Framework Nazionale per la Cybersecurity e la Data Protection

Febbraio 2019

Cyber Intelligence and Information Security Center

Sapienza Università di Roma

cini Cyber Security National Lab

CIS SAPIENZA
CYBER INTELLIGENCE AND INFORMATION SECURITY

Framework Nazionale per la Cybersecurity e la Data Protection

CIS-Sapienza
Research Center of Cyber Intelligence and Information Security
Sapienza Università di Roma

CINI Cybersecurity National Lab
Consorzio Interuniversitario Nazionale per l'Informatica

Versione 2.0
Febbraio 2019

cini Cybersecurity National Lab

Titolo: Framework Nazionale per la Cybersecurity e la Data Protection
Distribuito online – http://www.cybersecurityframework.it

Febbraio 2019

Realizzato da:

Autori in ordine alfabetico:

Marco Angelini
Claudio Ciccotelli
Luisa Franchina
Alberto Marchetti Spaccamela
Leonardo Querzoni

Gli autori ringraziano **Alessandro Bruttini** e **Andrea Lucariello** per i commenti ed i suggerimenti ricevuti durante la stesura di questo documento.

Con il supporto dell'Autorità Garante per la Protezione dei Dati Personali e del Dipartimento delle Informazioni per la Sicurezza della Presidenza del Consiglio dei Ministri.

Indice dei contenuti

1 Executive Summary

Il panorama nazionale di cybersecurity è profondamente mutato negli ultimi anni acquisendo una maggiore consapevolezza del rischio cyber e della necessità di adeguate misure di sicurezza. In particolare, la pubblicazione del "Quadro strategico nazionale per la sicurezza dello spazio cibernetico" [1] a cui è seguito il relativo piano operativo [2] (recentemente aggiornato) ha definito i rischi e le priorità nel campo; il piano, tra i vari interventi, suggeriva nell'indirizzo operativo 7 (punto 7.2) di "*Elaborare e pubblicare documenti di riferimento quali manuali […] da utilizzare per lo scambio di informazioni*".

In questo contesto, nel 2015 è stato presentato il *Framework Nazionale per la Cybersecurity* [3], frutto della collaborazione tra accademia, enti pubblici, e imprese private. Il Framework, ispirato al Cybersecurity Framework [5] ideato dal NIST (National Institute of Standards and Technology), fornisce uno strumento operativo per organizzare i processi di cybersecurity adatto alle organizzazioni pubbliche e private, di qualunque dimensione.

Il panorama economico italiano è costituito, nella stragrande maggioranza, da piccole e medie imprese nelle quali personale specifico per affrontare in modo sistematico pratiche di cybersecurity non è presente per questioni strutturali e/o di fatturato. Per queste ragioni, il Framework Nazionale per la Cybersecurity è di difficile attuazione per queste imprese. Per rispondere a queste esigenze nel 2016 il CIS ha presentato il documento *Controlli essenziali di Cybersecurity* [4], che descrive 15 controlli essenziali di facile e, quasi sempre, economica implementazione e che rappresentano le pratiche di sicurezza che non possono essere ignorate.

Il 25 maggio 2018, a due anni dalla sua entrata in vigore, è diventato operativo il Regolamento Generale sulla Protezione dei Dati (GDPR – nel seguito di questo documento anche indicato semplicemente come *Regolamento*) che disciplina il trattamento e la circolazione dei dati personali. Il Regolamento ha imposto un cambiamento di prospettiva rispetto alla protezione dei dati personali introducendo il principio dell'accountability. A più di sei mesi dalla piena applicazione del Regolamento l'implementazione dello stesso rappresenta un passo fondamentale per qualsiasi organizzazione che intenda trattare dati personali.

Negli ultimi anni le minacce cyber sono ulteriormente evolute in qualità e quantità. Oggi un problema fondamentale è rappresentato dai data breach che sottraggono in modo fraudolento dati, anche sensibili, dalle banche dati di industrie, enti pubblici ed organizzazioni di ogni genere. I data breach rappresentano un danno spesso ingente per le organizzazioni e oggi, alla luce delle norme previste dal Regolamento, possono essere causa di consistenti multe.

Questo documento propone un *Framework Nazionale per la Cybersecurity e la Data Protection* (in seguito indicato solamente come *Framework*) per supportare le organizzazioni che necessitano di strategie e processi volti alla protezione dei dati personali e alla sicurezza cyber. Rispetto alla versione presentata nel 2015 questo documento introduce contributi volti a cogliere gli aspetti fondamentali legati alla protezione dei dati secondo quanto previsto nel Regolamento.

Si noti che il Framework è uno strumento di supporto alle organizzazioni e non può in alcun modo essere considerato uno strumento per il rispetto ai regolamenti vigenti. Ciononostante, la sua adozione può aiutare le organizzazioni nel definire un percorso volto alla cybersecurity e alla protezione dei dati coerente con i regolamenti stessi 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.

1.1 Guida alla lettura

La sezione 2 introduce la nuova versione del Framework, descrivendone i contenuti, proponendo una breve guida all'uso, e discutendo l'integrazione delle novità apportate con il documento sui Controlli Essenziali di Cybersecurity.

Per favorire una maggiore leggibilità e fornire un testo auto-contenuto, alcuni dei concetti fondamentali definiti in [3] sono brevemente introdotti nella Sezione 2.1. In particolare, si introducono le tre nozioni fondamentali di *Framework Core, Profile* e *Implementation Tier*. Il Framework Core rappresenta la struttura del ciclo di vita del processo di gestione della cybersecurity, sia dal punto di vista tecnico che organizzativo ed è strutturato gerarchicamente in *function*, *category* e *subcategory*. Il Framework definisce, per ogni function, category e subcategory, le attività abilitanti, quali processi e tecnologie, da realizzare per gestire la singola function. A questo scopo il Framework Core associa ad ogni singola subcategory i riferimenti alle pratiche di sicurezza previste da standard di settore o da regolamentazioni generali vigenti e che sono il punto di partenza per una implementazione corretta e sicura. L'Appendice A presenta il Framework Core nella sua interezza.

Le diverse subcategory del Framework sono molte e hanno l'obiettivo di coprire in modo esaustivo tutte le possibili esigenze di una organizzazione. Pertanto, nella maggioranza dei casi, una singola organizzazione è interessata solamente ad un sottoinsieme delle stesse. I Profili rappresentano il risultato della selezione di specifiche subcategory del Framework; la selezione è basata su diversi fattori: la valutazione del rischio, il contesto di business, l'applicabilità delle varie subcategory all'organizzazione ecc. I Profili possono anche essere utilizzati come opportunità per migliorare lo stato di sicurezza mettendo a confronto un profilo attuale con il profilo desiderato. Infine, gli Implementation Tier forniscono contesto sul livello di integrazione dei processi di gestione del rischio cyber. La Sezione 2.1 prosegue introducendo i concetti dei *livelli di priorità* e *livelli di maturità* che permettono di realizzare uno strumento flessibile che si adatta alle specifiche esigenze dell'organizzazione e tiene conto della sua maturità nell'affrontare il rischio cyber. Infine viene introdotto un nuovo strumento, dal nome di *prototipi di contestualizzazione,* adatto a rappresentare norme, regolamenti o best practice di settore attraverso un a opportuna selezione di subcategory.

Gli elementi del Framework, precedentemente introdotti, sono generali ed indipendenti rispetto al settore produttivo, alla tipologia degli impiegati, alla dimensione e alla dislocazione sul territorio di una organizzazione che intende adottare il Framework. Quando si applica il Framework, tutti o alcuni degli elementi precedentemente descritti possono essere tenuti in considerazione. Nella Sezione 2.2 si presenta la guida all'utilizzo del Framework attraverso la contestualizzazione ad uno specifico ambito applicativo e le modalità di applicazione ad una singola organizzazione. Contestualizzare il Framework per uno specifico ambito applicativo (es. un settore produttivo o una categoria omogenea di organizzazioni) richiede di specificare il core di interesse selezionando le function, category e subcategory rilevanti, e di definire i livelli di priorità e maturità per le subcategory selezionate eventualmente facendo uso di prototipi precedente te definiti.

Nella Sezione 2.3 si presentano i 15 Controlli Essenziali di Cybersecurity [4] organizzati in otto tematiche. Per ciascuna tematica, sono discusse la relazione dei relativi controlli con la nuova versione del Framework Nazionale coerente con la protezione dei dati personali.

La Sezione 3 e l'Appendice B presentano il prototipo di contestualizzazione del Framework per cogliere gli elementi fondamentali del Regolamento. Il prototipo fornisce una guida di supporto alla pianificazione delle attività necessarie per adeguarsi alla normativa e di successivo monitoraggio per l'implementazione e gestione delle attività previste dal Regolamento. Per ciascuna subcategory individuata si forniscono i relativi riferimenti alla normativa GDPR di interesse.

2 Framework Nazionale per la Cybersecurity e la Data Protection

Come l'originale *Framework Nazionale di Cybersecurity* [3], anche la versione presentata in questo documento è basata sul Cybersecurity Framework sviluppato dal National Institute of Standards and Technology, recentemente aggiornato alla versione 1.1 [5]. In particolare, sono stati integrati i cambiamenti apportati dal NIST al Framework *Core,* includendo quindi elementi volti a considerare le problematiche di sicurezza delle filiere di approvvigionamento (*supply chain*) e ad approfondire la sicurezza dei processi di autenticazione e gestione delle identità.

La nuova versione del Framework include inoltre 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 subcategory e una nuova category che colgono i seguenti aspetti legati alla data protection:

- i processi di data management, con particolare riferimento a quelli applicabili ai dati personali;
- le modalità di trattamento dei dati personali;
- i ruoli e le responsabilità nella gestione dei dati personali;
- la valutazione di impatto sulla protezione dei dati personali;
- le modalità di documentazione e comunicazione a seguito di incidenti che si configurino come violazione dei dati personali.

Tali elementi, assenti nella versione precedente del Framework, allineano lo stesso ai diversi standard che già trattano il problema della protezione dei dati personali e lo rendono applicabile anche in contesti in cui le regolamentazioni generali o di settore impongono specifici requisiti sul trattamento dei dati.

Infine, viene introdotto un nuovo strumento per la contestualizzazione del Framework sotto forma di *prototipi di contestualizzazione*. Tale strumento permette di definire dei *template* applicabili in fase di contestualizzazione per poter integrare più facilmente nella stessa concetti legati a normative, regolamenti o best practice.

2.1 Elementi fondamentali del Framework

Il Framework eredita le tre nozioni fondamentali del Cybersecurity Framework NIST: *Framework Core, Profile e Implementation Tier*. Di seguito ne diamo una breve descrizione, rimandando al documento originale [5] per maggiori dettagli.

Framework Core – Il core rappresenta la struttura del ciclo di vita del processo di gestione della cybersecurity, sia dal punto di vista tecnico sia organizzativo. Il core è strutturato gerarchicamente in *function*, *category* e *subcategory*. Le function, concorrenti e continue, sono: *IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER* e costituiscono le principali tematiche da affrontare per operare una adeguata gestione del rischio cyber in modo strategico. Il Framework quindi definisce, per ogni function, category e subcategory, le attività abilitanti, quali processi e tecnologie, da mettere in campo per gestire la singola function. Il Framework Core presenta inoltre delle *informative reference*, dei riferimenti che legano la singola subcategory alle pratiche di sicurezza note previste da standard di settore (ISO, SP800-53r4, COBIT-5, SANS20 e altri) o da regolamentazioni generali vigenti (Regolamento UE 2016/679 General Data Protection Regulation, Direttiva UE 2016/1148 NIS). Tali riferimenti hanno principalmente uno scopo illustrativo e non devono essere interpretati come esaustivi. La struttura del Framework Core è riportata in Figura 1.

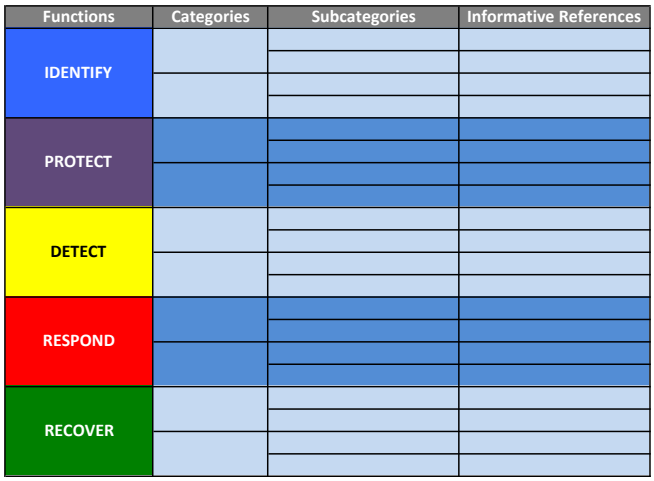

Figura 1: Struttura del Framework Core (cfr. [5]).

Di seguito è riportata una breve descrizione delle 5 function:

IDENTIFY - La function IDENTIFY è legata alla comprensione del contesto aziendale, degli asset che supportano i processi critici di business e dei relativi rischi associati. Tale comprensione permette a un'organizzazione di definire risorse e investimenti in linea con la strategia di gestione del rischio e con gli obiettivi aziendali. Le category all'interno di questa function sono: Asset Management, Business Environment; Governance, Risk Assessment, Risk Management Strategy, Supply Chain Risk Management e Data Management.

PROTECT - La function PROTECT è associata all'implementazione di quelle misure volte alla protezione dei processi di business e degli asset aziendali, indipendentemente dalla loro natura informatica. Le category all'interno di questa function sono: Identity Management, Authentication and Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, Protective Technology.

DETECT - La function DETECT è associata alla definizione e attuazione di attività appropriate per identificare tempestivamente incidenti di sicurezza informatica. Le category all'interno di questa function sono: Anomalies and Events, Security Continuous Monitoring, Detection Processes.

RESPOND - La function RESPOND è associata alla definizione e attuazione delle opportune attività per intervenire quando un incidente di sicurezza informatica sia stato rilevato. L'obiettivo è contenere l'impatto determinato da un potenziale incidente di sicurezza informatica. Le category all'interno di questa function sono: Response Planning, Communications, Analysis, Mitigation, Improvements.

RECOVER - La function RECOVER è associata alla definizione e attuazione delle attività per la gestione dei piani e delle attività per il ripristino dei processi e dei servizi impattati da un incidente. L'obiettivo è garantire la resilienza dei sistemi e delle infrastrutture e, in caso di incidente, supportare il recupero tempestivo delle business operations. Le category all'interno di questa function sono: Recovery Planning, Improvements, Communications.

