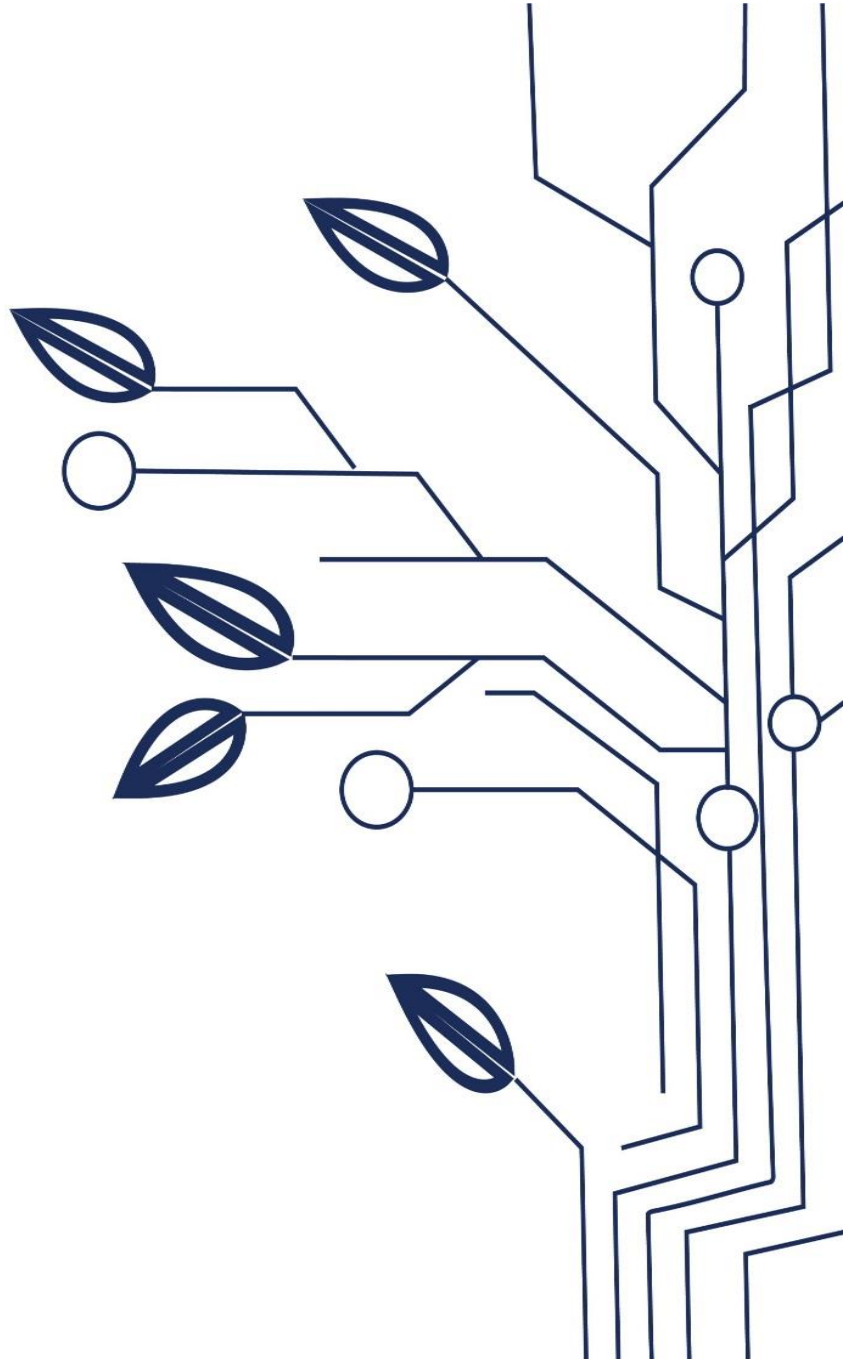
COLIN
CONSULENTE LEGALE INFORMATICO

NIS2: come prepararsi ai prossimi adempimenti

COMPLIANCE NIS2: CHE COSA DEVE ESSERE DOCUMENTABILE

Avv. Alessandro Ceccehetti
Socio e Manager Colin & Partners



Chi siamo

Colin & Partners S.r.l. è titolare del network **www.consulentelegaleinformatico.it**, fondato nel 2002 dall'Avv. Valentina Frediani.

