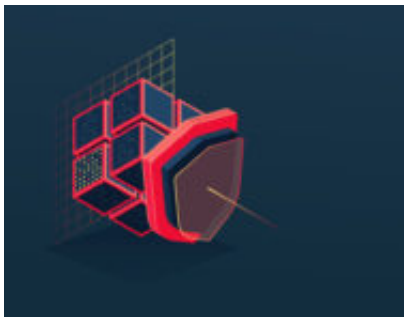
Il Framework Nazionale per la Cybersecurity e la Data Protection: proposta di integrazione con ISO/IEC 27701 e ISD©10003

Author : Massimo Montanile

Date : 12 Febbraio 2020



Il quadro normativo nazionale ed europeo in tema di cybersecurity definisce in modo chiaro quali siano gli obblighi che le organizzazioni devono rispettare a fronte di un incidente di sicurezza, dettagliando cosa fare e quando farlo, lasciando tuttavia alle singole organizzazioni la scelta di come organizzare i propri processi interni per ottimizzare la **gestione degli incidenti di sicurezza**, nel rispetto della legge.

Il legislatore infatti - riconoscendo che rischi, minacce, vulnerabilità e tolleranze di rischio sono peculiari a ciascuna organizzazione - non impone le misure da adottare per la gestione del rischio cyber. Ciascuna organizzazione **determina in autonomia** le azioni da intraprendere, le priorità e l'entità degli investimenti necessari per ridurre e gestire tali rischi, in una logica classica di valutazione costi/benefici.

La cybersecurity è tuttavia un problema complesso che richiede l'attuazione di un modello strutturato di intervento per essere affrontato in modo efficace. Le organizzazioni devono necessariamente **abbandonare la logica individualista** e cooperare con le altre organizzazioni, affinché le esperienze di ciascuna siano portate a fattor comune, implementando processi organizzativi e tecnologici in grado di abilitare una tale *vision*.

La letteratura propone vari framework per il disegno e l'implementazione di sistemi di gestione per la cybersecurity, che potrebbero vantaggiosamente essere utilizzati da un'organizzazione per contrastare i rischi cyber.

Il Framework del NIST

Il modello più noto è il Cybersecurity Framework del NIST (National Institute of Standards and Technology)[1].

Il Framework USA è stato sviluppato dal NIST, di concerto con le parti interessate, in esecuzione dell'Executive Order 13636 *“Improving Critical Infrastructure Cybersecurity”* emanato dal Presidente Barack Obama nel febbraio 2013.

Si tratta di un modello volontario (basato su standard, linee guida e *best practice*) per ridurre i rischi informatici ai quali sono esposti le infrastrutture critiche.

Il *tool* è in continuo aggiornamento, per recepire le trasformazioni che caratterizzano il mondo dei rischi cyber; la **versione attuale** del Cybersecurity Framework è la 1.1, pubblicata dal NIST il 16 aprile 2018.

Il Framework abilita un approccio *risk-based* alla gestione del rischio cyber e fornisce a ciascuna organizzazione una tassonomia comune per:

1. descrivere l’attuale livello di cybersecurity;
2. descrivere il livello target di cybersecurity;
3. identificare le azioni necessarie per raggiungere il livello target di cybersecurity e le relative priorità, con un approccio informato al miglioramento continuo;
4. valutare i progressi verso il livello target;
5. gestire la comunicazione con gli stakeholder relativamente al rischio cyber.

Il framework è diviso in tre parti, *"Core", "Tiers"* e *"Profile"*; perché sia efficace, deve essere inserito in un *loop* di valutazione continua, con cadenza stabilita dall’organizzazione, possibilmente in armonia con i cicli dei processi di *management*.

Il NIST rende disponibile, sul proprio sito web, linee guida all’utilizzo del Framework e ulteriori materiali di supporto, compresi i riferimenti informativi.

Il Framework Core

Il Framework Core consente di rappresentare, in modo altamente strutturato, la **visione strategica** di alto livello del ciclo di vita della gestione del rischio di cybersicurezza di un'organizzazione. Costituito da cinque funzioni (Identificare, Proteggere, Rilevare, Rispondere, Recuperare) articolate in Categorie e Sottocategorie, il Framework Core supporta e registra le attività ritenute necessarie per soddisfare gli obiettivi delle singole funzioni.

