natura.»





Risposta agli incidenti

L'"Incident Response" (risposta agli incidenti) è un approccio organizzato per affrontare e gestire le **conseguenze di un attacco informatico o di una violazione della sicurezza**, con l'obiettivo di **limitare il danno e ridurre il tempo di recupero e i costi**.





Risposta agli incidenti

Pensiamo a un incendio in un edificio: l'obiettivo principale è non **solo spegnere l'incendio** il più rapidamente possibile, ma anche **evacuare in sicurezza le persone, limitare i danni e investigare sulle cause per prevenire futuri incendi**.

In modo simile, l'Incident Response si occupa di "spegnere" gli attacchi informatici, proteggere i dati e le risorse, e apprendere dall'incidente per rafforzare le difese.

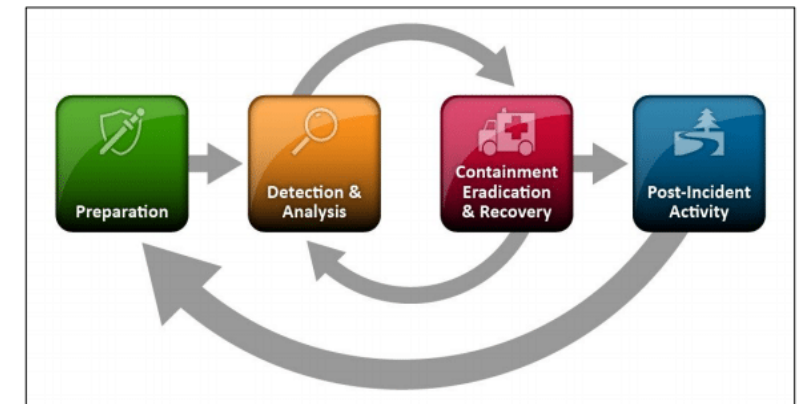




Risposta agli incidenti – processo di incident response

- **preparazione**: sviluppo di un **piano di risposta** agli incidenti, formazione del team di risposta e preparazione delle risorse necessarie
- **identificazione**: rilevamento di un **potenziale incidente** di sicurezza attraverso sistemi di monitoraggio, allarmi o segnalazioni
- **contenimento**: adozione di misure immediate **per limitare l'estensione del danno** che può includere l'isolamento della rete o dei dispositivi colpiti.
- **eradicazione**: **rimozione della causa dell'incidente**, che può implicare la disinfezione da malware o la chiusura di vulnerabilità sfruttate
- **recupero**: **ripristino dei sistemi e dei servizi** alla loro operatività normale, assicurandosi che non siano più vulnerabili agli stessi attacchi
- **post-incident review**: **analisi dell'incidente per trarre insegnamenti**, migliorare i processi di risposta e rafforzare le misure di sicurezza

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce





Risposta agli incidenti: perché è importante?

limitazione del danno

ridurre l'impatto finanziario e di reputazione derivante da violazioni o attacchi informatici

ripristino rapido

assicurare il ritorno alla normalità operativa in breve tempo e minimizzare l'interruzione delle attività

