RIVISTA ITALIANA
DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 1/2026 • DOI 10.32091/RIID0268 • articolo sottoposto a peer review • pubblicato in anteprima il 17 apr. 2026

Giovanni Comandè – Chiara Nasi

Oltre la Conformità: dalle scelte strategiche ISO e NIST 2.0 alla gestione proattiva del rischio

Il panorama digitale odierno richiede un approccio strategico alla sicurezza informatica. Questo studio presenta un modello operativo e pragmatico progettato per semplificare la complessa conformità normativa in un sistema di gestione aziendale facilmente applicabile. Il Modello si basa su un allineamento multilivello tra le misure di sicurezza operative e i due pilastri normativi internazionali: ISO/IEC 27001:2022 e NIST *Cybersecurity Framework* (CSF) 2.0. La metodologia utilizzata ha permesso di generare una mappatura innovativa che associa le misure operative ai controlli ISO e alle categorie NIST. L'utilità pratica del Modello è dimostrata come strumento di adattamento cruciale per le organizzazioni (note come "entità NIS") soggette agli obblighi della direttiva NIS2. Ciò consente l'implementazione operativa degli elementi essenziali di gestione del rischio richiesti dalla normativa. Il Modello è progettato per essere scalabile a qualsiasi quadro normativo, riducendo i costi di conformità e massimizzando l'efficacia operativa. In prospettiva, lo stesso mira ad evolversi in un sistema quantitativo di misurazione della sicurezza IT, fornendo alle organizzazioni un mezzo tangibile per dimostrare il proprio livello di sicurezza informatica.

Cybersicurezza – Conformità – Misure di sicurezza – ISO/IEC 27001:2022 – NIST CSF 2.0

Beyond Compliance: from ISO and NIST 2.0 strategic choices to proactive risk management

Today's digital landscape requires a strategic approach to cybersecurity. This study presents a model (hereinafter also "Smartlex Model"), an operational and pragmatic model designed to simplify complex regulatory compliance into an easily applicable business management system. The Model is based on a multi-level alignment between operational security measures and the two international regulatory pillars: ISO/IEC 27001:2022 and the NIST Cybersecurity Framework (CSF) 2.0. The methodology generates an innovative mapping that associates operational measures with ISO controls and NIST categories. The practical usefulness of the Model is demonstrated as a crucial adaptation tool for organisations (known as "NIS entities") subject to the obligations of the NIS2 Directive. This allows for the operational implementation of the essential risk management elements required by the regulation. The Model is designed to be scalable to any regulatory framework, reducing compliance costs and maximising operational effectiveness. Looking ahead, the Smartlex Model aims to evolve into a quantitative IT security measurement system, providing organizations with a tangible means of demonstrating their cybersecurity posture.

Cybersecurity – Compliance – Security Measures – ISO/IEC 27001:2022 – NIST CSF 2.0

G. Comandè è professore ordinario di Diritto privato comparato alla Scuola Superiore Sant'Anna e fondatore di Smartlex s.r.l. e di Inlesi s.r.l.

C. Nasi è esperta in regolamentazione e conformità dell'Unione europea presso Smartlex s.r.l.

This research is part of the PQ-NEXT project, funded by the European Union through the European Cybersecurity Competence Center under the Grant Agreement number 101225759

1. Introduzione

L'attuale panorama digitale è caratterizzato da un'esposizione sempre più evidente a rischi per lo più di natura informatica inerenti alla divulgazione non autorizzata di dati personali e non. Di fronte a minacce in continua evoluzione[1], ogni organizzazione è chiamata, ormai, a considerare la cybersecurity non più come un'opzione, bensì come un imperativo strategico. È fondamentale, infatti, che ogni organizzazione si impegni ad adottare una gestione proattiva e strutturata della sicurezza delle informazioni in luogo di un approccio meramente reattivo. Benché auspicabile, tale finalità presenta rilevanti criticità operative: raggiungere questo obiettivo è infatti difficile senza una mappatura coerente dei processi e dei rischi, idealmente trasformabile in uno strumento pratico per la conformità legale e organizzativa.

Questo studio ha l'intento di iniziare a colmare questo gap. Esso si pone infatti l'obiettivo principale di tradurre le complesse direttive ed i framework in materia di sicurezza in un modello operativo e facilmente applicabile da ogni realtà aziendale o pubblica, con lo scopo di soddisfarne le esigenze operative di compliance. Sebbene questo sia solo un primo piccolo passo, il potenziale di ulteriore sviluppo, sia pratico che teorico, è considerevole.

A tal fine, verrà illustrata un'opera di allineamento che associa le misure di sicurezza delle informazioni adottate quotidianamente nel contesto operativo aziendale e pubblico con due pilastri fondamentali della cybersecurity a livello internazionale:

- lo standard ISO/IEC 27001:2022, che fornisce un quadro per un Sistema di Gestione della Sicurezza delle Informazioni (ISMS) e
- il NIST *Cybersecurity Framework 2.0* (CSF)[2], che, invece, individua una serie di linee guida preordinate al miglioramento della gestione dei rischi di cybersicurezza in quelle che sono classificate come infrastrutture critiche[3].

1. Per una panoramica delle più recenti minacce informatiche e delle relative strategie difensive, si veda Obi–Akagha–Dawodu et al. 2024.
2. V. National Institute of Standards and Technology (di seguito NIST), *The NIST Cybersecurity Framework (CSF) 2.0*, 2024.
3. Sul punto, si veda Direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio. La direttiva si applica a undici settori considerati critici, e cioè: Energia; Trasporti; Settore bancario; Infrastrutture dei mercati finanziari; Salute; Acqua potabile; Acque reflue; Infrastrutture digitali; Enti della pubblica amministrazione; Spazio; Produzione, trasformazione e distribuzione di alimenti.

Il risultato di un simile allineamento ha permesso di strutturare un sistema che risulti, allo stesso tempo:

- conforme, in quanto aderisce allo standard ISO;
- orientato al rischio, attraverso i principi del CSF e
- pragmatico, in quanto adattato alle effettive esigenze operative dell'organizzazione.

L'integrazione di questi tre livelli – operativo, normativo (ISO) e strategico (CSF) – crea una sinergia che non solo consente di garantire la conformità, ma rafforza altresì l'intero sistema di sicurezza dell'organizzazione[4]. Ciò ancor più considerando l'introduzione – tanto per le strutture private quanto per la Pubblica Amministrazione – di recenti obblighi in materia di sicurezza delle reti e dei sistemi informativi introdotti ad opera della c.d. Direttiva NIS2 (Direttiva UE 2022/2555)[5]. L'Italia ha infatti recentemente introdotto significativi obblighi in materia di sicurezza delle reti e delle informazioni sia per gli enti privati che per la Pubblica Amministrazione ai sensi della Direttiva NIS2, recepita a livello nazionale con il decreto legislativo n. 138/2024[6] ed ulteriormente collegata alla legge italiana n. 90 del 2024[7] (anche nota come "Legge sulla Cybersecurity").

Introdotta nel dicembre 2022, la direttiva NIS2 ha ampliato il proprio ambito di applicazione a circa 100.000 organizzazioni, tra cui enti pubblici, infrastrutture critiche e fornitori di servizi digitali. Tra le altre cose, essa richiede la gestione dei rischi, una rigorosa segnalazione degli incidenti, la sicurezza della catena di approvvigionamento, la responsabilità dei dirigenti e sanzioni fino a 10 milioni di euro o al 2% del fatturato globale. In un simile scenario, la conformità non costituisce solo un obbligo burocratico, bensì una priorità assoluta per la protezione dell'organizzazione.

Come si avrà modo di illustrare, il lavoro presentato in questo articolo non costituisce un esercizio puramente teorico, ma mira a fornire uno strumento pratico che trasforma l'analisi concettuale in un quadro attuabile, per tradurre i requisiti di sicurezza in un sistema di protezione coerente e dimostrabile. Il principale contributo innovativo dello studio consiste, infatti, nel convertire questo allineamento in un quadro con implicazioni operative immediate, tangibili e scalabili. Progettata per adattarsi alle future architetture normative, la mappatura mira a ridurre i costi di conformità, migliorando al contempo l'efficacia delle misure implementate.

Inoltre, la metodologia sino a qui delineata pone le fondamenta per affrontare una delle sfide più complesse della cybersecurity: quella di garantire l'oggettività e la misurabilità delle azioni e dei rischi che esse sono preordinate a mitigare. Essa evidenzia l'impatto sistemico di questa mappatura sulla valutazione dei rischi e introduce un approccio più obiettivo al principio di proporzionalità, alla base della regolamentazione della sicurezza informatica. Sulla base di questi risultati, la ricerca futura si concentrerà sull'evoluzione del Modello in un sistema per la misurazione quantitativa delle prestazioni in materia di sicurezza delle informazioni.

In conclusione, verrà poi esposto un esempio pratico (tratto dal contesto giuridico italiano) dell'utilità e dei vantaggi concreti che le

4. L'integrazione tra ISO/IEC 27001:2022 e CSF è evidente, tanto che i due strumenti possono essere considerati complementari nella gestione dei rischi di cybersecurity: ciascuno dei controlli riportati nel celeberrimo standard sono infatti collocabili all'interno di una delle cinque funzioni di cui si compone – come sarà più avanti illustrato nel dettaglio – il c.d. *Core* del CSF. Tuttavia, recenti studi hanno dimostrato come, tra le cinque funzioni, la più "compatibile" con quasi tutti i controlli di cui alla normativa ISO sia quella nota come "Protect". Sul punto, si veda Malatji 2023.
5. Direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio (Direttiva NIS2).
6. Decreto legislativo del 4 settembre 2024, n. 138, 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.
7. Legge 28 giugno 2024, n. 90, Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici.

organizzazioni possono ottenere grazie all'utilizzo della mappatura realizzata.

2. ISO e NIST 2.0: due modelli a confronto

Prima di illustrare come realizzare un sistema di misure di sicurezza conforme e frutto dell'allineamento tra "realtà" all'apparenza distanti[8], si rende necessario approfondire e contestualizzare, seppur brevemente, i due parametri che verranno in seguito utilizzati per la classificazione: la normativa ISO/IEC 27001:2022 (di seguito, ISO) ed il NIST *Cybersecurity Framework 2.0* (di seguito, CSF o NIST 2.0). Detto approfondimento si rende quantomai opportuno considerando che la costruzione di un sistema di gestione del rischio risulta fortemente influenzata dagli standard e dalle linee su cui si basa.

2.1. Lo standard ISO/IEC 27001

La normativa ISO/IEC 27001:2022[9] (Information security, cybersecurity and privacy protection – Information security management systems - Requirements) è uno standard europeo che, trattando di sicurezza informatica e di sistemi di gestione, individua i requisiti necessari a stabilire, implementare, mantenere e migliorare un sistema di gestione della sicurezza delle informazioni all'interno di un'organizzazione. Si tratta di un documento fortemente incentrato sulla gestione del rischio e, ovviamente, sui relativi controlli necessari per contrastarlo, elencati nel suo Allegato A. Sebbene la versione attuale risalga ad ottobre 2022, lo standard in esame vanta una storia ben più lunga: pubblicato per la prima volta nel 2005, è stato poi oggetto di un'ulteriore importante revisione, avvenuta nel 2013[10].

