UNIVERSITÀ POLITECNICA DELLE MARCHE

DII
Dipartimento di Ingegneria dell'Informazione

unimc

NIS2: Obblighi e opportunità per le aziende. Caso pratico di adeguamento

Ing. Roberta Moruzzi
r.moruzzi@acquambientemarche.it

Giovedì 2 ottobre 2025

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

- La **DIRETTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 14 dicembre 2022** costituisce l'aggiornamento della precedente Direttiva NIS del 2016 ed ha come obiettivo principale quello di aumentare il livello generale di cybersicurezza degli stati membri dell'UE.
- In Italia la direttiva è stata recepita con il **DECRETO LEGISLATIVO 4 settembre 2024, n. 138.**
- **Determinazioni ACN**
  - Determinazione ACN 38565/2024
  - Determinazione ACN 283727/2025
  - Determinazione ACN 164179/2025

ampliamento del campo di applicazione a 18 settori di cui 11 altamente critici e 7 critici (Allegati I,II,III e IV)

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		

- Azienda del SII:
  - Acque potabili
  - Acque reflue
  - Società in house

Rientra nell'ambito NIS2

Non certificata ISO 27001

IDENTIFICAZIONE DELL' AUTORITA' COMPETENTE NIS nell'ACN (Agenzia per la cybersicurezza nazionale)

Art. 1

a) sovrintende all'implementazione e all'attuazione del presente decreto;

b) predispone i provvedimenti necessari a dare attuazione al presente decreto;

c) svolge le funzioni e le attività di regolamentazione di cui al presente decreto, anche adottando linee guida, raccomandazioni e orientamenti non vincolanti;

d) individua i soggetti essenziali e i soggetti importanti ai sensi degli articoli 3 e 6, nonché redige l'elenco di cui all'articolo 7, comma 2;

e) partecipa al Gruppo di cooperazione NIS, nonché ai consessi e alle iniziative promosse a livello di Unione europea relativi all'attuazione della direttiva (UE) 2022/2555;

f) definisce gli obblighi di cui all'articolo 7, comma 6, e al capo IV;

g) svolge le attività ed esercita i poteri di cui al capo V.

REGISTRAZIONE entro il 28 febbraio 2025

Art.7

1. **censimento del PUNTO DI CONTATTO** corrispondente ad un dipendente delegato dal rappresentante legale. (In particolare dalla **Determinazione ACN 38565/2024 art.4**):

a) ha compito di **curare l'attuazione delle disposizioni del decreto NIS** per conto del soggetto stesso.

b) accede al Portale ACN e ai Servizi NIS, effettua, per conto del soggetto la registrazione e interloquisce con ACN

c) riferisce direttamente al vertice gerarchico in quanto "**Resta ferma**, in ogni caso, **la responsabilità degli organi di amministrazione e direttivi del soggetto NIS**."

d) Può "**soddisfare l'obbligo di nomina e comunicazione del referente per la cybersicurezza**"

1. Identificazione del Punto di Contatto e sua registrazione nella piattaforma ACN
2. Associazione del punto di contatto all'azienda
3. Compilazione del modulo on line per la registrazione dell'azienda
   - elenco codici ATECO
   - nr. Dipendenti
   - fatturato

Tipo di soggetto	Differenze
SOGGETTO ESSENZIALE	• Obblighi più stringenti • vigilanza preventiva (audit, ispezioni, richieste di evidenze) • Sanzioni più severe
IMPORTANTE	• Obblighi meno stringenti • vigilanza ex post attivata in presenza di indizi o violazioni. • Sanzioni meno severe
FUORI AMBITO	non rientrante negli obblighi NIS2 eventuale notifica degli incidenti su base volontaria

Aggiornamento annuale delle informazioni

Art. 7, commi 3 e 4, del decreto NIS

La **cadenza è annuale**, con un termine fisso previsto ogni anno tra il 15 aprile e il 31 maggio

MA

è obbligatorio e fondamentale aggiornare tempestivamente le informazioni sul portale ACN ogni volta che si verificano dei cambiamenti

Punto di contatto attraverso accesso alla piattaforma:

- verifica la correttezza dei dati anagrafici e di contatto, nonché della delega, del punto di contatto
- designazione del sostituto punto di contatto
- indicazione degli indirizzi IP pubblici e statici che il soggetto NIS utilizza
- Indicazione dei nomi di dominio che il soggetto NIS utilizza
- Indicazione degli eventuali servizi offerti e le sedi nell'UE
- Indicazione degli "organi di amministrazione" e "organi direttivi". Ciascun componente invitato dal punto di contatto deve accettare e completare l'iscrizione nel portale fornendo i propri dati personali

