NOTIZIARIO

Sicur Book®

N°	Mese	Anno
SPECIALE CYBER SECURITY NIS2	FEBBRAIO	2025

NIS - Network Information Security

Dal 16 ottobre 2024 è in vigore la nuova normativa Network and Information Security (direttiva NIS) di derivazione europea. SCADE IL 28.02.205

Il recepimento della direttiva con il decreto legislativo del 4 settembre 2024, n. 138 (decreto NIS: apre un link esterno), mira a garantire l'aumento del livello di sicurezza informatica del tessuto produttivo e delle Pubbliche Amministrazioni del Paese, in armonia con gli altri Stati membri dell'Unione Europea.

L'Agenzia per la cybersicurezza nazionale è l'Autorità competente NIS.

Dal 1° dicembre 2024 al 28 febbraio 2025, le medie e grandi imprese, in alcuni casi anche le piccole e microimprese, e le Pubbliche amministrazioni a cui si applica la nuova normativa devono registrarsi sul portale servizi ACN.

In seguito, si avvierà, ad aprile 2025, un percorso condiviso di rafforzamento della sicurezza informatica.

1. **Chi è Soggetto agli Obblighi della NIS 2?**

ATTENZIONE: sul sito è presente il seguente pulsante:

Consulta il dettaglio degli ambiti di applicazione.

Sul sito: https://www.acn.gov.it/portale/nis/ambito

Agenzia per la cybersicurezza nazionale

COME INDIVIDUARE SE SI APPARTIENE AD UNA GRANDE – MEDIA O PICCOLA IMPRESA

Sul sito dell'agenzia al punto: domande frequenti il sito riporta la seguente risposta:

Per la definizione di media impresa occorre far riferimento ai requisiti dimensionali indicati nell'articolo 2, paragrafo 1, dell'allegato alla raccomandazione 2003/361/CE: apre un link esterno nonché, in modo più specifico, alla Guida dell'utente alla definizione di PMI: apre un link esterno (pubblicata dalla Commissione europea nel 2020).

Confrontando i propri dati con le soglie stabilite dalla citata disciplina, un'impresa può determinare se è una microimpresa, una piccola o una media impresa.

⚠ ***Le microimprese sono definite come imprese con meno di 10 occupati e che realizzano un fatturato annuo oppure un totale di bilancio annuo non superiore a 2 milioni di euro.***

⚠ ***Le piccole imprese sono definite come imprese con meno di 50 occupati e che realizzano un fatturato annuo oppure un totale di bilancio annuo non superiore a 10 milioni di euro.***

⚠ ***Le medie imprese sono definite come imprese con meno di 250 occupati e che realizzano un fatturato annuo non superiore a 50 milioni di euro oppure un totale di bilancio annuo non superiore a 43 milioni di euro.***

Si evidenzia che devono essere sempre presenti, sia il criterio del numero di effettivi, sia almeno uno dei due parametri contabili (fatturato o bilancio) tra loro alternativi, essendo sufficiente che almeno uno dei due rientri nei parametri dimensionali.

Se i valori dei parametri contabili sono superati entrambi, oppure se si supera anche solo il criterio del numero di effettivi, si ricade nella categoria di PMI superiore.
Per esempio:

- *un'organizzazione con meno di 50 occupati, un fatturato di almeno 2 milioni non superiore ai 10 milioni ma un bilancio superiore ai 43 milioni, cade nella categoria delle piccole imprese;*
- *un'organizzazione con meno di 10 occupati, un fatturato e un bilancio di almeno 10 milioni ma non superiore 43 milioni, cade nella categoria delle medie imprese;*
- *un'organizzazione con meno di 10 occupati, un fatturato superiore ai 50 milioni e un bilancio di almeno 10 milioni ma non superiore 43 milioni, cade nella categoria delle medie imprese;*
- *un'organizzazione con meno di 10 occupati, un fatturato di almeno 50 milioni e un bilancio di almeno 43 milioni, ricade nella categoria delle grandi imprese;*
- *un'organizzazione con almeno 50 e meno di 250 dipendenti, un fatturato e un bilancio non superiore ai 10 milioni, ricade nella categoria delle medie imprese;*
- *un'organizzazione con almeno 250 dipendenti, un fatturato e un bilancio non superiore ai 10 milioni, ricade nella categoria delle grandi imprese.*

La raccomandazione prevede che il calcolo del numero di effettivi, fatturato e bilancio, tenga conto delle imprese associate o collegate (articolo 6, paragrafo 2).

