DataVerso
Protezione e governance per il patrimonio delle informazioni

CyberGo
Cybersecurity and Governance to drive your business

Referente CSIRT e Incident Response Plan

AI SENSI DELL'ART. 7 DELLA DETERMINAZIONE ACN 333017 DEL 19/09/2025

DataVerso è una gamma di servizi progettati e coordinati da Soluzioni srl

SOLUZIONI S.R.L. | VIA COGNE, 25 - 40026 IMOLA (BO)

Rev. 1.3 - dicembre 2025

INTRODUZIONE

Premessa

Il panorama della sicurezza informatica impone oggi un approccio proattivo e normato alla gestione del rischio e il servizio risponde all'esigenza di conformità introdotta dalla **Direttiva (UE) 2022/2555 (per brevità Direttiva NIS 2)** – 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 –, recepita in Italia dal **D.lgs. 138/2024 (per brevità Decreto NIS 2)**. Tali norme rafforzano gli obblighi di cybersicurezza per i Soggetti NIS che erogano servizi essenziali e importanti per la società e l'economia.

Un elemento chiave, nel panorama dell'assetto organizzativo aziendale di un Soggetto NIS, è l'istituzione della figura del **Referente CSIRT**, formalizzata dalla **Determinazione ACN n. 333017/2025**. Questa figura è essenziale per assicurare la corretta esecuzione degli obblighi di notifica degli incidenti (ai sensi degli artt. 25 e 26 del Decreto NIS 2) e la comunicazione operativa con l'Autorità competente, il CSIRT Italia (Computer Security Incident Response Team), istituito presso l'Agenzia per la Cybersicurezza Nazionale (ACN) con Decreto-legge n. 82/2021, si occupa principalmente delle attività di natura reattiva.

Nello specifico, il CSIRT Italia fornisce informazioni e assistenza ai Soggetti NIS nell'attuazione di misure proattive volte a ridurre i rischi di incidenti relativi alla sicurezza informatica, nonché nella risposta a tali incidenti quando si verificano.

Inoltre, il CSIRT Italia garantisce una cooperazione efficiente a livello dell'Unione partecipando alle reti dei CSIRT europei garantendo, in questo modo, un livello di sicurezza informatica esteso su tutti i paesi dell'Unione Europea.

Infine, segnalare un incidente di sicurezza informatica all'autorità competente, quale il Garante per la protezione dei dati in caso di violazione di dati personali o al CSIRT Italia per gli incidenti significativi, non è solo un onere normativo, ma un'opportunità per ottenere aiuto esperto, mitigare i danni, proteggere la propria reputazione e contribuire a rafforzare la sicurezza dell'intero ecosistema digitale.

In linea generale il CSIRT non fornisce un supporto diretto nella risoluzione dei problemi informatici ai Soggetti NIS, per cui questi dovranno rivolgersi ai rispettivi fornitori di servizi informatici o al personale dipendente specializzato in tematiche di gestione degli incidenti di sicurezza informatica.

INQUADRAMENTO DEL SERVIZIO

Scopo del servizio

La finalità del servizio consiste nel supportare le aziende nell'elevare il proprio livello di sicurezza informatica e nel coordinare le attività necessarie per un tempestivo ripristino della continuità operativa dei sistemi informativi e delle reti, a prescindere da eventuali obblighi normativi.

Inoltre, per i Soggetti NIS che sono tenuti a nominare un Referente CSIRT, la proposta si arricchisce mettendo a disposizione consulenti esperti in grado di esaminare ogni possibile incidente (circoscritti ai c.d. incidenti significativi di base, a quanto disposto dalla Determinazione ACN 164179 del 14/04/25, e data breach, a quanto disposto dagli artt. 33 e 34 del Regolamento (UE) 2016/679 – GDPR), non soltanto dal punto di vista tecnologico, ma anche considerando gli aspetti giuridici e organizzativi.

Infatti, il servizio si avvale di un team multidisciplinare, guidato da un project manager che, nei casi previsti, assume anche il ruolo di Referente CSIRT – a quanto disposto dall'art. 7 della Determinazione ACN 333017/2025 –, garantendo così un approccio integrato e trasversale nella gestione degli incidenti.

