La “struttura” prevista dalla Legge 90/2024

Il governo della sicurezza IT e della privacy

Informazioni documento
Versione 3.0
2 luglio 2026

Credits & copyright

Ing. Francesco Volani
Computer Systems Engineer - MEng - MBCS - CITP® - CISA® - CISM® - CRISC® - CGEIT® - CDPSE® - CSA STAR™ - CPMA - CPSM - ISO/IEC 27001 LA / 20000 LA / 42001 AI MSA - ISO 22301 LA - ISO 19011 - NIST CSF - COBIT® - ITIL®

Questo documento è di proprietà di FV Engineering. La condivisione e la divulgazione sono autorizzate, a condizione di citare correttamente la fonte. Il file originale è disponibile per il download su www.fvengineering.eu.

Il presente documento analizza e indirizza l’istituzione di una *struttura di governo per la sicurezza informatica* che si affianchi oppure si integri alle esistenti strutture organizzative che si occupano di protezione del dato alla luce delle previsioni della **Direttiva NIS2**[1] (*Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione*), delle recenti disposizioni della **legge 90/2024**[2] (*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*), del **GDPR** (*Regolamento generale sulla protezione dei dati*), delle **determinazioni, linee guida, regolamenti e raccomandazioni di ACN**[3] e delle **best practices e degli standard internazionali di settore**[4].

---

[1] Decreto Legislativo 4 settembre 2024, n.138 riguardante il Recepimento della Direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell’Unione (NIS2).

[2] Alla legge è seguito il recente DPCM uscito in Gazzetta Ufficiale il 5 maggio 2025 (*Disciplina dei contratti di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici e della sicurezza nazionale*) che declina l’art. 14 comma 1 relativamente agli elementi essenziali di cybersicurezza nella disciplina dei contratti di beni e servizi informatici.

[3] ACN, Determinazioni del Direttore Generale dell’Agenzia per la cybersicurezza nazionale di cui all’art. 31 del Decreto Legislativo 4 settembre 2024, n. 138; ACN, Determinazioni del Direttore Generale dell’Agenzia per la cybersicurezza nazionale di cui all’art. 7, comma 6 del Decreto Legislativo 4 settembre 2024, n. 138; ACN, Linee Guida per il rafforzamento della resilienza dei soggetti di cui all’articolo 1, comma 1, della Legge 28 giugno 2024, n. 90. Novembre 2024; ACN, Regolamento per le infrastrutture digitali e per i servizi cloud per la Pubblica Amministrazione (Regolamento 221); ACN, La minaccia cibernetica al settore sanitario - Analisi e raccomandazioni, gennaio 2023-marzo 2025; ACN, Guida alla notifica degli incidenti al CSIRT Italia; ACN, Ransomware - Caratteristiche, preparazione e risposta agli attacchi ransomware, 19 dicembre 2024; ACN, La tassonomia cyber dell’ACN - Definizione della tassonomia cyber dell’Agenzia per la cybersicurezza nazionale, 31 luglio 2024. Per un elenco esaustivo fare riferimento ai riferimenti normativi in Appendice.

[4] Quali, a titolo d’esempio, gli standard ISO/IEC 27001:2022 (Information security, cybersecurity and privacy protection), ISO/IEC 27005:2022 (Information security risks), ISO 31000:2018 (Risk management), ISO/IEC 42001:2023 (Artificial intelligence), il NIST Cybersecurity Framework (CSF), il Framework Nazionale per la Cybersecurity e la Data Protection, il framework COBIT 2019.

La protezione del dato: sicurezza IT e privacy

La sicurezza IT[5] e la privacy hanno implicazioni in parte sovrapposte perchè, a titolo diverso, si occupano - in ultima sintesi - della *protezione del dato* che assume valore di *asset critico aziendale* per garantire servizi di qualità e in sicurezza[6].

Tuttavia è doveroso evidenziare che, seppur vi siano aspetti di sovrapposizione, i due ambiti non devono essere confusi perché hanno anche autonoma declinazione.