La versione del Framework presentata in questo documento incorpora nel core nuovi elementi riguardanti la protezione dei dati personali che non sono erano sufficientemente colti dalle subcategory già presenti nel Framework originale. In particolare, vengono introdotte delle nuove category e subcategory evidenziate in giallo nella tabella seguente ed identificate dal prefisso "DP-".

Tabella 1: Nuove category e subcategory introdotte nel Framework Nazionale per la Cybersecurity e la Data Protection.

FUNCTION	CATEGORY	SUBCATEGORY
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)
		DP-ID.AM-8: I trattamenti di dati personali sono identificati e catalogati
	Risk Assessment (ID.RA): L'impresa comprende il rischio di cybersecurity inerente all'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
	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
		DP-ID.DM-2: Sono definiti, implementati e documentati i processi riguardanti l'informazione dell'interessato in merito al trattamento dei dati
		DP-ID.DM-3: Sono definiti, implementati e documentati i processi di raccolta e revoca del consenso dell'interessato al trattamento di dati
		DP-ID.DM-4: Sono definiti, implementati e documentati i processi per l'esercizio dei diritti (accesso, rettifica, cancellazione, ecc.) dell'interessato
		DP-ID.DM-5: Sono definiti, implementati e documentati i processi di trasferimento dei dati in ambito internazionale
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

In aggiunta a tali elementi, il Framework integra i cambiamenti apportati al core del Cybersecurity Framework NIST con l'introduzione della versione 1.1 [5], e in particolare:

- È stata introdotta una category *Supply Chain Risk Management* (ID.SC) nella function IDENTIFY, al fine di gestire il rischio cyber all'interno delle filiere produttive complesse e nelle catene di approvvigionamento.
- La category PR.AC della function PROTECT è stata rinominata *Identity Management, Authentication and Access Control* ed ora include elementi legati alla gestione delle

identità e dei relativi processi di autenticazione. In particolare, la category ora include due nuove subcategory (PR.AC-6 e PR.AC-7) dedicate alla gestione delle identità e dei processi di autenticazione.

- È stata introdotta una subcategory PR.DS-8 che introduce l'uso di meccanismi di controllo dell'integrità applicati ai dispositivi hardware.
- È stata introdotta una subcategory PR.PT-5 che introduce l'uso di meccanismi per il soddisfacimento di requisiti di resilienza.
- È stata introdotta una subcategory RS.AN-5 per trattare informazioni inerenti alle vulnerabilità.

Profili – I Profili rappresentano il risultato della selezione, da parte di un'organizzazione, di specifiche subcategory del Framework. Tale selezione è basata su diversi fattori: la valutazione del rischio, il contesto di business, l'applicabilità delle varie subcategory all'organizzazione. I profili possono essere utilizzati come opportunità per migliorare lo stato di sicurezza mettendo a confronto un profilo attuale (profilo *corrente*), con il profilo desiderato (profilo *target*). Rimandando a [3] per una trattazione dettagliata, si ricorda che, per sviluppare un profilo, un'organizzazione deve esaminare ciascuna delle subcategory e, sulla base dei propri obiettivi e della valutazione dei propri rischi, determinare quali siano applicabili nel proprio contesto. Le subcategory potranno essere integrate con ulteriori pratiche non previste dal Framework al fine di gestire in maniera completa il rischio. Il profilo attuale può quindi essere utilizzato per definire priorità e misurare i progressi verso il profilo desiderato. I profili possono essere utilizzati, inoltre, per effettuare un'autovalutazione o per comunicare il proprio livello di gestione del rischio cyber all'interno o all'esterno dell'organizzazione.

Implementation Tier – Gli Implementation Tier forniscono contesto sul livello di integrazione dei processi di gestione del rischio cyber all'interno dell'organizzazione. Sono previsti quattro livelli di valutazione, dal più debole al più forte:

Parziale - Il modello di gestione del rischio di cybersecurity di una organizzazione è parziale se questo non tiene conto in modo sistematico del rischio cyber o delle minacce ambientali. Il rischio cyber è gestito con processi *ad hoc* e spesso in modo reattivo. Il livello di consapevolezza del rischio a livello organizzativo è limitato. Non esistono processi di condivisione delle informazioni inerenti alla cybersecurity con entità esterne.

Informato - Il modello di gestione del rischio cyber di una organizzazione è informato se l'organizzazione ha dei processi interni che tengono conto del rischio cyber, ma questi non sono estesi a tutta l'organizzazione. Il livello di consapevolezza del rischio cyber è sufficientemente esteso, ma questo non è accompagnato da processi di gestione pervasivi che coinvolgano tutti i livelli dell'organizzazione. L'organizzazione comprende il suo ruolo nell'ecosistema di riferimento, ma lo scambio informativo relativo agli eventi di cybersecurity è limitato e tipicamente passivo.

Ripetibile - Il modello di gestione del rischio cyber di una organizzazione è ripetibile se è formalmente definito ed approvato e se l'organizzazione aggiorna regolarmente le proprie pratiche di cybersecurity basandosi sull'output del processo di risk management. La gestione del rischio cyber è pervasiva a tutti i livelli organizzativi ed il personale è formato per gestire i ruoli che in merito gli vengono assegnati. L'organizzazione scambia regolarmente informazione inerenti alla cybersecurity con altri attori operanti nello stesso ecosistema.

Adattivo - Il modello di gestione del rischio cyber di una organizzazione è adattivo se l'organizzazione adatta le sue procedure di cybersecurity regolarmente attraverso l'utilizzo delle esperienze passate e degli indicatori di rischio. Attraverso un processo adattivo l'organizzazione si adegua in modo continuo a minacce in continua evoluzione ed è capace di

rispondere efficacemente ad attacchi sofisticati. Lo scambio informativo con altri attori operanti nello stesso ecosistema è continuo ed avviene in tempo reale.

Livelli di priorità – I livelli di priorità permettono di supportare le organizzazioni e le aziende nella definizione di un programma di implementazione per raggiungere un profilo target che favorisca in modo prioritario gli interventi che maggiormente riducono i livelli di rischio a cui sono sottoposte. L'obiettivo complessivo è:

- semplificare l'individuazione delle subcategory essenziali da implementare immediatamente e inderogabilmente;
- supportare le organizzazioni durante il processo di analisi e gestione del rischio.

La determinazione dei livelli di priorità assegnati alle subcategory deve essere effettuata sulla base di due specifici criteri:

- capacità di ridurre il rischio cyber, agendo su uno o più fattori chiave per la sua determinazione, ovvero:
  - esposizione alle minacce, intesa come l'insieme dei fattori che aumentano o diminuiscono la probabilità con cui la minaccia stessa può manifestarsi;
  - probabilità di loro accadimento, ovvero la frequenza con cui una specifica minaccia può verificarsi nel tempo;
  - impatto conseguente sulle Business Operations o sugli Asset aziendali, intesa come entità del danno conseguente al verificarsi di una minaccia;
- semplicità di implementazione delle subcategory, anche considerando il livello di maturità tecnologica e organizzativa tipicamente richiesto per realizzare la specifica azione.

Il Framework prevede tre livelli generali di priorità:

ALTA: interventi che permettono di ridurre sensibilmente uno dei tre fattori chiave del rischio cyber. Questi interventi sono prioritari e per loro natura sono da attuare indipendentemente dalla complessità realizzativa degli stessi;

MEDIA: interventi che permettono di conseguire una riduzione di uno dei tre fattori chiave del rischio cyber e che risultano generalmente anche di semplice implementazione;

BASSA: interventi che permettono di conseguire una riduzione di uno dei tre fattori chiave del rischio cyber, ma la cui complessità realizzativa è generalmente considerata elevata (ad esempio cambiamenti organizzativi rilevanti e/o modifiche infrastrutturali significative).

Da notare che le subcategory assumono priorità specifica per la contestualizzazione (si veda §2.2) adottata oppure assumono priorità specifica al contesto dell'organizzazione (eventualmente basati sulla valutazione del rischio associato), pertanto ogni organizzazione, nell'adozione del Framework o nel corso dell'attività di contestualizzazione, potrebbe ridefinire specifici livelli di priorità per ogni subcategory.

Livelli di maturità – I livelli di maturità permettono di fornire una misura della maturità di un processo di sicurezza, della maturità di attuazione di una tecnologia specifica o una misura della quantità di risorse adeguate impiegate per l'implementazione di una data subcategory.

I livelli di maturità forniscono un punto di riferimento in base al quale ogni organizzazione può valutare la propria implementazione delle subcategory e fissare obiettivi e priorità per il loro miglioramento. I livelli devono essere definiti in progressione crescente, dal minore al maggiore. Ogni livello deve prevedere pratiche e controlli incrementali rispetto al livello di

maturità inferiore. Un'organizzazione valuterà la soddisfazione dei controlli per identificare il livello di maturità raggiunto. Per alcune subcategory potrebbe non essere possibile definire livelli di maturità.

Si devono prevedere le seguenti caratteristiche nella definizione dei livelli di maturità:

- specificità per subcategory - un'organizzazione potrà avere livelli differenti di maturità per subcategory differenti;
- completezza delle pratiche di sicurezza - il livello di maturità di una subcategory è almeno quello in cui tutte le relative pratiche di sicurezza sono implementate.

Questo consente di:

- definire il proprio livello di maturità in maniera parziale o complessiva;
- identificare il livello desiderato: parziale o complessivo;
- identificare le pratiche di sicurezza necessarie per raggiungere il livello desiderato.

Prototipi di contestualizzazione – I prototipi di contestualizzazione sono un nuovo strumento introdotto nel Framework per permettere la definizione di *template* utilizzabili per la contestualizzazione in specifici settori (si veda in proposito §2.2). I prototipi possono essere utilizzati, ad esempio, per cogliere attraverso il Framework:

- specifiche normative che richiedono l'attuazione di determinate pratiche indirizzate alla cybersecurity o alla data protection;
- regolamenti tecnici e di attuazione che indicano puntuali controlli legati alla cybersecurity o alla data protection;
- *best practice* di settore inerenti alla cybersecurity o alla data protection.

Un prototipo di contestualizzazione contiene i seguenti elementi:

1. Per ogni subcategory del Framework core definisce la relativa classe di implementazione tra le seguenti opzioni:
    - **OBBLIGATORIA**: la subcategory deve essere inclusa in tutte le contestualizzazioni che implementano il prototipo;
    - **CONSIGLIATA**: si suggerisce l'inclusione della subcategory in tutte le contestualizzazioni che implementano il prototipo;
    - **LIBERA**: l'inclusione della subcategory nelle contestualizzazioni che implementano il prototipo è lasciata alla libera scelta di chi definisce tali contestualizzazioni.
2. Per ogni subcategory può definire un livello di priorità per la relativa implementazione.

Viene inoltre accompagnato da una guida all'implementazione, un documento che descrive:

- Il contesto di applicazione del prototipo;
- Ulteriori vincoli sulla selezione delle subcategory e la definizione dei livelli di priorità;
- Un elenco di controlli di sicurezza, per le subcategory considerate, che andranno, in fase di implementazione del prototipo in una contestualizzazione, opportunamente organizzati nei diversi livelli di maturità eventualmente previsti.

Un prototipo di contestualizzazione rappresenta, a tutti gli effetti, un elemento fondamentale sulla base del quale è possibile costruire una nuova contestualizzazione o che può essere adottato ed implementato in una contestualizzazione esistente. È quindi importante sottolineare che i prototipi di contestualizzazione non sostituiscono le contestualizzazioni, ma forniscono

uno strumento di supporto che facilità la creazione e l'aggiornamento di una contestualizzazione, attraverso la composizione di più prototipi.

2.2 Guida all'uso del Framework

L'utilizzo del Framework si realizza attraverso due attività fondamentali descritte nel seguito di questa sezione: (i) la contestualizzazione del Framework ad uno specifico ambito applicativo e (ii) l'applicazione del Framework ad una organizzazione.

2.2.1 Contestualizzazione

Contestualizzare il Framework per un ambito applicativo (es. un settore produttivo o una categoria omogenea di organizzazioni) significa specificare il suo core selezionando le function, category e subcategory rilevanti, e definire i livelli di priorità e maturità per le subcategory selezionate.

Gli elementi fondanti del Framework, introdotti in §2.1, sono generali ed indipendenti rispetto, ad esempio, al settore produttivo, alla tipologia degli impiegati, alla dimensione e alla dislocazione sul territorio di una organizzazione che intende adottare il Framework. Quando si contestualizza il Framework, tutti o alcuni degli elementi precedentemente descritti possono essere tenuti in considerazione.

Una contestualizzazione del Framework si crea attraverso i seguenti passi:

1. selezionare l'elenco delle function, category, subcategory che sono pertinenti per l'organizzazione in base a tutti o alcuni dei precedenti elementi (settore produttivo, dimensione e dislocazione sul territorio dell'organizzazione, ecc.);
2. definire i livelli di priorità per l'implementazione delle subcategory selezionate;
3. definire delle linee guida almeno per le subcategory a priorità alta;
4. specificare i livelli di maturità almeno per le subcategory a priorità alta.

Tutte le organizzazioni che decidono di adottare una specifica contestualizzazione del Framework (cfr. §2.2.2) devono sempre implementare le subcategory a priorità alta, almeno al livello minimo di maturità.

La definizione di una contestualizzazione è usualmente demandata alla singola organizzazione che decide di adottare il Framework, ma può essere anche fornita da una associazione di settore, un regolatore o, più in generale, da qualsiasi attore sia in grado di identificare ed applicare alla contestualizzazione un insieme di caratteristiche proprie di una o più organizzazioni.

Nel processo di definizione è possibile implementare uno o più prototipi per cogliere nella contestualizzazione risultante i concetti che gli stessi includono. Ad esempio, una organizzazione potrebbe voler includere nella propria contestualizzazione del Framework elementi normativi rappresentati da diversi prototipi di contestualizzazione, per poi raffinare la contestualizzazione risultante rispetto alle proprie specificità.

