Il ruolo del CISO e del DPO con la NIS2: le nuove sfide per le organizzazioni

18 Settembre 2025 | 10:00 - 12:00

Webinar

Enzo Veiluva

I numeri ….

DPO Circa 71,000
(Fonte Garante Privacy)

CISO ??
Circa 58% delle aziende grandi
ha istituito il ruolo

Punto di contatto e
Sostituto punto di contatto.. Circa 40,000
(fonte ACN 15.000 soggetti importanti ,
5000 essenziali)

CYBERSECURITY360 | Cybersecurity Nazionale

DIRETTIVA

DPO e CISO, alleanza necessaria: due funzioni, un'unica visione

Home > Norme E Adeguamenti

In uno scenario di convergenza di protezione dei dati e sicurezza delle informazioni verso un unico campo di responsabilità condivisa, DPO e CISO rappresentano due presìdi complementari. Ecco ruoli, funzioni e punti di contatto tra le due figure, anche alla luce della Direttiva NIS 2 e del GDPR

Pubblicato il 25 mar 2025

Giuseppe Alverone
Consulente e formatore Privacy. DPO certificato UNI CEI EN 17740:2024

Monica Perego
Consulente, Formatore Privacy & DPO

COMPETENZE PRIVACY E CYBER

Convergenza GDPR-NIS2: l'era dei profili ibridi oltre Ciso e DPO

Home > Sicurezza Digitale

Con l'evoluzione della normativa NIS2, nasce una figura ibrida che unisce la protezione dei dati e la gestione del rischio informatico. Il Cyber Legal, Policy & Compliance Officer è la chiave per garantire un'efficace cyber resilience nelle organizzazioni

Pubblicato il 22 lug 2025

Adriano Bertolino
Esperto in Privacy e Cybersecurity

CHI SIAMO SERVIZI CONTATTI IT

Hinto Group

Blog

NIS2 e GDPR: nuove sfide per la protezione delle reti e dei dati nelle aziende

14 luglio 2025

Agenda Digitale.eu | Cittadinanza digitale

NORMATIVA

CISO e DPO, cosa fanno in azienda e come supportano l'efficienza

Home > Sicurezza Digitale > Privacy

CISO e DPO sono figure emerse nelle realtà produttive con l'introduzione delle norme del GDPR, la loro importanza è anche di natura strategica: vediamo il loro ruolo

Pubblicato il 16 ott 2023

Federica Maria Rita Livelli
Business Continuity & Risk Management Consultant, BCI Cyber Resilience Group, Clusit, ENIA

DPO & CISO in NIS2

Impatto sul CISO (Chief Information Security Officer)

Gestione della supply chain:

- La NIS2 pone una forte attenzione alla sicurezza della catena di approvvigionamento, quindi il CISO deve estendere i suoi controlli di sicurezza ai fornitori, verificandone gli standard e documentando la loro conformità.

Responsabilità estese:

- Il CISO è tenuto a implementare e gestire le misure di sicurezza informatica, la prevenzione e la risposta agli incidenti, nonché la gestione della continuità operativa, con una maggiore responsabilità diretta.

Collaborazione con il DPO:

- Il CISO deve collaborare strettamente con il DPO per garantire che le misure di sicurezza informatica non violino la privacy e per sviluppare piani di risposta agli incidenti che considerino entrambi gli aspetti

Impatto sul DPO (Data Protection Officer)

Ruolo di governance:

- La NIS2 trasforma il DPO in un soggetto chiave per la governance della cyber security, estendendo il suo ruolo oltre la sola protezione dei dati personali.

Formazione e consapevolezza:

- Il DPO collabora con il CISO per la formazione del personale in materia di cyber security, garantendo che tutti comprendano le nuove direttive e il loro impatto sulla protezione dei dati.

Collaborazione con il CISO:

- Il DPO deve lavorare a stretto contatto con il CISO per assicurare un'integrazione completa tra le politiche di protezione dei dati e quelle di sicurezza informatica, diventando un punto di riferimento per la compliance complessiva.