La Società svolge attività di consulenza aziendale altamente qualificata nell'ambito della **compliance al diritto delle nuove tecnologie**, dove il punto di forza riconosciuto è il connubio delle conoscenze legali con quelle informatiche.

Il supporto è di tipo strategico e trasversale sulle aree aziendali, con la capacità di inserirsi negli equilibri di realtà articolate, garantendo un supporto al management aziendale funzionale ad un vantaggio competitivo aziendale, favorendo ed ottimizzando le esigenze di business in modo pragmatico e con tempistiche legate alle strategie del Committente.

Le Nostre Sedi: *Montecatini Terme, Milano, Bologna*

Per consultare la brochure, **clicca qui**.

L’art. 24 del Decreto NIS2 introduce una nuova ACCOUNTABILTY sulla cybersecurity

Per gestire i rischi di **sicurezza dei sistemi informatici e di rete** che utilizzano nella loro attività **o** nella fornitura di servizi

Tenuto conto dei rischi **esistenti**

Introduzione di misure **tecniche + operative + organizzative**

ADEGUATE E PROPORZIONATE(in base al grado di esposizione del soggetto, delle dimensioni, della probabilità degli incidenti, della gravità, e del loro impatto sociale ed economico)

Per **prevenire** o **ridurre al minimo** l’impatto degli **incidenti** per i destinatari dei loro servizi.

Gli organi amministrativi e direttivi: il ruolo rispetto alla compliance

COLIN
CONSULENTE LEGALE INFORMATICO

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

Approvano le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica adottate da tali soggetti ai sensi dell'articolo 24

Sovrintendono all'implementazione degli obblighi sanciti dalla normativa

Sono **responsabili delle violazioni** di cui al presente decreto

Sono **tenuti a seguire una formazione** in materia di sicurezza informatica

Promuovono l'offerta periodica di una formazione 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.

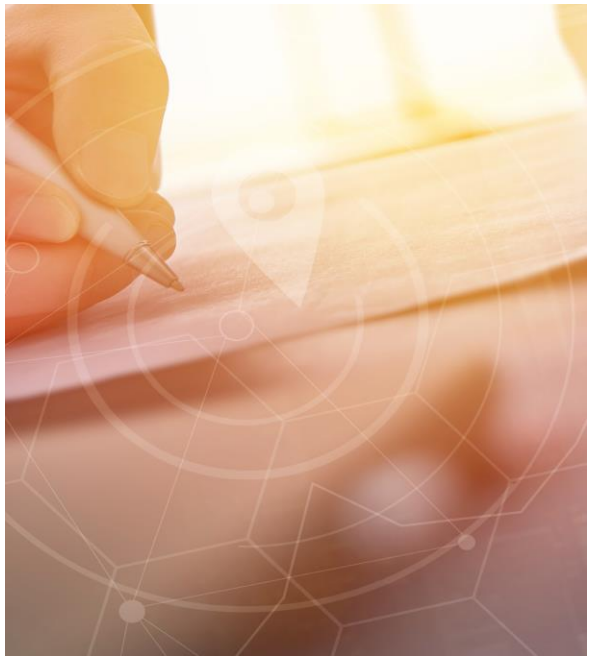
Sono **informati su base periodica o, se opportuno, tempestivamente, degli incidenti e delle notifiche**

Gli organi amministrativi e direttivi: che s'intende?

Cfr: FAQ **ACN – AUTORITA' CYBERSICUREZZA NAZIONALE**

L'elencazione dei **componenti del Consiglio di amministrazione** dell'organizzazione, o strutture analoghe tenuto conto della natura giuridica e alla struttura organizzativa dell'organizzazione

Pertanto, ai fini dell'adempimento in parola, **non è attesa l'elencazione** delle persone fisiche che svolgono le funzioni di punto di contatto (e sostituto), di CISO o di responsabile della sicurezza aziendale, né **altre figure apicali sotto ordinate al CDA, salvo che essi siano anche componenti del CDA**



Le sanzioni interdittive personali sui componenti degli Organi Amministrativi e Direttivi

L'applicazione della **sanzione amministrativa accessoria della incapacità a svolgere funzioni dirigenziali** all'interno del medesimo soggetto. Tale sospensione temporanea è applicata finché il soggetto interessato non adotta le misure necessarie a porre rimedio alle carenze **o a conformarsi alle diffide**.