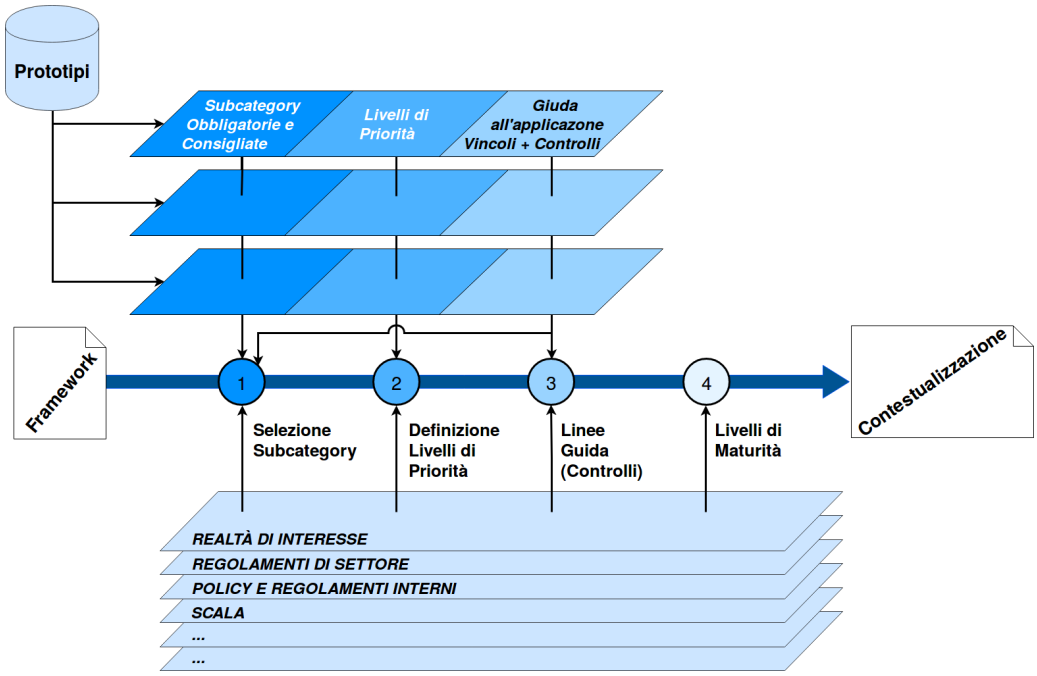

Figura 2: Contestualizzazione del Framework attraverso l'implementazione di prototipi.

Il processo di implementazione di un prototipo in una contestualizzazione, rappresentato in Figura 2, avviene seguendo i seguenti passi:

1. tutte le subcategory indicate come obbligatorie nel prototipo vengono selezionate nella contestualizzazione;
2. la selezione nella contestualizzazione delle subcategory indicate come consigliate nel prototipo deve essere attentamente valutata in considerazione delle specifiche caratteristiche dell'ambito applicativo previsto per la contestualizzazione;
3. gli eventuali ulteriori vincoli sulla selezione delle subcategory documentati nella guida di applicazione del prototipo devono essere applicati;
4. per ogni subcategory selezionata a seguito dei precedenti passi deve essere indicato nella contestualizzazione un livello di priorità, preferibilmente almeno pari o superiore a quello indicato nel prototipo, tenendo conto di eventuali vincoli documentati nella guida di applicazione del prototipo;
5. gli eventuali controlli di sicurezza documentati nella guida di applicazione del prototipo possono essere integrati nelle linee guida all'applicazione della contestualizzazione.

A valle di questo processo di implementazione, ripetuto per tutti i prototipi di interesse, la contestualizzazione risultante può essere ulteriormente specializzata, laddove se ne ravveda la necessità.

2.2.2 Applicazione

L'obiettivo principale del Framework è fornire alle organizzazioni interessate uno strumento di supporto al processo di gestione e trattamento del rischio cyber. È plausibile che in molte realtà si siano già avviati da tempo programmi di cybersecurity e siano già implementati standard per la data protection, in ragione dei quali l'introduzione del Framework è da intendersi non tanto per sostituire quanto già in essere, ma come ulteriore riferimento al fine di:

- migliorare o definire, se non presente, un programma di cybersecurity e data protection in maniera strutturata e integrata, fondato sulla gestione del rischio, che possa essere implementato in presenza di modelli preesistenti di governance della security;
- permettere di determinare agevolmente il livello di maturità delle attività di cybersecurity e data protection identificando, a seconda dei casi, gli interventi migliorativi o di razionalizzazione dei costi, a favore di una redistribuzione ragionata delle risorse;
- completare benchmark tra aziende e organizzazioni operanti in settori specifici o aventi analoghe caratteristiche che possano, a livello nazionale, favorire il miglioramento dei livelli di sicurezza, abilitando contestualmente il mercato del cyber insurance;
- agevolare e facilitare la comunicazione con il top management (es. amministratori e consigli di amministrazione, azionisti ecc.) e con gli interlocutori esterni (ad esempio agenzie di rating, fornitori e partner), affinché siano rappresentati chiaramente i livelli di rischio cyber al quale le organizzazioni sono esposte e affinché siano identificati gli investimenti e le risorse da mettere in campo per un adeguata riduzione del rischio.

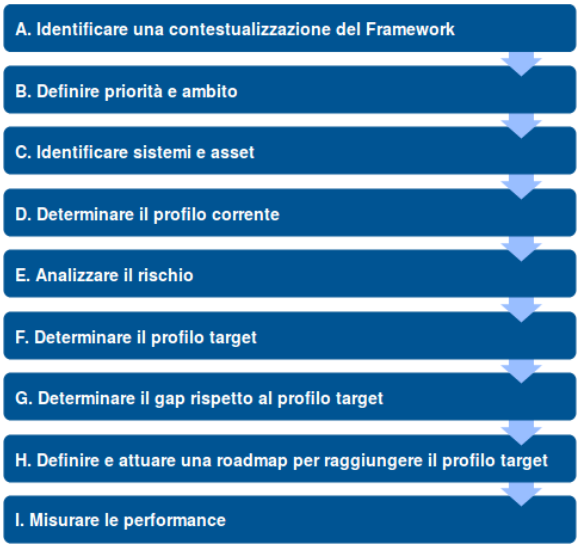

Figura 3: Applicazione del Framework.

L'applicazione del Framework prevede i seguenti passi essenziali (si veda Figura 3):

A. Identificare una contestualizzazione del Framework - Nel caso in cui l'organizzazione appartenga ad un settore regolato, questa dovrebbe utilizzare una delle contestualizzazioni fornite dal proprio regolatore di settore, o definire una propria contestualizzazione implementando eventuali prototipi che colgono i regolamenti applicabili. Nel caso in cui l'organizzazione non appartenga ad un settore regolato può identificare tra le contestualizzazioni disponibili quella da utilizzare nel processo di implementazione del Framework, piuttosto che definirne una specifica.

B. Definire priorità e ambito - Identificare periodicamente gli obiettivi strategici e le priorità di business dell'organizzazione in modo da selezionare aree e funzioni chiave che necessitino specifica focalizzazione.

C. Identificare sistemi e asset - Individuazione delle informazioni e dei sistemi (sia dell'ambito IT che di quello industriale) che l'organizzazione ritiene vitali e critici per garantire

l'operatività dell'organizzazione stessa. Tale passaggio è importante soprattutto per le fasi successive, in quanto consente di valutare propriamente gli impatti durante l'analisi dei rischi e di agevolare pertanto la comprensione delle effettive necessità di protezione;

D. Determinare il profilo corrente - È previsto che sia valutato lo stato di implementazione e il livello di maturità per ciascuna subcategory del Framework. Questo permette di definire uno o più profili correnti in relazione alle aree/funzioni previste per l'implementazione del programma;

E. Analizzare il rischio - Determinare e valutare i rischi mediante l'adozione di una metodologia considerata appropriata, in relazione alle specifiche caratteristiche organizzative e di mercato nel quale opera l'organizzazione. Alcuni spunti in merito al processo di analisi e gestione dei rischi sono forniti in [3] §7.2;

F. Determinare il profilo target - Attraverso il processo di trattamento del rischio, l'organizzazione deve poter definire un profilo target che, differentemente da quello corrente, rappresenta il livello di implementazione e di maturità che si ambisce a conseguire per ciascuna subcategory del Framework. Laddove questo sia possibile è auspicabile che la selezione di tali livelli possa essere effettuata avendo a priori integrato il cybersecurity risk management all'interno del programma di enterprise risk management, in modo che la gestione del rischio cyber possa beneficiare di decisioni prese al livello organizzativo più elevato (i.e., top management), avvalendosi di una visione sistemica complessiva a supporto del processo decisionale;

G. Determinare il gap rispetto al profilo target - Completare una comparazione tra il profilo target e quello corrente per identificare i gap esistenti nella gestione della cybersecurity;

H. Definire e attuare una roadmap per raggiungere il profilo target - La fase attuativa del processo di adozione del Framework consiste nel definire l'insieme di attività necessarie a raggiungere il profilo target determinato nella fase precedente. Ciò significa elaborare un piano specifico per realizzare i singoli controlli del Framework, secondo un piano temporale che varierà in relazione agli effettivi rischi individuati e in funzione delle condizioni specifiche in cui opera la singola organizzazione;

I. Misurare le performance - Affinché l'efficienza del profilo target sia oggetto di revisioni periodiche e miglioramento continuo, è necessario che siano definite delle metriche di monitoraggio in grado di evidenziarne anche i costi operativi. Le valutazioni sull'efficienza del profilo corrente devono essere utilizzate per definire il nuovo profilo target.

È previsto che il Framework possa essere impiegato per la valutazione del livello di maturità delle attività e processi di cybersecurity. Questa applicazione, complementare alla precedente, prevede un processo più snello che permetta di valutare rapidamente i gap esistenti e di definire un piano di azione per il loro miglioramento. Il processo operativamente prevede passaggi analoghi a quelli descritti in precedenza, fatto salvo per il passaggio relativo alla valutazione del rischio.

2.3 Integrazione dei Controlli Essenziali

L'illusione che solo le grandi imprese siano bersaglio di attacchi da parte dei cyber-criminali lascia spesso le medie, piccole e micro imprese totalmente impreparate ad affrontare la minaccia cyber. Ciò non solo espone le imprese stesse a minacce in grado di minarne la sopravvivenza, ma aumenta il rischio cyber all'interno dell'intera filiera produttiva in cui esse operano.

Per tali imprese implementare una gestione del rischio cyber basata sul Framework Nazionale può risultare troppo complesso e oneroso. È chiaro quindi che un percorso volto a raggiungere

un livello adeguato di protezione contro la minaccia cyber debba partire da una base di semplice e relativamente economica implementazione. In quest'ottica nell'Italian Cybersecurity Report del 2016 [4] sono stati proposti 15 Controlli Essenziali di Cybersecurity derivati dal Framework Nazionale attraverso un processo di progressiva semplificazione. È evidente che la sola implementazione di questi 15 controlli non assicura un livello adeguato di sicurezza. Essi rappresentano un insieme minimo di pratiche di sicurezza che non possono essere ignorate; una base dalla quale deve partire un percorso di miglioramento progressivo che porti ad allinearsi con la metodologia di gestione della cybersecurity basata sul Framework Nazionale.

In Tabella 2 sono riportati i 15 Controlli Essenziali organizzati in otto tematiche di cybersecurity. Per una discussione approfondita sulle tematiche e i relativi controlli si rimanda il lettore al documento originale [4]. Nei prossimi paragrafi, invece, per ciascuna tematica, verrà discussa la relazione dei relativi controlli con la nuova versione del Framework Nazionale.

Tabella 2: I Controlli Essenziali di Cybersecurity

Tematiche		Controlli Essenziali di Cybersecurity
Inventario dispositivi e software	1	Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale.
	2	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc...) offerti da terze parti a cui si è registrati sono quelli strettamente necessari.
	3	Sono individuate le informazioni, i dati e i sistemi critici per l'azienda affinché siano adeguatamente protetti.
	4	È stato nominato un referente che sia responsabile per il coordinamento delle attività di gestione e di protezione delle informazioni e dei sistemi informatici.
Governance	5	Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in tema di cybersecurity che risultino applicabili per l'azienda.
Protezione da malware	6	Tutti i dispositivi che lo consentono sono dotati di software di protezione (antivirus, antimalware, ecc...) regolarmente aggiornato.
Gestione password e account	7	Le password sono diverse per ogni account, della complessità adeguata e viene valutato l'utilizzo dei sistemi di autenticazione più sicuri offerti dal provider del servizio (es. autenticazione a due fattori).
	8	Il personale autorizzato all'accesso, remoto o locale, ai servizi informatici dispone di utenze personali non condivise con altri; l'accesso è opportunamente protetto; i vecchi account non più utilizzati sono disattivati.
	9	Ogni utente può accedere solo alle informazioni e ai sistemi di cui necessita e/o di sua competenza.
Formazione e consapevolezza	10	Il personale è adeguatamente sensibilizzato e formato sui rischi di cybersecurity e sulle pratiche da adottare per l'impiego sicuro degli strumenti aziendali (es. riconoscere allegati e-mail, utilizzare solo software autorizzato, ...). I vertici aziendali hanno cura di predisporre per tutto il personale aziendale la formazione necessaria a fornire almeno le nozioni basilari di sicurezza.

Protezione dei dati	11	La configurazione iniziale di tutti i sistemi e dispositivi è svolta da personale esperto, responsabile per la configurazione sicura degli stessi. Le credenziali di accesso di default sono sempre sostituite.
	12	Sono eseguiti periodicamente backup delle informazioni e dei dati critici per l'azienda (identificati al controllo 3). I backup sono conservati in modo sicuro e verificati periodicamente.
Protezione delle reti	13	Le reti e i sistemi sono protetti da accessi non autorizzati attraverso strumenti specifici (es: Firewall e altri dispositivi/software anti-intrusione).
Prevenzione e mitigazione	14	In caso di incidente (es. venga rilevato un attacco o un malware) vengono informati i responsabili della sicurezza e i sistemi vengono messi in sicurezza da personale esperto.
	15	Tutti i software in uso (inclusi i firmware) sono aggiornati all'ultima versione consigliata dal produttore. I dispositivi o i software obsoleti e non più aggiornabili sono dismessi.

2.3.1 Inventario dispositivi e software

Nella tematica di sicurezza "Inventario dispositivi e software" troviamo i primi quattro Controlli Essenziali, la cui relazione con la nuova versione del Framework Nazionale è riassunta nella Tabella 3. La tabella mostra gli elementi del Framework su cui ciascun controllo ha un impatto. Tra questi elementi sono stati evidenziati in giallo quelli introdotti nella nuova versione del Framework. In particolare, le subcategory DP-ID.AM-7 e DP-ID.AM-8.