La sicurezza IT, infatti, si occupa primariamente della *messa in protezione dei servizi tecnologici* (quali reti, sistemi, applicazioni, tecnologie e più in generale dispositivi IoT[7] connessi), degli archivi digitali, della continuità operativa e della gestione degli incidenti informatici, all'interno di un contesto regolamentato da policy e procedure operative e con un approccio basato sul contenimento del rischio informatico. La privacy completa questo quadro focalizzandosi sulla *dimensione di riservatezza del dato personale* e sulla sua movimentazione tra soggetti incaricati a trattarlo, con una forte connotazione di conformità normativa al GDPR, alla regolamentazione di settore e ponendo al centro delle riflessioni l'interessato al trattamento.

Le emergenti sfide legate all'interoperabilità del dato e all'intelligenza artificiale toccano trasversalmente sia aspetti di sicurezza IT sia aspetti di privacy così come richiamato dalle recenti normative europee quali la già citata **Direttiva NIS2**, l'AI Act (**Regolamento sull'Intelligenza Artificiale**), il Cyberresilience Act (**Regolamento sulla cyberresilenza**), il Cybersecurity Act (**Regolamento sulla cybersicurezza**) e il Data Governance Act (**Regolamento sulla governance dei dati**) che formano un robusto quadro normativo volto a garantire che tutte le tecnologie digitali operino in modo affidabile, sicuro e rispettoso dei diritti fondamentali, con particolare riferimento alla privacy e alla protezione dei dati.

[5] Nel presente documento con "sicurezza IT" si intendono sia gli ambiti di information security sia quelli di cybersecurity. Per non generare confusione nella lettura si è preferito utilizzare un unico termine generale.
[6] Lo stesso standard ISO/IEC 27001:2022 è stato di recente intitolato "Information security, cybersecurity and privacy protection — Information security management systems — Requirements" evidenziando molto bene la compresenza dei temi di sicurezza IT e privacy sotto un medesimo standard per la protezione delle informazioni.
[7] I dispositivi IoT (Internet of Things) si riferiscono a un'ampia gamma di oggetti fisici connessi a Internet che raccolgono e scambiano dati, o che controllano infrastrutture critiche. L'integrazione di dispositivi IoT all'interno dell'ecosistema tecnologico è fondamentale per promuovere l'automazione, l'efficienza e il monitoraggio avanzato, ma presenta anche sfide di sicurezza significative a causa delle vulnerabilità intrinseche di alcuni di essi, dovute a diffusione capillare, basso livello di gestione e rapida obsolescenza.

La normativa vigente orientata alla protezione del dato

L'attuale quadro normativo orientato alla protezione del dato, può essere sintetizzato nel seguente:

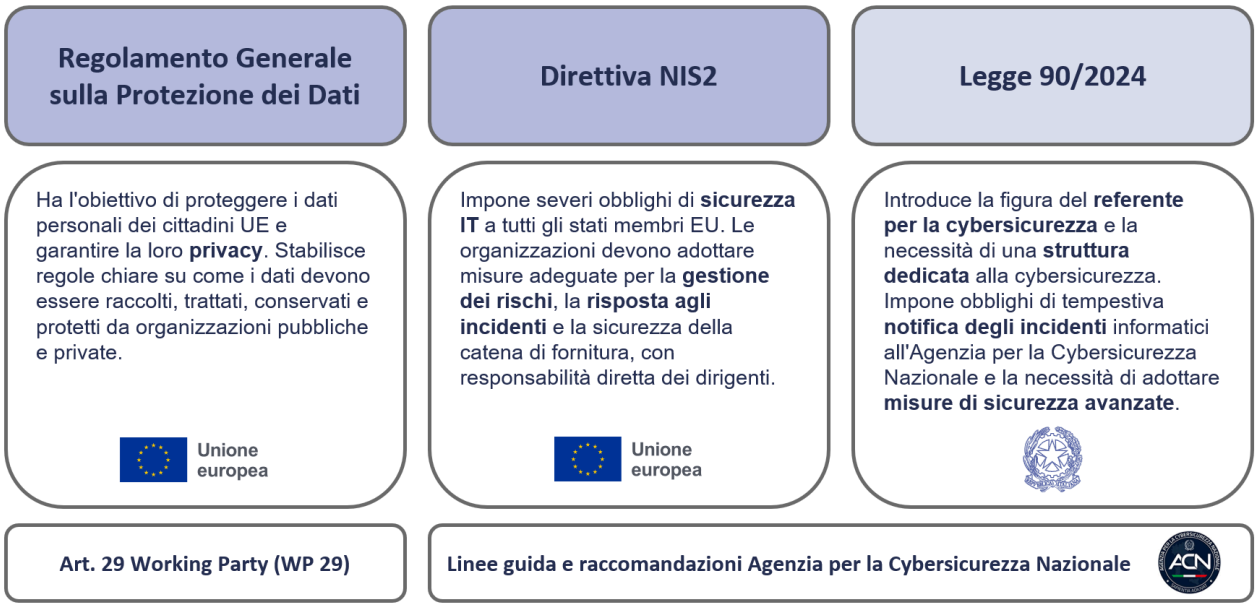
1. **GDPR e Codice della Privacy (D.lgs. 196/2003)**
   Il Regolamento (UE) 2016/679 (GDPR) stabilisce le linee guida per la protezione dei dati personali nell'Unione Europea. In Italia, è integrato dal Codice della Privacy, aggiornato dal D.lgs. 101/2018, che armonizza la normativa nazionale con il GDPR.

