UNIVERSITÀ POLITECNICA DELLE MARCHE

DII
Dipartimento di Ingegneria dell'Informazione

unimc

Direttiva UE 2022/2555 (NIS 2), D.lgs. 138/2024 e gli adempimenti a carico delle imprese che si occupano della gestione dei rifiuti

Cofanelli Emanuele

Giovedì 02 ottobre 2025

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Scaletta

1. Evoluzione normativa della Cyber Security in Italia;
2. NIS 2 e Decreto NIS: aspetti principali;
3. Piccolo focus impresa gestione rifiuti;
4. NIS 2 e GDPR considerazioni finali.

Evoluzione normativa della Cyber Security in Italia

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Evoluzione normativa della Cyber Security in Italia

- DPCM 24 gennaio 2013 «Decreto Monti»: **definisce**, considerando la minaccia cibernetica come un rischio per la sicurezza nazionale, **l'architettura istituzionale per la tutela della cybersicurezza**, attribuendo compiti specifici a ciascuna componente coinvolta, con i principali **obbiettivi di ridurre le vulnerabilità delle infrastrutture critiche**, di promuovere la cooperazione tra settore pubblico e privato e di garantire il ripristino tempestivo delle funzionalità dei sistemi in caso di crisi;

- DPCM 17 febbraio 2017 «Decreto Gentiloni»: **aggiorna e rafforza l'architettura istituzionale per la cybersicurezza** impostata dal Decreto Monti **semplificandola e integrandola con le nuove esigenze della Direttiva NIS** (UE 2016/1148). Il decreto ha l'obbiettivo di rafforzare il coordinamento tra le istituzioni centralizzando le funzioni di gestione delle crisi cibernetiche sotto il Presidente del Consiglio e il CISR, coinvolgendo il Dipartimento delle informazioni per la sicurezza (DIS) e il Nucleo per la sicurezza cibernetica.

Evoluzione normativa della Cyber Security in Italia

- **Direttiva UE 2016/1148 e D.lgs. 65/2018:** Conosciuta come **direttiva NIS**, recepita in Italia con il **D.lgs. 65/1018**, ha introdotto misure per migliorare la sicurezza delle reti e dei sistemi informativi nell'UE, individuando **operatori di servizi essenziali** (OSE) e **fornitori di servizi digitali** (FSD) soggetti a obblighi di sicurezza e notifica degli incidenti.

- **D.L. 105/2019, convertito in L. 133/2019** : introduzione di disposizioni urgenti – complementari a quelle della NIS e del D.lgs. 65/2018 – per istituire e regolamentare il **Perimetro di Sicurezza Nazionale Cibernetica (PSNC)**, con il fine di proteggere le infrastrutture critiche da cui dipendono le funzioni essenziali dello Stato e i servizi fondamentali per gli interessi nazionali. **Tale normativa si affianca alla Direttiva NIS**, che tutela le reti e i sistemi informativi necessari per il mercato interno, andando a creare **due domini complementari e interdipendenti**: il primo per la sicurezza del mercato, il secondo per la sicurezza nazionale, coordinati per una protezione cibernetica integrata;

Evoluzione normativa della Cyber Security in Italia

- D.L. 82/2021, convertito in L. 109/2021: introduzione di misure urgenti finalizzate al rafforzamento della cybersicurezza nazionale, con l'obbiettivo di aggiornare l'architettura italiana di cybersicurezza, **creando l'Agenzia per la Cybersicurezza Nazionale (ACN),** chiamata a coordinare le attività di sicurezza informatica a livello nazionale e a promuovere la resilienza cibernetica.

- L. 28 giugno 2024 n.90**:** ridefinisce il quadro normativo nazionale in materia di cybersicurezza **introducendo disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici.** In particolare, **introduce l'obbligo**, in capo a una vasta gamma di enti pubblici, di **notifica degli incidenti di sicurezza che devono essere segnalati entro 24 ore e notificati entro 72 ore.** Tale legge stabilisce inoltre che gli enti devono individuare una **struttura interna deputata alla gestione della sicurezza informatica** e introduce la figura del referente per la cybersicurezza che assolve la funzione di punto di contatto unico con l'Autorità (ACN).