Altre sanzioni previste

Le sanzioni variano in base alla tipologia ed ai soggetti

- per quelli ***essenziali*** sono pari a un **massimo di almeno 10 000 000 EUR o a un massimo di almeno il 2 % del totale del fatturato mondiale annuo** per l'esercizio precedente dell'impresa cui il soggetto essenziale appartiene, se tale importo è superiore
- per quelli ***importanti*** le sanzioni pecuniarie amministrative sono pari a un **massimo di almeno 7 000 000 EUR o a un massimo di almeno l'1,4 % del totale del fatturato mondiale annuo** per l'esercizio precedente dell'impresa cui il soggetto importante appartiene, se tale importo è superiore
- **la sospensione temporanea o richiesta** a un organismo di certificazione o autorizzazione, oppure a un organo giurisdizionale, secondo il diritto nazionale, **di sospendere temporaneamente un certificato o un'autorizzazione relativi a una parte o alla totalità dei servizi o delle attività pertinenti svolti dal soggetto essenziale**

La Vigilanza dell'Autorità

Ispezioni in loco

Audit periodici sulla sicurezza

Audit ad hoc

Scansioni di sicurezza

Richieste di informazioni sulle misure adottate documentazione

Richieste di accesso a dati, documenti ed altre informazioni

Richieste di dati che dimostrino l'applicazione di politiche di cybersecurity

Le Determinazioni di ACN sulle MISURE DI BASE per i soggetti essenziali ed importanti

Ambiti Politiche	Requisiti
a) Gestione del rischio.	GV.OC-04: punto 1. GV.RM-03: punto 1. ID.RA-05: punti 1, 2 e 3. ID.RA-06: punti 1, 2 e 3.
b) Ruoli e responsabilità.	GV.RR-02: punti 1, 2, 3 e 4.
c) Affidabilità delle risorse umane.	GV.RR-04: punti 1 e 2.
d) Conformità e audit di sicurezza.	GV.PO-01: punti 1, 2 e 3. GV.PO-02: punti 1 e 2. ID.IM-01: punti 1 e 2.
e) Gestione dei rischi per la sicurezza informatica della catena di approvvigionamento.	GV.SC-01: punto 1. GV.SC-02: punto 1. GV.SC-04: punto 1. GV.SC-05: punto 1. GV.SC-07: punti 1 e 2.
f) Gestione degli asset.	ID.AM-01: punto 1. ID.AM-02: punto 1. ID.AM-04: punto 1.
g) Gestione delle vulnerabilità.	ID.RA-01: punto 1. ID.RA-08: punti 1, 2, 3 e 4.
h) Continuità operativa, ripristino in caso di disastro e gestione delle crisi.	ID.IM-04: punti 1, 2, 3, 4 e 5.
i) Gestione dell'autenticazione, delle identità digitali e del controllo accessi.	PR.AA-01: punti 1, 2 e 3. PR.AA-03: punti 1 e 2. PR.AA-05: punti 1 e 2. PR.IR-01: punti 1 e 2.
j) Sicurezza fisica	PR.AA-06: punto 1.
k) Formazione del personale e consapevolezza.	PR.AT-01: punti 1, 2 e 3.
l) Sicurezza dei dati.	PR.DS-01: punti 1 e 2. PR.DS-02: punto 1. PR.DS-11: punto 1.
m) Sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete.	PR.PS-02: punti 1, 2. PR.PS-04: punti 1, 2 e 3. PR.PS-06: punto 1.
n) Protezione delle reti e delle comunicazioni.	PR.IR-01: punto 3.
o) Monitoraggio degli eventi di sicurezza.	DE.CM-01: punti 1 e 2. DE.CM-09: punto 1.
p) Risposta agli incidenti e ripristino.	RS.MA-01: punti 1, 2 e 3. RS.CO-02: punti 1 e 2. RC.RP-01: punto 1.

N.B. LA GOVERNANCE E' ESSENZIALE. QUALI SOGGETTI INTERNI INCARICARE?

I ruoli, le responsabilità e i correlati poteri relativi alla gestione del rischio di cybersecurity **sono stabiliti**, comunicati, compresi e applicati.