Qualora il soggetto ritenga che ciò non sia proporzionato - tenuto anche conto dell'indipendenza dello stesso dalle sue imprese associate o collegate in termini di servizi che fornisce e di sistemi informativi e di rete che utilizza nella fornitura di tali servizi - potrà richiedere una deroga ai sensi dell'articolo 3, comma 4, del decreto NIS, in presenza degli specifici criteri stabiliti dal DPCM sull'applicazione della clausola di salvaguardia, adottato ai sensi dell'articolo 40, comma 1, lettera a), del decreto NIS.

ESTRATTO: IN PARTICOLARE

Settore	Dettaglio	Grandi imprese	Medie imprese	Piccole e micro imprese
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 **

Schema degli ambiti di applicazione
* Possibile identificazione dell'Autorità come essenziali
** Possibile identificazione dell'Autorità come importanti o essenziali

Ambito di applicazione

La nuova normativa NIS amplia il campo di applicazione della normativa a 18 settori di cui 11 altamente critici (originariamente 8) e 7 critici (di nuova introduzione) per oltre 80 tipologie di soggetti, distinguendo i soggetti in essenziali e importanti.

Per ulteriori dettagli si fa riferimento agli allegati I, II, III e IV del Decreto legislativo 4 settembre 2024, n. 138.

Consulta il dettaglio degli ambiti di applicazione.

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		

Schema degli ambiti di applicazione
* Possibile identificazione dell'Autorità come essenziali
** Possibile identificazione dell'Autorità come importanti o essenziali

QUALI SONO LE SCADENZE?

- **SOGGETTI Registrazione sulla piattaforma** ACN (articolo 7, comma 1, articolo 42, comma 1, lettera a):
- entro il 17 gennaio 2025 per 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 decreto (v. FAQ 2.1);
- **entro il 28 febbraio 2025** per tutti gli altri soggetti che rientrano nell'ambito di applicazione del decreto (v. FAQ 2.1).
- **AUTORITÀ NAZIONALE COMPETENTE NIS Entro metà aprile 2025:**
- costituzione dell'elenco dei soggetti NIS e notifica agli stessi della loro inclusione (articolo 7, commi 2 e 3);
- adozione degli obblighi di base in materia di misure di sicurezza informatica e notifica di incidenti.
- **SOGGETTI Entro metà maggio 2025**, trasmissione e aggiornamento, tempestivo (comunque non oltre 14 giorni dalla modifica) delle informazioni dei soggetti NIS (articolo 7, commi 4, 5 e 7).

- **SOGGETTI Entro gennaio 2026** (entro 9 mesi dalla ricezione della notifica di inserimento nell'elenco dei soggetti NIS), adempimento agli obblighi di base in materia di notifica di incidente.
- **SOGGETTI Entro ottobre 2026** (entro 18 mesi dalla ricezione della notifica di inserimento nell'elenco dei soggetti NIS), adempimento agli obblighi di base in materia di sicurezza informatica.

Riassumendo:

La NIS 2 si applica a due categorie di soggetti:

Enti Essenziali (Essential Entities - EE)
- Settore energetico (elettricità, gas, petrolio, idrogeno).
- Trasporti (ferrovie, aerei, marittimi, stradali).
- Sanità (ospedali, fornitori di servizi sanitari digitali).
- Servizi digitali (cloud, data center, DNS).
- Acqua potabile e reflui.
- Infrastrutture finanziarie (banche, borse, istituzioni di pagamento).
- Pubblica Amministrazione.

Enti Importanti (Important Entities - IE)
- Settore alimentare e della distribuzione.
- Servizi postali e corrieri.
- Produttori di dispositivi elettronici e ICT.
- Fornitori di servizi digitali, software e gestione dati.
- Imprese manifatturiere critiche.

⚠ **Criterio di Applicazione:** Aziende con almeno 50 dipendenti e un fatturato superiore a 10 milioni di euro.

---

2. Adempimenti Previsti dalla NIS 2

A. Obblighi di Gestione del Rischio e Misure Tecnico-Organizzative

Tutti i soggetti coinvolti devono adottare misure per ridurre i rischi informatici. Tra le misure richieste:

- Gestione degli incidenti informatici (piani di risposta e recovery).
- Sicurezza della supply chain (fornitori e partner devono rispettare gli standard di sicurezza).
- Protezione degli accessi e dell'identità digitale (autenticazione multifattoriale, zero-trust security).
- Aggiornamento software e patching regolare per eliminare vulnerabilità.
- Backup sicuri e test di ripristino dei dati.
  Criptografia e protezione delle informazioni sensibili.
- Resilienza operativa in caso di cyber attacchi.

B. Obblighi di Notifica degli Incidenti di Sicurezza

⚠ Le aziende devono segnalare gli incidenti informatici gravi alle autorità nazionali competenti.