Direttiva NIS 2 e Decreto NIS: aspetti principali

Direttiva NIS 2 e Decreto NIS: aspetti principali

La **Direttiva NIS 2** (Network and Information Security 2) è il nuovo quadro normativo dell'Unione Europea per la sicurezza delle reti e dei sistemi informativi. Il suo obiettivo principale è **rafforzare la resilienza digitale delle infrastrutture critiche e dei servizi essenziali**, ampliando il campo di applicazione e introducendo requisiti di sicurezza più severi rispetto alla precedente Direttiva NIS 1.

Con il **decreto legislativo 4 settembre 2024, n. 138** l'Italia ha recepito nell'ordinamento nazionale la direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di sicurezza informatica nell'Unione abrogando la precedente direttiva.

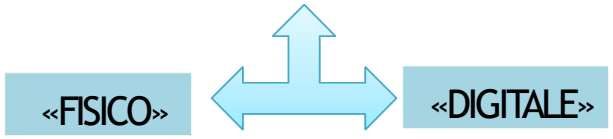
Direttiva NIS 2 e Decreto NIS: aspetti principali

- Ampliano il campo di applicazione della normativa in materia di cybersicurezza, sostituendo le categorie di «operatori di servizi essenziali» e «fornitori di servizi essenziali» con «**soggetti essenziali**» e «**soggetti importanti**», stabilendo criteri uniformi a livello europeo;
- Il **Decreto NIS** si applica a medie e grandi imprese in settori chiave e alla PA centrale, includendo micro e piccole imprese in settori strategici;
- Il **Decreto NIS** amplia l'applicazione della normativa a soggetti operanti nei settori definiti dagli allegati del decreto, indipendentemente dalle dimensioni (vedi appunti corso);
- **ACN** è incaricata di identificare i soggetti essenziali e importanti, gestendo un elenco aggiornato annualmente basato su registrazioni obbligatorie da parte degli interessati;
- Il **Decreto NIS** è strettamente legato alla norma **ISO/IEC 27001:2022**, offrendo uno schema per le organizzazioni già conformi o meno a tale standard.

Direttiva NIS 2 e Decreto NIS: aspetti principali

La Direttiva NIS 2 ed il Decreto NIS adottano due tipi di approcci, finalizzati a contrastare le minacce cibernetiche:

MULTI-DIMENSIONALE



Combina le protezioni fisiche e digitali: i soggetti essenziali e importanti oltre ad implementare misure di cybersecurity devono proteggere anche le infrastrutture fisiche nelle quali sono poste le reti e i sistemi informatici.

MULTI-LIVELLO

1 - STRATEGICO
2 - OPERATIVO

Coordina le strategie operative e gestionali, creando un sistema più rigoroso e coordinato per contrastare le crescenti minacce su più fronti.

Direttiva NIS 2 e Decreto NIS: aspetti principali

Il **Decreto NIS** conferma il **ruolo dell'ACN come Autorità nazionale competente NIS** e Punto di contatto unico. Sono inoltre identificati **9 Ministeri quali Autorità di settore che supportano l'attuazione della normativa con la propria competenza settoriale**, collaborando nel contesto del Tavolo per l'attuazione della disciplina NIS presieduto da ACN, a cui prendono parte anche rappresentanti della Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano.

Direttiva NIS 2 e Decreto NIS: aspetti principali

Chi sono i «**soggetti essenziali**» e «**soggetti importanti**»?

