Un approccio olistico alla Cybersecurity nazionale

Author : Federica Maria Calì

Date : 8 Ottobre 2019

Il NIST (National Institute of Standard and Technology) ha elaborato un framework per aiutare le organizzazioni a implementare un **sistema di gestione e controllo sulla sicurezza dei dati**. Il Framework è un approccio basato sulla gestione del rischio di cybersecurity ed è composto da tre parti:

- *Framework Core;*
- *Framework Implementation Tiers;*
- *Framework Profile.*

Ogni componente del Framework rafforza la connessione tra i fattori di *business/mission* e le attività di cybersecurity.

Il Framework Core è un insieme di attività di cybersecurity, risultati desiderati e riferimenti applicabili comuni a tutti i settori. Il nucleo presenta standard, linee guida e pratiche del settore in un modo che consente la comunicazione delle attività e dei risultati della cybersecurity in tutta l'organizzazione, dal livello esecutivo al livello di implementazione/operazioni.

Il Framework Core comprende **cinque funzioni** simultanee e continue: **identificazione, protezione, rilevamento, risposta e recupero**. Tali funzioni forniscono una visione strategica di alto livello del ciclo di vita della gestione del rischio di cybersecurity da parte di un'organizzazione. Vengono identificate quindi le sottostanti categorie chiave e relative sottocategorie per ciascuna funzione e associate con esempi di riferimenti informativi come standard, linee guida e pratiche esistenti per ciascuna sottocategoria.

I livelli di implementazione del framework (*"tiers"*) descrivono il grado delle pratiche di gestione del rischio di cybersecurity di un'organizzazione. I *Tier* caratterizzano le pratiche di un'organizzazione su un intervallo, da *Partial* (*Tier 1*) ad *Adaptive* (*Tier 4*). Durante il processo di selezione del *Tier*, un'organizzazione deve considerare le sue attuali pratiche di gestione del rischio, l'ambiente delle minacce, i requisiti legali e normativi, gli obiettivi di business/missione e i vincoli organizzativi.

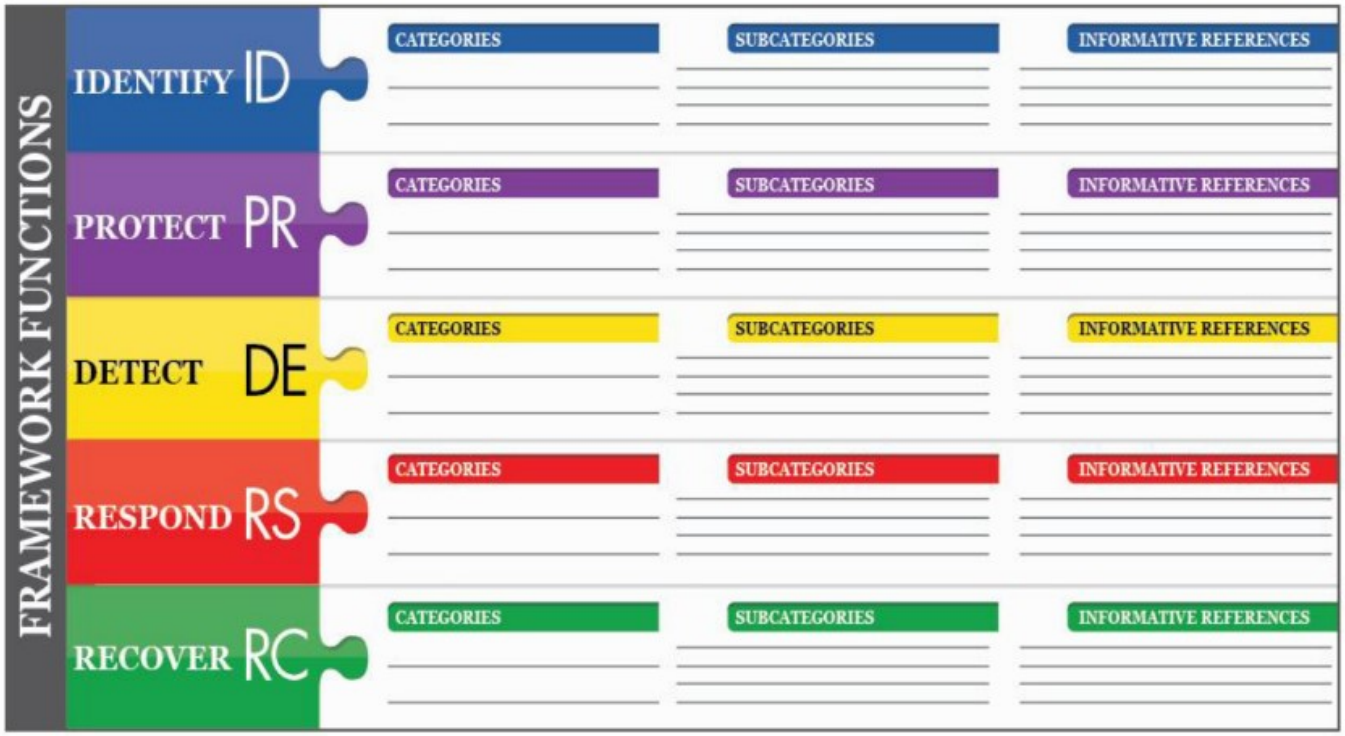
Il ***Framework Profile*** rappresenta i risultati in base alle esigenze aziendali che un'organizzazione ha selezionato dalle Categorie e Sottocategorie della struttura.