Approccio metodologico

L'approccio metodologico per la gestione del rischio e degli incidenti si allinea al **Framework Nazionale per la Cybersecurity e Data Protection** (edizione 2025 v. 2.1 e per brevità FNCDP) derivato dal Cybersecurity Framework (CSF) 2.0 del NIST, uno standard internazionale che organizza le attività di cybersicurezza in sei funzioni principali:

- **Governo**, la nuova funzione che pone la sicurezza al livello di governance;
- **Identificazione**, che comprende le misure di sicurezza utili per identificare i principali rischi a cui sono sottoposti i Sistemi informativi e reti dei Soggetti NIS;
- **Protezione**, che comprende le misure di sicurezza necessarie a mitigare i rischi individuati da ciascun Soggetto NIS;
- **Monitoraggio**, che comprende tutte le azioni necessarie per individuare per tempo le minacce;
- **Risposta**, che comprende tutte le misure di sicurezza attuate per rispondere ad una eventuale minaccia in corso;
- **Ripristino**, che comprende tutte le azioni necessarie per il ritorno alla piena continuità operativa dei Sistemi informativi e di rete nel più breve tempo possibile.

In particolare, lo specifico servizio si concentra sulle funzioni di **Governo, Risposta e Ripristino**, assicurando che la risposta agli incidenti sia immediata e integrata nella strategia aziendale.

Profilo professionale del referente CSIRT

Il referente CSIRT è la persona fisica incaricata dall'organo di amministrazione e direttivo del Soggetto NIS nonché designato formalmente dal Punto di Contatto attraverso la dedicata procedura telematica resa disponibile dalla piattaforma dei servizi ACN, a quanto disposto dell'art. 7 della Determinazione ACN n. 333017/2025, che possieda competenze di sicurezza informatica e di gestione di incidenti informatici, nonché una conoscenza approfondita dei sistemi informativi e di rete del Soggetto NIS.

Missione e finalità del referente CSIRT

Il principale obiettivo del referente CSIRT consiste nell'assicurare la gestione tempestiva, coordinata e conforme degli incidenti significativi che coinvolgono i sistemi informativi e le reti della Società nonché le eventuali violazioni sui dati personali.

Il Referente CSIRT rappresenta l'interfaccia operativa tra la Società e lo CSIRT Italia, garantendo la corretta esecuzione delle notifiche di incidenti significativi e la comunicazione tecnica con lo CSIRT stesso.

Allo stesso tempo, il referente CSIRT si interfaccia con il Data Protection Officer (c.d. DPO), se presente, oppure supporta il Titolare del trattamento per la notificazione al Garante per la protezione dei dati personali, a quanto disposto dagli artt. 33 e 34 del GDPR.

Il ruolo contribuisce in modo determinante alla resilienza organizzativa e alla protezione delle infrastrutture digitali, operando con autonomia funzionale e competenza tecnica.

In particolare, il referente CSIRT deve:

- **Gestire, coordinare e notificare** gli incidenti informatici significativi, garantendo tempestività, secondo quanto previsto dagli artt. 25 e 26 del Decreto NIS 2 e determinazione ACN n. 164179 del 14/04/2025 e suoi allegati, nonché eventuali data breach ai sensi di quanto disposto dal Regolamento (UE) 2016/679 – GDPR, nel caso in cui il soggetto NIS non abbia individuato un DPO.
- **Promuovere una risposta efficace agli incidenti**, integrata con le procedure interne della Società e coerente con gli standard di mercato.
- **Assicurare la continuità dei flussi informativi** tra il soggetto NIS, DPO se presente o Garante per la protezione dei dati, lo CSIRT Italia e l'ACN.

Posizione del referente CSIRT nell'organizzazione del Soggetto NIS

Il ruolo del referente CSIRT può essere ricoperto da personale interno del Soggetto NIS oppure da un fornitore esterno in base a un contratto di servizi e in questa ultima fattispecie, i compiti stabiliti per il referente CSIRT potranno essere assolti efficacemente da un team operante sotto l'autorità di un contratto principale designato e "responsabile" per il singolo cliente. In tal caso, è indispensabile che i soggetti, appartenente al fornitore esterno operante quale referente CSIRT, dimostrino di possedere esperienza e competenze complementari per garantire un intervento di gestione degli incidenti qualificato e coerente con quanto richiesto dal CSIRT Italia.