1.È definita, approvata dagli organi di amministrazione e direttivi, **e resa nota alle articolazioni competenti** del soggetto NIS, **l'organizzazione per la sicurezza informatica e ne sono stabiliti ruoli e responsabilità**.

2. È mantenuto un **elenco aggiornato del personale dell'organizzazione di cui al punto 1 avente specifici ruoli e responsabilità** ed è reso noto alle articolazioni competenti del soggetto NIS.

3. All'interno dell'organizzazione per la sicurezza informatica di cui al punto 1, **sono inclusi** il punto di contatto, e almeno un suo sostituto, di cui alla determina adottata ai sensi dell'articolo 7, comma 6 del decreto NIS.

4. I ruoli e le responsabilità di cui al punto 1 sono riesaminati e, se opportuno, **aggiornati periodicamente e comunque almeno ogni due anni**, nonché qualora si verifichino incidenti

Obbligo di notifica Art. 25

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.**

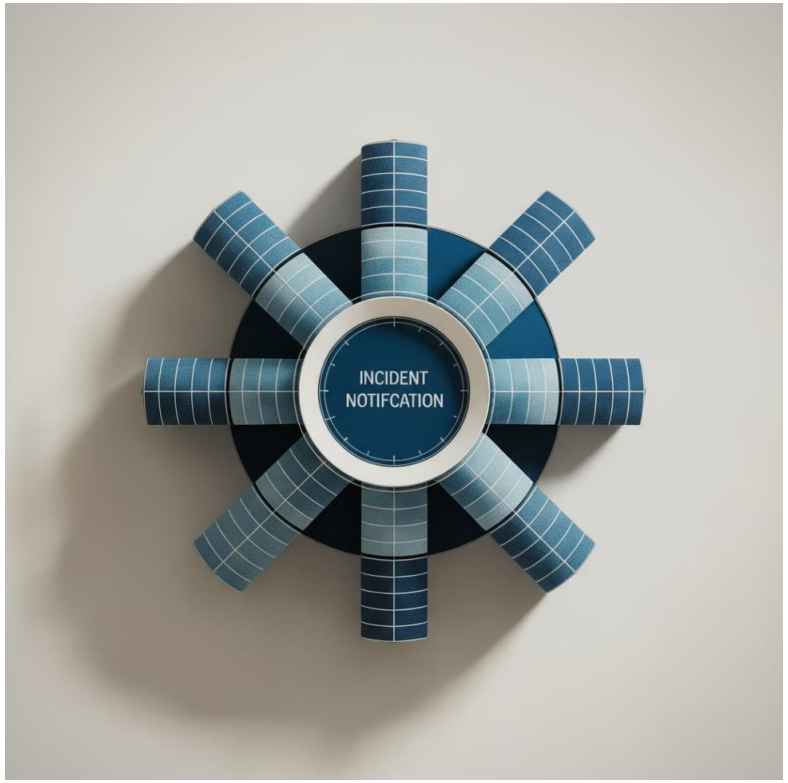
2. Le notifiche includono le informazioni che consentono al CSIRT Italia di determinare un eventuale **impatto transfrontaliero** dell'incidente.

3. La notifica **non espone il soggetto** che la effettua a una maggiore responsabilità rispetto a quella derivante dall'incidente.

4. **Un incidente è considerato significativo se:**

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

b) ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

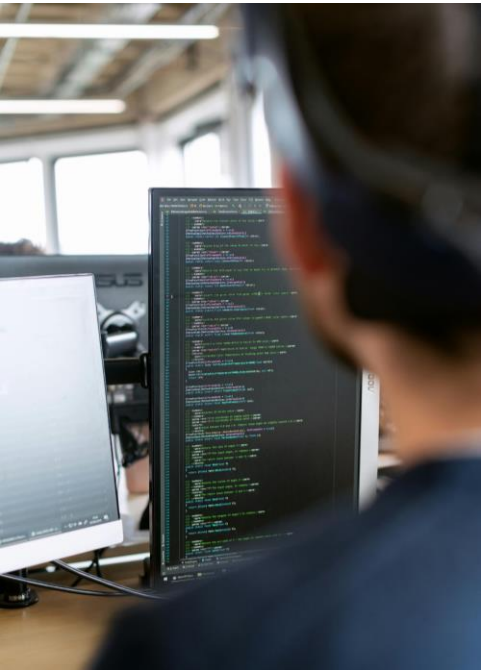


Il referente CSIRT

è una **persona fisica** designata dal Punto di Contatto, a partire dal 20 novembre ed entro il 31 dicembre 2025, tramite la dedicata procedura telematica resa disponibile dal Portale ACN