conformità legale

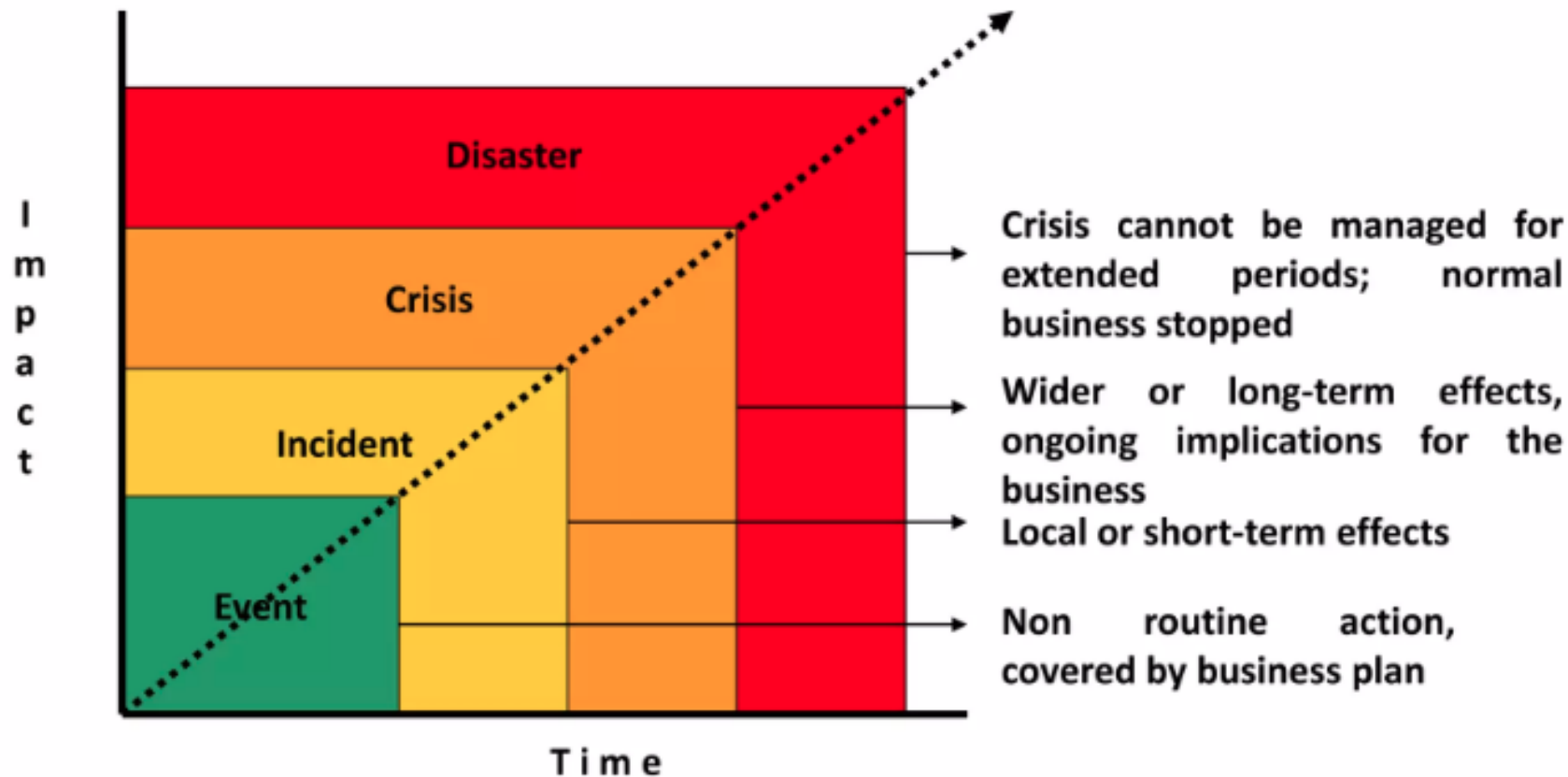
molte normative richiedono piani di risposta agli incidenti e notifiche in caso di violazioni dei dati

miglioramento continuo

ogni incidente offre l'opportunità di rafforzare le difese contro future minacce



What is a crisis?



Supply Chain





Incident Response: Supply Chain

Secondo il rapporto dell'ENISA “**Good Practices for supply chain cybersecurity**”, pubblicato lo scorso giugno 2023, si evidenzia che un'ampia percentuale delle organizzazioni intervistate, compresa tra il 39% e il 62%, ha subito un incidente informatico causato da terze parti

nel 66% dei casi di attacchi alla supply chain analizzati, i fornitori non erano consapevoli di come fossero stati compromessi o mancavano di trasparenza al riguardo





Incident Response: Supply Chain – Key Good Practice

- **Valutazione del Rischio:** Effettuare regolarmente analisi approfondite per individuare vulnerabilità nella supply chain, includendo la verifica delle pratiche di sicurezza dei fornitori.
- **Certificazione dei Fornitori:** Richiedere certificazioni di sicurezza per garantire l'adesione a standard riconosciuti e uniformare le pratiche di cybersecurity.
- **Protocolli di Segnalazione:** Definire procedure chiare per la comunicazione tempestiva degli incidenti, permettendo interventi rapidi per ridurre gli impatti.





Incident Response: Supply Chain – Key Good Practice

Gestione Patch e Vulnerabilità: Applicare una politica rigorosa di patching, correggendo le vulnerabilità critiche entro un mese e mantenendo visibilità sugli asset.

Monitoraggio Continuo: Utilizzare strumenti di monitoraggio per rilevare minacce in tempo reale e adottare misure proattive.