Il profilo può essere caratterizzato dall'allineamento di standard, linee guida e pratiche al *Framework Core* in un particolare scenario di implementazione.
I profili possono, poi, essere utilizzati per condurre autovalutazioni e comunicare all'interno di un'organizzazione o tra organizzazioni.

Il *Framework Core* fornisce una serie di attività per raggiungere specifici risultati di cybersecurity e fornisce esempi di linee guida per raggiungere tali risultati. Il *Core* non è una lista di controllo delle azioni da eseguire, bensì presenta i risultati chiave identificati dagli *stakeholder* come utili nella gestione del rischio di cybersecurity.

Il nucleo comprende **quattro elementi:** funzioni, categorie, sottocategorie e riferimenti informativi.

Le **funzioni** sono: Identificare, Proteggere, Rilevare, Rispondere e Recuperare.



In tal modo si aiuta un'organizzazione a esprimere la propria gestione del rischio di cybersecurity organizzando informazioni, consentendo decisioni di gestione dei rischi, affrontando le minacce e imparando dalle attività precedenti. Le funzioni si allineano anche con le metodologie esistenti per la gestione degli incidenti e aiutano a mostrare l'impatto degli investimenti nella sicurezza informatica.

Le **categorie** sono le suddivisioni di una funzione in gruppi di risultati di cybersecurity

strettamente legati a esigenze programmatiche e attività particolari. Esempi di categorie includono "Gestione risorse", "Gestione identità e controllo accessi" e "Processi di rilevamento".

Le **sottocategorie** dividono ulteriormente una categoria in risultati specifici delle attività tecniche e/o gestionali. Forniscono una serie di risultati che, sebbene non esaustivi, aiutano a supportare il raggiungimento dei risultati in ciascuna categoria.

I **riferimenti informativi** sono sezioni specifiche di standard, linee guida e pratiche comuni ai settori delle infrastrutture critiche che illustrano un metodo per raggiungere i risultati associati a ciascuna sottocategoria. I riferimenti informativi presentati nel Framework sono illustrativi e non esaustivi.

Il panorama nazionale della cybersecurity è profondamente mutato negli ultimi anni, acquisendo una maggiore consapevolezza del rischio cyber e della necessità di adeguate misure di sicurezza; inoltre si è assistito a un aumento, in qualità e quantità, delle minacce cyber.

