DataVerso

Protezione e governance per il patrimonio delle informazioni

CyberGo

Cybersecurity and Governance to drive your business

PROGETTO PER LA CONFORMITA' A QUANTO DISPOSTO DAL D.LGS. 138/2024 (NORMATIVA NIS2)

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

Ver. agosto 2025

INTRODUZIONE

Principali riferimenti

I riferimenti principali considerati per la definizione del progetto sono:

- D.lgs. 138/2024: "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";
- Determinazione ACN 136117 del 10 aprile 2025 - Piattaforma, Punto di contatto e sostituto, aggiornamento delle informazioni e rappresentante NIS di cui all'articolo 7 del decreto NIS;
- Determinazione ACN 164179 del 14 aprile 2025 – Specifiche di base per l'adempimento agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del D.lgs. 138/2024.

PERCORSO CONSIGLIATO

Tabella sinottica degli interventi componenti il percorso consigliato

MODULO	AMBITO	INTERVENTO PROPOSTO
1	**Obbligo di comunicazione con cadenza annuale** *(a partire dalla scadenza del 31/05/25)*	Assistenza al Referente aziendale di progetto per le comunicazioni richieste dalle Normative NIS 2
2	**Conformità della situazione aziendale a quanto disposto dalle Normative NIS 2**	Realizzazione di una Gap analysis, con le specifiche indicate nella presente scheda tecnica

Progetto integrato con il GDPR

Integrare il percorso di adeguamento alle Normative NIS 2 e quelle relative alla protezione dei dati (quali GDPR e D.lgs. 196/2003 e s.m.i.) rappresenta oggi una necessità impellente, in quanto la crescente interconnessione dei sistemi e l'evoluzione delle minacce cibernetiche rendono indispensabile un approccio olistico alla sicurezza delle informazioni e alla protezione dei dati personali.

La necessità di tale integrazione deriva dalla sovrapposizione di ambiti e requisiti normativi. Sebbene il GDPR e il D.lgs. 196/2003 e s.m.i. si concentrino sulla protezione dei dati personali e la NIS 2 sulla cybersicurezza dei sistemi e delle reti, è evidente che un incidente informatico impatta frequentemente anche la riservatezza, integrità e disponibilità dei dati personali.

> *Adeguarsi separatamente comporterebbe ridondanze, inefficienze e potenziali lacune nella protezione complessiva.*

Affrontare congiuntamente questo percorso offre notevoli vantaggi. Permette di razionalizzare risorse e investimenti, adottando misure tecniche e organizzative che soddisfino i requisiti di tutte le normative contemporaneamente. Si crea così un quadro di sicurezza e data protection coerente e robusto, migliorando la resilienza aziendale e riducendo il rischio di sanzioni, che possono essere significative in caso di non conformità. Un approccio integrato favorisce, inoltre, una maggiore consapevolezza del personale sui rischi legati alla sicurezza dei dati e dei sistemi.

Solo una strategia unitaria e sostenibile, basata su una cultura della sicurezza e della protezione dei dati, può trasformare gli obblighi normativi in un vantaggio competitivo, rafforzando la resilienza digitale delle organizzazioni e tutti coloro che vedono questa sfida come un'opportunità possono garantire la

conformità normativa e migliorare la loro posizione competitiva e la fiducia degli stakeholder dimostrando un elevato livello di affidabilità.

MODULO 1
ASSISTENZA PER LE COMUNICAZIONI RICHIESTE DALLE NORMATIVE NIS2

Obiettivo

Lo scopo dell'intervento consiste nell'assistere il Referente aziendale di progetto nell'ottemperare agli adempimenti di comunicazione annuale.

Adempimenti comunicativi con cadenza annuale

Uno dei principali adempimenti richiesti dalle Normative NIS 2 riguarda il dovere dei Soggetti NIS di mantenere aggiornate le informazioni, che nel corso del tempo vengono inserite all'interno della piattaforma dei servizi di ACN. Tale strumento è essenziale per la gestione dei rapporti con l'ACN, consentendo agli operatori di interagire, comunicare e adempiere ai propri obblighi di legge.