👉Tempistiche di segnalazione:
- ❗1Entro 24 ore: prima segnalazione con valutazione iniziale.
- ❗2Entro 72 ore: aggiornamento dettagliato sull'incidente.
- ❗3Entro 1 mese: relazione finale con analisi dell'incidente e misure correttive adottate.

C. Valutazione del Rischio e Audit Periodici
- ❗Autovalutazione della sicurezza informatica almeno una volta all'anno.
- ❗Audit interni ed esterni obbligatori per verificare il rispetto della NIS 2.
- ❗Verifica della conformità della supply chain con test e certificazioni.

D. Formazione e Sensibilizzazione sulla Cybersecurity
- ❗Obbligo di formazione periodica per dipendenti e dirigenti.
- ❗Simulazioni di attacchi informatici per testare la preparazione del personale.
- ❗Piani di awareness sulla sicurezza informatica per tutti i livelli aziendali.

---

3. Sanzioni per il Mancato Adeguamento alla NIS 2
Le aziende che non rispettano gli obblighi della NIS 2 possono subire multe elevate:
- ⚠Enti Essenziali (EE): fino a 10 milioni di euro o il 2% del fatturato globale.
- ⚠Enti Importanti (IE): fino a 7 milioni di euro o l'1,4% del fatturato globale.
- ⚠Possibilità di sospensione delle attività aziendali in caso di gravi violazioni.

---

4. Adempimenti Specifici per le Imprese
👉Passaggi chiave per adeguarsi alla NIS 2:
- ❗Mappare i sistemi IT e i dati critici per identificare vulnerabilità.
- ❗Implementare un piano di gestione della sicurezza informatica.
- ❗Nomina di un Responsabile della Sicurezza Informatica (CISO).
- ❗Stipulare una Cyber Insurance per proteggersi da danni economici.
- ❗Effettuare penetration test e vulnerability assessment periodici.

---

5. Autorità di Controllo in Italia
Il recepimento della NIS 2 in Italia sarà supervisionato da:
- Agenzia per la Cybersicurezza Nazionale (ACN).
- Ministero dell'Interno e Ministero della Difesa per infrastrutture critiche.
- Garante per la Protezione dei Dati Personali, in caso di violazioni di dati sensibili.

Conclusione: La NIS 2 impone misure di sicurezza informatica più stringenti, specialmente per le aziende che operano in settori critici. L'adeguamento è obbligatorio e richiede investimenti in cybersecurity, formazione e monitoraggio continuo.

Importante: nel dubbio si consiglia di andare a vedere il sito e iscriversi entro il 28.02.2028 sempre dal sito sotto riportato, e chiedere consiglio anche al Vostro Informatico:

Agenzia per la cybersicurezza nazionale

☞ **Informativa Protezione dati personali**

Spett.le Cliente, riceve la presente newsletter, sotto forma di notiziario SICURBOOK®, quale informativa specifica in materia di sicurezza sul lavoro e protezione dati personali, in quanto cliente che ha usufruito e/o usufruisce dei nostri servizi in materia di sicurezza sul lavoro e/o protezione dati personali; se non desidera più ricevere il presente notiziario, potrà disdirlo in qualunque momento, inviando una comunicazione via email come quella indicata a fondo pagina.

Se desidera ricevere informazioni in merito sui servizi da noi erogati, o in merito a quanto indicato nel presente notiziario dai propri collaboratori, Le chiediamo cortesemente di compilare il format sotto riportato e inviarlo a info@sicurezzascs.it:

Tipo Richiesta	Informazioni relative a:

Persona che richiede informazioni:

Nome	
Cognome	
Ruolo	
Telefono	
Indirizzo	
Cap	
Città	
Provincia	

Questo documento è inviato esclusivamente per il destinatario. Tutte le informazioni ivi contenute, compresi eventuali allegati, sono soggette a riservatezza a termini del vigente GDPR 679/2016 in materia di protezione dei dati personali e quindi ne è proibita l'utilizzazione. Se avete ricevuto per errore questa newsletter, Vi preghiamo cortesemente di contattare immediatamente il mittente e cancellare la e-mail dandocene immediata comunicazione, utilizzando il fac simile sotto riportato.
Informativa privacy art. 13 Regolamento UE n. 2016/679: Titolare del trattamento dei dati è SCS SICUREZZA SRLUNIPERSONALE con sede Via Sestri, 3/3 – 16154 Genova.
Sito internet www. scssicurezza.it tel 010.37762.92 - Contitolare Trattamento Roberto Ferro - Contitolare Trattamento CSA Centro Sicurezza Applicata di Alessandro Ferro & C. sas
Per cancellarti dal ricevere le newsletter di SICURBOOK invia Email a info@sicurezzascs.it unito ad un documento di riconoscimento della persona autorizzata (vedi anche sito Garante della privacy)