I **quattro allegati** del DECRETO NIS individuano il contesto di applicazione:

ALLEGATO I - Settori ad altra criticità

ALLEGATO II - Altri settori critici

ALLEGATO III - Amministrazioni centrali, regionali, locali e di altro tipo

ALLEGATO IV - Ulteriori tipologie di soggetti

Settore	Dettaglio	Grandi imprese	Medie imprese	Piccole e micro imprese
SETTORI ALTAMENTE CRITICI				
Energia	19 tipologie di soggetto	Essenziali	Importanti *	Fuori ambito **
Trasporti	10 tipologie di soggetto			
Settore bancario	DORA Lex specialis			
Infrastrutture dei mercati finanziari				
Settore sanitario	5 tipologie di soggetto			
Acqua potabile	1 tipologia di soggetto			
Acque reflue	1 tipologia di soggetto			
Infrastrutture digitali	9 tipologie di soggetto			
Gestione dei servizi TIC (b2b)	2 tipologie di soggetto		Importanti *	Fuori ambito **
Spazio	1 tipologia di soggetto			
SETTORI CRITICI				
Servizi postali e di corriere	1 tipologia di soggetto	Importanti *		Fuori ambito **
Gestione dei rifiuti	1 tipologia di soggetto			
Fabbricazione, produzione e distribuzione di sostanze chimiche	1 tipologia di soggetto			
Produzione, trasformazione e distribuzione di alimenti	1 tipologia di soggetto			
Fabbricazione	6 tipologie di soggetto			
Fornitori di servizi digitali	4 tipologie di soggetto			
Ricerca	2 tipologie di soggetto	Importanti *		Fuori ambito **
ULTERIORI TIPOLOGIE DI SOGGETTI				
Pubblica Amministrazione centrale	4 categorie di PA	Essenziali		
Pubblica Amministrazione regionale e locale	11 categorie di PA	Importanti *		
Ulteriori tipologie di soggetti	4 tipologie di soggetti	Identificazione dell'Autorità		

Direttiva NIS 2 e Decreto NIS: aspetti principali

Nell'ambito degli adempimenti, sono previsti, ai sensi degli **articoli 23, 24 e 25** del **Decreto NIS (D.lgs. 138/2024)**, obblighi per gli organi di amministrazione e direttivi, la gestione dei rischi per la sicurezza informatica e le notifiche di incidente:

- **Articolo 23** disciplina gli obblighi in carico agli **organi di amministrazione e direttivi** dei soggetti essenziali e importanti;

- **Articolo 24** disciplina gli **obblighi in materia di misure di gestione dei rischi per la sicurezza informatica** prevedendo che i soggetti essenziali e importanti adottino misure tecniche, operative e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete che i 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;

- **Articolo 25** disciplina gli **obblighi sulle notifiche di incidente** prevedendo che i soggetti essenziali e i soggetti importanti trasmettono al CSIRT Italia 3 ogni incidente che abbia un impatto significativo sulla fornitura dei loro servizi.

Direttiva NIS 2 e Decreto NIS: aspetti principali

Determinazione dell'Agenzia per la Cybersicurezza Nazionale n. 164179 del 14 aprile 2025

Per l'adempimento degli obblighi di cui agli articoli 23, 24, e 25 del decreto NIS, i soggetti NIS, sono tenuti ad adottare le misure di sicurezza di base e a notificare al **CSIRT Italia*** gli incidenti significativi di base stabiliti dalla **determinazione ACN 164179 del 14 aprile 2025**. Gli allegati tecnici alla determinazione sono stati elaborati sulla base dei riscontri pervenuti nel corso delle consultazioni con le Autorità di settore e con le associazioni di categoria anche per mezzo dei tavoli settoriali di cui all'articolo 11, comma 4, lettera f), del decreto NIS.

La determinazione riporta i seguenti allegati tecnici:

- **Allegato 1**: misure di sicurezza di base per i soggetti importanti.
- **Allegato 2**: misure di sicurezza di base per i soggetti essenziali.
- **Allegato 3**: incidenti significativi di base per i soggetti importanti.
- **Allegato 4**: incidenti significativi di base per i soggetti essenziali.

*__CSIRT Italia__ (*Computer Security Incident Response Team Italia*) è il team nazionale italiano per la risposta agli incidenti informatici. È stato istituito presso l'Agenzia per la Cybersicurezza Nazionale (ACN) ed è un organismo centrale nella strategia di difesa cibernetica del Paese.