È stato così sviluppato in ambito nazionale il **Framework Nazionale per la Cybersecurity e la *Data Protection***, per supportare le organizzazioni che necessitano di strategie e processi volti alla protezione dei dati personali e alla sicurezza cyber.

La sua adozione può aiutare le organizzazioni nel definire un percorso volto alla cybersecurity e alla protezione dei dati coerente con i regolamenti stessi (GDPR), riducendo i costi necessari e aumentando l’efficacia delle misure realizzate.

Inoltre, per le organizzazioni che già implementano misure coerenti con il Regolamento, il Framework può rappresentare un utile strumento per guidare le necessarie attività di continuo monitoraggio.

Il Framework include una serie di nuovi elementi indirizzati a guidare la corretta gestione dei dati personali, con specifico riferimento alla sicurezza degli stessi a fronte di possibili attacchi informatici. A tale scopo sono state introdotte nove nuove *subcategories* e una nuova *category* che colgono i seguenti aspetti legati alla *data protection.*

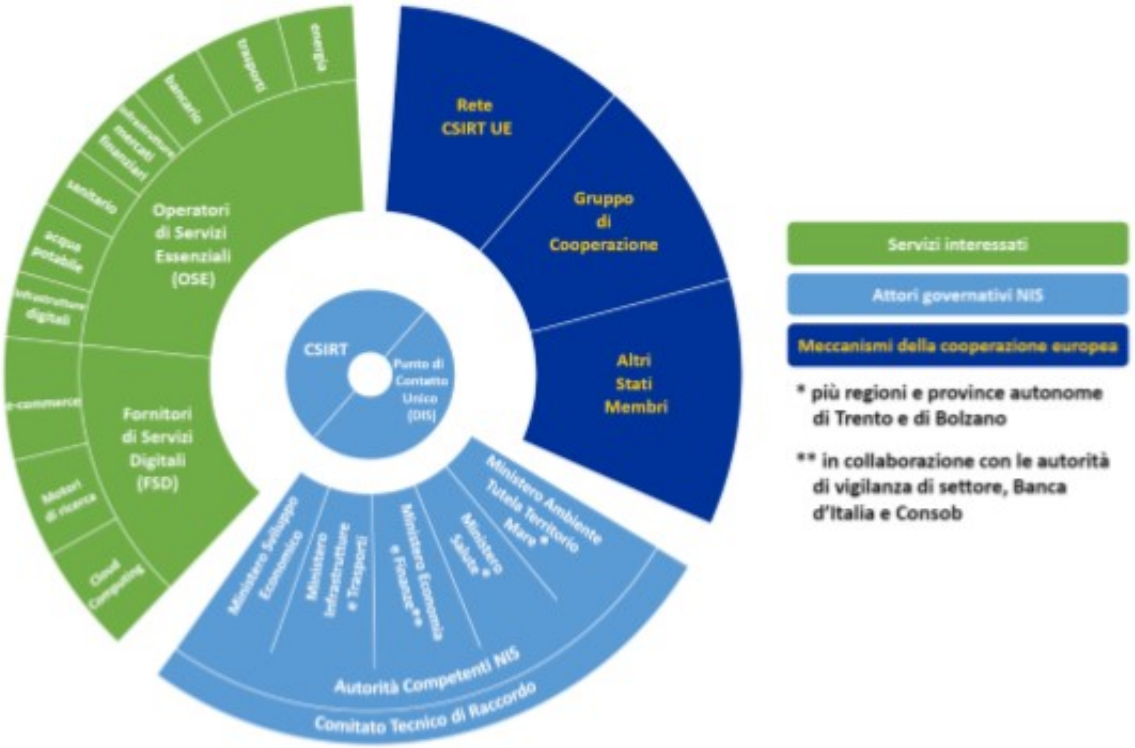
Nel 2016 l’Unione Europea ha adottato le sue prime misure nel settore della cybersecurity attraverso la direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio sulla sicurezza delle reti e dei sistemi informativi, la così detta **Direttiva NIS** (*Network and Information Security*). Questa è stata recepita dall’Italia con il decreto legislativo n.65/2018, pubblicato sulla Gazzetta Ufficiale il 9 giugno ed effettivo dal 24 giugno.