Le modifiche apportate rispetto a questa versione sono tutt'altro che irrilevanti, e cioè: il nominativo dello standard ed il contenuto del relativo abstract; l'aggiunta di nuovi requisiti; la riorganizzazione dei controlli di cui all'Allegato A[11]. Ciò che rileva maggiormente in questa sede sono, senza dubbio, le modifiche apportate nell'ambito dei controlli. Non solo, infatti, gli stessi sono stati ridotti da centoquattordici a novantatré, ma, originariamente suddivisi in quattordici sezioni[12], sono stati altresì riorganizzati (come sarà più avanti specificato) in sole quattro macro-aree. Al di là della ricollocazione, alcuni di essi sono stati rinominati e/o modificati[13] e all'elenco preesistente ne sono stati aggiunti ben undici nuovi[14]. Sebbene molti di questi aggiornamenti siano principalmente

8. Il lavoro che segue ha l'obiettivo di allineare, sottolineandone le somiglianze, la normativa ISO/IEC e il CSF. Tuttavia, preme sottolineare come, al di là degli evidenti punti di contatto che saranno più avanti messi in risalto, sussistono altresì delle importanti differenze. Si pensi, ad esempio, ai costi, alla possibilità di ottenere una certificazione (nel caso di ISO) ed al grado di maturità del rischio. Sul punto, si veda Alshar'e 2023.
9. "ISO" è l'abbreviazione di *Organization for Standardization*, un'organizzazione internazionale indipendente e non governativa la cui missione consiste nella realizzazione di standard (come quello oggetto della presente analisi) che garantiscano coerenza ed uguaglianza in tutto il mondo. Sul punto, si veda il sito dell'organizzazione: iso.org.
10. Per la storia di questo e degli altri standard, si rimanda al sito dell'ISO.
11. Per un'esaustiva comparazione delle due versioni, si veda Vakhula–Kurii–Opirskyy–Susukailo 2024.
12. Di seguito, l'elenco delle quattordici sezioni di cui alla versione del 2013 (in seguito riorganizzate, per esigenze di semplificazione, in sole quattro macro-aree): A.5 Politiche di sicurezza delle informazioni; A.6 Organizzazione della sicurezza delle informazioni; A.7 Sicurezza delle risorse umane; A.8 Gestione dei beni; A.9 Controllo degli accessi; A.10 Crittografia; A.11 Sicurezza fisica ed ambientale; A.12 Sicurezza delle operazioni; A.13 Sicurezza delle comunicazioni; A.14 Acquisizione, sviluppo e manutenzione del sistema; A.15 Relazioni con i fornitori; A.16 Gestione degli incidenti relativi alla sicurezza delle informazioni; A.17 Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa; A.18 Conformità.
13. Per quanto concerne ciò che maggiormente rileva in questa sede, ovverosia l'Allegato A, preme sottolineare come le modifiche apportate con la versione del 2022, lungi dal rappresentare modifiche di sostanza, sono intervenute, soprattutto, sulla forma: si pensi, ad esempio, alla ridenominazione di alcuni controlli (come il controllo A.6.2.1 Politica per i dispositivi portatili, poi modificato in A.8.1 *Endpoint* degli utenti).
14. Di seguito, gli undici controlli inseriti nella nuova versione nella normativa in esame: A.5.7 *Threat intelligence*; A.5.23 Sicurezza delle informazioni per l'utilizzo dei servizi *cloud*; A.5.30 Prontezza dell'ICT per la continuità

formali, essi hanno uno scopo importante: allineare la norma al panorama tecnologico in evoluzione e garantire la coerenza con il NIST 2.0 (per la sicurezza tecnologica) e con il GDPR (per gli obblighi di sicurezza delle informazioni) a livello europeo.

Dal punto di vista della sua architettura, la ISO 27001 risulta costruita su due pilastri principali:

1) le *Clausole 4-10*[15], ovverosia i requisiti obbligatori per istituire, attuare, mantenere e migliorare il Sistema di Gestione per la Sicurezza delle Informazioni (il come gestire la sicurezza), organizzati secondo il noto ciclo di miglioramento c.d. PDCA (Plan-Do-Check-Act);
2) l'*Allegato A*, da intendersi come catalogo non esclusivo di riferimento delle misure di sicurezza (i c.d. controlli) che le organizzazioni possono (e devono) adottare per mitigare i rischi eventualmente identificati.

Il collegamento tra detti pilastri è rappresentato dalla dichiarazione di applicabilità (c.d. SoA), un fondamentale documento preordinato a dimostrare la coerenza del Sistema di Gestione per la Sicurezza delle Informazioni, sia in termini di gestione dei rischi individuati che in termini di selezione dei controlli appropriati per la mitigazione di quest'ultimi.

Proprio in ragione di dette caratteristiche e, soprattutto, del suo scopo principale di fornire un sistema di organizzazione, implementazione e miglioramento delle misure di sicurezza all'interno di un'organizzazione, è innegabile il ruolo che la normativa in esame svolge anche rispetto alla cybersecurity: quello di quadro di gestione fondamentale. Ciò ancor più considerando i frequenti rimandi effettuati dalla ISO 27001 alla cybersicurezza, soprattutto nell'ambito dei controlli[16].

In sintesi, nel Modello che verrà presentato, un sistema di gestione della sicurezza delle informazioni costruito in conformità con la norma ISO 27001 può essere efficacemente integrato con le funzioni di valutazione dei rischi del quadro NIST per raggiungere un obiettivo comune: garantire un elevato livello di sicurezza delle informazioni insieme a una gestione solida e adeguata dei rischi di sicurezza informatica.

2.2. Il *Cybersecurity Framework (CSF) 2.0* di NIST

A prescindere dal settore o dalle dimensioni, il NIST *Cybersecurity Framework (CSF) 2.0* rappresenta una risorsa essenziale per le organizzazioni che desiderano affrontare la gestione dei rischi di sicurezza informatica in modo metodico[17]. Si tratta, infatti, di una linea guida volontaria (pubblicata per la prima volta nel febbraio 2024) che, seppur realizzata dal *National Institute of Standards and Technology* (NIST)[18] statunitense, gode di un'indiscussa reputazione anche a livello internazionale per la sua primaria utilità[19]: consentire alle organizzazioni di migliorare la propria "postura" di sicurezza informatica allineandosi, così, anche ad altre normative. Si pensi, ad esempio, alla Direttiva NIS2, sulla quale si tornerà in seguito.

operativa; A.7.4 Monitoraggio della sicurezza fisica; A.8.9 Gestione delle configurazioni; A.8.10 Cancellazione delle informazioni; A.8.11 Mascheramento dei dati; A.8.12 Prevenzione di *leakage* delle informazioni; A.8.16 Attività di monitoraggio; A.8.23 *Web filtering*; A.8.28 Sviluppo sicuro.

15. Di seguito l'elenco delle clausole: 4. Contesto dell'organizzazione; 5. Leadership; 6. Pianificazione; 7. Supporto; 8. Attività operative; 9. Valutazione delle prestazioni; 10. Miglioramento.
16. La cybersecurity è infatti un settore considerato dalla normativa ISO sin dal suo principio (ci si riferisce, in particolare, al suo titolo "*Information security, cybersecurity and privacy protection – Information security management systems – Requirements*"), ma non solo: si rinvengono riferimenti rilevanti anche nell'ambito dei controlli, dove sono ad esempio citati i servizi *cloud* (A.5.23), la *Threat Intelligence* (A.5.7), ecc.
17. Quello in esame non esaurisce, però, il novero dei framework in materia di cybersecurity: si pensi, ad esempio, all'Architettura Zero Trust (ZTA). Sul punto, si veda Rose–Borchert–Mitchell–Connelly 2020.
18. Per dettagli sul *National Institute of Standards and Technology* e sui suoi compiti, si rimanda al sito nist.gov.
19. Oltre che per la sua utilità, il CSF è noto altresì per la sua flessibilità, che ne permette non solo l'applicazione ad organizzazioni di diversa natura e dimensione, ma anche la compatibilità con standard di settore come ISO/IEC 27001:2022, altri framework (come il COBIT 5) e quadri normativi come il GDPR e il HIPAA. Sul punto, si veda Lokare–Bankar–Mhaske 2025.

A livello strutturale, il NIST *Cybersecurity Framework 2.0* si compone di tre elementi fondamentali:

1) il *Core*, che individua i risultati desiderati in ambito di cybersecurity, suddividendo gli stessi in Funzioni, Categorie e Sottocategorie;
2) i cc.dd. *Implementation Tiers*, ovverosia quattro livelli di implementazione (*Partial*, *Risk Informed*, *Repeatable*, *Adaptive*) che fungono da parametri di riferimento affinché l'organizzazione valuti il suo approccio alla gestione dei rischi legati alla sicurezza informatica;
3) i cc.dd. *Profiles*, che permettono all'organizzazione di testare il proprio livello di allineamento tra gli obiettivi di business e i requisiti di cybersecurity e di pianificarne eventuali attività di miglioramento.

Ai fini della realizzazione del Modello, tra i tre l'elemento che preme approfondire è il primo e, in particolare, le sei funzioni pensate per offrire una panoramica dei protocolli di sicurezza delle *best practice* che lo compongono, ovverosia[20]:

1) Governo (*Govern*): stabilisce, comunica e monitora la strategia, le aspettative e la politica dell'organizzazione relative alla gestione del rischio di cybersecurity. In sintesi, questa funzione fornisce la direzione e le linee guida necessarie per dare priorità e realizzare gli obiettivi delle altre cinque funzioni del framework;
2) Identificazione (*Identify*): garantisce che i rischi attuali di cybersecurity dell'organizzazione siano pienamente compresi e individua le opportunità di miglioramento per le politiche, i piani, i processi e le procedure che supportano la gestione del rischio di cybersecurity. In tal modo, questa funzione fornisce gli spunti necessari per informare e indirizzare gli sforzi di tutte le sei funzioni del framework;
3) Protezione (*Protect*): attua ed utilizza misure di sicurezza per gestire attivamente i rischi di cybersecurity dell'organizzazione. L'obiettivo di questa funzione è duplice: prevenire o ridurre la probabilità e l'impatto degli eventi avversi di cybersecurity, e, contestualmente, aumentare la possibilità di cogliere opportunità positive;
4) Rilevamento (*Detect*): rileva ed analizza potenziali attacchi e compromissioni di cybersecurity, facilitando così le funzioni successive;
5) Risposta (*Respond*): contiene l'effetto degli incidenti di cybersecurity adottando adeguate risposte, minimizzando, così, il relativo danno;
6) Ripristino (*Recover*): recupera e ripristina gli asset colpiti da un incidente di cybersecurity.

3. La classificazione delle misure di sicurezza: il metodo utilizzato

Venendo ora al lato "pratico" del presente studio, si tratta di illustrare la metodologia per mezzo della quale si è giunti all'allineamento tra misure operative, ISO e NIST 2.0. Il risultato finale che verrà in seguito proposto è stato ottenuto in quattro fondamentali passaggi.