La subcategory DP-ID.AM-7 riguarda la definizione di ruoli e responsabilità inerenti alla data protection. È evidente, quindi, come tale subcategory sia relazionata al Controllo Essenziale 4, che prevede la nomina di un referente che sia responsabile non solo della protezione dei sistemi informatici, ma anche delle informazioni. Infatti, se da un lato, tale controllo riguarda evidentemente la nomina di una figura con responsabilità inerenti alla cybersecurity, va anche notato che una corretta protezione delle informazioni non può prescindere dalla tutela dei dati personali contro trattamenti illeciti e violazioni che possano ledere i diritti e le libertà delle persone, oltre che risultare in ingenti sanzioni.

La subcategory DP-ID.AM-8, riguarda l'individuazione e catalogazione dei trattamenti di dati personali. Questa subcategory è relazionata al Controllo Essenziale 3. Infatti, quest'ultimo richiede l'individuazione delle informazioni, dei dati e dei sistemi critici per l'azienda. Dato l'impatto che una eventuale violazione o trattamento illecito di dati personali può avere sugli individui e sull'azienda stessa in seguito a eventuali sanzioni, appare evidente come i dati personali debbano essere considerati dati critici per l'azienda e in quanto tali vadano individuati e catalogati al pari delle altre tipologie di dato e dei sistemi critici per l'azienda.

Tabella 3: Relazione dei Controlli Essenziali della tematica "Inventario dispositivi e software" con il Framework Nazionale per la Cybersecurity e la Data Protection.

<table>
<tr><th>FUNCTION</th><th>CATEGORY</th><th>SUBCATEGORY</th><th>CONTROLLO</th></tr>
<tr><td rowspan="4">IDENTIFY (ID)</td><td rowspan="4">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.</td><td>ID.AM-1: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione</td><td rowspan="2">1 - Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all’interno del perimetro aziendale.

2 - I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc...) offerti da terze parti a cui si è registrati sono quelli strettamente necessari.

3 - Sono individuate le informazioni, i dati e i sistemi critici per l’azienda affinché siano adeguatamente protetti.</td></tr>
<tr><td>ID.AM-2: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione</td></tr>
<tr><td>ID.AM-6: Sono definiti e resi noti ruoli e responsabilità inerenti alla cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)</td><td rowspan="2">4 - È stato nominato un referente che sia responsabile per il coordinamento delle attività di gestione e di protezione delle informazioni e dei sistemi informatici.</td></tr>
<tr><td>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)</td></tr>
<tr><td></td><td></td><td>DP-ID.AM-8: I trattamenti di dati personali sono identificati e catalogati</td><td>3 - Sono individuate le informazioni, i dati e i sistemi critici per l’azienda affinché siano adeguatamente protetti.</td></tr>
</table>

2.3.2 Governance

La tematica “Governance” raccoglie un solo Controllo Essenziale, che prescrive l’identificazione e il rispetto della normativa applicabile inerente alla cybersecurity.
Sebbene il controllo, originariamente proposto nel contesto di un Framework per la Cybersecurity, non faccia esplicitamente riferimento ad elementi di data protection è evidente come, nell’ambito della definizione di un programma che abbracci anche la protezione dei dati personali, tale controllo possa e debba essere esteso all’individuazione e il rispetto della normativa inerente alla data protection.
La relazione tra questo controllo e la nuova versione del Framework Nazionale rimane

invariata rispetto alla precedente versione. Infatti, come riportato in Tabella 4, questo controllo ha impatto principalmente sulla subcategory ID.GV-3, la quale, già nella precedente versione del Framework, è formulata in modo sufficientemente generale da includere sia elementi di cybersecurity che elementi di data protection (cfr. Tabella 4).

Tabella 4: Relazione del Controllo Essenziale della tematica "Governance" con il Framework Nazionale per la Cybersecurity e la Data Protection.

FUNCTION	CATEGORY	SUBCATEGORY	CONTROLLO
IDENTIFY (ID)	**Governance (ID.GV)**: Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity.	**ID.GV-3**: I requisiti legali in materia di cybersecurity, con l'inclusione degli obblighi riguardanti la privacy e le libertà civili, sono compresi e gestiti	**5 - Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in tema di cybersecurity che risultino applicabili per l'azienda.**

2.3.3 Gestione delle identità, protezione, formazione e consapevolezza

I Controlli Essenziali dal 6 al 13 abbracciano le seguenti tematiche:

- Protezione da malware
- Gestione password e account
- Formazione e consapevolezza
- Protezione dei dati
- Protezione delle reti

Per questi controlli la relazione con il Framework Nazionale rimane invariata rispetto alla precedente versione del Framework (cfr. [4], §§3.3-3.7). Infatti, tali controlli non risultano fortemente relazionati a nessuna delle nuove subcategory che sono state introdotte. Ciò non deve far pensare, tuttavia, che tali controlli non abbiano alcuna relazione con la data protection. Infatti, la maggior parte di essi impattano su subcategory della function PROTECT e riguardano l'adozione di misure di sicurezza efficaci tanto contro il rischio cyber quanto contro quello legato alla data protection. La protezione dei dati personali, invero, non può prescindere dalla protezione dei sistemi cyber che li gestiscono.

2.3.4 Prevenzione e mitigazione

Della tematica "Prevenzione e mitigazione" fanno parte gli ultimi due Controlli Essenziali. In

particolare, il penultimo riguarda le azioni da intraprendere in caso di incidenti cyber. Esso prevede che in caso di incidente vengano informati i responsabili della sicurezza e che i sistemi vengano messi in sicurezza da personale esperto. Nell'ambito di una gestione non solo della sicurezza cyber, ma anche della data protection, tra i responsabili chiamati a coordinare le azioni di risposta agli incidenti dovrebbe essere presente anche un responsabile per la data protection (figura che può o meno coincidere con quella di responsabile della sicurezza). In caso di incidente tale figura dovrebbe essere tempestivamente informata per accertare se ci sia stata o meno una violazione di dati personali ed eventualmente intraprendere le azioni di risposta, tra cui quelle previste dalla normativa applicabile, quali ad esempio, informare le autorità di riferimento ed eventualmente comunicare la violazione ai diretti interessati (ossia le persone fisiche identificate o identificabili dai dati violati).

La Tabella 5 riassume la relazione tra i Controlli Essenziali della tematica "Prevenzione e mitigazione" e il Framework Nazionale per la Cybersecurity e la Data Protection. In particolare, rispetto alla precedente versione del Framework, il Controllo Essenziale 14 ha un impatto anche sulla subcategory DP-RS.CO-6 (evidenziata in giallo). Si tratta di una subcategory introdotta nella nuova versione del Framework che riguarda la risposta agli incidenti che si configurano come violazioni di dati personali. Essa prevede di informare le autorità di riferimento e gli interessati, se del caso.

Tabella 5: Relazione tra i Controlli Essenziali in "Prevenzione e mitigazione" con il Framework Nazionale per la Cybersecurity e la Data Protection.

<table>
<tr><th>FUNCTION</th><th>CATEGORY</th><th>SUBCATEGORY</th><th>CONTROLLO</th></tr>
<tr><td rowspan="4">RESPOND (RS)</td><td>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).</td><td>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</td><td rowspan="3">14 - In caso di incidente (es. venga rilevato un attacco o un malware) vengono informati i responsabili della sicurezza e i sistemi vengono messi in sicurezza da personale esperto.</td></tr>
<tr><td rowspan="3">Mitigation (RS.MI): Vengono eseguite azioni per prevenire l'espansione di un evento di sicurezza, per mitigare i sui effetti e per risolvere l'incidente.</td><td>RS.MI-1: In caso di incidente vengono messe in atto procedure atte a contenerne l'impatto</td></tr>
<tr><td>RS.MI-2: In caso di incidente vengono messe in atto procedure atte a mitigarne gli effetti</td></tr>
<tr><td>RS.MI-3: Le nuove vulnerabilità sono mitigate o documentate come rischio accettato</td><td>15 - Tutti i software in uso (inclusi i firmware) sono aggiornati all'ultima versione consigliata dal produttore. I dispositivi o i software obsoleti e non più aggiornabili sono dismessi.</td></tr>
</table>

3 Guida alla Contestualizzazione per il GDPR

Questa sezione descrive come il Framework può essere contestualizzato per cogliere gli elementi fondamentali del Regolamento; in questo modo le organizzazioni potranno utilizzare il Framework come strumento di supporto alla pianificazione delle attività necessarie per adeguarsi alla normativa e di successivo monitoraggio per la corretta implementazione e gestione delle stesse. A questo scopo viene qui introdotto un prototipo di contestualizzazione che recepisce gli elementi fondamentali del GDPR.

3.1 Elementi introduttivi

La presente sezione ha l'obiettivo di inquadrare le principali novità introdotte dal Regolamento. Tali elementi sono recepiti all'interno del Framework attraverso la revisione del core proposta attraverso questo documento.

Di seguito vengono analizzati gli elementi di novità del Regolamento.

Accountability e approccio basato sul rischio

L'accountability ("responsabilizzazione") è uno dei principi cardine del GDPR e riguarda tutti quei soggetti (titolari e responsabili) che effettuano trattamenti di dati personali. In ossequio a tale principio, il titolare del trattamento deve, da un lato, attuare le disposizioni del Regolamento e, dall'altro, essere in grado di comprovare la conformità dei trattamenti al medesimo Regolamento. Nell'ottemperare a tali aspetti, titolari e responsabili devono adottare un approccio basato sul rischio, ovvero devono considerare i rischi che potrebbero configurarsi per i diritti e le libertà degli interessati in relazione alle attività di trattamento. A tale scopo si sottolineano in particolare, senza pretesa di esaustività, i seguenti elementi: data protection by design e by default (art. 25); valutazione d'impatto sulla protezione dei dati personali (art. 35); registro delle attività di trattamento (art. 30); sicurezza del trattamento (art. 32); notifica dei data breach (artt. 33-34).

a. Data protection by design e by default

Tali principi, di carattere innovativo, mirano a determinare un processo di protezione dei dati che tenga in considerazione tutto il ciclo di vita del trattamento e in particolare le sue fasi prodromiche. Infatti, la *data protection by design* implica che le misure tecniche e organizzative adottate dal titolare del trattamento siano, fin dall'inizio, coerenti con i vincoli normativi e con le finalità del trattamento nonché adeguate rispetto ai rischi per i diritti e le libertà degli interessati. La *data protection by default*, invece, riguarda il fatto che, per impostazione predefinita, siano trattati solo dati personali necessari per ogni specifica finalità con particolare riferimento alle misure tecniche e organizzative in grado di garantire l'adeguatezza della portata del trattamento, del periodo di conservazione e della quantità di dati personali raccolti, nonché l'accessibilità ai dati medesimi.

b. Valutazione di impatto sulla protezione dei dati personali (DPIA)

Ancor prima di procedere al trattamento, il titolare può e, a certe condizioni, deve compiere una valutazione di impatto sulla protezione dei dati personali (*Data Protection Impact Assessment*, DPIA). Le casistiche per le quali è necessario procedere in tal senso sono individuate, oltre che dal Regolamento, dalle Linee Guida elaborate dal WP Art. 29 (WP248). Si tratta, in sintesi, di una analisi dei rischi per i diritti e le libertà degli interessati sulla base della quale è possibile determinare probabilità, minacce, impatti e misure di sicurezza in grado di mitigare il rischio rilevato.

c. Registro delle attività di trattamento

Il Registro delle attività di trattamento è un importante strumento che consente al titolare di disporre un quadro sempre aggiornato dei trattamenti all'interno dell'organizzazione ai fini della corretta gestione dei dati personali. In particolare, per ciascuna attività di trattamento, devono essere riportate in tale registro le tipologie di dati, le misure tecniche e organizzative adottate, le categorie di interessati, le finalità del trattamento e le basi giuridiche.

d. Sicurezza del trattamento

L'*accountability* e l'approccio basato sul rischio impongono che ci sia da parte del titolare l'adozione di adeguate misure di sicurezza, tecniche e organizzative, per la protezione dei dati personali, tenuto conto dei costi di attuazione e dei rischi per i diritti e le libertà degli interessati. Il Regolamento all'art. 32 suggerisce, a titolo esemplificativo, gli elementi da considerare al fine di garantire la sicurezza dei dati personali. Tra questi vengono individuati: la cifratura e la pseudonimizzazione; la capacità di assicurare permanentemente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; la capacità di ripristinare la disponibilità e l'accesso dei dati personali in caso di incidente; una procedura per testare e verificare l'efficacia delle misure tecniche e organizzative.

e. Notifica dei data breach

La violazione dei dati personali comporta, qualora la stessa presenti un rischio per i diritti e le libertà dell'interessato, l'obbligo in capo al titolare di notifica all'Autorità entro delle tempistiche prestabilite (72 ore dal momento in cui ne viene a conoscenza). Inoltre, in alcuni casi di particolare gravità in relazione ai rischi per i diritti e le libertà dell'interessato, la comunicazione deve essere fatta anche nei confronti dell'interessato in modo tale da permettere a quest'ultimo di proteggersi da eventuali conseguenze negative della violazione. I contenuti della notifica all'Autorità e della comunicazione agli interessati sono indicati agli artt. 33 e 34.

Ruoli e responsabilità (DPO, Titolare, Responsabile)

Il Regolamento prevede i seguenti ruoli e responsabilità in materia di data protection.

f. Titolare del trattamento

Il titolare è la persona fisica/giuridica (anche enti e autorità pubbliche) che determina le finalità e i mezzi del trattamento di dati personali. Tali operazioni possono essere svolte mediante l'ausilio di altri soggetti, sia interni (persona autorizzata al trattamento) che esterni (responsabile del trattamento). Il titolare deve garantire la protezione dei dati personali mediante l'adozione di adeguate misure di sicurezza tecniche ed organizzative nonché impartire opportune istruzioni a chiunque agisca sotto la sua responsabilità. Inoltre, in ossequio al principio di *accountability*, deve essere in grado di dimostrare che il trattamento sia effettuato conformemente alle disposizioni del Regolamento.

g. Responsabile del trattamento

Il responsabile è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali "per conto" del titolare del trattamento. Il responsabile deve presentare garanzie sufficienti rispetto alle misure tecniche e organizzative implementate e, rispetto alle attività di sua competenza, effettua attività di trattamento per le sole finalità indicate dal titolare.

h. Data Protection Officer (DPO)

La figura del responsabile della protezione dei dati (DPO, *Data Protection Officer*), per quanto non rappresenti una novità nello scenario europeo, costituisce un importante elemento innovativo nel panorama normativo nazionale. Si tratta di un soggetto (persona fisica/giuridica) che deve essere designato, qualora ne ricorrano i presupposti. Il DPO deve essere scelto sulla

base delle competenze (tecniche, informatiche, giuridiche, ecc.) in tema di protezione di dati personali e i suoi compiti sono riassumibili nelle seguenti mansioni: assistenza/consulenza a chi effettua il trattamento; sorveglianza sull'osservanza della normativa in materia di data protection; contatto/collaborazione per le Autorità garanti e per gli interessati.