Per favorire efficienza e correttezza e prevenire conflitti di interesse a carico dei componenti del team, si raccomanda di procedere a una chiara ripartizione dei compiti tra i componenti del referente CSIRT esterno, attraverso il contratto di servizi e di prevedere che sia un solo soggetto a fungere da contatto principale e "incaricato" per ciascun cliente, coadiuvato da uno o più sostituti per garantire la continuità nel tempo in caso di assenza del soggetto incaricato.

Inoltre, per garantire un servizio di qualità adeguato, il referente CSIRT o il suo team di collaboratori, deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti gli sviluppi tecnologici intrapresi dal Soggetto NIS che possano avere un impatto sulla gestione degli incidenti di sicurezza informatica.

Assicurare il tempestivo e immediato coinvolgimento del referente CSIRT, tramite la sua informazione e consultazione fin dalle fasi iniziali, **promuoverà l'applicazione del principio di protezione dei sistemi informativi e di rete fin dalla fase di progettazione**; pertanto, questo dovrebbe rappresentare l'approccio standard all'interno della struttura del Soggetto NIS. Inoltre, è importante che il referente CSIRT sia annoverato fra gli interlocutori all'interno dell'organizzazione del Soggetto NIS e che partecipi ai gruppi di lavoro che si occupano delle attività di sicurezza delle informazioni.

Inoltre, il referente CSIRT:

- Riferisce funzionalmente all'organo di amministrazione e direttivo del Soggetto NIS e opera in autonomia funzionale, nell'ambito dell'incarico affidato.
- Collabora strettamente con il Punto di Contatto e il suo sostituto, il CISO, con i team IT, il DPO e con eventuali Referenti per la cybersicurezza o incident response interni al Soggetto NIS.
- Dispone delle risorse e dell'accesso alle informazioni necessarie per svolgere la sua funzione, per il quale è tenuto al segreto professionale.
- Nell'esercizio corretto delle proprie funzioni, il referente CSIRT non può essere penalizzato.

Infine, il Referente CSIRT e il suo team di collaboratori non sono responsabili personalmente in caso di inosservanza degli obblighi in materia di conformità al Decreto NIS 2. Spetta al Soggetto NIS garantire ed essere in grado di dimostrare che le misure di sicurezza siano state attuate conformemente al Decreto NIS 2. La responsabilità di garantire l'osservanza del Decreto NIS 2 ricade sempre sul Soggetto NIS e il referente CSIRT deve aiutare nello svolgere questo compito in modo efficace ed efficiente.

INTERVENTO

Criteri per la definizione dell'intervento

I criteri da prendere come riferimento per definire il tipo di intervento si fondano sulla volontà di designare il referente CSIRT su base volontaria o sull'obbligo di legge e il servizio si distingue in due tipologie:

1) Consulenza per la redazione del piano e servizio per la gestione dell'incidente;
2) Incarico referente CSIRT e consulenza per la redazione del piano e servizio per la gestione dell'incidente;

Consulenza per la redazione del piano e servizio per la gestione dell'incidente

Scopo del servizio consiste nel mettere il cliente in condizione di rispondere a un incidente in modo coordinato, documentato e misurabile, con corsia preferenziale e vantaggi economici verso il team di Incident Response.

Fasi principali

A seguire la tabella che descrive le fasi presenti nel servizio, che dovranno essere adattate in funzione del grado di esposizione dei Soggetti NIS ai rischi, delle dimensioni dei Soggetti stessi e della probabilità che si verifichino incidenti, nonché della loro gravità, compreso il loro impatto sociale ed economico, in cui si dovrà sviluppare il servizio.