In una prima fase, sono state individuate una serie di misure di sicurezza delle informazioni che rispecchiassero accuratamente le pratiche organizzative tipiche sulla base dell'esperienza e che, dunque, garantissero (in combinazione tra di loro) un'adeguata protezione dei dati personali contenuti tanto su supporto digitale quanto su quello cartaceo.

Successivamente, per garantire un maggior ordine oltre che una migliore fruibilità pratica, le misure individuate sono state raggruppate in due macrocategorie – misure di sicurezza organizzative e misure di sicurezza tecniche –, seguendo la struttura del GDPR. Ciascuna categoria è stata ulteriormente suddivisa in sottocategorie (sensibilizzazione degli utenti, protezione dei locali e delle postazioni di lavoro, etc.).

Il risultato di questa prima fase di analisi è stato riassunto nella classificazione presentata in Tab. 1 e Tab. 2.

In una seconda fase, grazie all'esperienza sul campo, si è ritenuto di organizzare le misure operative in modo più corretto e rigoroso anche sul piano generale, utilizzando criteri ufficiali e riconosciuti. A tal fine, la classificazione è stata rivista sulla scorta delle indicazioni fornite da ENISA nel suo report pubblicato nel 2019, ove le misure di sicurezza risultavano distinte come in Fig. 1.

20. Per una descrizione completa delle funzioni, v. NIST, *The NIST Cybersecurity Framework (CSF) 2.0*, cit., p. 3 ss.

a)	Misure di sicurezza organizzative
	Sensibilizzazione degli utenti
1.	Formazione del personale
2.	Istruzioni di sicurezza fisica e comportamentale dettagliate agli utenti
3.	Lucchetto con cavo di sicurezza per dispositivi mobili pc
4.	Manuale del trattamento dei dati
	Protezione dei locali e delle postazioni di lavoro
1.	Accesso non consentito al pubblico
2.	Allarme centralizzato
3.	Allarme locale
4.	Armadi ignifughi con serratura
5.	Cassetti o armadi chiusi
6.	Chiusura con serratura
7.	Controllo degli accessi
8.	Distruzione sicura dei supporti fisici
9.	Etichettatura dei dispositivi portatili
10.	Finestre con inferriate
11.	Misure antiallagamento
12.	Misure antincendio
13.	Misure antincendio automatiche
14.	Scaffalature
	Protezione delle sale server
1.	Armadi blindati
2.	Armadi ignifughi e stagni con serratura
3.	Armadi protetti
4.	Armadi senza serratura
5.	Cassaforte
6.	Controllo degli accessi
7.	Locali dotati di impianto di allarme antifurto collegato all'esterno
8.	Locali server dotati di sistema antincendio automatico
9.	Sensori ambientali nei locali server (temperatura, umidità, allagamento)
	Altre misure organizzative
1.	Accordi di riservatezza con i dipendenti ed i fornitori
2.	Adozione di un piano di continuità operativa
3.	Conservazione dei supporti comunque contenenti dati personali, in apposite custodie o contenitori
4.	Gestione e controllo delle esternalizzazioni
5.	Politiche BYOD (Bring Your Own Device)
6.	Politiche di manutenzione e di distruzione dei dati
7.	Procedure di data breach e gestione incidenti con ruoli chiari e simulazioni periodiche
8.	Procedure di on-boarding e off-boarding (es.: disattivazione account, restituzione dispositivi, etc.)
9.	Sicurezza degli scambi con altri organismi

Tab. 1 — *Classificazione iniziale delle misure di sicurezza organizzative*

b)	Misure di sicurezza tecniche
	Infrastruttura e Server
1.	Aggiornamento automatico del registro delle minacce
2.	Antivirus
3.	Backup cifrati e conservati off-site o in cloud sicuro
4.	Backup di sicurezza: continuo, settimanale, giornaliero
5.	Controllo degli accessi a livello di sistema operativo/server (RBAC)
6.	Controllo degli accessi discrezionale
7.	Controllo e filtraggio del traffico in ingresso/uscita
8.	Crittografia dei dati a riposo e in transito
9.	Disaster Recovery Plan testato periodicamente (se non già incluso nel piano di continuità operativa)
10.	Firewall di rete
11.	Gruppo di continuità o UPS
12.	Monitoraggio e logging degli accessi e delle attività
13.	NAT/PAT
14.	Protezione da malware ed exploit
15.	Ridondanza
16.	Segmentazione della rete
17.	Sistemi di rilevamento e prevenzione intrusione (IDS/IPS)
18.	Wireless sicuro
	Postazioni di lavoro (desktop e laptop)
1.	Aggiornamento automatico del registro minacce
2.	Antivirus
3.	Archiviazione sicura: livello protezione del cartaceo o tecniche di protezione dei dati tipo criptatura
4.	Autenticazione a più fattori (MFA)
5.	Autenticazione dell'accesso con password sicura
6.	Backup di sicurezza: continuo, settimanale, giornaliero
7.	Blocco della navigazione su siti non sicuri
8.	Crittografia del disco (es.: BitLocker, FileVault) su laptop e desktop
9.	Estensione dei controlli a dispositivi rimovibili connessi
10.	Firewall di rete
11.	Gestione centralizzata degli endpoint (MDM/EDR)
12.	Gruppo di continuità o UPS
13.	Politiche di timeout di sessione/inattività
14.	Predisposizione del ripristino con snapshot
15.	Profili di accesso unici
16.	Protezione da malware ed exploit
17.	Salvaschermo protetto con password sicura

Tab. 2 — *Classificazione iniziale delle misure di sicurezza tecniche*

Organizational Security Measures Categories
Security management
Security policy and procedures for the protection of personal data
Roles and responsibilities
Access control policy
Resource/asset management
Change management
Data processors
Incident response and business continuity
Incidents handling / Personal data breaches
Business continuity
Human resources
Confidentiality of personnel
Training

Technical Security Measures Categories
Access control and authentication
Logging and monitoring
Security of data at rest
Server/Database security
Workstation security
Network/Communication security
Back-ups
Mobile/Portable devices
Application lifecycle security
Data deletion/disposal
Physical security

Fig. 1 — *Classificazione delle misure di sicurezza operata da ENISA (ENISA 2019, p. 14)*

Il rapporto ENISA ha così fornito solide basi metodologiche per ricollocare le misure di sicurezza precedentemente individuate in categorie standardizzate. Nello specifico, il quadro ENISA 2019 classifica le misure in due ambiti generali: Organizzativo e Tecnico.

– Le *misure organizzative* comprendono azioni relative alla *governance*, quali lo sviluppo di politiche, i processi di gestione dei rischi e la formazione del personale, volte a integrare la sicurezza nella struttura organizzativa.
– Le *misure tecniche* si riferiscono alle misure di sicurezza tecnologiche, tra cui la crittografia, il controllo degli accessi e i meccanismi di sicurezza della rete, progettate per proteggere i sistemi informativi da accessi non autorizzati o compromissioni.

Adottando queste categorie, la classificazione iniziale è stata perfezionata per allinearla agli standard riconosciuti a livello internazionale, ottenendo la tassonomia aggiornata delle misure di sicurezza delle informazioni presentata in Tab. 3 e Tab. 4. Questo allineamento non solo migliora il rigore metodologico, ma anche la conformità, armonizzando le pratiche organizzative con le aspettative normative e rafforzando la gestione dei rischi attraverso una definizione più chiara delle priorità e delle responsabilità.

Sebbene coerente e accurata, tale organizzazione risultava però indubbiamente ispirata alla classificazione dei controlli così come riportata nell'Allegato A alla precedente versione dello standard ISO/IEC 27001 risalente, ormai, all'anno 2013.

Come già anticipato, infatti, nella precedente versione dello standard ISO/IEC 27001, i controlli risultavano organizzati nelle seguenti quattordici sezioni: politiche di sicurezza delle informazioni; organizzazione della sicurezza delle informazioni; sicurezza delle risorse umane; gestione degli asset; controllo degli accessi; crittografia; sicurezza fisica e ambientale; sicurezza operativa; sicurezza delle comunicazioni; acquisizione, sviluppo e manutenzione dei sistemi; rapporti con i fornitori; gestione degli incidenti di sicurezza delle informazioni; aspetti di sicurezza delle informazioni della gestione della continuità operativa; conformità. Tuttavia, tale suddivisione non è stata riutilizzata nella nuova versione dello standard.

Pertanto, nel terzo (nonché penultimo) passaggio, si è preso atto delle "novità" introdotte in tema di controlli dall'ultima versione della normativa, risalente al 2022. Da ciò, ne è conseguita un'ulteriore rivisitazione della classificazione, necessaria affinché la stessa risultasse conforme alla suddivisione dei "nuovi" controlli così come operata nell'Allegato A dell'ultima versione dell'ISO 27001.

In occasione dell'aggiornamento della normativa, infatti, i novantatré controlli elencati sono stati suddivisi nelle seguenti quattro macrocategorie: controlli organizzativi, sul personale, fisici e tecnologici. Per tale motivo, le misure di sicurezza precedentemente identificate sono state quindi parzialmente riassegnate a queste nuove categorie, che sono state ulteriormente suddivise in sottocategorie tematiche per migliorare l'usabilità e garantire una maggiore chiarezza.

Infine, ogni misura di sicurezza è stata associata al relativo controllo corrispondente riportato nell'Allegato A alla ISO/IEC 27001:2022. I risultati ottenuti in questa fase (e, dunque, la classificazione definitiva delle misure di sicurezza dell'informazione), sono riportati nella Tab. 5.

Nella quarta ed ultima fase – considerata, da chi scrive, la più innovativa – sono stati apportati alla mappatura elaborata ulteriori perfezionamenti ottenuti grazie allo studio della *Cybersecurity Framework 2.0* di NIST.

Come già in parte menzionato, questo documento individua sei funzioni principali – Governo (GV), Identificazione (ID), Protezione (PR), Rilevazione (DE), Risposta (RS) e Recupero (RC) – preposte a garantire il massimo livello di sicurezza informatica dell'organizzazione (vedi Fig. 2). Il formato di codifica adottato è XX.YY, dove XX rappresenta la Funzione e YY la Categoria[21]. Questa integrazione garantisce la coerenza con una tassonomia riconosciuta a livello internazionale e facilita l'interoperabilità tra le pratiche organizzative e i quadri normativi[22].