Direttiva NIS 2 e Decreto NIS: aspetti principali

Determinazione dell'Agenzia per la Cybersicurezza Nazionale n. 164179 del 14 aprile 2025

Gli allegati tecnici costituiscono le cosiddette specifiche di base, ossia le **misure di sicurezza di base*** (indicate anche per brevità come misure di sicurezza) che i soggetti NIS, sia essenziali che importanti, sono tenuti ad adottare per l'assolvimento degli obblighi di cui agli articoli 23 e 24 del decreto e le tipologie di incidenti significativi di base (indicati anche per brevità come incidenti significativi) che i medesimi soggetti sono tenuti a notificare al **CSRIT Italia** per l'assolvimento degli obblighi di cui all'articolo 25 del decreto.

*Il termine per l'adozione delle misure di sicurezza di base è fissato in **diciotto mesi dalla ricezione, da parte del soggetto NIS della comunicazione di inserimento nell'elenco dei soggetti NIS**. Il termine per l'adempimento dell'obbligo di notifica degli incidenti significativi di base è fissato in **nove mesi** dalla ricezione, da parte del soggetto NIS, della medesima comunicazione.

Direttiva NIS 2 e Decreto NIS: aspetti principali

Determinazione dell'Agenzia per la Cybersicurezza Nazionale n. 164179 del 14 aprile 2025

Le misure sono state sviluppate in accordo al **Framework nazionale*** e sono organizzate in funzioni, categorie, sottocategorie e requisiti.

Nel complesso sono state definite **37 misure di sicurezza con 87 requisiti per i soggetti importanti e 43 misure di sicurezza con 116 requisiti per i soggetti essenziali**. Sono stati definiti requisiti e misure di sicurezza aggiuntivi per i soggetti essenziali rispetto ai soggetti importanti, in considerazione di quanto indicato dall'articolo 31 del decreto NIS che prevede – nello stabilire gli obblighi – di tener 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.

Framework Nazionale per la Cybersecurity e la Data Protection (FNCS) è uno strumento di supporto alle organizzazioni che necessitano di strategie e processi volti alla protezione dei dati personali e alla sicurezza cyber. L'elemento principale è il cosiddetto Framework Core strutturato in funzioni, categorie e sottocategorie. Le misure di sicurezza di base fanno uso della versione 2025 del framework.

NIS 2 e impresa gestione rifiuti

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

NIS 2 e impresa di gestione rifiuti

ALLEGATO II Decreto NIS – ALTRI SETTORI CRITICI

SETTORE	TIPO DI SOGGETTO
2. Gestione dei rifiuti	Imprese che si occupano della gestione dei rifiuti quali definite **all'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio***, escluse quelle per cui la gestione dei rifiuti non è la principale attività economica.