A titolo informativo e non esaustivo, gli adempimenti comunicativi a cadenza almeno annuale che devono essere rispettati dai Soggetti NIS sono i seguenti:

- *Registrazione o aggiornamento annuale sulla piattaforma digitale*: i soggetti rientranti nell'ambito di applicazione delle Normative NIS 2, dal 1° gennaio al 28 febbraio di ogni anno, successivo alla data di entrata in vigore della normativa NIS 2, devono effettuare la registrazione oppure, nel caso di registrazione già effettuata, aggiornare le informazioni precedentemente inserite;
- *Aggiornamento annuale delle ulteriori informazioni e dell'elenco degli accordi di condivisione*: i Soggetti NIS che hanno ricevuto la comunicazione di inclusione o permanenza nell'elenco dei Soggetti essenziali o importanti, ai sensi dell'art. 7, c 3, lettere a) e b), del decreto NIS, dal 15 aprile al 31 maggio di ogni anno successivo alla data di entrata in vigore del decreto, tramite la piattaforma digitale, devono fornire o aggiornare le ulteriori informazioni, specificate nella determina 136117 del 10/04/2025 e l'elenco degli accordi di condivisione delle informazioni sulla sicurezza informatica;
- *Comunicazione e aggiornamento annuale dell'elenco attività e servizi*: dal 1° maggio al 30 giugno di ogni anno, a partire dalla ricezione della prima comunicazione di inclusione nell'elenco dei Soggetti NIS, tali Soggetti, essenziali e importanti, comunicano e aggiornano, tramite la piattaforma digitale, l'elenco delle proprie attività e dei propri servizi;
- *Designazione e aggiornamento annuale del rappresentante NIS in Italia*: i Soggetti NIS, stabiliti fuori dall'UE che offrono servizi nella Comunità Europea, devono trasmettere e aggiornare, dal 1° settembre al 30 novembre di ogni anno, la documentazione relativa alla designazione del loro rappresentante NIS in Italia.

Oltre agli obblighi annuali specifici sopra indicati è importante notificare all'ACN qualsiasi modifica delle informazioni trasmesse tempestivamente e, in ogni caso, entro quattordici giorni dalla data della modifica. Il rispetto di questi obblighi comunicativi è fondamentale, in quanto l'osservanza delle modalità stabilite dall'ACN, ai sensi dell'art. 7 del D.lgs. 138/2024, così come la registrazione, comunicazione o aggiornamento delle informazioni richieste evita possibili sanzioni amministrative pecuniarie.

Attività di competenza di SOLUZIONI e termini per la comunicazione della richiesta d'intervento

In relazione agli adempimenti comunicativi periodici, il Consulente SOLUZIONI incaricato effettua l'intervento a seguito di richiesta comunicata via mail con un preavviso minimo di 3 giorni lavorativi.

Per garantire una corretta e adeguata elaborazione delle attività necessarie, eventuali richieste ricevute con un preavviso minore di quanto sopra indicato saranno valutate caso per caso.

MODULO 2

GAP ANALYSIS DELL'ATTUALE SITUAZIONE PER LA VERIFICA DELLA CONFORMITA' ALLE NORMATIVE NIS

Obiettivo

Il progetto proposto per il modulo 2 si pone il seguente obiettivo:

- individuare e valutare la situazione aziendale in relazione a quanto disposto dalle Normative NIS 2 e GDPR, con evidenziazione delle eventuali criticità in relazione all'estensione e all'articolazione degli ambiti di rischio aziendali verso cui la Società è esposta;
- definire e condividere, in base agli esiti della valutazione svolta, gli interventi per la realizzazione del percorso relativo all'adeguamento a quanto disposto dalle Normative NIS 2 e GDPR.

Ambito dell'analisi

In particolare, l'intervento focalizzerà l'attenzione sui principali pilastri della sicurezza delle informazioni, con riferimento al Framework identificato da ACN nelle fattispecie degli allegati alla determinazione ACN 164179 del 14 aprile 2025.