In sintesi, in questo ultimo passaggio, si è provveduto a collegare le categorie elaborate da NIST nella *Cybersecurity Framework 2.0* alle misure di

21. Si precisa che, ai fini del presente studio, non è stata presa in considerazione la sottocategoria. Nel CSF, infatti, ogni funzione (XX) si compone di una categoria (YY) e, altresì, di una sottocategoria (NN).
22. V. NIST, *The NIST Cybersecurity Framework (CSF) 2.0*, cit., p. 15.

a)	Misure di sicurezza organizzative
	Gestione della sicurezza
1.	Accesso non consentito al pubblico
2.	Armadi blindati
3.	Armadi ignifughi con serratura
4.	Armadi ignifughi e stagni con serratura
5.	Armadi protetti
6.	Armadi senza serratura
7.	Cassetti o armadi chiusi
8.	Cassaforte
9.	Chiusura con serratura
10.	Conservazione dei supporti comunque contenenti dati personali, in apposite custodie o contenitori
11.	Controllo degli accessi
12.	Etichettatura dei dispositivi portatili
13.	Finestre con inferriate
14.	Gestione e controllo delle esternalizzazioni
15.	Istruzioni di sicurezza fisica e comportamentale dettagliate agli utenti
16.	Lucchetto con cavo di sicurezza per dispositivi mobili pc
17.	Manuale del trattamento dei dati
18.	Politiche BYOD (*Bring Your Own Device*)
19.	Scaffalature
20.	Sicurezza degli scambi con altri organismi
	Risposta agli incidenti e continuità operativa
1.	Adozione di un piano di continuità operativa
2.	Allarme centralizzato
3.	Allarme locale
4.	Locali dotati di impianto di allarme antifurto collegato all'esterno
5.	Locali server dotati di sistema antincendio automatico
6.	Misure antiallagamento
7.	Misure antincendio
8.	Misure antincendio automatiche
9.	Procedure di *data breach* e gestione incidenti con ruoli chiari e simulazioni periodiche
10.	Sensori ambientali nei locali server (temperatura, umidità, allagamento)
	Risorse umane
1.	Accordi di riservatezza con i dipendenti ed i fornitori
2.	Formazione del personale
3.	Procedure di *on-boarding* e *off-boarding* (es.: disattivazione account, restituzione dispositivi, etc.)

Tab. 3 — *Classificazione delle misure di sicurezza organizzative basata sulle indicazioni fornite da ENISA*

b)	Misure di sicurezza tecniche
	Controllo degli accessi e autenticazione
1.	Autenticazione a più fattori (MFA)
2.	Autenticazione dell'accesso con password sicura
3.	Controllo degli accessi a livello di sistema operativo/server (RBAC)
4.	Controllo degli accessi discrezionale
5.	Politiche di *timeout* di sessione/inattività
6.	Profili di accesso unici
7.	Salvaschermo protetto con password sicura
	Registrazione e monitoraggio
1.	Monitoraggio e *logging* degli accessi e delle attività
2.	Sistemi di rilevamento e prevenzione intrusione (IDS/IPS)
	Sicurezza dei dati a riposo
1.	Aggiornamento automatico del registro delle minacce
2.	Antivirus
3.	Archiviazione sicura - livello di protezione del cartaceo o tecniche di protezione dei dati tipo criptatura
4.	Crittografia dei dati a riposo e in transito
5.	Crittografia del disco (es.: *BitLocker*, *FileVault*) su laptop e desktop
6.	Protezione da *malware* ed *exploit*
	Sicurezza della rete/comunicazione
1.	Blocco della navigazione su siti non sicuri
2.	Controllo e filtraggio del traffico in ingresso/uscita
3.	*Firewall* di rete
4.	NAT/PAT
5.	Segmentazione della rete
6.	Wireless sicuro
	Backup
1.	Backup cifrati e conservati *off-site* o in *cloud* sicuro
2.	Backup di sicurezza: continuo, settimanale, giornaliero
3.	*Disaster Recovery Plan* testato periodicamente (se non già incluso nel piano di continuità operativa)
4.	Gruppo di continuità o UPS
5.	Predisposizione del ripristino con *snapshot*
6.	Ridondanza
	Dispositivi mobili/portatili
1.	Estensione dei controlli a dispositivi rimovibili connessi
2.	Gestione centralizzata degli endpoint (MDM/EDR)
	Sicurezza del ciclo di vita delle applicazioni
1.	Analisi statica e dinamica del codice (SAST/DAST)
2.	Modellazione delle minacce (Threat modeling)
3.	*Patch management* e aggiornamenti di sicurezza
4.	Test di penetrazione periodici (*Penetration testing*)
	Cancellazione/smaltimento dei dati
1.	Cancellazione sicura del software
2.	Distruzione sicura dei supporti e/o dei documenti cartacei
3.	Politiche di manutenzione, conservazione e distruzione dei dati

Tab. 4 — *Classificazione delle misure di sicurezza tecniche basata sulle indicazioni fornite da ENISA*

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Fig. 2 — *Le sei funzioni principali del CSF e i nomi delle categorie con i rispettivi identificatori*

sicurezza delle informazioni precedentemente enucleate dalla realtà operativa ed associate ai controlli della normativa ISO. Questa integrazione ha dato vita a una struttura unificata che collega l'implementazione pratica con gli standard riconosciuti a livello internazionale, migliorando così la coerenza, la tracciabilità e la conformità normativa.

3.1. La mappatura multilivello delle misure di sicurezza

La mappatura multilivello finale ottenuta dal lavoro sopra descritto consiste, come già anticipato, nell'associazione tra la classificazione delle misure di sicurezza delle informazioni elaborata[23] da chi scrive e, da un lato, i controlli di cui alla ISO/IEC 27001:2022 (Allegato A) e, dall'altro, le categorie coniate dalla NIST 2.0 (riportate sotto forma di codici identificativi similmente alla Fig. 2). La mappatura effettuata è stata poi suffragata dalla UNI/PdR 174:2025[24].

23. Da qui in poi denominata "Modello Smartlex" o il "Modello, in quanto basato anche sull'esperienza pratica di Smartlex. Si veda il sito smartlex.eu.

24. Per l'associazione tra normativa ISO e NIST 2.0, si veda UNI – Ente Italiano di Normazione *UNI/PdR 174:2025. Sistema di gestione per la cybersicurezza e la sicurezza delle informazioni armonizzato alla norma UNI CEI EN ISO/IEC 27001 e al Framework NIST CSF 2.0 – Requisiti*.

Il Modello Smartlex	ISO/IEC 27001:2022 (numero controllo allegato A)	NIST 2.0
a) Misure di sicurezza organizzative		
Gestione della sicurezza		
Adozione di un piano di continuità operativa	5.24;5.29;5.30; 7.11	GV.SC;ID.IM;DE.AE; PR.IR;RS.MI;RC.RP
Disaster Recovery Plan testato periodicamente (se non già incluso nel piano di continuità operativa)	7.11	RC.RP;PR.IR
OMISSIS	*OMISSIS*	*OMISSIS*
Threat Intelligence (Intelligenza sulle Minacce)	5.7	ID.RA;GV.RM;GV.RR; GV.OV;DE;RS.CO
b) Misure di sicurezza sul personale		
Gestione delle risorse umane		
Accordi di riservatezza con i dipendenti ed i fornitori	6.6;8.30	GV.OC;GV.SC;GV.RR; ID.RA;PR.PS;PR.AA; DE.CM
Formazione del personale	6.3;7.7	GV.RR;PR.AT;PR.DS; ID.AM
OMISSIS	*OMISSIS*	*OMISSIS*
Screening e normazione dipendenti	6.1;6.2;6.3;6.4; 6.5;6.7	GV.OC;GV.RR; GV.PO;ID.AM;PR.AA;PR.AT; PR.DS;DE.CM
c) Misure di sicurezza fisiche		
Sicurezza dei locali e delle attrezzature fisiche	7.1;7.3;7.9	GV.OC;PR.AA; PR.IR;PR.DS;PR.PS; DE.CM;ID.AM
Accesso non consentito al pubblico	7.2;7.4	ID.AM;DE.AE
OMISSIS	*OMISSIS*	*OMISSIS*
Controllo degli accessi ai locali	5.17;7.2;7.4	ID.AM;DE.AE
Finestre con inferriate		
Locali dotati di impianto di allarme antifurto collegato all'esterno		
Videosorveglianza		
Protezione ambientale	7.3;7.4;7.5;7.7; 7.8; 7.9;7.12;7.13	GV.OC;GV.RM; GV.RR;ID.AM; PR.AA;PR.DS; PR.IR;PR.PS
OMISSIS	*OMISSIS*	*OMISSIS*
Gruppo di continuità o UPS	7.11	
Locali server dotati di sistema antincendio automatico		
Misure antiallagamento	7.12	
Misure antincendio	7.12	
Misure antincendio automatiche		

Sensori ambientali nei locali server (temperatura, umidità, allagamento)		
d) Misure di sicurezza tecnologiche		
Controllo degli accessi e dell'autenticazione		GV.OC;GV.RM; GV.RR;PR.AA;PR.DS; PR.PS;DE.CM;RS.MA
OMISSIS	*OMISSIS*	*OMISSIS*
Autenticazione a più fattori (MFA)	8.2;8.3;8.4;8.5	ID.RA
Autenticazione dell'accesso con password sicura	8.2;8.3;8.4	ID.RA
OMISSIS	*OMISSIS*	*OMISSIS*
Controllo degli accessi discrezionale	8.2;8.3	
OMISSIS	*OMISSIS*	*OMISSIS*
Profili di accesso unici	8.2;8.3;8.18	
OMISSIS	*OMISSIS*	*OMISSIS*
Protezione da minacce	5.1;8.1;8.2; 8.3;8.4;8.5;8.12	GV;ID;PR.AA; PR.DS;PR.PS; DE.CM
Aggiornamento automatico del registro delle minacce	8.8	ID.RA
Antivirus	8.7	RS.MI
OMISSIS	*OMISSIS*	*OMISSIS*
Test di penetrazione periodici (Penetration testing)		ID.RA
Sicurezza della rete/ comunicazione	8.98.12;8.17; 8.19; 8.20;8.21;8.24;8.27	GV.OC;GV.RM; GV.OV;ID;PR.PS; PR.DS;PR.IR;DE; RS.AN
OMISSIS	*OMISSIS*	*OMISSIS*
Controllo e filtraggio del traffico in ingresso/ uscita	8.23	
OMISSIS	*OMISSIS*	*OMISSIS*
Segregazione della rete	8.22	
Wireless sicuro	8.23;8.24	
Registrazione e monitoraggio	8.9;8.16;8.34	GV.OC;GV.OV; GV.RM;ID;PR;DE; RS.MA
Monitoraggio e logging degli accessi e delle attività	8.3;8.4;8.15	RS.AN
Sistemi di rilevamento e prevenzione intrusione (IDS/IPS)	8.3;8.4;8.8	ID.RA
Sicurezza del ciclo di vita delle applicazioni		GV.OC;GV.RM; GV.OV;PR.PS; PR.DS;ID.AM; DE.CM
Analisi statica e dinamica del codice (SAST/ DAST)	7.10;8.15;8.22; 8.25; 8.26	DE.AE;RS.AN;RS.MA;PR.IR;ID.RA
OMISSIS	*OMISSIS*	*OMISSIS*
Patch management e aggiornamenti di sicurezza	5.7;5.25;5.26	GV.SC;ID.RA; DE.AE;RS.CO;RS.MA; RS.MI;RC.RP
OMISSIS	*OMISSIS*	*OMISSIS*