ha il compito di **interloquire con lo CSIRT Italia**, di cui all'articolo 2, comma 1, lettera i) del decreto NIS, ed **effettuare le notifiche di cui agli articoli 25 e 26** del medesimo decreto per conto del soggetto NIS

possono essere designati uno o più sostituti referente CSIRT. I sostituti referente CSIRT, ove designati, supportano il referente CSIRT nell'esercizio delle funzioni di cui al comma 2 e possono svolgerle per suo conto.



REQUISITI: Il referente CSIRT e i suoi sostituti, ove designati, possiedono almeno competenze di base in materia di sicurezza informatica e di gestione di incidenti informatici, nonché una conoscenza approfondita dei sistemi informativi e di rete del soggetto per conto del quale operano. Quali competenze sono o dovrebbero essere presenti in azienda?

RAPPORTO GIURIDICO: può essere interno o esterno. Come deve essere inquadrato giuridicamente?

SOVRAPPOSIZIONE DI RUOLI: può anche essere sia il punto di contatto che il sostituto del punto di contatto. Quali scelte di governance sono state fatte?

Cyber security della supply chain

Fornitori critici: le azioni principali

- Flusso rispetto all'ufficio acquisti
- Integrazioni contrattuali
- Audit e modalità delle remediations

Quali temi devono essere dimostrabili

È essenziale essere in grado di dimostrare di aver valutato

- Governance
- Procedure organizzative
- Misure di sicurezza
- Definizione catena di approvvigionamento
- Formazione

NIS COMPLIANCE PROGRAM

Scadenze e prossimi passi

- ✓ **Entro il 31 dicembre 2025 (dal 20 novembre):** deve essere individuato e nominato il referente CSIRT (ed in caso i suoi sostituti) e notificati in piattaforma ACN da parte del Punto di Contatto
- ✓ **Gap Analysis:** al fine di individuare le modalità attuali di gestione dei requisiti individuati dalla norma e strutturare un piano dimensionato di adeguamento (c.d. NIS2 compliance program)
- ✓ **Entro il 31 dicembre 2025:** in base ai risultati della GA deve essere fatte delle scelte ed implementate le misure funzionali alla notifica degli incidenti ex art. 25 e 26. **N.B. NON E' DA IMPLEMENTARE SOLO LA PROCEDURA DI NOTIFICA MA TUTTE LE PROCEDURE CONNESSE ALLA PREVENZIONE, RILEVAZIONE E GESTIONE DELL'INCIDENTE**
  - Pre-allarme **entro 24 ore**
  - senza indebito ritardo, e comunque **entro 72 ore** dalla conoscenza dell'incidente significato con riferimento ad un aggiornamento delle informazioni andando ad indicare una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione
  - su richiesta di un CSIRT o, se opportuno, di un'autorità competente, una relazione intermedia sui pertinenti aggiornamenti della situazione
  - **entro un mese** relazione finale

COLIN
CONSULENTE LEGALE INFORMATICO

GRAZIE

Avv. Alessandro Cecchetti

acecchetti@consulentelegaleinformatico.it

Linkedin: https://it.linkedin.com/in/acecchetti

Contatti

Sede legale
Via Privata Maria Teresa, 7 – Milano 20123
Tel. +39 0287198390
Sede operativa e amministrativa:
Via Cividale, 51 – Montecatini Terme (PT) 51016
Tel. +39 0572 78166
Fax +39 0572 294540
Sede operativa
Via Del Lavoro, 57 – Casalecchio di Reno (BO) 40033

Partita Iva e Codice Fiscale: 01651060475
Le nostre sedi: Montecatini Terme (PT), Milano
www.consulentelegaleinformatico.it

Per richieste progetti e preventivi:
info@consulentelegaleinformatico.it
Per organizzare eventi:
comunicazione@consulentelegaleinformatico.it
Per organizzare corsi di formazione:
thinkfactory@consulentelegaleinformatico.it