N°	Ambito	Descrizione Compito
1	**Incident Response Plan (IRP) NIS2 - GDPR**	Una gestione efficace degli incidenti informatici richiede una struttura chiara che definisca scopo, governance, criteri di gravità, catene di escalation e il modello RACI, che specifica ruoli e responsabilità. La matrice RACI aiuta a stabilire chi è responsabile, chi prende le decisioni, chi viene consultato e chi deve essere informato. Inoltre, occorre organizzare le comunicazioni, raccogliere evidenze, coinvolgere le funzioni legali e assicurative nonché notificare eventuali incidenti alle autorità competenti, quali il CSIRT Italia e il Garante per la protezione dei dati, garantendo così una risposta tempestiva e coordinata agli incidenti.
		Un piano operativo essenziale dovrebbe prevedere procedure dettagliate per affrontare almeno quattro scenari critici: attacco **ransomware**, **compromissione della posta elettronica aziendale (BEC)**, **esfiltrazione non autorizzata di dati** e **violazione dell'Active Directory o delle identità digitali**. Per ciascuno di questi casi, è importante stabilire azioni chiare e coordinate che consentano di reagire tempestivamente, limitare i danni e ripristinare la normale operatività dei sistemi informativi e di rete. L'adozione di un approccio strutturato permette di garantire una risposta efficace, tutelando sia le risorse aziendali che la reputazione dell'organizzazione.
		È utile disporre di strumenti organizzativi che consentano di tenere traccia di ciò che accade e delle decisioni prese durante la gestione di una situazione critica. Allo stesso modo, è importante avere modelli prestabiliti per comunicare tempestivamente a chi di dovere eventuali problemi riscontrati. Un valido supporto può essere rappresentato anche da elenchi di controllo che aiutano a verificare che tutte le azioni necessarie siano state svolte, dalla fase iniziale di contenimento del problema fino al completo ripristino della normalità. Infine, al termine della gestione, è fondamentale riflettere su quanto accaduto per trarre insegnamenti utili a migliorare la risposta futura.
		Per essere in regola con le attuali normative sulla sicurezza, è importante che ogni persona coinvolta sappia chiaramente quali sono i propri compiti, come devono essere gestite le diverse fasi di una situazione critica e quali informazioni devono essere raccolte e conservate. Inoltre, è fondamentale ricordare che, quando si verifica un problema che può avere conseguenze importanti, è necessario avvisare tempestivamente gli enti competenti: a partire da un primo segnale entro 24 ore, una comunicazione più dettagliata entro 72 ore e, infine, un resoconto completo entro un mese. In questo modo si garantisce trasparenza e collaborazione, proteggendo l'organizzazione e rafforzando la fiducia verso l'esterno.
2	**Simulazione di un incidente informatico mettendo alla prova l' IRP**	Progettazione: creazione di uno scenario personalizzato che tenga conto delle caratteristiche specifiche del settore e delle tecnologie utilizzate, definizione degli obiettivi formativi da raggiungere e predisposizione di elementi che stimolino la riflessione e favoriscano scelte strategiche in situazioni complesse
		L'attività si svolge nell'arco di una giornata, sotto la guida di un consulente esperto che accompagna i partecipanti in ogni fase. Durante il percorso, vengono annotate le scelte effettuate e i tempi di reazione, così da raccogliere elementi utili per riflettere insieme sull'efficacia delle risposte adottate.
		Resoconto conclusivo: documento che evidenzia le aree di miglioramento individuate propone suggerimenti ordinati per importanza e aggiorna il piano delle azioni future da intraprendere.

N°	Ambito	Descrizione Compito
3	**Accesso prioritario al Team Incident Response**	Accesso prioritario al Team di Incident Response con presa in carico entro 60 minuti dalla segnalazione e reperibilità in relazione alle esigenze del cliente
		Attivazione e accesso del gruppo di gestione della crisi che riunisce tutti gli attori (tecnici, legali, e management) coinvolti nella gestione dell'incidente con canali di comunicazione dedicati e strumenti di project management per garantire trasparenza sulle operazioni in corso ed evitare inefficienze
		Kickstart kit: guida "prime 4 ore", checklist comprendente le azioni da svolgere nell'immediato post incidente

Incarico referente CSIRT e consulenza per la redazione del piano e servizio per la gestione dell'incidente;

Lo scopo del servizio comprende tutte le fasi previste per la consulenza necessaria per la redazione del piano e servizio per la gestione dell'incidente compreso di assunzione dell'incarico del ruolo di Referente CSIRT esterno e una valutazione completa del Sistema informativo e di rete del Soggetto NIS per arrivare a una postura adeguata, solida e misurabile a quanto predisposto dal Decreto NIS 2.