Diritti degli interessati, informativa, base giuridica del trattamento

Il Regolamento prevede una partecipazione attiva dell'interessato (persona fisica identificata o identificabile a cui il dato si riferisce) nel processo di trattamento dei propri dati personali. Infatti, i diritti che gli vengono riconosciuti possono essere considerati come articolazioni del più generale diritto di "autodeterminazione informativa", intesa quale "potere di governare il flusso delle proprie informazioni".

Tra i diritti previsti dal Regolamento, agli artt. 15-22, figurano i seguenti: Diritto di accesso, Diritto di rettifica, Diritto alla cancellazione (oblio), Diritto di limitazione, Diritto alla portabilità, Diritto di opposizione.

In ossequio al principio di correttezza e trasparenza è necessario che l'interessato venga informato in maniera concisa, accessibile e comprensibile, con l'uso di un linguaggio semplice e chiaro (in particolare qualora il trattamento riguardi minori). L'interessato deve quindi essere informato circa l'identità e i dati di contatto del titolare del trattamento e del DPO, le finalità perseguite e tutte le altre informazioni che assicurino un trattamento corretto e trasparente, tra cui il periodo di conservazione, il diritto di presentare un reclamo all'Autorità di controllo e l'intenzione del titolare di trasferire i dati in Paesi terzi. Non sono prescritte formalità particolari per l'informativa, potendo la stessa essere fornita anche in formato elettronico o orale.

Ogni trattamento di dati personali deve trovare fondamento in un'idonea base giuridica; i fondamenti di liceità del trattamento previsti dal Regolamento sono: il consenso, l'adempimento di obblighi contrattuali, gli interessi vitali della persona interessata o di terzi, gli obblighi di legge cui è soggetto il titolare, l'interesse pubblico o l'esercizio di pubblici poteri, l'interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati.

Trasferimento di dati personali verso Paesi terzi

Il trasferimento di dati personali all'estero può essere effettuato soltanto nel caso in cui sia assicurata una protezione adeguata dei dati personali trasferiti nel Paese terzo. Esso è dunque consentito se sia posto in essere sulla base di una decisione di adeguatezza del Paese terzo riconosciuta dalla Commissione europea; ovvero sulla base di garanzie adeguate di natura contrattuale o pattizia che devono essere fornite dai titolari e responsabili coinvolti, quali le clausole contrattuali tipo, purché debitamente adottate, e, nel caso di un trasferimento dati extra UE all'interno di un gruppo imprenditoriale, le c.d. "binding corporate rules", ossia le norme vincolanti d´impresa (ulteriori strumenti, ora contemplati, sono inoltre i codici di condotta e gli schemi di certificazione).

Resta invece necessaria l'autorizzazione del Garante se un titolare desidera utilizzare clausole contrattuali ad-hoc (cioè non riconosciute come adeguate tramite decisione della Commissione) oppure accordi amministrativi stipulati tra autorità pubbliche.

È infine previsto, in assenza di ogni altro presupposto, l'utilizzo di deroghe al divieto di trasferimento applicabili in specifiche situazioni.

3.2 Prototipo di contestualizzazione

In questo paragrafo viene discusso in dettaglio il prototipo di contestualizzazione GDPR (nel seguito indicato semplicemente prototipo GDPR). Come già menzionato in §2.2.1 questo rappresenta una base di partenza per creare contestualizzazioni, calando il prototipo nello

specifico contesto del proprio settore, organizzazione o azienda. Questo lavoro di *specializzazione* si concretizza nella revisione ed eventuale modifica delle subcategory selezionate e dei livelli di priorità definiti dal prototipo, in base alle specificità del proprio contesto, nonché all'eventuale definizione dei livelli di maturità.

3.2.1 Selezione delle subcategory

Al fine di agevolare il lavoro di selezione delle subcategory in fase di creazione di una contestualizzazione a partire dal prototipo GDPR, le subcategory del Framework sono state organizzate nelle tre classi:

- **Obbligatorie**: fanno parte di questa classe tutte le subcategory che si ritiene debbano essere presenti in una contestualizzazione coerente con il prototipo GDPR. Non selezionare anche una sola di queste subcategory significherebbe trascurare un aspetto fondamentale del Regolamento.
- **Consigliate**: fanno parte di questa classe quelle subcategory che si suggerisce fortemente di prendere in considerazione per l'implementazione di una contestualizzazione basata sul prototipo GDPR. In particolare, appartengono a questa classe tutte quelle subcategory che, pur non riuscendo a coprire in maniera completa aspetti fondamentali del Regolamento se considerate singolarmente, permettono, quando combinate opportunamente, di coprire quegli aspetti su cui la normativa lascia maggiore libertà in merito alle modalità di implementazione, quali, ad esempio, le misure tecniche e organizzative di cui all'art. 32 del Regolamento e la protezione dei dati fin dalla progettazione e per impostazione predefinita (art. 25 del Regolamento). D'altra parte, il termine usato per classificare tali subcategory non deve lasciar intendere che sia l'implementazione degli aspetti del Regolamento ad esse connessi ad essere "consigliata" e dunque in qualche misura "facoltativa" o "secondaria". Al contrario, essi vanno implementati secondo le modalità che meglio si adattano al proprio contesto (purché conformi al Regolamento), selezionando coerentemente le subcategory "Consigliate" (ed eventualmente integrandole con ulteriori subcategory "Libere", qualora necessario od opportuno per lo specifico contesto).
- **Libere**: fanno parte di questa classe tutte le altre subcategory. Per queste subcategory non si hanno elementi che facciano propendere nettamente per la loro selezione. Del resto, non si deve pensare che la selezione di queste subcategory sia "sconsigliata". Al contrario queste possono essere selezionate o meno in base alle specificità del proprio contesto.

Le subcategory "Obbligatorie" vanno considerate selezionate in tutte le contestualizzazioni coerenti con il prototipo GDPR. Queste non sono deselezionabili. Le subcategory "Consigliate" vanno considerate come selezionate per impostazione predefinita. In fase di creazione della contestualizzazione quelle ritenute non adatte al proprio contesto possono essere deselezionate. Le subcategory della classe "Libere" vanno considerate non selezionate per impostazione predefinita. In fase di creazione della contestualizzazione possono essere selezionate quelle ritenute necessarie per lo specifico contesto.

In Appendice A sono riportate tutte le subcategory del prototipo di contestualizzazione GDPR con indicazione della corrispondente classe.

3.2.2 Livelli di priorità

Ferma restando la possibilità di ridefinire i livelli di priorità in fase di creazione della contestualizzazione per meglio adattarla alle specificità del proprio contesto, il prototipo GDPR specifica dei livelli di priorità "predefiniti" per tutte le subcategory "Obbligatorie" e "Consigliate".

In particolare, la priorità di ciascuna subcategory è definita su una scala a tre livelli ("Alta", "Media", "Bassa"), come da definizione del documento originale del Framework [3].

Inoltre, il prototipo GDPR impone il seguente vincolo sui livelli di priorità: "tutte le subcategory 'Obbligatorie' devono essere considerate a priorità 'Alta'". La loro implementazione dovrebbe risultare prioritaria indipendentemente dalla complessità.

In Appendice A sono riportati i livelli di priorità per tutte le subcategory "Obbligatorie" e "Consigliate".

3.3 Guida all'implementazione delle subcategory

Nel paragrafo precedente abbiamo visto come il prototipo di contestualizzazione GDPR fornisca una sorta di "configurazione predefinita", in termini di subcategory selezionate e livelli di priorità, che può essere modificata in fase di creazione della contestualizzazione adattandola allo specifico contesto. Abbiamo anche visto che esiste un insieme di subcategory, definite "Obbligatorie", che devono essere selezionate in ogni contestualizzazione conforme al prototipo GDPR e la cui priorità deve essere "alta". Questo paragrafo fornisce una guida all'implementazione di questo insieme minimo di subcategory, presenti in ogni contestualizzazione conforme al prototipo GDPR.

La presente guida è organizzata nelle seguenti aree di indirizzo:

1. Ruoli e responsabilità
2. Registri delle attività di trattamento
3. Principi
4. Valutazione d'impatto sulla protezione dei dati personali
5. Informazioni all'interessato
6. Consenso dell'interessato
7. Diritti dell'interessato
8. Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali
9. Gestione incidenti che si configurano come violazioni di dati personali

Per ciascuna area è definita una serie di controlli organizzati nelle subcategory del Framework. Per ogni controllo vengono riportati i riferimenti normativi al Regolamento.

Ruoli e responsabilità

Di questa area di indirizzo fanno parte i controlli che definiscono ruoli e responsabilità per le figure inerenti al trattamento e alla protezione dei dati personali. Nel contesto GDPR queste figure sono:

- Il titolare del trattamento (ed eventuali contitolari)
- Il responsabile del trattamento
- Il rappresentante del titolare del trattamento e il rappresentante del responsabile del trattamento
- Il responsabile della protezione dei dati

In particolare, i primi due controlli richiedono che il titolare metta in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, la conformità al Regolamento dei trattamenti eseguiti sotto la sua responsabilità (**DP-ID.AM-7-01**) e che dette misure

tecniche siano riesaminate e aggiornate qualora necessario (**DP-ID.AM-7-02**). Il controllo **DP-ID.AM-7-03** assegna al titolare del trattamento la responsabilità circa la definizione ed attuazione di politiche adeguate in materia di protezione dei dati personali. Il controllo **DP-ID.AM-7-04** riguarda invece i rappresentanti dei titolari o dei responsabili dei trattamenti. Esso richiede che i titolari e i responsabili non stabiliti nell'Unione che effettuano trattamenti riguardanti l'offerta di beni o servizi a interessati che si trovano nell'Unione o il monitoraggio del comportamento degli stessi, designino un rappresentante stabilito nell'Unione (in uno degli Stati membri in cui si trovano gli interessati i cui dati personali sono trattati). Il controllo **DP-ID.AM-7-05** assegna al titolare la responsabilità circa la definizione di ruoli e responsabilità del responsabile del trattamento e specifica che ciò debba avvenire per mezzo di un contratto o altro atto giuridico. Il controllo **DP-ID.AM-7-06** impone che chiunque abbia accesso a dati personali (inclusi il responsabile del trattamento e chiunque agisca sotto la sua responsabilità) non possa trattare dati personali se non è istruito in tal senso dal titolare del trattamento. Il controllo **DP-ID.AM-7-07** riguarda invece i contitolari del trattamento. In particolare, specifica che questi debbano definire, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento. I successivi tre controlli riguardano il responsabile della protezione dei dati (Data Protection Officer, DPO). In particolare, essi specificano che il titolare e il responsabile del trattamento devono nominare un responsabile della protezione dei dati in funzione delle sue qualità professionali (**DP-ID.AM-7-08**), definendo i suoi compiti e le sue funzioni (vedi art. 39 del Regolamento), che esso è tenuto a svolgere in piena autonomia ed indipendenza ed in assenza di conflitti di interesse, e coinvolgendolo in tutte le questioni riguardanti la protezione dei dati personali (**DP-ID.AM-7-10**). Inoltre, i suoi dati di contatto devono essere pubblicati e comunicati all'autorità di controllo (**DP-ID.AM-7-09**). Infine, gli ultimi due controlli assegnano al titolare del trattamento la responsabilità circa l'adozione di adeguate misure tecniche e organizzative atte a garantire i principi di protezione dei dati fin dalla progettazione (**DP-ID.AM-7-11**) e per impostazione predefinita (**DP-ID.AM-7-12**).

FUNCTION	**IDENTIFY (ID)**
CATEGORY	**Asset Management (ID.AM)**
SUBCATEGORY	
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)	
CONTROLLI	**RIFERIMENTI GDPR**
DP-ID.AM-7-01: Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento.	Art. 24(1)
DP-ID.AM-7-02: Il titolare del trattamento riesamina e aggiorna le misure tecniche di cui al controllo **DP-ID.AM-7-01** qualora necessario.	Art. 24(1)
DP-ID.AM-7-03: Il titolare del trattamento definisce ed attua politiche adeguate in materia di protezione dei dati personali.	Art. 24(2)
DP-ID.AM-7-04: Qualora il trattamento riguardi l'offerta di beni o servizi a interessati che si trovano nell'Unione o il monitoraggio del comportamento degli stessi, il titolare del trattamento o il responsabile del trattamento, se non stabilito nell'Unione, designa per iscritto un rappresentante nell'Unione, in uno degli Stati membri in cui si trovano gli interessati.	Art. 27(1),(3)
DP-ID.AM-7-05: Il titolare del trattamento definisce, nell'ambito di un contratto o altro atto giuridico, i ruoli e le responsabilità dei responsabili del trattamento.	Art. 28

DP-ID.AM-7-06: Il titolare del trattamento deve istruire tutti i soggetti che hanno accesso ai dati personali circa l'esecuzione dei compiti loro assegnati.	Art. 29
DP-ID.AM-7-07: Nel caso di contitolarità del trattamento, i contitolari del trattamento definiscono, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza del Regolamento.	Art. 26
DP-ID.AM-7-08: Il titolare del trattamento e il responsabile del trattamento designano, in funzione delle sue qualità professionali (conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e capacità di assolvere i propri compiti), un responsabile della protezione dei dati (data protection officer - DPO).	Art. 37
DP-ID.AM-7-09: Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.	Art. 37(7)
DP-ID.AM-7-10: Il titolare o il responsabile del trattamento definiscono, nell'ambito dell'atto di designazione, compiti e funzioni che il DPO è tenuto a svolgere in piena autonomia ed indipendenza ed in assenza di conflitti di interesse, e lo coinvolgono in tutte le questioni riguardanti la protezione dei dati personali.	Artt. 38(3), 39
DP-ID.AM-7-11: Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate volte ad attuare in modo efficace i principi di protezione dei dati (ad esempio pseudonimizzazione, minimizzazione) fin dalla progettazione (data protection by-design).	Art. 25(1)
DP-ID.AM-7-12: Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita (data protection by-default), solo i dati personali necessari per ogni specifica finalità del trattamento.	Art. 25(2)

Registri delle attività di trattamento

Questa area di indirizzo prevede un solo controllo (**DP-ID.AM-8-01**) che riguarda la tenuta dei registri delle attività di trattamento da parte del titolare del trattamento e del responsabile del trattamento. In particolare, occorrerà prestare la massima attenzione alle informazioni che il titolare e il responsabile del trattamento devono includere nei relativi registri. Per i trattamenti svolti sotto la propria responsabilità Il titolare del trattamento dovrà tenere un registro contenente (art. 30 par. 1 del Regolamento):

- i propri dati di contatto e, ove applicabile, quelli del contitolare, del rappresentante del titolare e del responsabile per la protezione dei dati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari (es. responsabili del trattamento, altri titolari del trattamento) a cui i dati personali sono stati o saranno comunicati;
- indicazione di eventuali trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali;
- i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- una descrizione generale delle misure di sicurezza tecniche e organizzative messe in atto per garantire la sicurezza del trattamento (art. 32, par. 1 del Regolamento).