Infatti, tale determina stabilisce le modalità e le specifiche di base per ottemperare agli obblighi di cui agli articoli da 23 a 25, 29 e 32 del D.lgs. 138/2024. A titolo esemplificativo e non esaustivo, si riporta di seguito una sintesi dei relativi aspetti principali:

- **Governo**: questa funzione si concentra sull'organizzazione e strutturazione delle politiche e dei processi volti a garantire la sicurezza informatica. Essa include la mappatura del contesto organizzativo, l'adozione di policy specifiche sulla cybersicurezza, la definizione di strategie e processi per la gestione dei rischi oltre l'assegnazione chiara di ruoli, responsabilità e poteri. Inoltre, viene posta particolare attenzione ai controlli rigorosi sui fornitori, al fine di assicurare un monitoraggio efficace e una gestione proattiva delle relazioni esterne;
- **Identificazione**: Il processo di identificazione si concentra sulla mappatura degli asset rilevanti e dei flussi di informazioni, garantendo una comprensione approfondita delle risorse fondamentali per l'organizzazione. Questo include la definizione di piani di ripristino in caso di disastro per assicurare una pronta risposta alle emergenze. Inoltre, viene dato ampio spazio al miglioramento continuo dei controlli di sicurezza, alla valutazione dei rischi legati agli asset e ai fornitori, e alla creazione di procedure efficaci di gestione delle patch, essenziali per mantenere una postura di sicurezza aggiornata e resiliente.
  Inoltre, la metodologia di valutazione dei rischi deve prevedere le seguenti fasi:

- *identificazione dei rischi*: Individuare e documentare i rischi per la sicurezza dei sistemi informativi e di rete, considerando, in particolare, quelli relativi a terzi (catena di approvvigionamento) e i singoli punti di vulnerabilità;

- *analisi dei rischi*: Analizzare i rischi individuati, valutando la minaccia, la probabilità, l'impatto potenziale e il livello di rischio. Questa analisi deve considerare le informazioni di intelligence relative alle minacce informatiche e alle vulnerabilità;

- *valutazione dei rischi*: Valutare i rischi identificati e analizzati sulla base di criteri di rischio prestabiliti. Per questa fase, i soggetti devono aver definito un livello di tolleranza e criteri di rischio pertinenti;

- *trattamento dei rischi*: Sulla base dei risultati della valutazione, individuare le opzioni (prevenzione, riduzione, accettazione) e le misure adeguate a trattare i rischi e definirne l'ordine di priorità. Le misure scelte devono essere documentate in un piano di trattamento dei rischi, indicando responsabilità e tempistiche.

- **Protezione**: questa funzione nel framework NIS 2 si concentra sull'implementazione concreta delle misure di gestione dei rischi identificate. Si basa sui risultati della valutazione dei rischi e copre un'ampia gamma di misure *tecniche* (quali controllo accessi logico/fisico, crittografia, sicurezza delle piattaforme/software e gestione vulnerabilità), *organizzative* (quali definizione politiche, formazione e consapevolezza del personale). L'obiettivo è salvaguardare gli asset critici (dati, sistemi, servizi), garantendone la riservatezza, integrità e disponibilità, così da contribuire alla resilienza complessiva del Soggetto NIS;
- **Rilevamento**: questa funzione nelle misure specifiche di base NIS 2 è essenziale per la gestione proattiva della sicurezza, in quanto consiste nel monitorare costantemente sistemi e reti per identificare eventi, quasi incidenti e incidenti di cybersecurity. Si mira a rilevare tempestivamente anomalie e attacchi e a valutare gli eventi stessi. Lo scopo primario è comprendere lo stato di sicurezza per poter riconoscere incidenti significativi (perdita riservatezza/integrità/disponibilità) e attivare prontamente le necessarie azioni di risposta;
- **Risposta**: questa funzione nelle misure di base NIS 2 si focalizza sulla gestione degli incidenti e sulla resilienza operativa. Comporta la notifica tempestiva degli incidenti significativi al CSIRT Italia, con una pre-notifica entro 24 ore e una completa entro 72 ore, ricevendo supporto. Include l'adozione di piani di continuità operativa e ripristino per ristabilire rapidamente i servizi. Prevede misure per mitigare l'impatto degli incidenti e delle vulnerabilità. Richiede inoltre la possibilità di comunicare (previa consultazione CSIRT Italia) con i destinatari dei servizi potenzialmente colpiti da minacce o incidenti e, se richiesto da ACN, con gli stakeholder. Questa funzione è cruciale per l'effettiva resilienza del Soggetto NIS;
- **Ripristino**: questa funzione nelle misure di base NIS 2, è volta a recuperare le capacità operative dei Soggetti NIS a seguito di incidenti. Comporta la definizione e attuazione di un piano di continuità operativa e ripristino, basato sulla valutazione dei rischi. Tale piano deve includere procedure per il ripristino del normale funzionamento, specificando ruoli, responsabilità e risorse necessarie, come backup e ridondanze. È fondamentale che il piano venga testato, riesaminato e aggiornato per stabilire obiettivi di recupero. Costituisce una parte essenziale della gestione incidenti ed è cruciale per la resilienza complessiva.