N°	Ambito	Descrizione Compito
1	**Incarico referente CSIRT**	Formale assunzione dell'incarico in oggetto con dettaglio dei compiti e responsabilità
		Attività di interfaccia con il CSIRT Italia e ACN
		Condivisione delle attività e risultati con il Punto di contatto e il referente di progetto aziendale
2	**Assessment CSIRT per comprendere l'infrastruttura (Hardware e software) oggetto del servizio e l'assetto organizzativo aziendale per la sicurezza delle informazioni**	Obiettivo: nell'ambito della gestione di un incidente informatico, è fondamentale assicurarsi che solo le persone autorizzate possano accedere ai sistemi e alle informazioni aziendali. Occorre inoltre monitorare i dispositivi utilizzati, le connessioni di rete, i servizi online e la posta elettronica. È importante garantire la disponibilità di copie di sicurezza e procedure di ripristino, tenere traccia delle attività svolte e delle informazioni raccolte, verificare la presenza di eventuali punti deboli e coinvolgere con attenzione eventuali fornitori esterni.
		Metodologia: interviste, revisioni configurazioni dispositivi, scansioni della rete mirate e condivisione della documentazione relativa all'architettura IT
		Report di rischio con classificazione delle criticità e piano di miglioramento,
		Best practise: Framework Nazionale per la Cybersecurity e la Data Protection come da disposizione Determinazione ACN n. 164179 del 14/04/2025 – Misure di sicurezza di base per Soggetti Importanti ed Essenziali

Tempi di realizzazione dell'intervento

Il referente CSIRT, per adempiere in modo adeguato ai suoi doveri, dovrà definire una strategia per far fronte a tutti i compiti in questione, sulla base di un programma semestrale o annuale, con una certa flessibilità per tener conto di eventuali imprevisti (un improvviso problema di protezione dati, oppure un incidente di sicurezza delle informazioni a carico del Soggetto NIS, oppure un'ispezione decisa dall'autorità di controllo).

Per cui, in funzione del contesto in cui il referente CSIRT dovrà intervenire, si definiranno le modalità e tempistiche di realizzazione adeguate all'intervento richiesto.

Personale e competenze impiegate

L'intervento verrà svolto attraverso un Gruppo di Progetto multidisciplinare.

La scelta dei professionisti che compongono il Gruppo di Progetto è finalizzata a garantire la copertura delle diverse professionalità necessarie.

Risultati attesi

- Riduzione dei tempi di rilevazione e gestione degli incidenti.
- Notifiche complete e tempestive.
- Supporto all'adozione e aggiornamento del piano di risposta agli incidenti informatici.
- Miglioramento della postura di cybersecurity del Soggetto NIS.

IL SERVIZIO INTEGRATO PROPOSTO DA SOLUZIONI

Manager dei dati: ruolo chiave per un percorso di effettiva sostenibilità di ogni azienda

In un contesto di mercato unico digitale Europeo, che assume un ruolo sempre più centrale per la crescita economica, si impone alle aziende la necessità di adottare un approccio integrato nella gestione della compliance alle normative cogenti. La libera circolazione dei dati, la salvaguardia dei diritti e delle libertà individuali, la tutela dei sistemi informativi e reti aziendali, insieme all'adozione di comportamenti etici da parte degli stakeholder del settore digitale, richiedono non solo solide competenze giuridiche per l'applicazione efficace di regolamenti come il GDPR e la Direttiva NIS 2, ma anche una visione manageriale aggiornata e trasversale. Questo approccio integrato deve contemplare sia le innovazioni regolatorie sia quelle tecnologiche, rivelandosi così imprescindibile per garantire la competitività e lo sviluppo sostenibile di ogni realtà imprenditoriale.

> *La valorizzazione dei dati come motore di crescita aziendale si realizza attraverso un percorso che parte dalla tutela dei diritti e delle libertà individuali, passa per la protezione dei dati personali e arriva alla difesa del patrimonio informativo. In questo contesto, il ruolo svolto dal DPO e dal referente CSIRT si configura come centrale: secondo la visione di Soluzioni, tali figure non devono agire separatamente, ma operare in maniera strettamente integrata, così da garantire un approccio efficace e coeso nella gestione della sicurezza e della conformità aziendale.*

DataVerso è una suite di servizi progettati e coordinati da Soluzioni srl

Servizio in collaborazione con

MOTI-F Srl | VIA BENEDETTO CROCE, 34 – 00142 ROMA

T-CONSULTING Srl | VIA LUIGI GALVANI, 27 – 47122 FORLI'

Soluzioni s.r.l.

via Cogne, 25 - 40026 Imola BO

tel. e fax: 0542 640084

P.IVA, Cod. Fisc. e n. iscrizione al Reg. Imprese BO: 02996441206

R.E.A. BO 483301 - Capitale sociale 16.000,00 € i.v.