2. **Direttiva NIS2 (D.lgs. 138/2024)**
   La Direttiva (UE) 2022/2555 (NIS2) mira a rafforzare la sicurezza delle reti e dei sistemi informativi nell'UE. È stata recepita in Italia con il D.lgs. 138/2024, che amplia l'ambito di applicazione, distingue tra soggetti essenziali e importanti e introduce requisiti più stringenti per la gestione del rischio informatico e la notifica degli incidenti.

3. **Legge 90/2024**
   La Legge 28 giugno 2024, n. 90 (Legge 90/2024) rafforza la cybersicurezza nazionale, introducendo misure specifiche e inasprendo le sanzioni per i reati informatici. La legge si articola in due capi:

   - Capo I: rafforza le misure di cybersicurezza, imponendo di nominare un referente per la cybersicurezza, istituire strutture dedicate e adottare misure in caso di incidenti informatici;
   - Capo II: introduce modifiche al Codice Penale, inasprendo le pene per i reati informatici e introducendo il nuovo reato di estorsione informatica.

Mediante uno schema di sintesi:



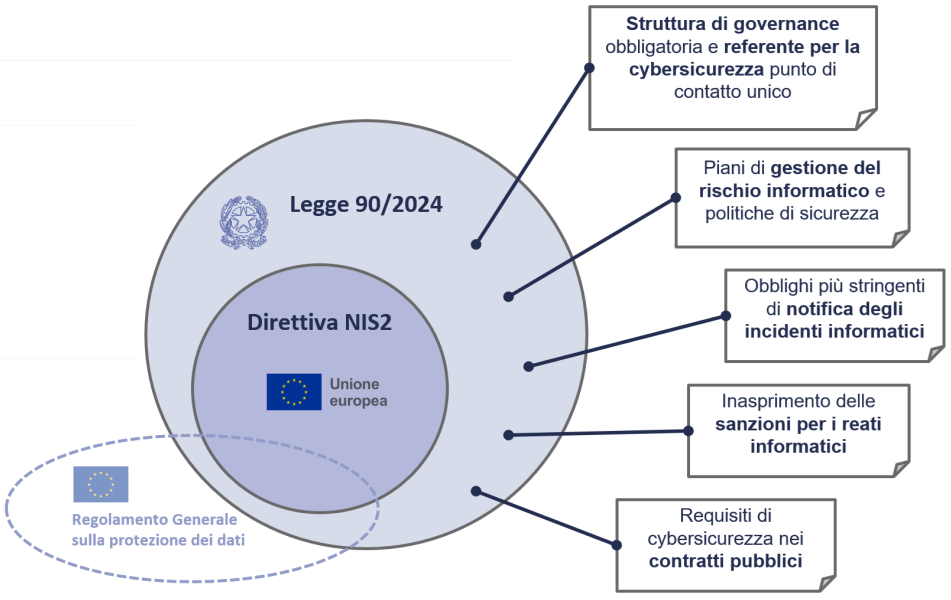
La Direttiva NIS2, recepita in Italia con il D.lgs. 138/2024, rafforza i requisiti di sicurezza e introduce misure di supervisione e requisiti di applicazione più rigorosi, con specifico riferimento agli articoli 24 e 25 che indicano espressamente una serie di misure di sicurezza tecniche e organizzative per contrastare le minacce informatiche riassumibili nelle seguenti:

- politiche di analisi dei rischi e di sicurezza dei sistemi informativi
- procedure di gestione degli incidenti
- gestione delle crisi e continuità operativa
- sicurezza della supply chain
- sicurezza dell'acquisizione, dello sviluppo e della manutenzione della rete e dei sistemi informativi; gestione e divulgazione delle vulnerabilità
- strategie e procedure per verificare l'efficacia delle misure di gestione dei rischi cyber
- pratiche di igiene informatica di base e formazione in materia di cybersecurity
- politiche e procedure relative all'uso della crittografia e della cifratura
- sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi
- sistemi di identificazione e autenticazione a più fattori o continua, e di comunicazione protetta
- obbligo di segnalazione e notifica al Computer Security Incident Response Team (CSIRT)

La Legge 90/2024 introduce *specificità operative e organizzative* che vanno oltre le disposizioni della Direttiva NIS2, adattandole al contesto nazionale italiano. Queste possono essere riassunte dalle seguenti:

- istituzione di una *struttura di governance* e nomina di un *referente per la cybersicurezza*
- predisposizione di piani per la gestione del rischio informatico e politiche di sicurezza
- obblighi stringenti di notifica degli incidenti informatici
- inasprimento delle sanzioni per i reati informatici
- introduzione di requisiti di cyber sicurezza nei contratti pubblici

E' possibile visualizzare il rapporto tra le varie normative mediante il seguente schema di sintesi:



Alla luce delle previsioni della legge 90/2024 risulta importante comprendere il ruolo della struttura richiamata all'art. 8 comma 1, finalizzata al governo della sicurezza informatica.

Tale nuovo *soggetto organizzativo* può integrare in maniera complementare le competenze già presenti in materia di privacy operando quale "seconda linea di difesa" per tutti gli aspetti riconducibili alla protezione del dato: la *proposta* delineata è quindi quella di considerare un'unica struttura deputata alla sicurezza IT e alla privacy per i motivi di seguito elencati.

- **Previsione di legge**: la struttura per la sicurezza IT è prevista dalla recente legge 90/2024 con precisi ambiti di responsabilità. Inoltre è prevista la figura del *referente* per la cybersicurezza a capo della suddetta struttura con precisi compiti di presidio del rischio e punto unico di contatto verso le istituzioni preposte alla cybersicurezza nazionale[8]. Più in generale, l'applicazione del Decreto NIS, sollecitata dalla Determinazione ACN del 14 aprile 2025, evidenzia il ruolo di diretta responsabilità degli organi apicali aziendali[9] che può essere efficacemente esercitato con un'adeguata struttura di staff a governo degli ambiti di sicurezza IT e privacy;

- **Responsabilità in capo alla struttura per la sicurezza IT**: la legge 90/2024 evidenzia in maniera puntuale specifiche responsabilità in capo alla struttura per la sicurezza IT, che all'art. 8 sono elencate nelle seguenti[10]:
    - sviluppo delle politiche e delle procedure di sicurezza delle informazioni

[8] Il referente deve possedere "specifiche e comprovate professionalità e competenze in materia di cybersicurezza" (art. 8 comma 2). Tale previsione può sintetizzarsi in esperienza, formazione, conoscenze ed eventuali certificazioni possedute. È preferibile che il referente abbia una laurea in informatica o discipline affini e una pluriennale esperienza nel settore della sicurezza IT e della protezione del dato. Deve avere una conoscenza delle principali normative e standard di sicurezza informatica, oltre a capacità di analisi e problem-solving. Sebbene non siano obbligatorie per legge, le certificazioni in ambito cybersecurity sono considerate un valore aggiunto significativo e possono aiutare a dimostrare le competenze. Alcune delle certificazioni tra le più riconosciute includono CISSP, CISM e le certificazioni ISO.