Separazione degli ambienti di sviluppo, test e produzione	8.19;8.25;8.26; 8.27;8.29;8.30; 8.31	ID.RA
Crittografia	8.24;8.26	PR.DS;DE.CM;ID.RA
Crittografia dei dati a riposo e in transito		
Crittografia del disco (es.: *BitLocker*, *FileVault*) su laptop e desktop	6.7;7.9;7.13	PR.IR;PR.PS;ID.AM
Backups	8.13;8.34	PR.DS;PR.PS;RC.RP; RS.MA;DE.CM; ID.AM; ID.RA; GV.OC; GV.RM
Backup cifrati e conservati *off-site* o in *cloud* sicuro	5.20;5.23	GV.SC
Backup di sicurezza: Continuo, Settimanale, Giornaliero		
Predisposizione del ripristino con *snapshot*	5.33	PR.PS;DE.AE;RS.AN
Ridondanza	8.14	PR.PS;PR.IR
Dispositivi mobili/ portatili	5.11;6.2;6.7; 7.13;8.26	GV.OC;GV.RR; GV.RM;ID.AM;ID.RA; PR.DS;PR.IR; PR.PS;DE.CM;
OMISSIS	*OMISSIS*	*OMISSIS*
Gestione centralizzata degli endpoint (MDM/ EDR)	8.1	PR.PS
Lucchetto con cavo di sicurezza per dispositivi mobili pc	7.5;7.8;7.9	PR.IR;PR.PS
Cancellazione/smaltimento dei dati	5.11;7.10; 8.10	GV.OC; GV.RM; ID;PR.DS;PR.PS DE.CM
Cancellazione sicura del software	7.14	
OMISSIS	*OMISSIS*	*OMISSIS*
Politiche di manutenzione, conservazione e distruzione dei dati	7.13;8.14	PR.IR

Tab. 5 — *Esempi di come le misure di sicurezza del Modello Smartlex possono essere associate ai controlli ISO/IEC 27001:2022 e alle categorie NIST 2.0*

La Tabella 5[25] mostra alcuni esempi tratti dalla mappatura[26]. Basandosi su questo quadro integrato, la sezione successiva ne illustra l'applicazione in un contesto giuridico e organizzativo concreto. Esaminando un caso tratto dal contesto normativo italiano, è dimostrabile, così, come la classificazione proposta funzioni nella pratica, evidenziandone la capacità di semplificare i processi di conformità, ridurre la complessità di attuazione e rafforzare la responsabilità. L'esempio che segue ha lo scopo, infatti, di dimostrare l'utilità pratica del Modello e il suo potenziale di adattamento a diversi contesti organizzativi.

25. Alcune delle misure di sicurezza inserite all'interno della tabella e contenute nella categoria delle misure di sicurezza tecnologiche sono considerate come necessarie per la costituzione di un valevole "sistema immunitario digitale" in un'era, come quella in cui si scrive, caratterizzata da continue minacce di cybersecurity in evoluzione. Sul punto, si veda Shaji George–Hovan George–Baskar 2023.
26. Il lavoro di mappatura completo è protetto da *copyright* di Smartlex s.r.l.

4. Gli obblighi di Cybersecurity per le organizzazioni pubbliche e private: una guida introduttiva all'applicazione del Modello

Come già anticipato, l'allineamento sopra descritto è stato precipuamente elaborato anche per fungere da Modello pratico per le organizzazioni che intendano conformarsi agli obblighi previsti a loro carico in materia di cybersicurezza[27]. Tale esigenza è divenuta ancor più urgente in seguito all'adozione della Direttiva NIS2 (Direttiva UE 2022/2555), pietra miliare della più ampia strategia della Commissione europea in materia di sicurezza informatica[28]. La direttiva impone requisiti rigorosi ad un'ampia gamma di soggetti in materia di attuazione delle misure di sicurezza e di notifica degli incidenti[29], con l'obiettivo di raggiungere un livello senza precedenti di sicurezza delle informazioni sia nel settore privato che nelle amministrazioni pubbliche.

In particolare, infatti, la direttiva si rivolge direttamente alle strutture pubbliche e private (di seguito, soggetti NIS) che operano in settori particolarmente critici come, ad esempio, il settore sanitario, quello delle infrastrutture digitali, ecc.[30] In Italia, tali obblighi sono stati recepiti con il decreto legislativo n. 138 del 4 settembre 2024 (di seguito, Decreto NIS)[31], che ha introdotto requisiti di conformità significativi strettamente connessi alla mappatura precedentemente descritta. Ci si riferisce, in particolare ed a titolo esemplificativo, a quanto stabilito negli articoli 23 e 24 del suddetto decreto: si tratta di disposizioni fondamentali che, come si avrà modo di approfondire più avanti, individuano specifici obblighi in materia di gestione del rischio per la sicurezza informatica e di notifiche degli incidenti. I suddetti requisiti legali costituiscono un banco di prova ideale per valutare l'utilità pratica del Modello proposto, in quanto richiedono non solo la conformità formale, ma anche pratiche di sicurezza dimostrabili ed efficaci.

Il recepimento italiano della direttiva NIS2 rappresenta un esempio perfetto di come il Modello qui illustrato possa fungere da strumento strategico per le organizzazioni che operano in contesti normativi complessi. Per dimostrarne la validità, è utile premettere un breve *excursus* sugli obblighi introdotti dalla legislazione italiana, concentrandosi principalmente sulla determinazione n. 164179 del 14 aprile 2025 emanata dall'Agenzia per la Cybersicurezza Nazionale (di seguito ACN). Tale provvedimento chiarisce le modalità di adempimento degli obblighi NIS2 e include quattro allegati che definiscono le specifiche di base, ovvero le misure minime di sicurezza richieste per i soggetti NIS essenziali e importanti ai sensi degli articoli 23 e 24 del Decreto NIS. Quest'ultimi descrivono inoltre in dettaglio le categorie di incidenti significativi che devono essere segnalati al CSIRT Italia in conformità con l'articolo 25.

27. Sono note, infatti, non solo le correlazioni tra NIST 2.0 e NIS2, ma anche tra quest'ultima direttiva e la normativa ISO/IEC. Ciò in quanto il recepimento della direttiva NIS2 può influire direttamente sulle politiche di un Sistema di Gestione della Sicurezza delle Informazioni (ISMS). Sul punto (e seppur con riferimento alla Repubblica Ceca) si veda Wanecki–Jasek–Drofova 2023.
28. Ci si riferisce, in particolare, al *Cybersecurity Act* (Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il Regolamento (UE) n. 526/2013) ed al *Cyber Resilience Act* (Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio del 23 ottobre 2024 relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i Regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la Direttiva (UE) 2020/1828). In realtà, la Direttiva NIS2 costituisce la "naturale" evoluzione della c.d. Direttiva NIS (Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione). Per un *excursus* sulle ragioni che hanno determinato il passaggio dalla Direttiva NIS alla Direttiva NIS2, si veda Casarosa–Comandè 2025.
29. In tema di segnalazione degli incidenti (e per la comparazione sul punto tra direttiva NIS e direttiva NIS2) si veda Schmitz-Berndt 2023.
30. Per l'elenco completo dei settori, si veda l'Allegato 1 alla Direttiva NIS2.
31. Per un'analisi dettagliata del decreto, si veda ACN 2025.

Il Modello illustrato integra questi requisiti nella sua struttura, garantendo alle organizzazioni la possibilità di mantenere un percorso di conformità aggiornato e mappato, che assicuri una sicurezza reale piuttosto che una mera adesione formale ai requisiti legali.

Per convalidare il quadro teorico e dimostrarne la rilevanza operativa, la sezione seguente presenta un'applicazione pratica nel contesto normativo italiano. Questo caso di studio illustra come il Modello proposto possa essere efficacemente integrato con gli obblighi nazionali in materia di sicurezza informatica, in particolare quelli introdotti dalla direttiva NIS2 e dalle sue misure di attuazione. Mappando i requisiti legali, quali i protocolli di gestione dei rischi e gli obblighi di notifica degli incidenti, sull'allineamento strutturato dei controlli ISO/IEC 27001 e delle categorie del quadro di riferimento per la sicurezza informatica del NIST, l'esempio evidenzia la capacità del Modello di trasformare la conformità da un esercizio formale a un sistema dimostrabile di governance della sicurezza. Questa illustrazione pratica funge da prova empirica dell'adattabilità e del valore strategico del Modello per le organizzazioni che operano in contesti normativi complessi.

4.1. Gli obblighi a carico dei soggetti NIS: gli articoli 23 e 24 del Decreto NIS

Prima di esaminare gli articoli 23 e 24 del Decreto NIS ed illustrare in che modo il Modello proposto sostenga le organizzazioni nell'adeguarsi agli obblighi in materia di cybersicurezza, è utile premettere che i cc.dd. soggetti NIS[32] tenuti all'adempimento degli obblighi in materia di cybersicurezza sono distinti in due categorie: soggetti essenziali e soggetti importanti. La distinzione riflette principalmente la criticità dei settori in cui operano e il livello intrinseco di rischio informatico associato alle loro attività. Nonostante queste differenze, i requisiti di sicurezza imposti a entrambe le categorie convergono sostanzialmente, rendendo il Modello proposto ugualmente applicabile ad entrambe.

Stante questa premessa, è ora possibile analizzare brevemente gli articoli 23 e 24 del Decreto NIS per verificare come essi possano essere più facilmente rispettati grazie all'ausilio della mappatura oggetto del presente lavoro.

L'articolo 23 definisce le responsabilità specifiche degli organi di amministrazione e degli organi direttivi dei soggetti essenziali e dei soggetti importanti in materia di sicurezza informatica, attribuendogli, tra l'altro, la funzione essenziale – in questa sede – di approvare le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica adottate dai soggetti NIS e di sovraintendere all'implementazione dei relativi obblighi. Sebbene sia previsto uno specifico obbligo formativo sul tema[33], è intuibile come gli organi di amministrazione non siano di norma composti da esperti del tema e abbisognino di strumenti agili per orientarsi e decidere. Ciò sottolinea l'importanza della mappatura proposta, non solo per i team tecnici responsabili dell'attuazione e del monitoraggio delle misure, ma anche, e forse soprattutto, per i decisori di alto livello, legalmente responsabili della governance della sicurezza.

L'articolo 24 del Decreto NIS delinea gli elementi essenziali che le organizzazioni devono necessariamente prendere in considerazione quando si trovino ad adottare misure di sicurezza informatica, rendendo così operativo il principio della gestione della sicurezza basata sul rischio. In particolare, la disposizione richiede alle entità di attuare misure proporzionate ai rischi identificati, tenendo conto di fattori quali la natura e la criticità dei servizi forniti, il potenziale impatto degli incidenti sulla continuità del servizio e il grado di esposizione alle minacce informatiche. La norma in esame sottolinea un approccio globale che integra misure di salvaguardia tecniche, organizzative e procedurali, garantendo la resilienza a tutti i livelli del sistema informativo. Inoltre, l'articolo 24 sottolinea la necessità di un monitoraggio continuo e di una rivalutazione periodica delle misure attuate, riflettendo la natura dinamica del rischio informatico. Questi requisiti sono strettamente in linea con la logica alla base del Modello proposto, che facilita la mappatura sistematica degli obblighi e supporta le organizzazioni nel dimostrare la conformità attraverso processi strutturati e verificabili.