RESPONSABILITA' DEI VERTICI – ORGANI DI AMMINISTRAZIONE E DIRETTIVI

Art.23

- **Approvano** le modalità di implementazione delle misure di sicurezza
- **Sovrintendono** all'implementazione degli obblighi
- Sono **responsabili** delle eventuali violazioni
- **Sono tenuti a seguire una formazione** in materia di cybersicurezza
- **Promuovono la formazione** dei propri dipendenti

PUNTO DI CONTATTO:

- Informa gli organi di amministrazione (CDA) in merito alla valutazione ricevuta da ACN e della necessità di adeguarsi a quanto richiesto dal decreto NIS2
- Relaziona al CDA:
  - PERIODICAMENTE sullo stato di avanzamento delle procedure
  - TEMPESTIVAMENTE in caso di incidente

OBBLIGHI IN MATERIA DI NOTIFICA DEGLI INCIDENTI entro il primo gennaio 2026

PREPARAZIONE ALLA NOTIFICA

- individuare il **numero di utenti** impattati dall'incidente;
- definire la **durata dell'incidente**, delimitato dal periodo tra il momento in cui si è verificata la prima interruzione completa o parziale del servizio e il momento del ripristino;

NOTIFICA AL CSIRT ITALIA

- numero di utenti impattati;
- durata dell'incidente;
- diffusione geografica;
- date e ora di rilevamento dell'incidente;
- asset impattati;
- ulteriori dettagli dell'incidente (es. IOC);
- evidenze rilevate (es. sample di malware, ransom note;

GESTIONE DELLA NOTIFICA

CSIRT Italia offre:

- **supporto diretto** nelle operazioni di incident handling;
- se necessario, **assistenza operativa e fornitura di informazioni utili**.

Una volta definite ed avviate le attività di ripristino, viene effettuata la **CHIUSURA DELL'INCIDENTE**

FORMAZIONE IN MATERIA DI CYBERSICUREZZA DEI DIPENDENTI E DEGLI AMMINISTRATORI

Art.23 comma 2

FORMAZIONE ORGANI AMMINISTRATIVI → Focus su:

- decreto NIS2

FORMAZIONE DEI DIPENDENTI → Focus su:

- Creare, gestire e organizzare le password
- Riconoscere i tentativi di cyber frode
- Difendersi dagli attacchi di phishing
- Verificare autenticità e affidabilità dei siti web
- Utilizzo di usb
- Doppia autenticazione

PUNTO DI CONTATTO in accordo con i responsabili di settore propone un **calendario di formazione dei dipendenti** al CDA che procede con l'approvazione.

I dipendenti vengono informati dell'obbligo di partecipazione attraverso un ordine di servizio e ricevono attestazione alla presenza.

Sono programmati corsi di aggiornamento adattabili ai cambiamenti nel panorama delle minacce informatiche con cadenza annuale con attestazione di avvenuta partecipazione.

IMPLEMENTAZIONE DELLE MISURE DI SICUREZZA DI BASE PREVISTE DALLA NORMATIVA
SCADENZA OTTOBRE 2026 - Art. 23, 24, e 25 del decreto NIS

ACN:

1. **Allegati tecnici determinazione ACN 164179 del 14 aprile 2025:**
   - Allegato 1 misure di sicurezza di base soggetti importanti.
   - Allegato 2 misure di sicurezza di base soggetti essenziali.
   - Allegato 3 incidenti significativi per i soggetti importanti.
   - Allegato 4 incidenti significativi per i soggetti essenziali.
2. **Linee Guida NIS Specifiche di base Guida alla lettura** (pubblicate a settembre 2025) a supporto delle organizzazioni comprende delle Appendici con:
   - Appendice A mappatura tra elementi decreto NIS e misure di sicurezza di base della determinazione ACN
   - Appendice B **requisiti con clausole basate sul rischio**
   - Appendice C documenti approvati dal CDA

Azienda:

1. **Gap Analysis** Identificare le aree non conformi rispetto ai requisiti della NIS 2, sia per quanto riguarda le procedure che i sistemi.
2. Attenta **ANALISI DEI RISCHI** approfondita del rischio cyber per identificare vulnerabilità e potenziali impatti sulle operazioni aziendali, censendo tutti gli asset digitali (dispositivi, server, ecc.) e attribuire un punteggio di rischio.
   VULNERABILITY TEST
   PENETRATION TEST
3. Gestione della **SUPPLY CHAIN**
4. Stesura della **DOCUMENTAZIONE RICHIESTA** con attenzione a quelli che richiedono approvazione dagli organi amministrativi

FOCUS SU DOCUMENTAZIONE

Documento
Organizzazione per la sicurezza informatica.
Politiche di sicurezza informatica.
Valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete.
Piano di trattamento del rischio.
Piano di gestione delle vulnerabilità.
Piano di adeguamento.
Piano di continuità operativa.
Piano di ripristino in caso di disastro.
Piano di gestione delle crisi.
Piano di formazione.
Piano per la gestione degli incidenti di sicurezza informatica.