[9] Determinazione ACN, Art. 2 (Adozione delle specifiche di base). 1. In fase di prima applicazione del decreto NIS sono adottate le specifiche di base di cui agli allegati 1, 2, 3 e 4, facenti parte integrante della presente determinazione. 2. Le misure di sicurezza di base, a carico degli organi di amministrazione e direttivi e in materia di misure di gestione dei rischi per la sicurezza informatica, sono stabiliti: a) per i soggetti importanti, nell'allegato 1; b) per i soggetti essenziali, nell'allegato 2. 3. Gli incidenti significativi di base sono stabiliti: a) per i soggetti importanti, nell'allegato 3; b) per i soggetti essenziali, nell'allegato 4.

[10] Legge 90/2024, Art. 8 (Rafforzamento della resilienza delle pubbliche amministrazioni e referente per la cybersicurezza). Comma 1. I soggetti di cui all'articolo 1, comma 1, individuano, ove non sia gia' presente, una struttura, anche tra quelle esistenti, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente, che provvede: a) allo sviluppo delle politiche e delle procedure di sicurezza delle informazioni; b) alla produzione e all'aggiornamento di sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico; c) alla produzione e all'aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione; d) alla produzione e all'aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'amministrazione; e) alla pianificazione e all'attuazione di interventi di potenziamento delle capacita' per la gestione dei rischi informatici, in coerenza con i piani di cui alle lettere b) e d); f) alla pianificazione e all'attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la cybersicurezza nazionale; g) al monitoraggio e alla valutazione continua delle minacce alla sicurezza e delle vulnerabilita' dei sistemi per il loro pronto aggiornamento di sicurezza.

- produzione e aggiornamento di sistemi di analisi preventiva e rilevamento e di un piano per la gestione del rischio informatico
- produzione e aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione
- produzione e aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'amministrazione
- pianificazione e attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici
- pianificazione e attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la cybersicurezza nazionale
- monitoraggio e valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza

Le responsabilità richiamate dalla legge 90/2024 promuovono aspetti di *governance* che dovrebbero integrarsi ed orchestrarsi in maniera virtuosa con le attività di *management* svolte dalla complessiva articolazione aziendale;

- **Centralità della funzione sicurezza informatica**: la legge 90/2024 sottolinea l'importanza cruciale della sicurezza informatica per la resilienza operativa digitale delle pubbliche amministrazioni e delle infrastrutture critiche. Un posizionamento della funzione di governo della sicurezza informatica e privacy in staff all'Alta Direzione risponde a questa necessità di centralità, garantendo un diretto riporto e allineamento strategico con i vertici aziendali[11], una complessiva visione di insieme e una più efficace comunicazione con tutti i soggetti interessati: la struttura si pone infatti quale funzione di coordinamento e supervisione di tutte le attività in ambito sicurezza IT e privacy operate dalle funzioni aziendali di taglio più operativo;

- **Separazione tra governo e gestione operativa della sicurezza IT e della privacy**: la separazione tra funzioni di governo (seconda linea di difesa) e funzioni di gestione (prima linea di difesa) permette un corretto disaccoppiamento tra esigenze operative ed esigenze di presidio del rischio[12], promuovendo una virtuosa collaborazione e comunicazione tra ambiti aziendali che, altrimenti, opererebbero esclusivamente a "silos";

- **Supervisione e approccio trasversale alla sicurezza e alla privacy**: un corretto posizionamento apicale permette alla struttura di porsi a copertura di tutti gli ambiti di necessità aziendale interessati alla sicurezza tecnologica e alla protezione del dato, promuovendo la separazione tra compiti di indirizzo e controllo (seconda linea di difesa) da quelli operativi (prima linea di difesa) e garantendo allo stesso tempo un'efficace orchestrazione delle esigenze di sicurezza del dato tra le varie articolazioni aziendali. Le tematiche di governo della sicurezza IT e della privacy toccano infatti non solo ambiti tecnici ma anche ambiti organizzativi e di processo: si pensi ad esempio al tema dell'identità digitale, che implica aspetti di organizzazione delle risorse umane, di accesso