Formazione e Sensibilizzazione: Offrire formazione regolare su best practice di cybersecurity per dipendenti e fornitori, creando una cultura di sicurezza.

Collaborazione e Condivisione: Favorire la cooperazione e lo scambio di informazioni tra partner per rafforzare la sicurezza e individuare minacce emergenti.



Tassonomia ACN





Tassonomia Cyber ACN

“Tassonomia Cyber dell’Agenzia per la Cybersicurezza Nazionale” (TC-ACN), ossia il linguaggio comune per lo scambio delle informazioni relative a eventi e minacce di cybersicurezza.

<https://www.acn.gov.it/portale/isac-italia/linee-guida-operative>

Dettagli

https://www.acn.gov.it/portale/documents/d/guest/acn_tassonomia_cyber_clear



Tassonomia Cyber

L'ACN ha definito una "*tassonomia cyber*" (TC-ACN) in grado di:

- agevolare lo scambio di informazioni a livello nazionale attraverso l'adozione di un lessico comune che rappresenti una base metodologica sia per la condivisione di informazioni riguardo agli eventi cyber sia per la notifica degli incidenti al CSIRT Italia;
- identificare, definire e caratterizzare gli eventi cyber attraverso un'unica tassonomia rilevante a livello nazionale;
- fornire alle organizzazioni un documento che si armonizzi con le tassonomie internazionali in materia di cybersecurity e che sia al contempo adeguato al contesto normativo nazionale.

[Scarica linea guida →](#)