In sintesi, l'articolo 24 identifica con precisione gli elementi essenziali che devono essere presi

32. Per l'elenco dei soggetti NIS, v. art. 6 del Decreto NIS.

33. V. art. 20, comma 2, NIS2 e 23 del Decreto NIS.

a) Politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete
b) Gestione degli incidenti
c) Continuità operativa, ivi inclusa la gestione di backup, il ripristino in caso di disastro, ove applicabile, e la gestione delle crisi
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
e) Sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità
f) Politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi per la sicurezza informatica
g) Pratiche di igiene di base e di formazione in materia di sicurezza informatica
h) Politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura
i) Sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli asset
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

Tab. 6 — *Elenco degli elementi essenziali che devono essere presi in considerazione ai sensi dell'art. 24 del Decreto NIS al momento dell'adozione delle misure di sicurezza*

in considerazione al momento dell'adozione delle misure di sicurezza, come indicati nella Tab. 6.

L'opera di allineamento effettuata da chi scrive ha permesso di associare una o più misure di sicurezza, derivate da pratiche organizzative reali, a ciascun requisito stabilito dall'articolo 24. Attraverso questo Modello, tali misure sono state sistematicamente collegate ai corrispondenti controlli ISO/IEC 27001 e alle linee guida del NIST *Cybersecurity Framework 2.0*, garantendo un'integrazione coerente e funzionale. Questo approccio strutturato non solo facilita la conformità, ma fornisce anche alle organizzazioni uno strumento pratico per mappare gli obblighi legali agli standard riconosciuti a livello internazionale, migliorando così sia l'efficienza operativa che la responsabilità. Nella Tab. 7 si riportano alcuni esempi[34].

Prima di proseguire con l'illustrazione del risultato finale del presente lavoro, si ritiene opportuno soffermarsi su alcuni degli esempi, così da comprendere al meglio il vantaggio della mappatura.

(a) Politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete

Quest'obbligo è soddisfatto garantendo che la sicurezza non sia lasciata al caso, ma sia strutturata e basata su dati. Le politiche di sicurezza delle informazioni e il Manuale del trattamento dei dati costituiscono, in tal caso, il pilastro della governance, nella misura in cui stabiliscono ruoli, obiettivi e regole di base. L'inclusione della *Threat Intelligence* assicura poi che il processo di analisi dei rischi non sia teorico, ma alimentato da informazioni aggiornate sulle minacce. Infine, l'implementazione di procedure di *data breach* dimostra che l'organizzazione ha definito la sua reazione in caso di materializzazione del rischio in piena conformità con la legislazione applicabile mappata all'interno del Modello. Sebbene il Modello non richieda alle organizzazioni di ottenere la certificazione ISO/IEC 27001, esso adotta una struttura di responsabilità comparabile per fornire prove verificabili della conformità legale.

Questo approccio strutturato migliora la governance e la preparazione agli audit, creando un sistema trasparente e tracciabile che collega ogni misura di sicurezza ai requisiti normativi e agli standard riconosciuti, consentendo così alle organizzazioni di dimostrare proporzionalità e *due diligence* nella loro postura in materia di sicurezza informatica. In questo modo, il Modello rende operativo il principio di proporzionalità incorporato nelle normative sulla sicurezza informatica: le misure non vengono applicate in modo uniforme, ma calibrate in base al livello di rischio, alla complessità organizzativa e alla criticità specifica del settore. Ciò garantisce che la conformità

34. Per un'esaustiva illustrazione della corrispondenza tra misure di sicurezza di base e gli elementi di cui all'art. 24, comma 2, del Decreto NIS, si veda ACN 2025, cit., p. 13. Il lavoro di mappatura completo è protetto da *copyright* di Smartlex s.r.l.

Decreto NIS, art. 24	Misure di sicurezza (Modello Smartlex)
a) Politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete	Procedure di data breach e gestione incidenti con ruoli chiari e simulazioni periodiche; Politiche di sicurezza delle informazioni; Manuale del trattamento dei dati; Threat Intelligence
b) Gestione degli incidenti	Procedure di data breach e gestione degli incidenti con ruoli chiari e simulazioni periodiche; Relazione con autorità e gruppi specialistici
c) Continuità operativa, ivi inclusa la gestione di backup, il ripristino in caso di disastro, ove applicabile, e la gestione delle crisi	Adozione di un piano di continuità operativa; Disaster Recovery Plan testato periodicamente; Backup; Ridondanza
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	Gestione e controllo delle esternalizzazioni; Sicurezza delle informazioni per l'uso dei servizi cloud; Accordi di riservatezza con i dipendenti ed i fornitori
e) Sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità	Patch management e aggiornamenti di sicurezza; Analisi statica e dinamica del codice (SAST/DAST); Aggiornamento automatico del registro delle minacce; Segregazione della rete
f) Politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi per la sicurezza informatica	Politiche di sicurezza delle informazioni; Adozione di un piano di continuità operativa; Gestione e controllo delle esternalizzazioni; Procedure di data breach e gestione incidenti con ruoli chiari e simulazioni periodiche
g) Pratiche di igiene di base e di formazione in materia di sicurezza informatica	Formazione del personale; Salvaschermo protetto con password sicura; Screening e normazione dipendenti; Politiche BYOD (Bring Your Own Device); Procedure di on-boarding e off-boarding (es.: disattivazione account, restituzione dispositivi, etc.)
h) Politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura	Crittografia dei dati a riposo e in transito; Crittografia del disco (es.: BitLocker, FileVault) su laptop e desktop
i) Sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli asset	Screening e normazione dei dipendenti; Procedure di on-boarding e off-boarding; Accordi di riservatezza con i dipendenti ed i fornitori; Controllo degli accessi a livello di sistema operativo/server (RBAC); Controllo degli accessi ai locali; Accesso non consentito al pubblico; Formazione del personale; Videosorveglianza
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	Autenticazione a più fattori (MFA); Profili di accesso unici; Controllo degli accessi discrezionale; Autenticazione dell'accesso con password sicura

Tab. 7 — *Esempi di come le misure di sicurezza del Modello Smartlex si rapportano ai requisiti di cui all'art. 24 del Decreto NIS*

non sia meramente formale, ma sostanzialmente allineata alla natura dinamica delle minacce informatiche e alle aspettative legali di una gestione della sicurezza basata sul rischio.

(c) Continuità operativa, ivi inclusa la gestione di backup, il ripristino in caso di disastro, ove applicabile, e la gestione delle crisi

L'obiettivo principale di quest'obbligo è, senza dubbio, quello di garantire la resilienza dei sistemi e dei servizi critici. L'adozione di un piano di continuità operativa e di un *Disaster Recovery Plan*, fornisce la struttura documentale per il ripristino dei servizi critici. Un requisito fondamentale per la conformità è il test periodico del *Disaster Recovery Plan*, fondamentale per convalidarne l'efficacia e l'affidabilità. A integrazione di questi piani, le misure di backup e ridondanza costituiscono la base tecnica per la continuità: i backup consentono il recupero dei dati,

mentre la ridondanza garantisce la disponibilità immediata dei sistemi critici. Insieme, queste misure rispondono in modo completo al mandato normativo in materia di continuità e ripristino dei servizi, traducendo i requisiti legali in resilienza operativa.

(e) Sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità

Si tratta del requisito della *Security by Design/Default*. Il *Patch management* e gli aggiornamenti di sicurezza costituiscono la base della manutenzione sicura. L'analisi statica e dinamica del codice è invece essenziale per la sicurezza nello sviluppo e nell'acquisizione, in quanto garantisce che le applicazioni non introducano vulnerabilità sin dall'origine. L'aggiornamento automatico del registro delle minacce alimenta la gestione delle vulnerabilità. Infine, la segregazione della rete è una misura di protezione fisica e logica che garantisce che un'eventuale compromissione in un'area non si propaghi a sistemi critici. È fondamentale collegare queste misure al principio di proporzionalità e all'approccio basato sul rischio: la portata e la complessità delle strategie di continuità e di ripristino devono corrispondere al livello di rischio e alla criticità dei servizi forniti. Ciò consente un'allocazione efficiente delle risorse, evitando sia una protezione insufficiente che un investimento eccessivo e non necessario.

Il Modello proposto integra questi obblighi associando ogni requisito a specifici controlli ISO/IEC 27001 e a categorie del NIST *Cybersecurity Framework*, creando un percorso di conformità strutturato e verificabile. Questo allineamento consente alle organizzazioni di dimostrare che le misure di continuità e ripristino non siano solo implementate, ma anche proporzionate alla loro esposizione al rischio, soddisfacendo così sia gli obblighi giuridici che le aspettative di *governance*. In questo modo, il Modello trasforma principi normativi astratti in pratiche attuabili e basate su prove concrete che migliorano la resilienza e la preparazione agli *audit* e la accountability.

(g) Pratiche di igiene di base e di formazione in materia di sicurezza informatica

Quest'obbligo si concentra non solo sulla *Cyber Hygiene* ma anche sulla gestione del fattore umano, che può, senza dubbio, rappresentare l'anello più vulnerabile della catena di sicurezza. Per questo, il cuore dell'adempimento è rappresentato dalla formazione del personale (accompagnata dall'ulteriore misura di screening e normazione dei dipendenti), necessaria per elevare la cultura della sicurezza. Le altre misure costituiscono esempi pratici di "igiene di base": ad esempio, il salvaschermo protetto è un controllo di accesso fisico di primo livello; le politiche BYOD e le procedure di *on-boarding* e *off-boarding* garantiscono invece che la gestione sicura del dispositivo e degli accessi degli utenti sia standardizzata, applicando così l'igiene in ogni fase del rapporto lavorativo. Collettivamente, queste misure rendono operativi i principi di sicurezza incorporando meccanismi di igiene e di controllo in ogni fase dell'interazione organizzativa, riducendo così l'esposizione alle vulnerabilità connesse al fattore umano[35].

Queste misure sono direttamente mappate sui controlli ISO/IEC 27001, come A.6.3 (Consapevolezza, istruzione, formazione e addestramento sulla sicurezza delle informazioni) e A.5.17 (Informazioni di autenticazione), e sulle categorie del quadro di riferimento per la sicurezza informatica del NIST 2.0, tra cui PR.AT (Sensibilizzazione e formazione) e PR.AC (Controllo degli accessi). Questo doppio allineamento garantisce che gli obblighi relativi al fattore umano non siano trattati come pratiche isolate, ma integrati in un quadro di conformità strutturato. Il Modello proposto facilita questa integrazione fornendo una chiara mappatura tra requisiti normativi, misure operative e standard internazionali, consentendo così alle organizzazioni di dimostrare proporzionalità e responsabilità nel loro approccio alla gestione dei rischi legati al fattore umano.

35. Sul punto, si veda ENISA 2025. In questo report, l'ENISA ha condotto un'analisi dettagliata delle minacce informatiche che hanno colpito l'Unione europea tra luglio 2024 e giugno 2025. Tra le principali minacce figura il *phishing*, strettamente legato al fattore umano e responsabile del 60% degli attacchi iniziali. Altre minacce significative includono lo sfruttamento delle vulnerabilità (21,3% degli attacchi), seguito dai *botnets* (9,9%), dalle applicazioni dannose (8%) e dai rischi interni (0,8%).

(i) Sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli asset
Si tratta dell'obbligo più complesso in quanto impone una gestione olistica che non si focalizza solo sulla tecnologia, ma integra persone, processi e asset fisici. La sua natura multidimensionale sottolinea l'utilità della mappatura proposta, che consente un controllo strutturato in tutti i domini e garantisce la coerenza nell'implementazione.