[11] Nello specifico ambito della privacy, sia con il Titolare al Trattamento che con il DPO aziendale

[12] Si attua infatti la separazione dei ruoli per non generare potenziali conflitti di interesse e permettere alla sicurezza IT di operare con indipendenza e corretto riporto apicale.

fisico e controllato a dati e locali, di accesso logico ad informazioni critiche e sensibili, di mobilità e gestione del dato tra sistemi “periferici” e sistemi centralizzati, di trattamento ai fini privacy, di condivisione tra soggetti privati e istituzionali diversi;

- **Interconnessione tra sicurezza e privacy**: la sicurezza informatica è un pilastro fondamentale per garantire la protezione dei dati personali e il rispetto della normativa privacy (GDPR e normativa nazionale). Integrare le competenze di sicurezza IT con quelle della privacy in un’unica struttura favorisce una visione integrata e una gestione coordinata degli aspetti legati alla protezione del dato, promuovendo i principi di *security by design* e *privacy by design* richiesti dalle normative. L’analisi del rischio IT, richiamata dalla legge 90/2024 e dalla Direttiva NIS2, diventa pertanto pervasiva, coprendo l’intero perimetro di protezione dell’informazione, sia in termini di riservatezza, che in termini di integrità e disponibilità. Ad esempio, la gestione di incidenti informatici e la conseguente valutazione e notifica di potenziali “data breach” secondo l’art. 33 del GDPR diventa un processo integrato, dove necessità di ripristino in sicurezza si integrano con gli obblighi di notifica agli enti preposti (Garante Privacy, CSIRT Italia). E’ inoltre opportuno ricordare che l’analisi del rischio e l’individuazione delle misure di sicurezza è attività prevista e normata anche dagli art. 32 e 35 del GDPR, ricalcando lato privacy il processo di analisi e gestione del rischio informatico previsto dall’art. 8 della legge 90/2024 in ambito sicurezza IT: ciò conferma in buona parte la sovrapposizione dei due ambiti e l’opportunità di una virtuosa convergenza tra le tematiche di sicurezza IT e di privacy.

- **Approccio olistico alla protezione dei dati**: un'unica struttura permette di sviluppare e implementare in maniera omogenea politiche e procedure che affrontano sia gli aspetti di sicurezza tecnologica (prevenzione degli attacchi, gestione degli incidenti, ecc.) sia gli aspetti legali e organizzativi della protezione dei dati personali (gestione dei consensi, diritti degli interessati, valutazione d'impatto, polizze cyber ecc.) sia infine gli sfidanti aspetti emergenti legati all’uso dell’intelligenza artificiale e alla movimentazione su larga scala del dato aziendale. Le iniziative legate alla ricerca e alla gestione di grandi moli di dati, anche mediante l'utilizzo dell'Intelligenza Artificiale (AI), devono essere opportunamente intercettate, coordinate ed orchestrate tra necessità di compliance normativa, esigenze organizzative ed implementazioni tecniche, promuovendo un adeguato presidio del rischio mediante opportune misure di prevenzione e protezione;

- **Efficienza ed ottimizzazione delle risorse**: concentrare le competenze di sicurezza informatica e privacy in un'unica struttura può portare a una maggiore efficienza nell'utilizzo delle risorse umane e finanziarie, evitando duplicazioni di ruoli e responsabilità, efficientando attività che hanno numerose sovrapposizioni in termini organizzativi ed esecutivi. Si pensi, ad esempio, alla gestione di un incidente, che ha impatti sul piano normativo, legale, contrattuale, tecnico ed organizzativo;

Vantaggi di una struttura unica per il governo della sicurezza IT e della privacy in Staff all’Alta Direzione individuata possono essere riassunti nei punti che seguono:

- **Allineamento Strategico**: la struttura permetterebbe un più efficace allineamento con gli obiettivi strategici della Direzione Generale, garantendo che la sicurezza informatica e la privacy siano considerate priorità aziendali e driver all'interno degli indirizzi strategici per la gestione del dato aziendale e per il presidio del rischio;

- **Separazione tra governo e gestione:** una struttura di vertice permetterebbe di separare le valutazioni e le scelte strategiche di sicurezza basate sul rischio dalle attività gestionali svolte dalle varie articolazioni aziendali, evitando il conflitto di interesse tra esigenze di sicurezza e scelte operative.