Tassonomia Cyber ACN: le macrocategorie

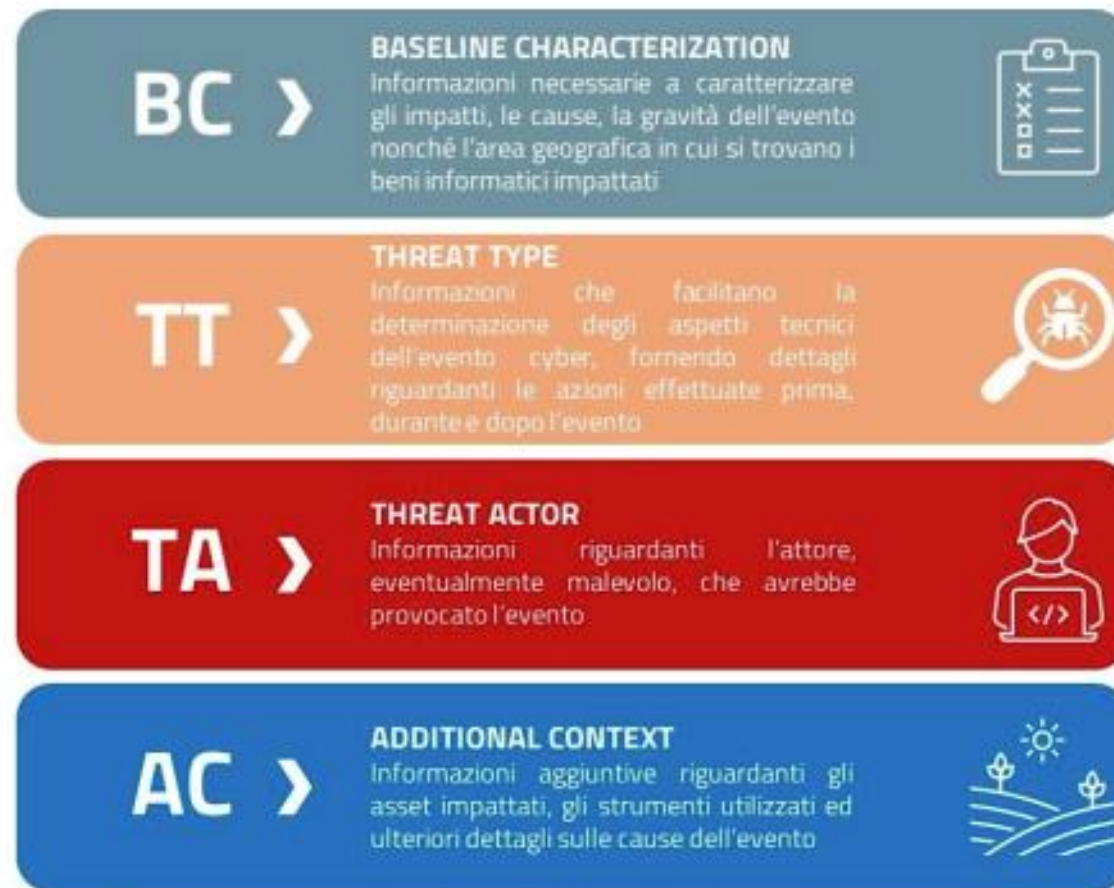


Figura 1: Struttura della tassonomia degli eventi cyber - Macrocategorie



Tassonomia Cyber ACN: i predicati

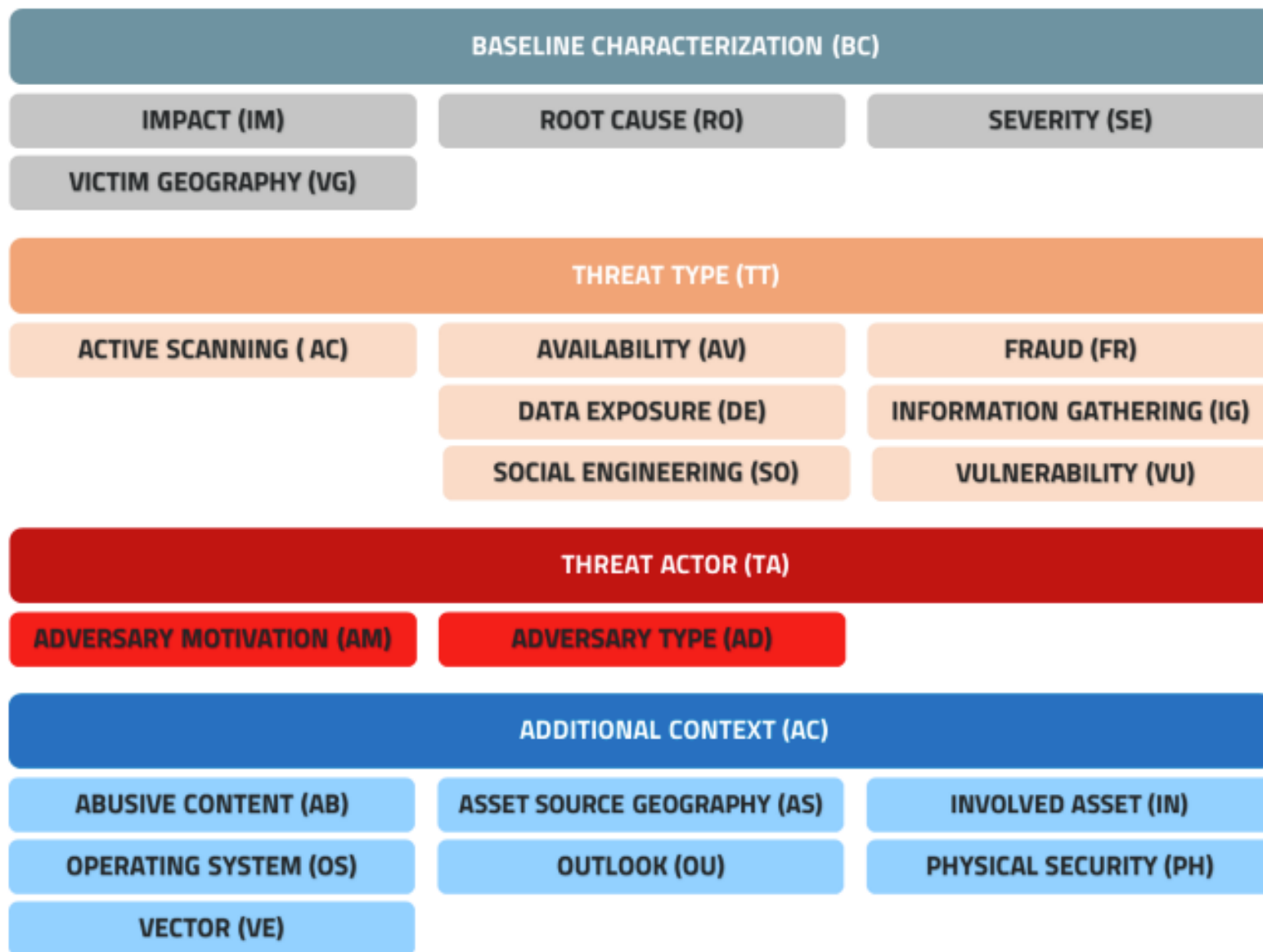


Figura 2: Struttura della tassonomia degli eventi cyber - Predicati



Flusso di Segnalazione Legge 90/2024 -> NIS2

AGENZIA PER LA CYBERSICUREZZA NAZIONALE

DETERMINA 9 febbraio 2026

Tassonomia degli incidenti di cui all'articolo 1, comma 1, della legge 28 giugno 2024, n. 90. (26A00713)