> *Il Framework Nazionale per la Cybersecurity e la Data Protection, identificato dall'ACN, come precedentemente indicato, costituisce uno strumento per valutare la postura di sicurezza di un'organizzazione in termini di maturità e completamento delle attività mirate a ridurre il rischio cibernetico. Inoltre, esso permette di prendere in considerazione gli aspetti legati alla protezione dei dati previsti dal GDPR. Pertanto, il Framework offre un'analisi approfondita delle diverse dimensioni relative alla cybersecurity.*

Fasi principali e attività

Il progetto prevede la realizzazione di un intervento di Gap Analysis con l'articolazione nelle fasi principali riepilogata nella tabella seguente.

FASE	AMBITO	ATTIVITA' NELL'AMBITO D'INTERVENTO
1	Organizzazione e pianificazione delle attività	• Incontro con i referenti aziendali per la condivisione dell'impostazione e del calendario delle attività del progetto • Costituzione gruppo di lavoro (componenti interni aziendali e consulenti incaricati) • Riunione informativa del gruppo di lavoro e condivisione degli obiettivi, definizione del dominio di assessment e degli asset informativi e delle attività di progetto *La definizione del dominio di assessment finalizza e limita l'ambito di azione di tutte le attività successive di assessment definendo, inoltre, gli interlocutori con cui rapportarsi per lo sviluppo di tutto l'assessment*
2	Analisi del contesto aziendale	Raccolta documentazione aziendale esistente in riferimento agli adempimenti delle Normative NIS 2 e ad ambiti correlati
		Analisi della documentazione aziendale acquisita
		Individuazione dei Responsabili e/o dei Collaboratori da cui raccogliere informazioni
		Colloqui di approfondimento con Responsabili e/o Collaboratori
		Consolidamento con categorizzazione informazioni e individuazione ambiti rilevanti
3	Gap Analysis per la valutazione della conformità	Valutazione dello stato di attuazione degli adempimenti, di applicazione delle misure di sicurezza e del loro allineamento a quanto richiesto dalle Normative NIS 2 e GDPR
		Individuazione delle aree di adeguamento a quanto richiesto dalle Normative NIS 2 e GDPR per il superamento delle criticità rilevate
4	Presentazione e discussione degli esiti della valutazione	Redazione della relazione illustrativa dell'analisi e delle valutazioni svolte, con indicazione delle eventuali aree di adeguamento individuate
		Incontro con i referenti aziendali per la presentazione, discussione e condivisione degli esiti delle valutazioni svolte, delle eventuali aree di adeguamento individuate per l'aggiornamento del sistema di gestione della sicurezza delle informazioni e delle proposte per l'attuazione
5	Predisposizione e trasmissione della versione condivisa della relazione illustrativa della valutazione svolta	Predisposizione e trasmissione ai referenti aziendali della versione condivisa della relazione illustrativa, delle valutazioni svolte e delle eventuali aree di adeguamento individuate per l'aggiornamento del sistema di gestione della sicurezza delle informazioni e delle proposte per l'attuazione

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.