Una terza figura in ascesa…

ANRA
Associazione Nazionale dei Risk Manager e Responsabili Assicurazioni Aziendali

ANRA | Risk Management | Formazione | Eventi

Il profilo di due figure professionali in ascesa: il Risk Manager e l'Insurance Manager

Risk Manager
Il Risk Manager è la figura professionale preposta all'identificazione e valutazione dei rischi aziendali fornendo supporto al management nella gestione degli stessi.

Compito del Risk Manager è, infatti, individuare e analizzare i potenziali rischi in cui può incorrere l'impresa e che possono comprometterne il raggiungimento degli obiettivi strategici e operativi nel breve, medio e lungo termine.

Al fine quindi di supportare la continuità operativa dell'azienda e la creazione di valore per gli stakeholder, valuta il potenziale impatto di tali eventi e contribuisce alla definizione della migliore strategia di gestione degli stessi nel rispetto delle soglie di accettabilità dei rischi definite dal Consiglio di Amministrazione.

Una volta definito il profilo di rischio dell'azienda, il Risk Manager monitora l'esposizione dei rischi identificati e la relativa efficacia di strategie e azioni di mitigazione. Il ruolo del Risk Manager può essere svolto internamente all'azienda, ovvero ricoperto da un dipendente dell'azienda stessa oppure affidato a un consulente esterno.

Ma iniziamo l’approfondimento….

Determinazione entrata in vigore il 31 luglio 2025

ACN.AOO_ACN-US.REGISTRO UNICO.0283727.22-07-2025.I

Agenzia per la Cybersicurezza Nazionale

Determinazione del Direttore generale dell'Agenzia per la cybersicurezza nazionale

di cui all'articolo 7, comma 6, del decreto legislativo 4 settembre 2024, n. 138, adottata secondo le modalità di cui all'articolo 40, comma 5, recante termini, modalità e procedimenti di utilizzo e accesso alla piattaforma digitale nonché ulteriori informazioni che i soggetti devono fornire all'Autorità nazionale competente NIS e termini, modalità e procedimento di designazione dei rappresentanti NIS sul territorio nazionale.

IL DIRETTORE GENERALE

VISTO il decreto legislativo 12 gennaio 2019, n. 14, recante "*Codice della crisi d'impresa e dell'insolvenza in attuazione della legge 19 ottobre 2017, n. 155*";

VISTO il decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, recante "*Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*";

VISTO il decreto legislativo 4 settembre 2024, n. 138, recante "*Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148"* e, in particolare, l'articolo 7 e l'articolo 40, comma 5, lettera b);

VISTO il Regolamento (CEE) n. 2137/85 del Consiglio del 25 luglio 1985 relativo all'istituzione di un gruppo europeo di interesse economico (GEIE);

VISTO il decreto legislativo 23 luglio 1991, n. 240, recante "Norme per l'applicazione del

2. **Tempistiche rigide e non derogabili:**
    1. **Registrazione iniziale**: dal primo gennaio al 28 febbraio.
    2. **Aggiornamento annuale**: dal 15 aprile al 31 maggio. ve.
    3. **Aggiornamento continuo**: entro 14 giorni da ogni variazione, disponibile fino al 14 aprile successivo..

3.Ruoli e responsabilità:

1. Il **punto di contatto** : persona fisica può essere un delegato interno o un dipendente di altra società del gruppo o di altra PA.
2. Il **sostituto punto di contatto:** obbligatorio entro il 31 maggio dell'anno di inserimento nell'elenco NIS.
3. I **componenti degli organi amministrativi** devono essere elencati con codice fiscale e PEC, e accettare esplicitamente la designazione via Portale ACN.

1.Portale ACN unico canale di comunicazione. Dal 31 luglio 2025 il Portale ACN diventa l'unico strumento valido per comunicare con l'Autorità nazionale competente.