Per i trattamenti svolti per conto di un titolare il responsabile del trattamento dovrà tenere un registro contenente (art. 30 par. 2 del Regolamento):

- i propri dati di contatto, quelli di ogni titolare per conto del quale svolge trattamenti e, ove applicabile, quelli del rappresentante del titolare o del responsabile del trattamento e del responsabile per la protezione dei dati;

- le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
- indicazione di eventuali trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali;
- una descrizione generale delle misure di sicurezza tecniche e organizzative messe in atto per garantire la sicurezza del trattamento (art. 32, par. 1 del Regolamento).

Il controllo **DP-ID.AM-8-01** trova collocazione all'interno del Framework nella subcategory **DP-ID.AM-8** che prevede l'identificazione e catalogazione dei trattamenti di dati personali.

FUNCTION	**IDENTIFY (ID)**
CATEGORY	**Asset Management (ID.AM)**
SUBCATEGORY	
DP-ID.AM-8: I trattamenti di dati personali sono identificati e catalogati.	
CONTROLLI	**RIFERIMENTI GDPR**
DP-ID.AM-8-01: Il titolare del trattamento e il responsabile del trattamento tengono, in forma scritta (anche in formato elettronico), un registro delle attività di trattamento svolte.	Art. 30(1-3)

Principi

Quest'area di indirizzo riguarda i principi applicabili al trattamento dei dati personali previsti dal Regolamento e comprende due controlli. Il controllo **ID.GV-3-01** prevede che vengano definiti e gestiti processi che permettano di garantire che i trattamenti di dati personali rispettino i principi del Regolamento (vedi art. 5). Il controllo **ID.GV-3-02** richiede che il titolare sia anche in grado di dimostrare il rispetto dei principi e la conformità dei trattamenti al Regolamento (accountability). Questi controlli di sicurezza si mappano nella subcategory **ID.GV-3** relativa alla comprensione e gestione dei requisiti legali.

FUNCTION	**IDENTIFY (ID)**
CATEGORY	**Governance (ID.GV)**
SUBCATEGORY	
ID.GV-3: I requisiti legali in materia di cybersecurity, con l'inclusione degli obblighi riguardanti la privacy e le libertà civili, sono compresi e gestiti.	
CONTROLLI	**RIFERIMENTI GDPR**
ID.GV-3-01: Sono definiti e gestiti processi volti a garantire che i trattamenti di dati personali rispettino i principi di liceità, correttezza, trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza (art. 5).	Art. 5(1)
ID.GV-3-02: Il titolare del trattamento è in grado di dimostrare il rispetto dei principi di cui al controllo **ID.GV-3-01** e la conformità delle attività di trattamento con il Regolamento (accountability).	Art. 5(2)

Valutazione d'impatto sulla protezione dei dati personali

In quest'area di indirizzo vengono proposti una serie di controlli legati alla valutazione d'impatto sulla protezione dei dati personali. Il controllo **DP-ID.RA-7-01** specifica che la valutazione d'impatto debba essere eseguita ogni qual volta un tipo di trattamento di dati personali

presenti un rischio elevato per i diritti e le libertà degli interessati. In questo caso il titolare del trattamento dovrà consultarsi con il responsabile della protezione dei dati, tra le cui responsabilità c'è quella di fornire pareri in merito alle valutazioni d'impatto. Il controllo **DP-ID.RA-7-02** richiede che il titolare del trattamento si assicuri che la valutazione d'impatto contenga almeno quanto previsto dal Regolamento. Il controllo **DP-ID.RA-7-03** richiede che il titolare del trattamento, nel valutare l'impatto dei trattamenti, tenga in considerazione l'eventuale rispetto di codici di condotta ed eventualmente senta il parere degli interessati o dei loro rappresentanti circa i trattamenti. Il controllo **DP-ID.RA-7-04** prevede che la valutazione d'impatto venga svolta periodicamente e comunque ogni volta che insorgano variazioni del rischio associato ai trattamenti. Infine, il controllo **DP-ID.RA-7-05** richiede che il titolare del trattamento consulti preventivamente l'autorità di controllo, qualora dalla valutazione d'impatto risulti che un trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare per ridurre il rischio. Questi controlli si mappano nella subcategory **DP-ID.RA-7** del Framework, relativa proprio alla valutazione di impatto.

FUNCTION	**IDENTIFY (ID)**
CATEGORY	**Risk Assessment (ID.RA)**
SUBCATEGORY	
DP-ID.RA-7: Viene effettuata una valutazione di impatto sulla protezione dei dati personali.	
CONTROLLI	**RIFERIMENTI GDPR**
DP-ID.RA-7-01: Qualora un tipo di trattamento di dati personali presenti un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento, consultato il responsabile della protezione dei dati, effettua una valutazione dell'impatto sulla protezione dei dati personali.	Art. 35(1-5)
DP-ID.RA-7-02: Il titolare del trattamento si assicura che la valutazione d'impatto contenga quanto previsto dal Regolamento.	Art. 35(7)
DP-ID.RA-7-03: Il titolare del trattamento, nell'effettuare la valutazione d'impatto sulla protezione dei dati personali, tiene conto del rispetto dei codici di condotta e, se del caso, delle opinioni degli interessati o dei loro rappresentanti sul trattamento.	Art. 35(8),(9)
DP-ID.RA-7-04: Il titolare del trattamento procede ad un riesame della valutazione di impatto con cadenza periodica e qualora insorgano variazioni del rischio rappresentato dalle attività relative al trattamento.	Art. 35(11)
DP-ID.RA-7-05: Qualora la valutazione di impatto sulla protezione dei dati personali indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate per attenuare il rischio, il titolare del trattamento consulta l'autorità di controllo.	Art. 36(1),(3)

Informazioni all'interessato

Quest'area di indirizzo contiene un unico controllo (**DP-ID.DM-2-01**) che richiede l'adozione di processi per fornire all'interessato tutte le informazioni inerenti al trattamento dei dati personali che lo riguardano, oltre all'esistenza e alle modalità di esercizio dei diritti previsti dal Regolamento. Nell'adottare tali misure occorrerà tenere in considerazione le differenti informazioni da fornire qualora i dati siano stati raccolti presso l'interessato (art. 13 del Regolamento) o presso terzi (art. 14 del Regolamento). Questo controllo trova collocazione nella subcategory **DP-ID.DM-2** del Framework inerente ai processi di informazione dell'interessato.

FUNCTION	IDENTIFY (ID)	
CATEGORY	Data Management (DP-ID.DM)	
SUBCATEGORY		
DP-ID.DM-2: Sono definiti, implementati e documentati i processi riguardanti l'informazione dell'interessato in merito al trattamento dei dati.		
CONTROLLI		RIFERIMENTI GDPR
DP-ID.DM-2-01: Il titolare del trattamento adotta processi per fornire all'interessato tutte le informazioni inerenti al trattamento dei dati personali comunque raccolti (sia presso lo stesso interessato che presso terzi) nonché l'esistenza e le modalità di esercizio dei diritti previsti dal Regolamento.		Artt. 12, 13, 14

Consenso dell'interessato

In quest'area di indirizzo vengono riuniti i controlli che riguardano i processi di raccolta e revoca del consenso dell'interessato al trattamento di dati. Il primo controllo (**DP-ID.DM-3-01)** pone all'attenzione la creazione da parte del titolare del trattamento di un insieme di processi che permettano di dimostrare, per tutti i trattamenti basati sul consenso, l'avvenuto ottenimento dello stesso da parte del titolare del trattamento. Il secondo controllo (**DP-ID.DM-3-02**) ha per oggetto il processo di revoca del consenso (**DP-ID.DM-3-02**).

FUNCTION	IDENTIFY (ID)	
CATEGORY	Data Management (DP-ID.DM)	
SUBCATEGORY		
DP-ID.DM-3: Sono definiti, implementati e documentati i processi di raccolta e revoca del consenso dell'interessato al trattamento di dati.		
CONTROLLI		RIFERIMENTI GDPR
DP-ID.DM-3-01: Il titolare del trattamento mette in atto processi che gli permettano di dimostrare che, per i trattamenti basati sul consenso, l'interessato, o nel caso di minori il titolare della responsabilità genitoriale, ha liberamente prestato uno specifico consenso per ciascun trattamento dei propri dati personali.		Art. 7(1),(2),(4) e art. 8
DP-ID.DM-3-02: Il titolare del trattamento mette in atto processi che gli permettano di gestire e documentare la revoca del consenso al trattamento dei dati personali da parte dell'interessato, o nel caso di minori del titolare della responsabilità genitoriale**.**		Art. 7(3) e art. 8

Diritti dell'interessato

In quest'area di indirizzo sono definiti i controlli che riguardano l'implementazione e la documentazione di tutti i processi inerenti all'esercizio dei diritti da parte dell'interessato così come sancito dal Regolamento. Il controllo **DP-ID.DM-4-01** impone la creazione di un processo che permetta al titolare del trattamento di fornire conferma all'interessato che sia o meno in corso un trattamento di dati personali che lo riguardano.

Il controllo **DP-ID.DM-4-02** richiede la creazione di processi per permettere all'interessato del trattamento di accedere ai propri dati personali ed alle informazioni relative al trattamento,

qualora ne venga fatta richiesta in forma elettronica.

Il controllo **DP-ID.DM-4-03** richiede la messa in atto di processi per garantire all'interessato l'esercizio del diritto di rettifica dei dati personali. Il controllo **DP-ID.DM-4-04** riguarda la definizione di processi per la cancellazione dei dati personali qualora l'interessato ne faccia richiesta.

Il controllo **DP-ID.DM-4-05**, facente riferimento al controllo **DP-ID.DM-4-04** concerne il caso in cui i dati personali di cui è stata richiesta la cancellazione siano stati resi pubblici, e richiede al titolare del trattamento di adottare misure ragionevoli, anche tecniche, per cancellare qualsiasi link, copia o riproduzione degli stessi.

Il controllo **DP-ID.DM-4-06** richiede la creazione di processi atti a garantire all'interessato del trattamento il diritto alla limitazione del trattamento dei dati personali, qualora sussistano le condizioni previste (esattezza, non liceità, accertamento in sede giudiziaria, opposizione), ed a trattare i dati personali dal momento della richiesta di limitazione in accordo a quanto previsto nel Regolamento.

Il controllo **DP-ID.DM-4-07** richiede da parte del titolare del trattamento la comunicazione a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Il controllo **DP-ID.DM-4-08** richiede la creazione di processi che garantiscano all'interessato il diritto alla portabilità dei dati personali in accordo a quanto sancito nel Regolamento.

Il controllo **DP-ID.DM-4-09** richiede la creazione di processi per garantire all'interessato il diritto all'opposizione al trattamento di dati personali in accordo a quanto sancito nel Regolamento. L'interessato deve essere informato di questo diritto in forma chiara e separata da altre informazioni, al più tardi alla prima comunicazione con l'interessato.

Il controllo **DP-ID.DM-4-10** richiede la creazione di processi che garantiscano all'interessato il diritto di non essere sottoposto ad una decisione basata esclusivamente sul trattamento automatizzato che produca effetti giuridici o abbia effetto sulla sua persona fisica.

Connesso al precedente, Il controllo **DP-ID.DM-4-11** richiede l'attuazione di misure appropriate per tutelare i diritti e le libertà dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.

FUNCTION	**IDENTIFY (ID)**
CATEGORY	**Data Management (DP-ID.DM)**
SUBCATEGORY	
DP-ID.DM-4: Sono definiti, implementati e documentati i processi per l'esercizio dei diritti (accesso, rettifica, cancellazione, ecc.) dell'interessato.	
CONTROLLI	**RIFERIMENTI GDPR**
DP-ID.DM-4-01: È definito un processo che garantisce al titolare del trattamento la capacità di fornire all'interessato la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano.	Art. 15
DP-ID.DM-4-02: Il titolare del trattamento mette in atto processi che garantiscono l'esercizio da parte dell'interessato del diritto di accesso ai dati personali ed alle informazioni relative al trattamento, qualora la richiesta avvenga tramite mezzi elettronici, utilizzando un formato elettronico di uso comune.	Art. 15

DP-ID.DM-4-03: Il titolare del trattamento mette in atto processi che garantiscono all'interessato l'esercizio del diritto di rettifica dei dati personali che lo riguardano qualora ne faccia richiesta, senza ingiustificato ritardo.	Art. 16
DP-ID.DM-4-04: Il titolare del trattamento mette in atto processi che garantiscono all'interessato l'esercizio del diritto di cancellazione dei dati personali che lo riguardano qualora ne faccia richiesta, senza ingiustificato ritardo, qualora sussista uno dei motivi di cui all'art. 17 par. 1.	Art. 17(1)
DP-ID.DM-4-05: In riferimento al controllo **DP-ID.DM-4-04**, il titolare del trattamento, qualora abbia reso pubblici i dati personali, adotta le misure ragionevoli, anche tecniche, per informare della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali, tutti gli ulteriori titolari del trattamento che stanno trattando i dati personali.	Art. 17(2)
DP-ID.DM-4-06: Il titolare del trattamento mette in atto processi che garantiscono all'interessato l'esercizio del diritto di limitazione del trattamento dei dati personali che lo riguardano e che successivamente alla limitazione i dati vengano trattati esclusivamente nelle circostanze previste dal Regolamento (es. consenso dell'interessato, accertamento diritti in sede giudiziaria, ecc.).	Art. 18(1-3)
DP-ID.DM-4-07: Il titolare del trattamento mette in atto processi per la comunicazione a ciascuno dei destinatari cui sono stati trasmessi i dati personali delle eventuali rettifiche, cancellazioni o limitazioni del trattamento richieste dall'interessato.	Art. 19
DP-ID.DM-4-08: Il titolare del trattamento mette in atto processi che garantiscono all'interessato l'esercizio del diritto di portabilità dei dati.	Art. 20
DP-ID.DM-4-09: Il titolare del trattamento mette in atto processi che garantiscono all'interessato l'esercizio del diritto di opposizione al trattamento dei dati personali, ove ne ricorrano i presupposti.	Art. 21
DP-ID.DM-4-10: Il titolare del trattamento mette in atto processi che garantiscono all'interessato il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.	Art. 22(1)
DP-ID.DM-4-11: In riferimento al controllo **DP-ID.DM-4-10**, nel caso in cui la decisione si basi sul consenso esplicito dell'interessato oppure sia necessaria per la conclusione o l'esecuzione di un contratto, il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato (almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione).	Art. 22(2-3)

Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali

In quest'area di indirizzo sono definiti controlli per l'implementazione, documentazione e gestione dei processi di trasferimento dei dati in ambito internazionale.