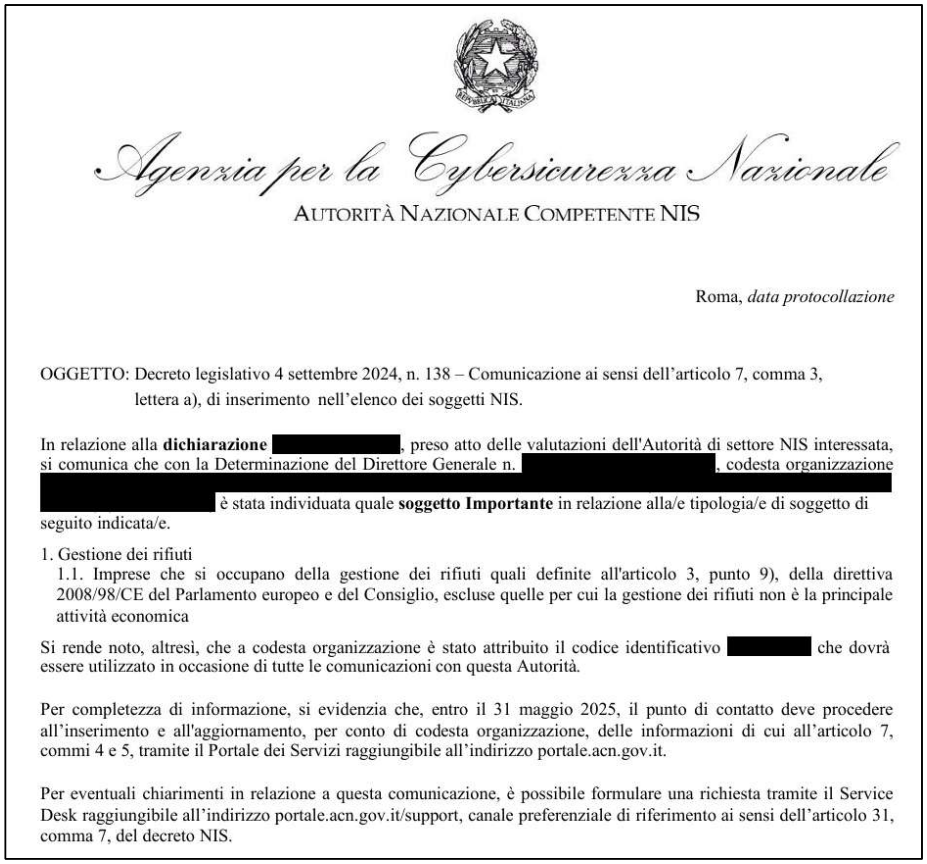
***«*gestione dei rifiuti*», la raccolta, il trasporto, il recupero (compresa la cernita), e lo smaltimento dei rifiuti, compresi la supervisione di tali operazioni e gli interventi successivi alla chiusura dei siti di smaltimento nonché le operazioni effettuate in qualità di commercianti o intermediari.

(Direttiva 2008/98/CE del Parlamento europeo e del Consiglio, del 19 novembre 2008, relativa ai rifiuti e che abroga alcune direttive (GU L 312 del 22.11.2008, pag. 3).

NIS 2 e impresa gestione rifiuti

Registrazione sulla piattaforma digitale dell'Agenzia per la Cybersicurezza Nazionale (ACN) **entro il 28 febbraio 2025**.

Riscontro da parte di ACN alla società:
SOGGETTO IMPORTANTE



Agenzia per la Cybersicurezza Nazionale

AUTORITÀ NAZIONALE COMPETENTE NIS

Roma, *data protocollazione*

OGGETTO: Decreto legislativo 4 settembre 2024, n. 138 – Comunicazione ai sensi dell'articolo 7, comma 3, lettera a), di inserimento nell'elenco dei soggetti NIS.

In relazione alla **dichiarazione** [redacted], preso atto delle valutazioni dell'Autorità di settore NIS interessata, si comunica che con la Determinazione del Direttore Generale n. [redacted], codesta organizzazione [redacted] è stata individuata quale **soggetto Importante** in relazione alla/e tipologia/e di soggetto di seguito indicata/e.

1. Gestione dei rifiuti
   1.1. Imprese che si occupano della gestione dei rifiuti quali definite all'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio, escluse quelle per cui la gestione dei rifiuti non è la principale attività economica

Si rende noto, altresì, che a codesta organizzazione è stato attribuito il codice identificativo [redacted] che dovrà essere utilizzato in occasione di tutte le comunicazioni con questa Autorità.

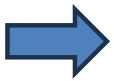
Per completezza di informazione, si evidenzia che, entro il 31 maggio 2025, il punto di contatto deve procedere all'inserimento e all'aggiornamento, per conto di codesta organizzazione, delle informazioni di cui all'articolo 7, commi 4 e 5, tramite il Portale dei Servizi raggiungibile all'indirizzo portale.acn.gov.it.

Per eventuali chiarimenti in relazione a questa comunicazione, è possibile formulare una richiesta tramite il Service Desk raggiungibile all'indirizzo portale.acn.gov.it/support, canale preferenziale di riferimento ai sensi dell'articolo 31, comma 7, del decreto NIS.

NIS 2 e impresa di gestione rifiuti

MISURE MINIME DI SICUREZZA O OBBLIGHI DI BASE – PER I SOGGETTI **IMPORTANTI**

Nello specifico, **ogni misura è costituita da un codice identificativo**, una descrizione e uno o più requisiti: **il codice identificativo e la descrizione fanno riferimento alle sottocategorie del Framework nazionale**, i requisiti indicano ciò che è richiesto ai fini dell'implementazione della misura.