Per ciascuna sottocategoria si riportano i Riferimenti Informativi ad altri framework o norme.

La funzione IDENTIFY (ID) è relativa alla comprensione del contesto dell’organizzazione, alla gestione degli asset, ai processi di business, alla gestione dei rischi, alla gestione della *supply chain*, alla gestione dei dati. Le categorie all’interno di questa *function* sono: *Asset Management, Business Environment; Governance, Risk Assessment, Risk Management Strategy, Supply Chain Risk Management* e *Data Management*.

L’elenco proposto dal NIST rappresenta un insieme di attività per la gestione del rischio cyber. Si tratta di un elenco senza priorità di 5 funzioni, 22 categorie, 98 sottocategorie e relativi

riferimenti informativi che descrivono specifiche attività di sicurezza informatica che possono considerarsi comuni a tutti i settori delle infrastrutture critiche.

Il Framework è estensibile ed ulteriori categorie, sottocategorie e riferimenti informativi possono essere aggiunti durante la creazione del Profilo.

I Tiers

I livelli di implementazione del Framework ("Tiers") descrivono, con una scala crescente da “Partial – Tier 1” ad “Adaptive – Tier 4”, il modo in cui un'organizzazione gestisce il rischio di sicurezza informatica e i processi in atto per gestire tale rischio.

Essi consentono di determinare in che misura la gestione dei rischi di sicurezza informatica sia informata dalle esigenze aziendali e sia integrata nelle pratiche generali di gestione dei rischi di un'organizzazione.

I Profile

Il profilo Framework ("Profilo") è la selezione delle funzioni, categorie e sottocategorie operate in linea con i requisiti, la tolleranza al rischio e le risorse dell'organizzazione. Un profilo consente di stabilire una roadmap per la riduzione dei rischi di sicurezza informatica, in armonia con gli obiettivi dell’organizzazione e nel rispetto dei requisiti legali/normativi e delle best practice di settore, in base anche alle priorità di gestione dei rischi.

I profili possono essere utilizzati per descrivere lo stato corrente (“AS-IS”) o lo stato di destinazione desiderato (“TO_BE”) di sicurezza informatica.

I profili supportano i requisiti aziendali/di missione e aiutano a **comunicare i rischi** all'interno e tra le organizzazioni.

Il confronto dei profili (ad esempio, il profilo attuale e il profilo di destinazione) può rivelare lacune da affrontare per soddisfare gli obiettivi di gestione dei rischi di sicurezza informatica e consentire la definizione di un adeguato piano di azione.

Il Framework Nazionale per la Cybersecurity e la Data Protection

In Italia nel 2015 è stato presentato il Framework Nazionale per la Cybersecurity, che è stato sviluppato dalla proficua collaborazione tra imprese private, accademia, enti pubblici. Esso si basa sul Framework del Nist, estendendolo con tre concetti (Priorità, Maturità, Contestualizzazioni) che lo rendono uno strumento di elevata efficacia applicativa:

- i Livelli di Priorità (Alta; Media; Bassa) sono associati alle singole Subcategory e permettono di supportare le organizzazioni nella definizione del cronoprogramma da implementare per raggiungere il profilo atteso di cybersecurity;
- i Livelli di Maturità, da specificare almeno per le Subcategory a priorità alta, consentono di valutare il grado di maturità raggiunto dallo specifico processo di sicurezza cui si

riferiscono. Definiti secondo una scala crescente, abilitano percorsi incrementali di miglioramento.

Con la contestualizzazione si adatta il Framework alle caratteristiche della singola organizzazione, attraverso un processo di selezione delle Subcategory pertinenti, delle priorità, dei livelli di maturità.

In questo lavoro si propone l'applicazione del Framework Nazionale per la Cybersecurity e la Data Protection, **integrandolo** sia con le pratiche di sicurezza previste dallo standard internazionale ISO/IEC 27701[2], sia con quelle dello Schema internazionale ISDP©10003[3].