Sono adottate e documentate politiche di sicurezza informatica per almeno i seguenti ambiti:

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.

eseguita e documentata la valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete, anche con riferimento alle eventuali dipendenze da fornitori e partner terzi, che comprende almeno:

a) l'identificazione del rischio;
b) l'analisi del rischio;
c) la ponderazione del rischio.

È definito, attuato, aggiornato e documentato un piano per la gestione degli incidenti di sicurezza informatica e la notifica al CSIRT Italia, in accordo a quanto previsto dall'articolo 25 del decreto NIS, che comprende almeno:

a) le fasi e le procedure di gestione e notifica degli incidenti con l'indicazione dei relativi ruoli e delle responsabilità;
b) le procedure per la predisposizione e la trasmissione delle relazioni di cui all'articolo 25, comma 5, lettere c), d) ed e) del decreto NIS;
c) le informazioni di contatto per la segnalazione degli incidenti;
d) le modalità di comunicazione interna, anche con riguardo al coinvolgimento degli organi di amministrazione e direttivi, ed esterna;
e) la reportistica da utilizzare per la documentazione dell'incidente.

SICUREZZA DELLA CATENA DI APPROVVIGIONAMENTO

Art.24 comma 2

"*d) 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;*"

Codici di misura di sicurezza allegato determinazione ACN

GV.SC-01, GV.SC-02
GV.SC-05, GV.SC-07.

i requisiti di sicurezza sono inseriti nelle richieste di offerta, bandi di gara, contratti, accordi e convenzioni relativi alle forniture con potenziale impatto sulla sicurezza dei sistemi informativi e di rete.

1. Estrapolazione elenco fornitori dalla piattaforma tuttogare (**inventario**)
2. Classificazione dei fornitori in base **all'oggetto della fornitura**, della **capacità di garantire l'approvvigionamento**, **l'assistenza e la manutenzione nel tempo**
3. **Analisi del rischio** in base a:
   - il livello di accesso del fornitore ai sistemi informativi e di rete del soggetto NIS;
   - l'accesso del fornitore alla proprietà intellettuale e ai dati anche sulla base della loro criticità;
   - l'impatto di una grave interruzione della fornitura;
   - i tempi e i costi di ripristino in caso di indisponibilità dei servizi;
   - i ruoli e le responsabilità del fornitore nel governo dei sistemi informativi e di rete.

ATTIVITA' DI VIGILANZA
Art.34

ACN svolge attività di vigilanza attraverso:

- *il monitoraggio, l'analisi e il supporto ai soggetti essenziali e ai soggetti importanti;*
- *la verifica e le ispezioni;*
- *l'adozione di misure di esecuzione;*
- *l'irrogazione di sanzioni amministrative pecuniarie e accessorie*"

VERIFICHE E ISPEZIONI
Art. 36

ACN può sottoporre i soggetti che rientrano nell'ambito di applicazione del decreto NIS2 a :

- *verifiche della documentazione e delle informazioni trasmesse all'Autorità nazionale competente NIS ai sensi del presente decreto;*
- *ispezioni in loco e a distanza, compresi controlli casuali;*
- *richieste di accesso a dati, documenti e altre informazioni necessari allo svolgimento dei poteri di cui al presente articolo, dichiarando la finalità della richiesta e specificando le informazioni richieste ai soggetti*

SANZIONI Art.34

I soggetti essenziali non conformi, rischiano sanzioni pari a un massimo di almeno 10 milioni di EUR o pari al **2% del totale del fatturato mondiale annuo dell'impresa di appartenenza**, se tale importo è superiore

Se azienda è certificata ISO 27001

30 aprile 2025 è stata pubblicata la **Prassi di Riferimento UNI/PdR 174:2025** che costituisce un ponte metodologico che consente ai soggetti già certificati ISO/IEC 27001 di estendere il proprio sistema di gestione ai controlli e alle «misure di sicurezza di base», ossia le specifiche di base per gli obblighi di cui agli articoli 23 e 24 del decreto NIS, contenuti nella Determinazione ACN n. 164179 del 14 aprile 2025.

Opportunità

- Rafforzamento della **resilienza cibernetica**, garantendo la **continuità operativa** in caso di attacchi.
- Accrescimento dell'**affidabilità** e della **fiducia di clienti e partner**,
- Miglioramento della **reputazione** aziendale
- Semplificazione della **gestione della compliance** con altri regolamenti europei come il GDPR.
- Lo CSIRT offre un supporto strategico:
  - Protezione strategica per il rafforzamento della resilienza
  - Supporto qualificato
  - Anticipo della minaccia verso terzi
- Priorità della formazione in materia di cybersicurezza

GRAZIE PER L'ATTENZIONE