La direttiva è volta a migliorare le difese delle **infrastrutture critiche** degli Stati membri, puntando su *intelligence* e prevenzione per raggiungere un adeguato livello di sicurezza cibernetica e di resilienza dei sistemi critici nazionali. Attraverso l’adozione di misure tecniche e organizzative che consentano di ridurre i rischi e l’impatto degli incidenti informatici, la Direttiva si sviluppa su tre piani:

- promozione della gestione del rischio e della segnalazione degli incidenti tra i principali

attori economici, in particolare tra gli operatori che forniscono servizi essenziali per il mantenimento di attività economiche e sociali, così come tra i fornitori di servizi digitali;
- miglioramento delle capacità nazionali in materia di sicurezza cibernetica;
- rafforzamento della cooperazione in questo settore, a livello nazionale e in ambito europeo.

L'applicazione della direttiva NIS riguarda principalmente le aziende che verranno identificate come Operatori di servizi essenziali **(OSE)** o Fornitori di servizi digitali **(FSD)**. Tanto gli OSE che gli FSD sono chiamati ad adottare misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi e a prevenire e minimizzare l'impatto degli incidenti a carico della sicurezza delle reti e dei sistemi informativi, al fine di assicurare la continuità del servizio. Hanno inoltre l'**obbligo di notificare**, senza ingiustificato ritardo, gli **incidenti** che hanno un impatto rilevante, rispettivamente sulla continuità e sulla fornitura del servizio, al *Computer Security Incident Response Team* (CSIRT) italiano, informandone anche l'Autorità competente NIS di riferimento.



Il **decreto 65/2018** resta molto fedele al testo della direttiva europea e identifica otto settori di intervento: energia, trasporti, banche, mercati finanziari, sanità, fornitura e distribuzione di acqua potabile, infrastrutture digitali, servizi digitali (quali motori di ricerca, servizi cloud e piattaforme di commercio elettronico).

Si prevede, inoltre, l'istituzione presso la Presidenza del Consiglio dei Ministri di un unico *Computer Security Incident Response Team*, detto **CSIRT italiano**, che andrà a sostituire, fondendoli, gli attuali CERT Nazionale (operante presso il Ministero dello Sviluppo

Economico) e CERT-PA (operante presso l'Agenzia per l'Italia Digitale).

Gli **operatori di servizi essenziali** dovranno adottare misure tecnico-organizzative "adeguate" alla gestione dei rischi e alla prevenzione degli incidenti informatici.

Il decreto specifica che, nell'adottare tali misure, gli operatori dovranno tenere in debita considerazione le linee guida recentemente predisposte dal Gruppo di Cooperazione. Le autorità competenti NIS potranno inoltre, sentiti gli operatori di servizi essenziali, imporre l'adozione di misure di sicurezza specifiche.

Analoghi obblighi in materia di sicurezza sono previsti a carico dei **fornitori di servizi digitali**, i quali dovranno adottare misure tecniche-organizzative per la gestione dei rischi e per la riduzione dell'impatto di eventuali incidenti informatici.

Per l'adozione di tali misure i soggetti coinvolti possono utilizzare framework come quello elaborato dal NIST (l'Istituto Nazionale degli Standard e della Tecnologia), o la certificazione ISO 27001, quali soluzioni di *best practice*, allo scopo di valutare il loro livello di sicurezza IT e impostare obiettivi per migliorare le procedure utilizzate per proteggere i dati sensibili.