La **ISO/IEC 27701**, che estende i controlli della ISO/IEC 27001 alla privacy, non è richiamata nel Framework, essendo stata pubblicata successivamente (ad agosto 2019) all'emissione dell'attuale Versione (2.0) del Framework, pubblicata a febbraio 2019, che, della famiglia ISO 27000, richiama solo la ISO/IEC 27001.

Le integrazioni alle *"Informative References"* del Framework Core relative alla ISO/IEC 27701 sono evidenziate in giallo.

Il GDPR (all'art. 42) incoraggia l'istituzione di meccanismi di certificazione della protezione dei dati per dimostrare la conformità al GDPR dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento.

Le caratteristiche degli Organismi di Certificazione (OdC) che certificano la conformità dei trattamenti di dati personali conformi al GDPR sono stabilite al successivo art. 43 del GDPR, che chiarisce che tali OdC debbano essere accreditati conformemente alla ISO/IEC 17065, che definisce i requisiti propri degli OdC che certificano prodotti, processi e servizi.

La ISO/IEC 27001 (e la sua estensione ISO/IEC 27701) non sono però in linea con l'art. 43 del GDPR; infatti esse sono riferite a Sistemi di Gestione e, come tali, possono essere certificate da Organismi di Certificazione accreditati secondo la ISO/IEC 17021-1, che definisce i requisiti degli organismi che forniscono audit e certificazione di sistemi di gestione.

Per questo motivo riteniamo opportuno introdurre nel contesto del Framework anche lo **schema ISD©10003**. Le relative integrazioni (che in questo lavoro sono limitate alle sole category e subcategory inserite nella nuova versione del Framework Nazionale riguardanti la protezione dei dati personali) alle "Informative References" del Framework Core sono evidenziate in verde.

Esse si concentrano soprattutto sulle nuove Category e Subcategory introdotte successivamente nel *core* del Framework per estendere quegli aspetti riguardanti la protezione dei dati personali che non erano sufficientemente coperti nel Framework originale:

Function	**Category**	**Subcategory**	**Informative References (Extended to ISO/IEC 27701:2019) (Extended to ISDP©10003, only for**

			the new Subcategories DP-XXX)
IDENTIFY (ID)	Asset Management (ID.AM): I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**DP-ID.AM-7:** Sono definiti e resi noti ruoli e responsabilità inerenti al trattamento e la protezione dei dati personali per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	· **GDPR** - Artt. 24, 26-29, 37-39 · **ISO/IEC 27701:2019** 5.2.1, 6.3.1.1, 6.4.2.2, 6.10.2.4, 6.11.2.1, 6.11.2.5, 6.12.1.2, 6.15.1.1, 6.15.1.3, A.7.2.6, A.7.2.7, A.7.2.8, B.8.2.1, B.8.2.2, B.8.2.4, B.8.2.5, B.8.3.1, B.8.4.2, B.8.5.4, B.8.5.6, B.8.5.7, B.8.5.8 · **ISDP©10003:2018** 5.3, A.2.1, A.2.2, A.2.3., A.2.4, A.5.3.2 · **D.Lgs. 30/6/2003 n. 196** Artt. 2-quaterdecies, 2-quinquiesdecies, 2-sexiesdecies · **ISO/IEC 29100:2011** 4.2, 4.3, 5.10
			· **GDPR** - Art. 5, 28, 30, 32 · **ISO/IEC 29100:2011** 4.4 · **ISO/IEC 27701:2019** 6.12.1.2, 6.15.1.1, A.7.2.8, A.7.5.2, A.7.5.3, A.7.5.4, B.8.2.6, B.8.4.2, B.8.5.2, B.8.5.3 · **ISDP©10003:2018** 7.6, 8.1, A.5.1
	Risk Assessment (ID.RA): L'impresa comprende il rischio di cybersecurity inerente l'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.	**DP-ID.RA-7:** Viene effettuata una valutazione di impatto sulla protezione dei dati personali	· **GDPR** - Artt. 35, 36 · **ISO/IEC 29100:2011** 4.5 · **ISO/IEC 29134:2017** · **ISO/IEC 27701:2019** A.7.2.5 · **ISDP©10003:2018** 6.2, 6.3, 7.6, 8.1, A.6.1
	Data Management (DP-ID.DM): i dati personali sono trattati attraverso processi definiti, in coerenza con le normative di riferimento.	**DP-ID.DM-1:** Il ciclo di vita dei dati è definito e documentato	· **GDPR** - Art. 5,6,9-11, 30 · **ISO/IEC 27701:2019** A.7.2.5, A.7.2.8 · **ISDP©10003:2018** 4.1, 6.2, 7.6, A.5.1.1, A.5.1.2, A.5.1.4, A.7.1.1, A.7.2
		DP-ID.DM-2: Sono definiti, implementati e	· **GDPR** - Artt. 12-14