(GU n.39 del 17-2-2026)

[...] medesimo art. 1;

Ritenuto, pertanto, in un'ottica di semplificazione degli oneri da parte dei soggetti interessati, di poter considerare assolto, in caso di prenotifica e notifica effettuata ai sensi dell'art. 25 del decreto NIS, anche l'obbligo di cui all'art. 1, comma 1, della legge n. 90 del 2024;

[...]

*** ATTO COMPLETO ***

Verso un Piano Cyber





Il ruolo del Responsabile Sicurezza IT



Tra le principali aree di competenze e responsabilità di questa figura si trovano le seguenti.

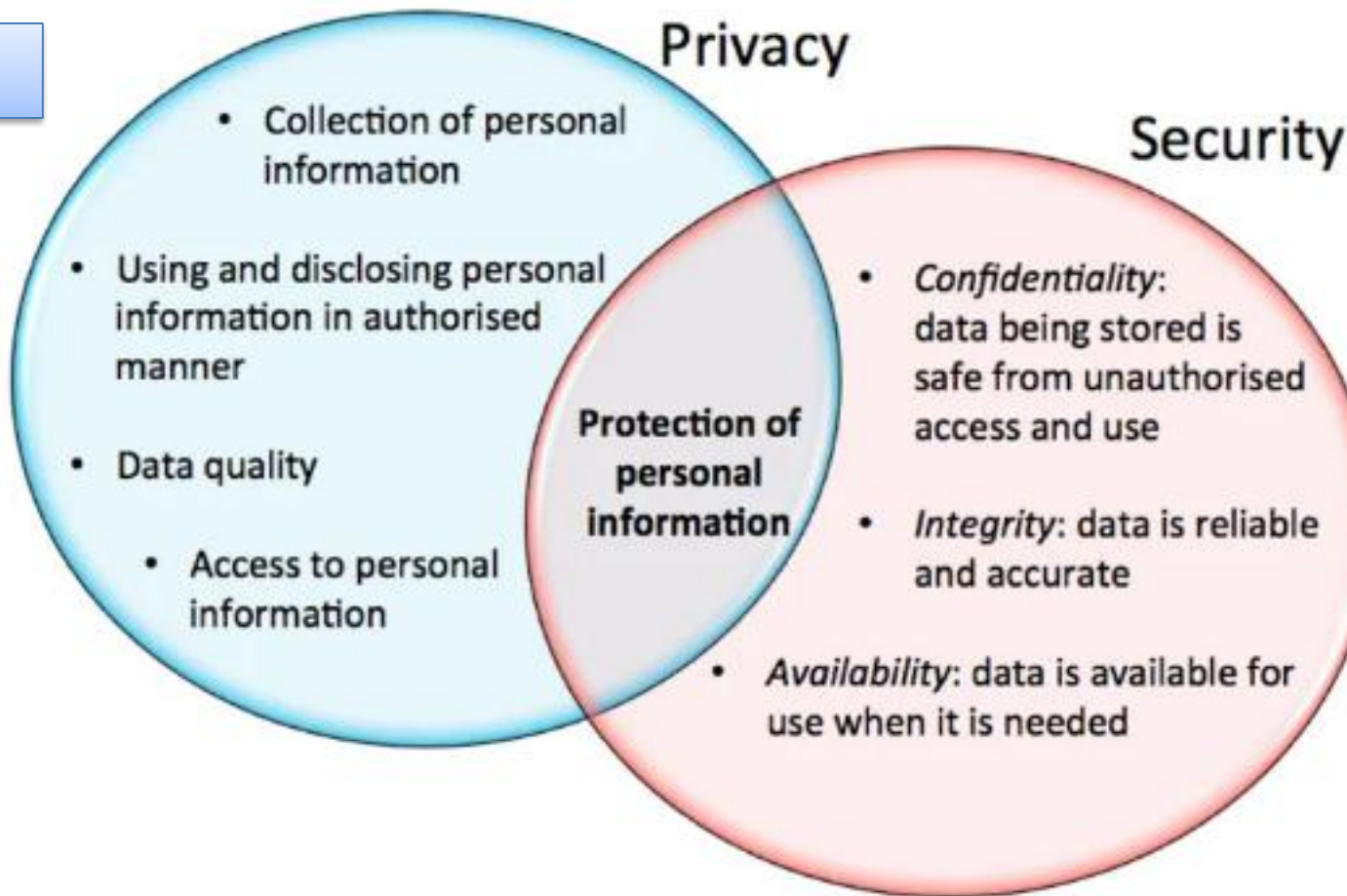
- **Assessment della sicurezza:** valutare lo stato dell'arte della sicurezza in azienda e individuare un piano strategico per aumentare la capacità di reagire alle cyber minacce;
- **Definizione delle policy:** definire regole e standard per la gestione della sicurezza;
- **Analisi del rischio cyber:** comprendere le vulnerabilità e le minacce per l'azienda o l'Ente in modo da compiere scelte adeguate per la gestione del rischio cyber in termini di politiche e strumenti;
- **Definizione delle architetture:** disegnare l'architettura per la gestione della sicurezza e monitoraggio delle scelte strutturali;
- **Identificazione delle minacce:** essere aggiornati sulle tipologie di minacce e di attacco;
- **Monitoraggio della sicurezza:** controllare il traffico sui diversi canali sviluppando un Security Operation Center (SOC) interno all'azienda o collaborando con un provider esterno;
- **Risposta agli incidenti:** rispondere in tempi brevi in caso di data breach per limitarne gli effetti;