- *Rischio derivante dal fattore umano:* misure quali accordi di riservatezza, screening e normazione dei dipendenti e procedure di *on-boarding* e *off-boarding* garantiscono una gestione coerente e documentata del rischio lungo tutta la durata del rapporto di lavoro.
- *A livello tecnologico:* il controllo degli accessi a livello di sistema operativo/server e la formazione del personale sono necessarie per definire un sistema di permessi robusto, che garantisca che gli utenti siano dotati solamente dell'accesso strettamente necessario per svolgere le loro mansioni.
- Gestione dei beni: la sicurezza fisica è rafforzata attraverso misure quali la videosorveglianza, il controllo degli accessi ai locali e le restrizioni all'ingresso del pubblico, salvaguardando così le infrastrutture critiche.

Queste misure sono sistematicamente mappate sui controlli ISO/IEC 27001 (ad esempio, A.6.3, A.9.1, A.11.1) e sulle categorie del NIST *Cybersecurity Framework* (ad esempio, PR.AC, PR.AT, PR.PT), garantendo che gli obblighi legali siano operativi all'interno di una struttura di conformità riconosciuta a livello internazionale. Il Modello facilita questa integrazione fornendo un quadro unificato che collega i requisiti normativi alle misure pratiche, consentendo alle organizzazioni di dimostrare proporzionalità, responsabilità e preparazione all'audit in tutti i settori della sicurezza.

Il processo di associazione si è basato sugli allegati 1 e 2[36] alla determinazione n. 164179/2025 dell'ACN[37], che sono stati concepiti per tradurre gli obblighi di legge in misure di sicurezza operative specifiche applicabili ai soggetti NIS. Dal punto di vista contenutistico, i due allegati si distinguono (quasi) esclusivamente per i soggetti ai quali sono destinati: se l'allegato 1, infatti, è rivolto ai c.d. soggetti importanti, il secondo, invece, individua quelle che sono le misure di sicurezza di base che ogni soggetto c.d. essenziale dovrebbe implementare. Nonostante questa differenziazione, i requisiti di sicurezza sottostanti presentano una sostanziale convergenza, consentendo lo sviluppo di un approccio di mappatura unificato all'interno del Modello proposto. Il ruolo principale degli allegati 1 e 2 della determinazione n. 164179/2025 dell'ACN è quello di fungere da meccanismo di traduzione primario tra gli obblighi giuridici di alto livello della direttiva/quadro NIS (*Network and Information Systems*) e i requisiti di sicurezza operativa specifici e attuabili imposti ai soggetti regolamentati. Gli allegati definiscono le "specifiche di base" (o requisiti minimi di sicurezza) descrivendo in modo sistematico le misure organizzative e tecniche necessarie per raggiungere un livello sufficiente di sicurezza per le reti e i sistemi informativi.

L'allegato 2 riguarda le entità essenziali (EE), che in genere forniscono servizi critici la cui interruzione potrebbe avere un impatto sociale o economico significativo (ad esempio, energia, trasporti, sanità). Le specifiche qui riportate sono state concepite per essere rigorose ed esaurienti, riflettendo la natura ad alto rischio dei servizi forniti.

L'allegato 1 riguarda invece le entità importanti (IE), che sono soggette a requisiti meno rigorosi rispetto alle EE, ma devono comunque mantenere un solido livello di sicurezza. Sebbene i requisiti di sicurezza fondamentali (domini di sicurezza) spesso coincidano con quelli dell'allegato 2, i dettagli specifici di attuazione, le prove richieste o il livello di controllo possono essere adeguati in base al principio di proporzionalità. In sostanza, questi allegati suddividono gli obblighi giuridici generali (come "garantire la sicurezza") in domini di sicurezza specifici.

L'utilità del Modello proposto risiede nella sua capacità di tradurre i requisiti nazionali obbligatori in materia di sicurezza informatica, stabiliti

36. Per il testo completo di entrambi gli allegati, si rimanda a *Modalità e specifiche di base – ACN*.

37. ACN, determinazione n. 164179/2025 di cui all'articolo 31, commi 1 e 2, del decreto legislativo 4 settembre 2024, n. 138, adottata secondo le modalità di cui all'articolo 40, comma 5, lettera l), che, ai sensi dell'articolo 42, comma 1, lettera c), in fase di prima applicazione, stabilisce le modalità e le specifiche di base per l'adempimento agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del decreto medesimo.

dagli allegati 1 e 2 dell'ACN, in standard di sicurezza attuabili e riconosciuti a livello internazionale per gli enti NIS.

Questa funzione colma il divario tra l'obbligo giuridico prescrittivo e l'attuazione operativa pratica.

In altre parole, gli Allegati ACN (e, in particolare, la determinazione n. 164179/2025) costituiscono il quadro normativo autorevole che codifica i requisiti essenziali di sicurezza informatica previsti dalla legge italiana per gli enti che operano in settori critici e di grande rilevanza nazionale. Questi allegati stabiliscono la base minima delle misure di sicurezza operativa che gli Enti Essenziali e Importanti devono implementare per mitigare i rischi per la loro rete e i loro sistemi informativi. Essi adottano un approccio prescrittivo dall'alto verso il basso, definendo ciò che deve essere raggiunto (l'obiettivo normativo) senza necessariamente specificare il *come* operativo e granulare (il meccanismo tecnico).

L'utilità principale del Modello Smartlex è quella di facilitare l'operatività della conformità colmando il divario tra prescrizioni normative ed esecuzione pratica. Il Modello consente alle organizzazioni regolamentate di interpretare i requisiti generali stabiliti negli allegati dell'ACN e di tradurli in controlli di sicurezza specifici e dimostrabili che si allineano alla loro realtà operativa (c.d. traduzione in esecuzione). Il meccanismo centrale del Modello è il processo di mappatura incrociata (standardizzazione e allineamento). Questa mappatura allinea gli obblighi identificati dall'ACN con una serie di controlli derivati dai principali standard internazionali di sicurezza informatica (ISO/IEC 27001 e NIST *Cybersecurity Framework*). Questo allineamento garantisce che gli sforzi di conformità non solo siano giuridicamente validi, ma sfruttino anche le migliori pratiche del settore, affinando così la sicurezza complessiva al di là della semplice adesione alle normative. Il quadro di mappatura risultante può quindi essere popolato con requisiti legislativi specifici derivanti da varie normative nazionali e settoriali pertinenti, fornendo un registro di conformità unificato e completo per il soggetto NIS[38].

La correlazione tra gli allegati ACN e il Modello può essere rappresentata come mostrato in Fig. 3.

Come illustrato nella Fig. 3:

- gli allegati dell'ACN stabiliscono ciò che la legge italiana richiede in materia di sicurezza informatica per gli enti che operano in settori altamente rilevanti, adottando un approccio prescrittivo;
- il Modello Smartlex consente alle organizzazioni interessate di comprendere come implementare i requisiti dell'ACN attraverso standard di sicurezza perfettamente aderenti alla realtà operativa.

In altre parole, la mappatura risultante da questo lavoro consente al soggetto NIS di implementare i requisiti identificati dall'ACN utilizzando misure di sicurezza specifiche e di allinearli ai due principali standard internazionali (ISO e NIST 2.0). Una volta eseguita la mappatura, è possibile inserirvi gli obblighi richiesti derivanti dalle normative pertinenti.

5. Esempi di implementazione

A conclusione del presente lavoro, vengono forniti in Tab. 8 alcuni esempi che illustrano come le misure di sicurezza del Modello possano essere utilizzate per implementare in maniera olistica e strategica i requisiti di cui agli allegati già menzionati.

Per comprendere sino in fondo i vantaggi apportati dal Modello Smartlex, segue un breve approfondimento di alcuni degli esempi riportati nella Tabella 8.

(a) ID.RA-01 – Le vulnerabilità negli asset sono identificate, confermate e registrate

Questo controllo impone un sistema in cui l'identificazione e il trattamento delle vulnerabilità costituiscano un'attività costante dell'organizzazione, lungi dall'esserne richiesta, invece, una semplicemente annuale. In tal senso, la fase di identificazione continua può essere soddisfatta, ad esempio, dall'utilizzo di test di penetrazione periodici: così l'organizzazione può dimostrare di aver adottato

38. Inoltre, occorre considerare due ulteriori aspetti: 1) l'integrazione tra il Modello Smartlex e gli allegati è estremamente semplice grazie all'utilizzo di un linguaggio comune, ovvero NIST 2.0; 2) il Decreto NIS impone un approccio basato sul rischio, che è preso in considerazione anche nel Modello Smartlex grazie all'associazione delle misure di sicurezza da adottare con lo standard ISO/IEC 27001:2022.

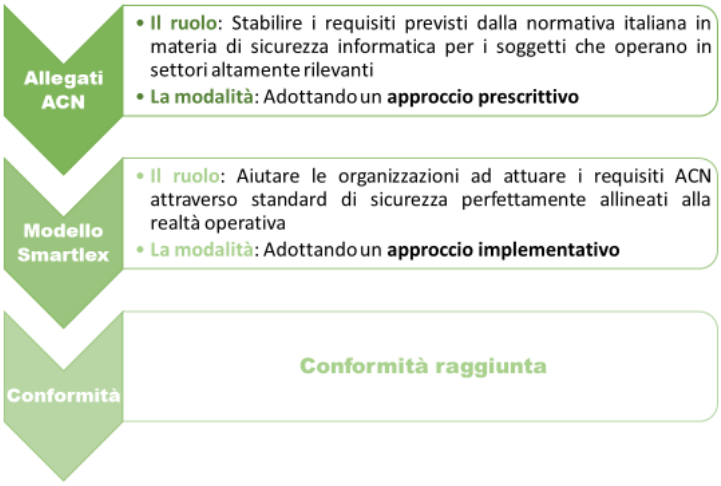

Fig. 3 — *Percorso che le organizzazioni intraprendono per raggiungere la conformità, partendo dagli allegati ACN e passando, poi, dal Modello Smartlex*

un approccio proattivo (in luogo di uno viceversa reattivo) non attendendo il verificarsi dell'incidente, ma ricercando attivamente gli eventuali punti deboli. La correttezza di una simile gestione è enfatizzata altresì dalla periodicità del test, che evidenzia come l'organizzazione riconosca la dinamicità dell'ambiente IT.

In tal modo, dunque, è possibile scoprire e registrare le vulnerabilità. Successivamente, grazie al *patch management* e agli aggiornamenti di sicurezza, le vulnerabilità possono essere mitigate. Le misure di sicurezza del Modello garantiscono, pertanto, un processo maturo e completo per la gestione delle vulnerabilità: l'organizzazione può infatti dimostrare non solo di aver definito il metodo per scoprire il rischio, ma anche il flusso di lavoro per gestirlo e risolverlo (l'intero "ciclo di vita della vulnerabilità").