		documentati i processi riguardanti l'informazione dell'interessato in merito al trattamento dei dati	· **ISO/IEC 29100:2011** 5.2, 5.8 · **ISO/IEC 27701:2019** A.7.3.3 · **ISDP©10003:2018** 7.6, A.3.3 · **ISO/IEC 29151:2017** A.3, A.9 · **ISO/IEC 27018:2014** A.1, A.7 · **GDPR** - Artt. 7, 8 · **D.Lgs. 30/6/2003 n. 196** Art. 2-quinquies · **ISO/IEC 29100:2011** 5.2 · **ISO/IEC 27701:2019** A.7.2.3, A.7.2.4, A.7.3.4, B.8.3.1 · **ISDP©10003:2018** 7.6, A.3.2.2, A.3.2.3, A.3.2.4, A.3.2.5, A.3.2.6, A.3.4.1, A.3.4.3, A.3.5.2 · **ISO/IEC 29151:2017** A.3 · **ISO/IEC 27018:2014** A.1
		DP-ID.DM-4: Sono definiti, implementati e documentati i processi per l'esercizio dei diritti (accesso, rettifica, cancellazione, ecc.) dell'interessato	· **GDPR** - Art 15-22 · **D.Lgs. 30/6/2003 n. 196** Art. 2-terdecies · **ISO/IEC 29100:2011** 5.4, 5.5, 5.6, 5.7, 5.8, 5.9 · **ISO/IEC 27701:2019** A.7.3 · **ISDP©10003:2018** 7.6, A.3.4, A.3.5 · **ISO/IEC 29151:2017** A.5, A.6, A.7, A.8, A.9, A.10 · **ISO/IEC 27018:2014** A.3, A.4, A.5, A.6, A.7, A.8
		DP-ID.DM-5: Sono definiti, implementati e documentati i processi di trasferimento dei dati in ambito internazionale	· **GDPR** - Artt. 44-49 · **ISO/IEC 29100:2011** 4.5 · **ISO/IEC 27701:2019** A.7.5 · **ISDP©10003:2018** A.7.1, A.7.2
RESPOND (RS)	Communications (RS.CO): Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**DP-RS.CO-6:** Gli incidenti che si configurano come violazioni di dati personali sono documentati ed eventualmente vengono informati le autorità di riferimento e gli interessati	· **GDPR** - Artt. 33, 34 · **ISO/IEC 29100:2011** 5.10 · **ISO/IEC 291510:2017** A.11 · **ISO/IEC 27018:2014** A.9.1 · **ISO/IEC 27001:2013** A.16 · **ISO/IEC 27701:2019 6.8** · **ISDP©10003:2018** A.5.2.4 · **Misure Minime AgID** ABSC

Tabella 1 - Nuove category e subcategory introdotte nel Framework Nazionale per la Cybersecurity e la Data Protection. (Tratta dal Framework Nazionale) integrate con ISO/IEC 27701 e ISDP©100003

Note

[1] Il National Institute of Standards and Technology (NIST), fondato nel 1901, attualmente fa parte dell'U.S. Department of Commerce.

[2] ISO/IEC 27701:2019 - Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines – First edition 2019-08

[3] Schema di certificazione Data Protection- GDPR accreditato in accordo con la norma EN ISO/IEC 17065:2012

Articolo a cura di **Massimo Montanile**