Il ruolo del Responsabile Sicurezza IT



DPO



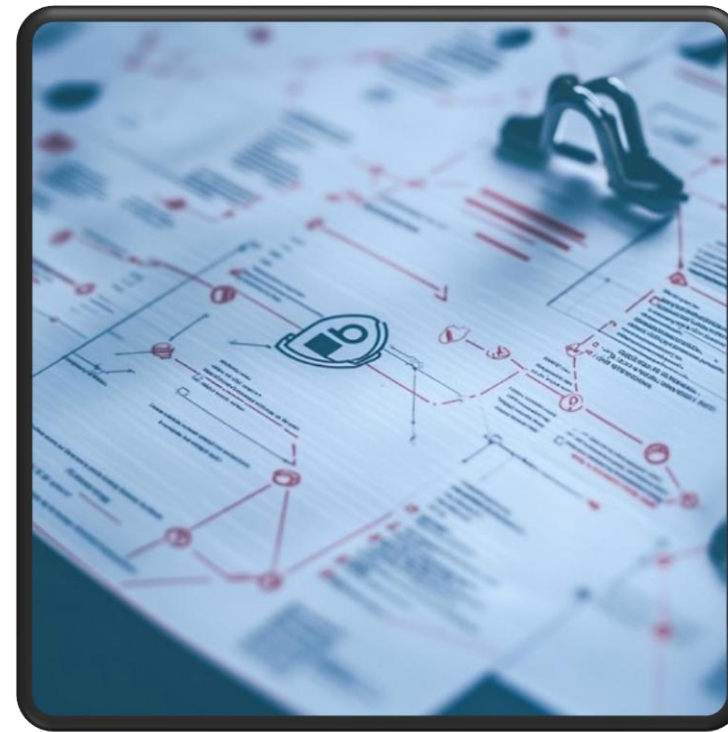
CISO



Verso un Piano Cyber

Linee Guida ACN:

[Linee guida per il rafforzamento della resilienza e referente per la cybersicurezza - ACN](#)





Le azioni da mettere in campo

Assessment & Gap analysis

- Identificare i principali gap attraverso un **assessment** generale
- Eseguire **Vulnerability Assessment** e **Penetration Test** periodicamente
- Condurre l'attività di **Threat Intelligence** per verificare esposizione ai rischi cyber
- **Phishing Campaign**