Come già detto, i livelli del Cybersecurity framework (parziale, consapevole del rischio informatico, replicabile e adattivo) spiegano quanto deve essere profonda l'implementazione della sicurezza informatica e con riferimento alle categorie e sottocategorie, è possibile stabilire dove siano le lacune e scegliere i piani d'azione più adeguati per colmarle.

La **ISO 27001** adotta un approccio più ampio poichè la sua metodologia si basa sul ciclo *Plan-Do-Check-Act* (PDCA), ovvero costruire un sistema di gestione che non solo progetta e implementa la cybersecurity, ma mantiene e migliora anche l'intero sistema di gestione delle informazioni.

La Direttiva NIS è stata affiancata, in via complementare, da un'altra norma europea.
Il 27 giugno 2019 infatti è entrato in vigore il **Cybersecurity Act**, il Regolamento volto a creare un quadro europeo per la certificazione della sicurezza informatica di prodotti ICT e servizi digitali e a rafforzare il ruolo dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA).

Il Cybersecurity Act costituisce una parte fondamentale della nuova strategia dell'UE per la sicurezza cibernetica, che mira a rafforzare la resilienza dell'Unione agli attacchi informatici, a creare un mercato unico in termini di prodotti, servizi e processi cibernetici e ad accrescere la fiducia dei consumatori nelle tecnologie digitali.

Il Cybersecurity Act non istituisce schemi di certificazione direttamente operativi, ma crea un "quadro" per l'istituzione di schemi europei per la certificazione dei prodotti e servizi digitali. In tal modo i certificati rilasciati secondo tali schemi saranno validi e riconosciuti in tutti gli Stati membri.

L'istituzione di tale sistema comune di certificazione, secondo la visione del legislatore

europeo, dovrebbe favorire la cosiddetta ***"security by design"*****,** ovvero la presa in considerazione della sicurezza informatica fin dagli stadi iniziali della progettazione dei prodotti ICT.

Con la Direttiva NIS e il suo decreto di recepimento si prevede l'adozione di una **strategia nazionale di sicurezza cibernetica**. La strategia dovrà prevedere in particolare le misure di preparazione, risposta e recupero dei servizi a seguito di incidenti informatici, la definizione di un piano di valutazione dei rischi informatici e programmi di formazione e sensibilizzazione in materia di sicurezza informatica.

Così, nel mese di luglio 2019 il nostro Paese ha visto, da un lato, la realizzazione e la diffusione delle *Linee guida per* gli OSE in ambito NIS e, dall'altro, lo "Schema di disegno di legge in materia di perimetro di sicurezza nazionale cibernetica".

Tutti questi interventi legislativi mostrano l'evoluzione che ormai da tempo coinvolge lo scenario nazionale e internazionale in tema di cybersecurity e sicurezza delle informazioni.

Proprio qualche giorno fa è stato pubblicato lo schema di decreto-legge recante disposizioni urgenti in materia di **perimetro di sicurezza nazionale cibernetica**.