Il controllo **DP-ID.DM-5-01** richiede la definizione di un processo per regolare il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali in conformità al principio di adeguatezza (art. 44) e senza che il livello di protezione delle persone fisiche sia pregiudicato.

In tal senso assume notevole importanza la verifica delle condizioni di adeguatezza (art. 45) affinché un trasferimento di dati possa avvenire, gestito tramite un processo definito nel controllo **DP-ID.DM-5-02**.

Il controllo **DP-ID.DM-5-03** richiede la creazione di un processo riguardante la verifica

dell'adeguatezza delle garanzie fornite dal paese terzo verso cui si vogliono trasferire dati personali qualora non vi sia stata decisione da parte della Commissione ai sensi dell'art. 45 par. 3.

Il processo dovrà considerare gli elementi di valutazione forniti nell'art. 46 parr. 2 e 3. Qualora anche questi non siano sufficienti a prendere una decisione, si farà capo a quanto sancito nell'art. 49.

FUNCTION	**IDENTIFY (ID)**
CATEGORY	**Data Management (DP-ID.DM)**
SUBCATEGORY	
DP-ID.DM-5: Sono definiti, implementati e documentati i processi di trasferimento dei dati in ambito internazionale.	
CONTROLLI	**RIFERIMENTI GDPR**
DP-ID.DM-5-01: È definito un processo per regolare il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali in conformità a quanto sancito nell'art. 44.	Art. 44
DP-ID.DM-5-02: È definito un processo atto a verificare che sussistano le condizioni affinché un trasferimento di dati personali verso paesi terzi o organizzazioni internazionali sia ammesso, ai sensi dell'art. 45.	Art. 45
DP-ID.DM-5-03: In mancanza di una decisione ai sensi dell'art. 45, par. 3, il titolare del trattamento o il responsabile del trattamento effettuano il trasferimento verso un paese terzo o organizzazione internazionale solo se sono in grado di fornire garanzie adeguate in conformità all'art. 46 parr. 2 e 3 oppure, in ultima analisi, qualora sussistano le specifiche condizioni, di cui all'art. 49.	Artt. 46, 47 e 49

Gestione incidenti che si configurano come violazioni di dati personali

In quest'area di indirizzo sono definiti controlli per la gestione, documentazione e comunicazione delle violazioni di dati personali.

Il controllo **DP-RS.CO-6-01** richiede di istituire un processo con cui il titolare del trattamento è in grado, a seguito di una violazione di dati personali, di notificare la violazione all'autorità di controllo competente, senza ingiustificato ritardo, ovvero entro 72 ore dal momento in cui ne è venuto a conoscenza. Per la comunicazione della violazione all'interessato del trattamento, in accordo a quanto richiesto dal controllo **DP-RS.CO-6-02**, occorre effettuare una valutazione del rischio per i diritti e le libertà delle persone fisiche al fine di valutare se esso sia o meno elevato e supportare quindi la decisione di comunicare o meno la violazione all'interessato.

Il controllo **DP-RS.CO-6-03** richiede al responsabile del trattamento di informare il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza di una violazione di dati personali.

Il controllo **DP-RS.CO-6-04** richiede di documentare (ad esempio, in un registro) tutte le violazioni di dati personali, in particolare in merito alle circostanze, alle conseguenze per gli interessati ed alle azioni intraprese per porvi rimedio.

FUNCTION	RESPOND (RS)
CATEGORY	Communications (RS.CO)
SUBCATEGORY	
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.	
CONTROLLI	**RIFERIMENTI GDPR**
DP-RS.CO-6-01: In caso di violazione dei dati personali che presenti un rischio per gli interessati, il titolare del trattamento notifica la violazione all'autorità di controllo competente senza ingiustificato ritardo, e comunque entro 72 ore dal momento in cui ne è venuto a conoscenza.	Art. 33
DP-RS.CO-6-02: In caso di violazione dei dati personali che presenti un rischio elevato per gli interessati, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.	Art. 34
DP-RS.CO-6-03: Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza di una violazione dei dati personali.	Art. 33(2)
DP-RS.CO-6-04: Il titolare del trattamento documenta tutte le violazioni dei dati personali, comprese le circostanze a esse relative, le loro conseguenze e i provvedimenti adottati per porvi rimedio.	Art. 33(5)

Appendice A. Framework Core

Function	Category	Subcategory	Informative References
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.	**ID.AM-1:** Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	· **CIS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8, PM-5 · **Misure Minime AgID** ABSC 1
		ID.AM-2: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	· **CIS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 · **NIST SP 800-53 Rev. 4** CM-8, PM-5 · **Misure Minime AgID** ABSC 2
		ID.AM-3: I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati	· **CIS CSC** 12 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8 · **Misure Minime AgID** ABSC 5.1.4, 13.3.1, 13.4.1, 13.6, 13.7.1, 13.8.1

Function	Category	Subcategory	Informative References
		ID.AM-4: I sistemi informativi esterni all'organizzazione sono catalogati	· **CIS CSC** 12 · **COBIT 5** APO02.02, APO10.04, DSS01.02 · **ISO/IEC 27001:2013** A.11.2.6 · **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Le risorse (es: hardware, dispositivi, dati, allocazione temporale, personale e software) sono prioritizzate in base alla loro classificazione (e.g. confidenzialità, integrità, disponibilità), criticità e valore per il business dell'organizzazione	· **CIS CSC** 13, 14 · **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.6 · **ISO/IEC 27001:2013** A.8.2.1 · **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6 · **Misure Minime AgID** ABSC 13.1.1, 13.2.1
		ID.AM-6: Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	· **CIS CSC** 17, 19 · **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1 · **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11 · **D.Lgs. 18/5/2018 n. 65** Art. 16(2)-(4) · **Misure Minime AgID** ABSC 5.2.1, 5.4, 5.10, 8.11.1
		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 · **D.Lgs. 30/6/2003 n. 196** Artt. 2-quaterdecies, 2-quinquiesdecies, 2-sexiesdecies · **ISO/IEC 29100:2011** 4.2, 4.3, 5.10

Function	Category	Subcategory	Informative References
		DP-ID.AM-8: I trattamenti di dati personali sono identificati e catalogati	· **GDPR** - Art. 30 · **ISO/IEC 29100:2011** 4.4
	Business Environment (ID.BE): La mission dell'organizzazione, gli obiettivi, le attività e gli attori coinvolti sono compresi e valutate in termini di priorità. Tali informazioni influenzano i ruoli, le responsabilità di cybersecurity e le decisioni in materia di gestione del rischio.	**ID.BE-1:** Il ruolo dell'organizzazione all'interno della filiera produttiva è identificato e reso noto	· **COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** CP-2, SA-12
		ID.BE-2: Il ruolo dell'organizzazione come infrastruttura critica e nel settore industriale di riferimento è identificato e reso noto	· **COBIT 5** APO02.06, APO03.01 · **ISO/IEC 27001:2013** Clause 4.1 · **NIST SP 800-53 Rev. 4** PM-8 · **D.Lgs. 18/5/2018 n. 65** Art. 4
		ID.BE-3: Sono definite e rese note delle priorità per quanto riguarda la missione, gli obiettivi e le attività dell'organizzazione	· **COBIT 5** APO02.01, APO02.06, APO03.01 · **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 · **NIST SP 800-53 Rev. 4** PM-11, SA-14
		ID.BE-4: Sono identificate e rese note interdipendenze e funzioni fondamentali per la fornitura di servizi critici	· **COBIT 5** APO10.01, BAI04.02, BAI09.02 · **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 · **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Sono identificati e resi noti i requisiti di resilienza a supporto della fornitura di servizi critici per tutti gli stati di esercizio (es. sotto stress/attacco, in fase di recovery, normale esercizio)	· **COBIT 5** BAI03.02, DSS04.02 · **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 · **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-13, SA-14

Function	Category	Subcategory	Informative References
	Governance (ID.GV): Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity.	**ID.GV-1:** È indetificata e resa nota una policy di cybersecurity	· **CIS CSC** 19 · **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02 · **ISA 62443-2-1:2009** 4.3.2.6 · **ISO/IEC 27001:2013** A.5.1.1 · **NIST SP 800-53 Rev. 4** -1 controls from all security control families · **D.Lgs. 18/5/2018 n. 65** Artt. 13(2), 15(2)
		ID.GV-2: Ruoli e responsabilità inerenti la cybersecurity sono coordinati ed allineati con i ruoli interni ed i partner esterni	· **CIS CSC** 19 · **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1 · **NIST SP 800-53 Rev. 4** PS-7, PM-1, PM-2
		ID.GV-3: I requisiti legali in materia di cybersecurity, con l'inclusione degli obblighi riguardanti la privacy e le libertà civili, sono compresi e gestiti	· **CIS CSC** 19 · **COBIT 5** BAI02.01, MEA03.01, MEA03.04 · **ISA 62443-2-1:2009** 4.4.3.7 · **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 · **NIST SP 800-53 Rev. 4** -1 controls from all security control families · **D.Lgs. 18/5/2018 n. 65** Art. 1-11 · **GDPR** - Artt. 5-11 · **D.Lgs. 30/6/2003 n. 196** Artt. 2-ter, 2-quater, 2-quinquies, 2-sexies, 2-septies, 2-octies, 2-novies, 2-decies · **ISO/IEC 29100:2011** 4.5.1**,** 5.3

Function	Category	Subcategory	Informative References
		ID.GV-4: La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity	· **COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 · **ISO/IEC 27001:2013** Clause 6 · **NIST SP 800-53 Rev. 4** SA-2, PM-3, PM-7, PM-9, PM-10, PM-11 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1), 14(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.	**ID.RA-1:** Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate	· **CIS CSC** 4 · **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 · **Misure Minime AgID** ABSC 4.1.1, 4.1.2, 4.6.1
		ID.RA-2: L'organizzazione riceve informazioni su minacce, vulnerabilità ed altri dati configurabili come Cyber Threat Intelligence da fonti esterne (e.g. CERT, fonti aperte, forum di information sharing)	· **CIS CSC** 4 · **COBIT 5** BAI08.01 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.6.1.4 · **NIST SP 800-53 Rev. 4** SI-5, PM-15, PM-16 · **Misure Minime AgID** ABSC 4.4.2

Function	Category	Subcategory	Informative References
		ID.RA-3: Le minacce, sia interne che esterne, sono identificate e documentate	· **CIS CSC** 4 · **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** Clause 6.1.2 · **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Sono identificati i potenziali impatti sul business e le relative probabilità di accadimento	· **CIS CSC** 4 · **COBIT 5** DSS04.02 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.16.1.6, Clause 6.1.2 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM-9, PM-11 · **Misure Minime AgID** ABSC 4.8.1
		ID.RA-5: Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio	· **CIS CSC** 4 · **COBIT 5** APO12.02 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16 · **Misure Minime AgID** ABSC 4.8.1
		ID.RA-6: Sono identificate e prioritizzate le risposte al rischio	· **CIS CSC** 4 · **COBIT 5** APO12.05, APO13.02 · **ISO/IEC 27001:2013** Clause 6.1.3 · **NIST SP 800-53 Rev. 4** PM-4, PM-9

Function	Category	Subcategory	Informative References
		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**
	Risk Management Strategy (ID.RM): Le priorità e i requisiti dell'organizzazione e la tolleranza al rischio sono definiti e utilizzati per supportare le decisioni sul rischio operazionale.	**ID.RM-1:** I processi di risk management sono stabiliti, gestiti e concordati tra i responsabili dell'organizzazione (c.d. stakeholder)	· **CIS CSC** 4 · **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 · **ISA 62443-2-1:2009** 4.3.4.2 · **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3, Clause 9.3 · **NIST SP 800-53 Rev. 4** PM-9 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1), 14(1), 14(13)
		ID.RM-2: Il rischio tollerato dall'organizzazione è identificato ed espresso chiaramente	· **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.2.6.5 · **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 · **NIST SP 800-53 Rev. 4** PM-9 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1), 14(1), 14(13)
		ID.RM-3: Il rischio tollerato è determinato tenendo conto del ruolo dell'organizzazione come infrastruttura critica e dei rischi specifici presenti nel settore industriale di appartenenza	· **COBIT 5** APO12.02 · **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 · **NIST SP 800-53 Rev. 4** SA-14, PM-8, PM-9, PM-11 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1), 14(1), 14(13)

Function	Category	Subcategory	Informative References
	Supply Chain Risk Management (ID.SC): Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-1:** I processi di gestione del rischio inerenti la catena di approvvigionamento cyber sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione	· **CIS CSC** 4 · **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 · **ISA 62443-2-1:2009** 4.3.4.2 · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9
		ID.SC-2: I fornitori e i partner terzi di sistemi informatici, componenti e servizi sono identificati, prioritizzati e valutati utilizzando un processo di valutazione del rischio inerente la catena di approvvigionamento cyber	· **COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 · **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
		ID.SC-3: I contratti con i fornitori e i partner terzi sono utilizzati per realizzare appropriate misure progettate per rispettare gli obiettivi del programma di cybersecurity dell'organizzazione e del Piano di Gestione del Rischio della catena di approvvigionamento cyber	· **COBIT 5** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 · **ISA 62443-2-1:2009** 4.3.2.6.4, 4.3.2.6.7 · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3 · **NIST SP 800-53 Rev. 4** SA-9, SA-11, SA-12, PM-9
		ID.SC-4: Fornitori e partner terzi sono regolarmente valutati utilizzando audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali	· **COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 · **ISA 62443-2-1:2009** 4.3.2.6.7 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12