Piano strategico delle iniziative Cyber

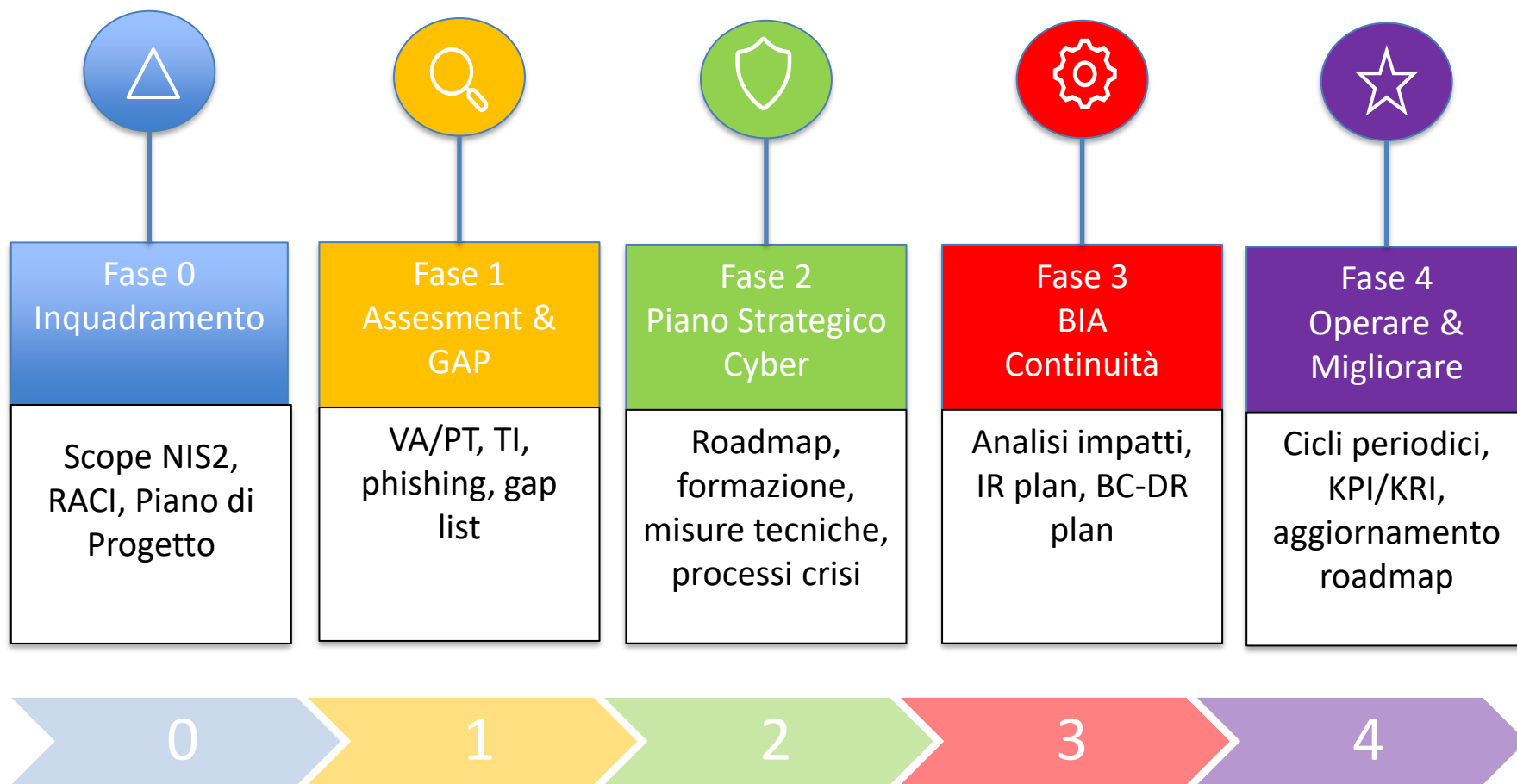
- Identificare le **azioni correttive** per coprire i gap individuati con le attività precedenti
- **Disegnare un percorso sostenibile** per le iniziative dell'Ente in ambito Security
- **Formazione** del personale
- Adozione di **misure tecniche** ed **organizzative**

BIA ed impostazione Piano di ripartenza dei servizi

- Eseguire la **Business Impact Analysis (BIA)** al fine di identificare i principali sistemi critici
- Redigere il **piano di risposta agli incidenti** e di **ripartenza dei servizi** sulla base dei risultati della **BIA**
- Definire il modello e i **processi di gestione della crisi ICT**



Le azioni da mettere in campo



Grazie

Marco Boz

marco.boz@csi.it