Garanzia di riservatezza e tutela della privacy **GDPR 679/2016**

Per cancellare o modificare gli argomenti di tuo interesse delle newsletter di SICURBOOK NEWS invia la presente:

☞ **Richiesta Cancellazione invio via email del SICURBOOK a: info@sicurezzascs.it**

(art. 21, paragrafo 2 del Regolamento (UE) 2016/679)

Il Sottoscritto: _____in qualità di _____
dell'azienda_____
con sede:_____email_____

richiede la cancellazione dell'invio di newsletter quale il notiziario SICURBOOK con effetto immediato
data___/____/_____ firma avente diritto richiesta

_____

[1]Allegare copia di un documento di riconoscimento

☞ Per informazioni:

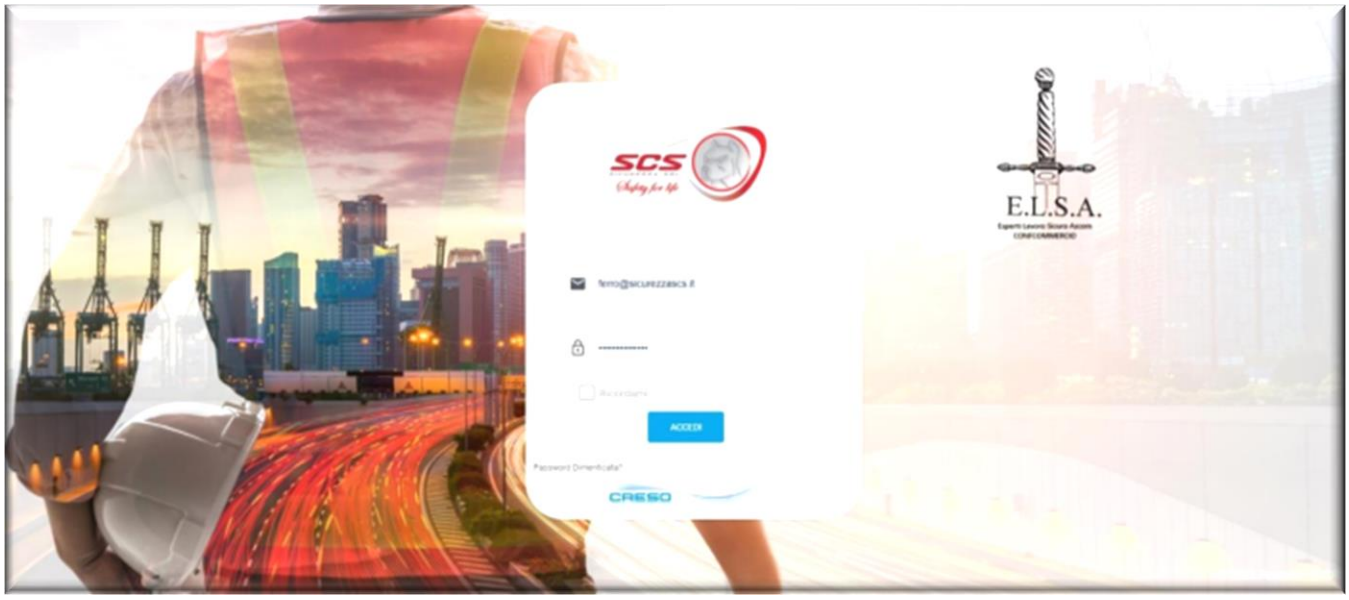
SCS SICUREZZA srl Unipersonale	Via Sestri 3/3 Genova tel.010.377.62.92 p.i. 01574270995	info@sicurezzascs.it web:www.scssicurezza.it
C.T.P. Roberto Ferro **Sicurezza sul lavoro** **DPO - GDPR 679/2016**	Tel:348.31.27.720	ferro@sicurezzascs.it info@sicurezzascs.it

In collaborazione con:

Avv. **Tommaso Ferro** Consulenza legale e formazione	Tel:347.14.20.113	avvtommasoferro@gmail.com

In collaborazione con:

CSA CENTRO SICUREZZA APPLICATA	Via delle Primule 101 16148 Genova Tel. 010.0899266/345	ufficio@csasicurezza.it csa.privacy@sicurezzascs.it
Alessandro Ferro	Tel:010.0899266/345	ufficio@csasicurezza.it
Dott.ssa Irene Carella	Tel:010.0899266/345	ufficio@csasicurezza.it
Dott. Nicolò Ferro	Tel:010.0899266/345	ufficio@csasicurezza.it



Sicur Book®

Sistema di gestione sicurezza e online