ALLEGATO 1

Misure di sicurezza di base per i soggetti importanti

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 compreso[1].

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.

1.3. **Ruoli, responsabilità e correlati poteri (GV.RR)**: I ruoli, le responsabilità e i correlati poteri in materia di cybersecurity per promuovere l'accountability, la valutazione delle prestazioni e il miglioramento continuo sono stabiliti e comunicati.

NIS 2 e impresa di gestione rifiuti

ESEMPIO CHECK-LIST GAP NIS 2 PER UN SOGGETTO IMPORTANTE
1. Comprensione dei requisiti NIS2 • Studiare i requisiti normativi specifici per il tuo settore (ad esempio settore rifiuti). • Identificare le misure tecniche e organizzative richieste (es. gestione dei rischi, risposta agli incidenti, business continuity, ecc.).
2. Definizione degli obiettivi dell'analisi • Chiarire cosa ottenere: conformità completa, identificazione delle priorità, preparazione a un audit, ecc.
3. Costituzione del team di lavoro • Coinvolgere figure chiave: CISO, IT manager, responsabili legali e della compliance, DPO-RPD.
4. Raccolta e analisi della documentazione • Politiche di sicurezza, procedure operative, registri degli incidenti, piani di continuità operativa, ecc.
5. Valutazione dello stato attuale • Confrontare le pratiche esistenti con i requisiti NIS2. • Usare checklist o framework di riferimento (es. ISO/IEC 27001, CIS Controls).
6. Identificazione dei gap • Evidenziare le aree non conformi o parzialmente conformi. • Classificare i gap per criticità e impatto.
7. Sviluppo del piano d'azione • Definire le misure correttive, le risorse necessarie e le tempistiche. • Assegnare responsabilità e priorità.
8. Monitoraggio e aggiornamento • Prevedere revisioni periodiche • Documentare i progressi e aggiornare il piano in base a nuove minacce o modifiche normative.

NIS 2 e impresa di gestione rifiuti

PROSSIME SCADENZE E ADEMPIMENTI PER UN SOGGETTO IMPORTANTE:

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.

NOTIFICHE DI INCIDENTE

Entro 9 mesi (gennaio 2026) dalla ricezione della comunicazione di inserimento nell'elenco nazionale NIS, i **soggetti importanti** sono tenuti a notificare al CSRIT Italia gli incidenti significativi riportati **nell'allegato 3** della determinazione ACN 164179 del 14 aprile 2025.

NIS 2 e GDPR considerazioni finali

NIS 2 e GDPR

OBBIETTIVI

Rafforzare la **sicurezza delle reti e dei sistemi informativi**, migliorando la resilienza delle infrastrutture critiche e la capacità di risposta a incidenti informatici.

Proteggere i diritti e le libertà fondamentali delle **persone fisiche**, in particolare il diritto alla **protezione dei dati personali**.

NIS 2 e GDPR

SOGGETTI E ASPETTI CHIAVE

- Responsabile IT
- Obblighi di notifica (**ART. 25: entro 24 ORE**)
- Analisi del rischio e responsabilizzazione
- Misure tecniche, operative e organizzative (**ART. 24**)
- Sanzioni

- DPO-RPD
- Obblighi di notifica (**ART. 33: entro 72 ORE**)
- Analisi del rischio e responsabilizzazione (*Accountability*)
- Misure di sicurezza (**ART. 32**)
- Sanzioni

NIS 2 e GDPR

GDPR e **NIS 2** rappresentano due facce della stessa medaglia: la prima riguarda la tutela della riservatezza dei dati personali, la seconda è relativa alla sicurezza dell'intera infrastruttura informatica.

Di conseguenza la sicurezza prevista dalla NIS 2 e DECRETO NIS è il presupposto necessario per rispettare il GDPR: **senza sistemi sicuri, la protezione dei dati personali non è un obbiettivo realizzabile**.

Grazie per l’attenzione