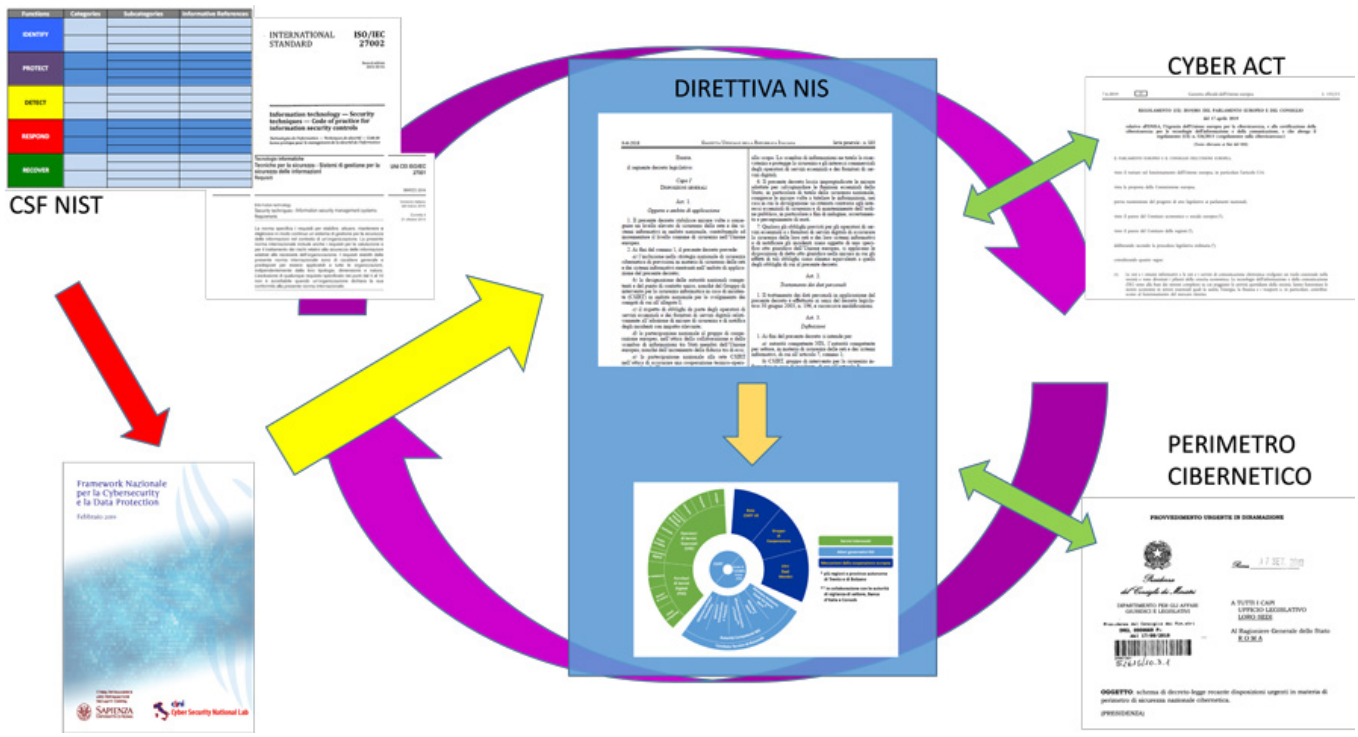
Il nuovo provvedimento sostituisce il vecchio disegno di legge e fissa a quattro mesi la scadenza per individuare le amministrazioni pubbliche, gli enti e gli operatori pubblici e privati che devono entrare a far parte del cosiddetto perimetro cibernetico, a garanzia della sicurezza di reti e servizi considerati "strategici".

Si prevede inoltre un **aggiornamento annuale** dell'elenco delle reti, dei sistemi informativi e dei servizi informatici e un arco di tempo di dieci mesi per definire le procedure secondo cui i soggetti che fanno capo al perimetro notificano gli incidenti che hanno impatto su reti, sistemi e servizi.

Il contesto legislativo degli ultimi mesi sembra sempre più focalizzato sul tema della sicurezza cibernetica, indice della maggiore consapevolezza dell'aumento delle minacce cyber. Un ottimo punto di inizio, dunque, per i tanti passi ancora da compiere.

È da prediligere un **approccio olistico** che metta in correlazione i diversi strumenti, collegandoli puntualmente: da un lato i modelli di gestione e di supporto (CSF NIST, ISO 27001 e ISO 27002), dall'altro la normativa e la legislazione nazionale ed europea, che impongono l'adozione delle regole di sicurezza e quelle sul trattamento dei dati.

Questi sono gli strumenti a disposizione delle organizzazioni, strettamente collegati e che - se ben adoperati - possono portare alla realizzazione di un modello da implementare.



Articolo a cura di **Federica Calì**