4. **Tracciabilità totale e responsabilità penale**: ogni dichiarazione è soggetta a DPR 445/2000 e le omissioni sono sanzionate ex art. 38 del Decreto NIS.

5.Verifiche di coerenza e clausola di salvaguardia. Le dichiarazioni sono soggette a controlli a campione entro 30 giorni, prorogabili di altri 20.

6.Designazione rappresentanti NIS UE. Per i soggetti extra-UE con attività in Italia, l'invio della documentazione per la nomina del rappresentante va effettuato dal 1° settembre al 30 novembre

Il documento contiene in particolare **due capitoli,** riferiti a:

•**misure di sicurezza di base**, ovvero:

- misure di sicurezza e loro struttura
- approccio basato sul rischio
- tipologie di requisiti
- principali evidenze documentali richieste

•**incidenti significativi di base**, che:

- illustra le fattispecie che costituiscono gli incidenti significativi in base al decreto NIS
- specifica i concetti di evidenza dell'incidente e di abuso dei privilegi concessi.

11 Documenti che devono essere portati all’attenzione del consigli di amministrazione

Appendice C – documenti approvati dagli organi di amministrazione e direttivi

La seguente tabella elenca i documenti che devono essere approvati dagli organi di amministrazione e direttivi e i riferimenti ai requisiti che ne richiedono l’approvazione.

Documento	Riferimento requisito
Organizzazione per la sicurezza informatica.	GV.RR-02 punto 1.
Politiche di sicurezza informatica.	GV.PO-01 punto 1.
Valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete.	ID.RA-05 punto 3.
Piano di trattamento del rischio.	ID.RA-06 punto 3.
Piano di gestione delle vulnerabilità.	ID.RA-08 punto 4.
Piano di adeguamento.	ID.IM-01 punto 1.
Piano di continuità operativa.	ID.IM-04 punto 1.
Piano di ripristino in caso di disastro.	ID.IM-04 punto 1.
Piano di gestione delle crisi.	ID.IM-04 punto 1.
Piano di formazione.	PR.AT-01 punto 1.
Piano per la gestione degli incidenti di sicurezza informatica.	RS.MA-01 punto 2.

Appendice A – corrispondenza elementi misure

La seguente tabella riporta la mappatura tra le misure di sicurezza di base e gli elementi di cui all'articolo 24, comma 2 del decreto NIS.

Elemento decreto NIS	Codice misura di sicurezza
a) Politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete;	GV.OC-04, GV.RM-03, GV.RR-02, GV.PO-01, GV.PO-02, ID.RA-05, ID.RA-06.
b) Gestione degli incidenti, ivi incluse le procedure e gli strumenti per eseguire le notifiche di cui agli articoli 25 e 26.	PR.PS-04, DE.CM-01, DE.CM-09, RS.MA-01, RS.CO-02.
c) Continuità operativa, ivi inclusa la gestione di backup, il ripristino in caso di disastro, ove applicabile, e gestione delle crisi.	ID.IM-04, PR.DS-11, RC.RP-01, RC.CO-03.
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.	GV.SC-01, GV.SC-02, GV.SC-04, GV.SC-05, GV.SC-07.
e) Sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità.	GV.SC-05, ID.RA-01, ID.RA-08, PR.PS-01, PR.PS-02, PR.PS-03, PR.PS-06.
f) Politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi per la sicurezza informatica.	ID.IM-01.
g) Pratiche di igiene di base e di formazione in materia di sicurezza informatica.	PR.AT-01, PR.AT-02.
h) Politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura.	PR.DS-01, PR.DS-02.
i) Sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli assetti.	GV.RR-04, ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-4, PR.AA-01, PR.AA-03, PR.AA-05, PR.AA-06, PR.IR-01.
l) Uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette, e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, ove opportuno.	PR.AA-03, PR.DS-02, PR.IR-03.

Mappatura requisiti - procedure