- **Coordinamento e comunicazione**: verrebbe notevolmente semplificato il coordinamento tra le diverse funzioni aziendali coinvolte nella sicurezza e nella privacy (IT, legale, risorse umane, DPO ecc...) promuovendo ed orchestrando, allo stesso tempo, la comunicazione tra le unità organizzative coinvolte, superando in tal modo l'esecuzione di attività per mero ambito di competenza (a "silos");

- **Visione integrata dei rischi**: la struttura promuoverebbe una valutazione e gestione più efficace dei rischi interconnessi tra sicurezza informatica e protezione dei dati personali, integrando le valutazioni con i servizi e le strutture che si occupano in maniera più estesa di rischio aziendale (es. Servizio Prevenzione e Protezione, Servizio Legale ecc...);

- **Programmazione e promozione della sicurezza IT**: la struttura fungerebbe da soggetto supervisore e di coordinamento di tutte le iniziative individuate nel "piano programmatico della sicurezza" previsto dalla legge 90/2024 per contenere il rischio informatico. Inoltre promuoverebbe l'adozione, entro le scadenze stabilite, delle misure obbligatorie previste dalle determinazioni e linee guida per la cybersicurezza emanate dall'Agenzia per la Cybersicurezza Nazionale (ACN)

- **Risposta unitaria agli incidenti**: in caso di incidenti di sicurezza che coinvolgono dati personali e sensibili, una struttura unica permetterebbe di gestire la risposta in modo più coordinato ed efficiente, sia dal punto di vista tecnico che legale, nel rispetto delle tempistiche di intervento e notifica previste dalla normativa[13];

- **Consistenza e conformità normativa delle politiche di sicurezza**: una struttura di vertice promuoverebbe lo sviluppo e l'implementazione di politiche e procedure coerenti e integrate in materia di sicurezza informatica e privacy, con una più rapida validazione sul piano normativo e legale;

- **Comunicazione semplificata**: un unico punto di contatto per le questioni relative al governo della sicurezza informatica e alla privacy semplificherebbe la comunicazione interna ed esterna (es. con l'Autorità Garante per la protezione dei dati personali, con ACN oppure con il CSIRT Italia). Si promuoverebbe anche una più efficace collaborazione con il DPO aziendale, con il servizio prevenzione e protezione e con il servizio legale;

[13] Ciò anche in forza della figura del *referente per la cybersicurezza* previsto dalla legge 90/2024 art.8 comma 2 che è chiamato a svolgere la funzione di punto di contatto unico dell'amministrazione con l'Agenzia per la cybersicurezza nazionale in relazione a quanto previsto dalla legge e dalle normative settoriali in materia di cybersicurezza cui è soggetta l'amministrazione.

- **Cultura della sicurezza e della privacy**: una struttura di vertice potrebbe efficacemente promuovere una cultura aziendale in cui la sicurezza informatica e la protezione dei dati sono considerate responsabilità condivise e integrate.

In sintesi, istituire una struttura per la sicurezza informatica in staff all'Alta Direzione che includa anche la competenza in materia di privacy rappresenta una soluzione strategica vantaggiosa, in linea con la crescente importanza della sicurezza informatica e la stretta correlazione con la protezione dei dati personali evidenziata dalla recente legge 90/2024, dalle previsioni della Direttiva NIS2, dal GDPR e dai citati standard di settore.

Posizionare la sicurezza informatica e la privacy in staff all'Alta Direzione può pertanto garantire che le politiche di sicurezza siano allineate con gli obiettivi aziendali e che ci sia un impegno diretto da parte della leadership nella promozione di un ambiente digitale sicuro. Inoltre promuoverebbe una supervisione ed orchestrazione delle iniziative tecnico-operative in ambito sicurezza promosse dalle varie unità organizzative, rendendole omogenee, coerenti e comunicanti all'interno di un quadro unico di gestione e contenimento del rischio.