(b) DE.CM-01 – Le reti e i servizi di rete sono monitorati per individuare eventi potenzialmente avversi

Si tratta del controllo più considerevole della funzione di rilevamento e funge da ponte operativo tra la protezione passiva e la risposta attiva agli attacchi. Esso presuppone infatti un sistema che garantisca l'intercettazione tempestiva di eventuali eventi avversi. Tramite le misure di sicurezza di monitoraggio e *logging* degli accessi e delle attività, l'organizzazione può registrare dettagliatamente ogni accesso e attività sui sistemi informativi e di rete rilevanti: senza *log* completi e conservati, non sarebbe, infatti, possibile risalire alla causa radice di un incidente.

In più, grazie ad ulteriori misure, quali i sistemi di rilevamento e prevenzione dell'intrusione e l'aggiornamento automatico del registro delle minacce, è possibile elevare le capacità di rilevazione dell'organizzazione. La prima, infatti, è una "sentinella" che esamina i flussi di rete e i *log*, cercando *pattern* di attacco noti o comportamenti anomali (si pensi, ad esempio, ad un utente che accede a troppi file contemporaneamente). L'aggiornamento del registro delle minacce è anch'esso cruciale: assicura che questi sistemi operino con le *signature* di attacco più recenti, rendendo la rilevazione precisa e tempestiva. Infine, l'avviso di potenziali intrusioni viene immediatamente intercettato grazie alle procedure di *data breach* e di gestione degli incidenti. In conclusione, il Modello consente di dimostrare la completa integrazione del ciclo di vita della rilevazione e della risposta: grazie ad esso, infatti, gli eventi avversi possono essere identificati e successivamente gestiti in maniera efficace.

6. Conclusioni e prossimi obiettivi

Il lavoro presentato ha raggiunto con successo il suo obiettivo fondamentale: dimostrare la traducibilità di complessi quadri normativi e di sicurezza informatica in un Modello pragmatico e operativo applicabile dalle organizzazioni. Sebbene il Modello richieda ancora ricerca e perfezionamento, la sua utilità attuale è oggettivamente già significativa. Il Modello proposto offre un allineamento multilivello che integra sistematicamente le misure operative di sicurezza delle informazioni con gli standard

Allegati 1 e 2	Misure di sicurezza del Modello Smartlex	Utilità del Modello Smartlex
GV.SC-01: Sono stabiliti e accettati dagli stakeholder dell'organizzazione il programma, la strategia, gli obiettivi, le politiche e i processi di gestione del rischio di cybersecurity della catena di approvvigionamento.	Gestione e controllo delle esternalizzazioni; Sicurezza delle informazioni per l'uso dei servizi cloud.	L'adozione delle misure di sicurezza di cui alla mappatura permette di dimostrare l'esistenza di clausole contrattuali e di un processo di due diligence sui fornitori cloud, mitigando i rischi della supply chain come richiesto dall'ACN.
ID.RA-01: Le vulnerabilità negli asset sono identificate, confermate e registrate.	Patch management e aggiornamenti di sicurezza; Test di penetrazione periodici.	La mappatura presenta un allineamento tra ID.RA e la funzione di risposta (RS) che permette di adottare un approccio completo che soddisfi il requisito del ciclo di vita delle vulnerabilità degli asset.
PR.DS-11: I backup dei dati sono creati, protetti, mantenuti e verificati.	Backup cifrati e conservati off-site o in cloud sicuro; Backup di sicurezza: Continuo, Settimanale, Giornaliero; Predisposizione del ripristino con snapshot; Ridondanza.	L'adozione delle misure di sicurezza individuate nella mappatura consente all'organizzazione di disporre di dati in ripristino che siano non solo presenti, ma anche disponibili, integri e protetti, come richiesto dagli standard di governance più elevati.
DE.CM-01: Le reti e i servizi di rete sono monitorati per individuare eventi potenzialmente avversi.	Monitoraggio e logging degli accessi e delle attività; Sistemi di rilevamento e prevenzione intrusione (IDS/IPS); Procedure di data breach e gestione degli incidenti; Aggiornamento automatico del registro delle minacce.	La mappatura fornisce il meccanismo (logging), la tecnologia (IDS/IPS) e la procedura (gestione incidenti) che assicurano che gli eventi di sicurezza sui sistemi rilevanti vengano non solo registrati, ma anche analizzati e gestiti secondo i requisiti NIS2/ACN.
RS.CO-02: Gli stakeholder interni ed esterni sono informati degli incidenti.	Procedure di data breach e gestione degli incidenti con ruoli chiari e simulazioni periodiche; Relazione con autorità e gruppi specialistici.	La mappatura prevede strumenti di che includono l'interazione con soggetti esterni, soddisfacendo così l'obbligo di coordinamento e informazione in caso di incidenti.

Tab. 8 — *Esempi di come le misure di sicurezza del Modello Smartlex possono essere utilizzate per attuare i requisiti di cui agli allegati 1 e 2*

internazionali consolidati e gli obblighi normativi specifici. Esso si basa su solidi pilastri internazionali poiché associa le misure di sicurezza organizzative a due fondamentali quadri internazionali di riferimento per la sicurezza informatica (ISO/IEC 27001:2022 e NIST *Cybersecurity Framework (CSF) 2.0*).

L'allineamento multilivello ha il pregio di trasformare i principi astratti di sicurezza in misure attuabili, garantendo sia la coerenza strategica che la resilienza operativa. Il nostro Modello integrato, che combina i controlli ISO/IEC 27001 con le categorie del NIST *Cybersecurity Framework*, insieme alla serie di misure di sicurezza informatica da noi individuate, offre vantaggi significativi: consente l'allineamento normativo, permettendo di armonizzare le pratiche organizzative con gli standard internazionali e i requisiti legali dell'Unione europea; fornisce un approccio strutturato per dare priorità e mitigare i rischi in modo efficace; in questo processo, contribuisce a ridurre i costi di conformità attraverso processi standardizzati e mappature chiare che migliorano l'efficienza operativa; infine, ma non meno importante, facilita una governance dimostrabile e la preparazione agli audit.

Inoltre, il Modello associa e traccia le misure adottate ai requisiti di conformità normativa

pertinenti. L'analisi degli obblighi imposti dalla legislazione italiana (Decreto Legislativo n. 138/2024, che recepisce la Direttiva NIS2) e la successiva determinazione dell'ACN sono servite come esempio definitivo per convalidare questa funzionalità.

Il contributo più significativo del Modello alle organizzazioni – in particolare, a quelle designate come soggetti NIS nell'esempio fornito – è la sua capacità di definire la metodologia concreta di implementazione dei requisiti prescrittivi dell'ACN. L'esempio illustra infatti come il Modello contribuisca a rendere operativi i requisiti: fornisce misure di sicurezza specifiche necessarie per soddisfare gli elementi essenziali della gestione del rischio previsti, ad esempio, dall'articolo 24 del Decreto NIS. Inoltre, detto quadro consente un monitoraggio semplice ed efficace dello stato di conformità, facilitando al contempo una dimostrabilità più agevole ed efficace della responsabilità e fornendo prove verificabili dell'attuazione dei controlli.

Nonostante i sostanziali risultati ottenuti, la mappatura realizzata deve considerarsi solo come un solido punto di partenza. Gli sviluppi futuri sono pianificati strategicamente per massimizzare la portata e l'utilità quantitativa del Modello. Essi dovrebbero sfruttare l'agnosticismo del quadro normativo ampliando la portata dello strumento per comprendere tutti i quadri normativi pertinenti, consentendo una mappatura unica, funzionale e coordinata di obblighi disparati. Si prevede che questa capacità produrrà significativi risparmi sui costi per gli utenti, riducendo al minimo i costi di conformità e massimizzando l'efficacia operativa delle misure di sicurezza adottate.

Da un punto di vista teorico e operativo, la ricerca futura dovrebbe concentrarsi anche sullo sviluppo di un metodo in grado di assegnare un valore quantitativo misurabile al rischio per la sicurezza affrontato da ogni singola misura di sicurezza. Questo obiettivo si basa sull'analisi precedente, che ha dimostrato le potenziali implicazioni sistemiche del Modello per la valutazione del rischio e per fornire un approccio più oggettivo al criterio di proporzionalità, alla base della regolamentazione della sicurezza informatica.

Si prevede che l'evoluzione finale del Modello sarà un sistema quantitativo completo di misurazione della sicurezza informatica, che consentirà alle organizzazioni di misurare con precisione il proprio "livello di sicurezza" e di dimostrare in modo tangibile la conformità e la mitigazione dei rischi alle autorità di regolamentazione e alle parti interessate.

Riferimenti bibliografici

ACN–Agenzia per la Cybersicurezza Nazionale (2025), *Linee guida NIS. Specifiche di base. Guida alla lettura*, in can.gov.it, 2025

M. Alshar'e (2023), *Cyber security framework selection: comparision of nist and iso27001*, in "Applied computing Journal", vol. 3, 2023, n. 1

F. Casarosa, G. Comandè (2025), *Il percorso di implementazione della Direttiva NIS 2: verso l'armonizzazione o una maggiore frammentazione?,* in "Annuario di Diritto Comparato", 2025, in corso di pubblicazione

Enisa–European Union Agency for Network and Information Security (2025), *ENISA Threat Landscape 2025*, in enisa.europa.eu, 2025

Enisa–European Union Agency for Network and Information Security (2019), *Reinforcing trust and security in the area of electronic communications and online services. Sketching the notion of "state-of-the-art" for SMEs in security of personal data processing*, in enisa.europa.eu, 2019

A. Lokare, S. Bankar, P. Mhaske (2025), *Integrating Cybersecurity Frameworks into IT Security: A Comprehensive Analysis of Threat Mitigation Strategies and Adaptive Technologies*, in Arxiv, arXiv:2502.00651, 2025

M. Malatji (2023), *Management of enterprise cyber security: A review of ISO/IEC 27001:2022*, in "International Conference On Cyber Management And Engineering (CyMaEn)" (Bangkok, 26-27 gennaio 2023), 2023

A. Obi, O.V. Akagha, S.O. Dawodu, A.C. Anyanwu, S. Onwusinkwue, I.A. Ahmad (2024), *Comprehensive review on cybersecurity: Modern threats and advanced defense strategies*, in "Computer Science & IT Research Journal", vol. 5, 2024, n. 2

S. Rose, O. Borchert, S. Mitchell, S. Connelly (2020), *Zero Trust Architecture*, NIST Special Publications 800-207, 2020

S. Schmitz-Berndt (2023), *Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive*, in "Journal of Cybersecurity", vol. 9, 2023, n. 1

A. Shaji George, A.S. Hovan George, T. Baskar (2023), *Digitally Immune Systems: Building Robust Defences in the Age of Cyber Threats*, in "Partners Universal International Innovation Journal (PUIIJ)", vol. 1, 2023, n. 4

O. Vakhula, Y. Kurii, I. Opirskyy, V. Susukailo (2024), *Security-as-Code Concept for Fulfilling. ISO/IEC 27001:2022 Requirements*, in "Cybersecurity Providing in Information and Telecommunication Systems", vol. 3654, 2024

P. Wanecki, R. Jasek, I. Drofova (2023), *The Contribution of the European NIS2 Directive to the Design of the Cyber Security Model,* in "2023 International Conference on Information and Digital Technologies (IDT)" (Zilina, 20-22 giugno 2023), 2023