Function	Category	Subcategory	Informative References
		ID.SC-5: La pianificazione e la verifica della risposta e del ripristino sono condotti con i fornitori e i partner terzi	· **CIS CSC** 19, 20 · **COBIT 5** DSS04.04 · **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 · **ISA 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 · **ISO/IEC 27001:2013** A.17.1.3 · **NIST SP 800-53 Rev. 4** CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
	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
		DP-ID.DM-2: Sono definiti, implementati e documentati i processi riguardanti l'informazione dell'interessato in merito al trattamento dei dati	· **GDPR** - Artt. 12-14 · **ISO/IEC 29100:2011** 5.2, 5.8 · **ISO/IEC 29151:2017** A.3, A.9 · **ISO/IEC 27018:2014** A.1, A.7
		DP-ID.DM-3: Sono definiti, implementati e documentati i processi di raccolta e revoca del consenso dell'interessato al trattamento di dati	· **GDPR** - Artt. 7, 8 · **D.Lgs. 30/6/2003 n. 196** Art. 2-quinquies · **ISO/IEC 29100:2011** 5.2 · **ISO/IEC 29151:2017** A.3 · **ISO/IEC 27018:2014** A.1

Function	Category	Subcategory	Informative References
		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 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

Function	Category	Subcategory	Informative References
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-1:** Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza	· **CIS CSC** 1, 5, 15, 16 · **COBIT 5** DSS05.04, DSS06.03 · **ISA 62443-2-1:2009** 4.3.3.5.1 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 · **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 · **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 5.6.1, 5.7, 5.8.1, 5.11 · **GDPR** - Artt. 25, 32 · **ISO/IEC 29100:2011** 5.11

Function	Category	Subcategory	Informative References
		PR.AC-2: L'accesso fisico alle risorse è protetto e amministrato	· **COBIT 5** DSS01.04, DSS05.05 · **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 · **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 · **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 5.11.2, 10.4.1 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.AC-3: L'accesso remoto alle risorse è amministrato	· **CIS CSC** 12 · **COBIT 5** APO13.01, DSS01.04, DSS05.03 · **ISA 62443-2-1:2009** 4.3.3.6.6 · **ISA 62443-3-3:2013** SR 1.13, SR 2.6 · **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-1, AC-17, AC-19, AC-20, SC-15 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 3.4.1, 8.3.2 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11

Function	Category	Subcategory	Informative References
		PR.AC-4: I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni	· **CIS CSC** 3, 5, 12, 14, 15, 16, 18 · **COBIT 5** DSS05.04 · **ISA 62443-2-1:2009** 4.3.3.7.3 · **ISA 62443-3-3:2013** SR 2.1 · **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 · **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 5.1.1, 5.1.2, 5.1.3, 13.9.1 · **GDPR** - Artt. 25, 32 · **ISO/IEC 29100:2011** 5.11
		PR.AC-5: L'integrità di rete è protetta (es. segregazione di rete, segmentazione di rete)	· **CIS CSC** 9, 14, 15, 18 · **COBIT 5** DSS01.05, DSS05.02 · **ISA 62443-2-1:2009** 4.3.3.4 · **ISA 62443-3-3:2013** SR 3.1, SR 3.8 · **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 4** AC-4, AC-10, SC-7 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 13.3.1 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11

Function	Category	Subcategory	Informative References
		PR.AC-6: Le identità sono comprovate, associate a credenziali e verificate durante le interazioni	· **CIS CSC**, 16 · **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 · **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 · **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 · **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.AC-7: Le modalità di autenticazione (es. autenticazione a fattore singolo o multiplo) per gli utenti, i dispositivi e altri asset sono commisurate al rischio della transazione (es. rischi legati alla sicurezza e privacy degli individui e altri rischi dell'organizzazione)	· **CIS CSC** 1, 12, 15, 16 · **COBIT 5** DSS05.04, DSS05.10, DSS06.10 · **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 · **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 · **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11

Function	Category	Subcategory	Informative References
	Awareness and Training (PR.AT): Il personale e le terze parti sono sensibilizzate in materia di cybersecurity e vengono addestrate per adempiere ai loro compiti e ruoli coerentemente con le politiche, le procedure e gli accordi esistenti	**PR.AT-1:** Tutti gli utenti sono informati e addestrati	· **CIS CSC** 17, 18 · **COBIT 5** APO07.03, BAI05.07 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 · **NIST SP 800-53 Rev. 4** AT-2, PM-13 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 8.7.2, 8.7.3, 8.7.4
		PR.AT-2: Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità	· **CIS CSC** 5, 17, 18 · **COBIT 5** APO07.02, DSS05.04, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** AT-3, PM-13 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 5.2.1, 5.6.1, 5.7.1, 5.7.2, 5.7.3, 5.7.6, 5.8.1, 5.9.1, 5.10.3, 5.10.4, 5.11.1
		PR.AT-3: Tutte le terze parti (es. fornitori, clienti, partner) comprendono i loro ruoli e responsabilità	· **CIS CSC** 17 · **COBIT 5** APO07.03, APO07.06, APO10.04, APO10.05 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** PS-7, SA-9, SA-16 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13)

Function	Category	Subcategory	Informative References
		PR.AT-4: I dirigenti ed i vertici aziendali comprendono i loro ruoli e responsabilità	· **CIS CSC** 17, 19 · **COBIT 5** EDM01.01, APO01.02, APO07.03 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** AT-3, PM-13 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13)
		PR.AT-5: Il personale addetto alla sicurezza fisica e alla cybersecurity comprende i suoi ruoli e responsabilità	· **CIS CSC** 17 · **COBIT 5** APO07.03 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** AT-3, IR-2, PM-13 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13)
	Data Security (PR.DS): I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-1:** I dati memorizzati sono protetti	· **CIS CSC** 13, 14 · **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 · **ISA 62443-3-3:2013** SR 3.4, SR 4.1 · **ISO/IEC 27001:2013** A.8.2.3 · **NIST SP 800-53 Rev. 4** MP-8, SC-12, SC-28 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 13.3.1 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11

Function	Category	Subcategory	Informative References
		PR.DS-2: I dati sono protetti durante la trasmissione	· **CIS CSC** 13, 14 · **COBIT 5** APO01.06, DSS05.02, DSS06.06 · **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 4** SC-8, SC-11, SC-12 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 3.3.2 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.DS-3: Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale	· **CIS CSC** 1 · **COBIT 5** BAI09.03 · **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.4.4.1 · **ISA 62443-3-3:2013** SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 · **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11

Function	Category	Subcategory	Informative References
		PR.DS-4: I sistemi hanno adeguate risorse a disposizione per poter garantire la disponibilità	· **CIS CSC** 1, 2, 13 · **COBIT 5** APO13.01, BAI04.04 · **ISA 62443-3-3:2013** SR 7.1, SR 7.2 · **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1 · **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.DS-5: Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak).	· **CIS CSC** 13 · **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02 · **ISA 62443-3-3:2013** SR 5.2 · **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 13.2.1, 13.7.1, 13.8.1, 13.9.1 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11

Function	Category	Subcategory	Informative References
		PR.DS-6: Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni	· **CIS CSC** 2, 3 · **COBIT 5** APO01.06, BAI06.01, DSS06.02 · **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 · **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 · **NIST SP 800-53 Rev. 4** SC-16, SI-7 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 3.5.1, 3.5.2, 10.3.1 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.DS-7: Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione	· **CIS CSC** 18, 20 · **COBIT 5** BAI03.08, BAI07.04 · **ISO/IEC 27001:2013** A.12.1.4 · **NIST SP 800-53 Rev. 4** CM-2 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 4.10.1, 8.2.3
		PR.DS-8: Sono impiegati meccanismi di controllo dell'integrità per verificare l'integrità del hardware	· **COBIT 5** BAI03.05 · **ISA 62443-2-1:2009** 4.3.4.4.4 · **ISO/IEC 27001:2013** A.11.2.4 · **NIST SP 800-53 Rev. 4** SA-10, SI-7 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11

Function	Category	Subcategory	Informative References
	Information Protection Processes and Procedures (PR.IP): Sono attuate e adeguate nel tempo politiche di sicurezza (che indirizzano scopo, ambito, ruoli e responsabilità, impegno da parte del management e coordinamento tra le diverse entità organizzative), processi e procedure per gestire la protezione dei sistemi informativi e degli assets.	**PR.IP-1:** Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)	· **CIS CSC** 3, 9, 11 · **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 · **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 · **ISA 62443-3-3:2013** SR 7.6 · **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 3.1.1, 3.1.2, 3.2.1, 5.3.1, 8.4 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.IP-2: Viene implementato un processo per la gestione del ciclo di vita dei sistemi (System Development Life Cycle).	· **CIS CSC** 18 · **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03 · **ISA 62443-2-1:2009** 4.3.4.3.3 · **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 · **NIST SP 800-53 Rev. 4** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 3.1.3, 3.2.2, 3.3 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11

Function	Category	Subcategory	Informative References
		PR.IP-3: Sono attivi processi di controllo della modifica delle configurazioni	· **CIS CSC** 3, 11 · **COBIT 5** BAI01.06, BAI06.01 · **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 · **ISA 62443-3-3:2013** SR 7.6 · **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 3.2.3, 3.5.3, 3.5.4, 3.6.1, 3.7.1, 5.4, 8.2.1, 8.2.2 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.IP-4: I backup delle informazioni sono eseguiti, amministrati e verificati	· **CIS CSC** 10 · **COBIT 5** APO13.01, DSS01.01, DSS04.07 · **ISA 62443-2-1:2009** 4.3.4.3.9 · **ISA 62443-3-3:2013** SR 7.3, SR 7.4 · **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 · **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 10.1, 10.2.1, 10.4.1 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11

Function	Category	Subcategory	Informative References
		PR.IP-5: Sono rispettate le policy ed i regolamenti relativi agli ambienti fisici in cui operano le risorse dell'organizzazione	· **COBIT 5** DSS01.04, DSS05.05 · **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 · **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 · **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 10.4.1 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.IP-6: I dati sono distrutti in conformità con le policy	· **COBIT 5** BAI09.03, DSS05.06 · **ISA 62443-2-1:2009** 4.3.4.4.4 · **ISA 62443-3-3:2013** SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 · **NIST SP 800-53 Rev. 4** MP-6 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **GDPR** - Art. 5, 17, 32 · **ISO/IEC 29100:2011** 5.11

Function	Category	Subcategory	Informative References
		PR.IP-7: I processi di protezione sono sottoposti a miglioramenti	· **COBIT 5** APO11.06, APO12.06, DSS04.05 · **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 · **ISO/IEC 27001:2013** A.16.1.6, Clause 9, Clause 10 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.IP-8: L'efficacia delle tecnologie di protezione viene condivisa	· **COBIT 5** BAI08.04, DSS03.04 · **ISO/IEC 27001:2013** A.16.1.6 · **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.IP-9: Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro	· **CIS CSC** 19 · **COBIT 5** APO12.06, DSS04.03 · **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 · **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 · **NIST SP 800-53 Rev. 4** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 10.4.1 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11

Function	Category	Subcategory	Informative References
		PR.IP-10: I piani di risposta e recupero a seguito di incidenti/disastri sono verificati nel tempo	· **CIS CSC** 19, 20 · **COBIT 5** DSS04.04 · **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 · **ISA 62443-3-3:2013** SR 3.3 · **ISO/IEC 27001:2013** A.17.1.3 · **NIST SP 800-53 Rev. 4** CP-4, IR-3, PM-14 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.IP-11: Le problematiche inerenti la cybersecurity sono incluse nei processi di gestione del personale (es: screening, deprovisioning)	· **CIS CSC** 5, 16 · **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 · **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 · **ISO/IEC 27001:2013** A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 · **NIST SP 800-53 Rev. 4** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11

Function	Category	Subcategory	Informative References
		PR.IP-12: Viene sviluppato e implementato un piano di gestione delle vulnerabilità	· **CIS CSC** 4, 18, 20 · **COBIT 5** BAI03.10, DSS05.01, DSS05.02 · **ISO/IEC 27001:2013** A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 · **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 4.7, 4.8, 4.9.1 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
	Maintenance (PR.MA): La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-1:** La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati	· **COBIT 5** BAI03.10, BAI09.02, BAI09.03, DSS01.05 · **ISA 62443-2-1:2009** 4.3.3.3.7 · **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 · **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5, MA-6 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 4.5, 8.2.2
		PR.MA-2: La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati	· **CIS CSC** 3, 5 · **COBIT 5** DSS05.04 · **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 · **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 · **NIST SP 800-53 Rev. 4** MA-4 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 3.4.1, 8.2.2

Function	Category	Subcategory	Informative References
	Protective Technology (PR.PT): Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-1:** Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi	· **CIS CSC** 1, 3, 5, 6, 14, 15, 16 · **COBIT 5** APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 · **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 · **NIST SP 800-53 Rev. 4** AU Family · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 5.5.1 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.PT-2: I supporti di memorizzazione removibili sono protetti ed il loro uso è ristretto in accordo alle policy	· **CIS CSC** 8, 13 · **COBIT 5** APO13.01, DSS05.02, DSS05.06 · **ISA 62443-3-3:2013** SR 2.3 · **ISO/IEC 27001:2013** A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 · **NIST SP 800-53 Rev. 4** MP-2, MP-3, MP-4, MP-5, MP-7, MP-8 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 5.9.1, 8.7.1, 8.8.1, 13.5 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11

Function	Category	Subcategory	Informative References
		PR.PT-3: Viene adottato il principio di minima funzionalità configurando i sistemi in modo che forniscano solo le funzionalità necessarie	· **CIS CSC** 3, 11, 14 · **COBIT 5** DSS05.02, DSS05.05, DSS06.06 · **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 · **ISO/IEC 27001:2013** A.9.1.2 · **NIST SP 800-53 Rev. 4** AC-3, CM-7 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 5.1.1, 5.1.2, 5.1.3, 5.9.1, 8.3.1 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.PT-4: Le reti di comunicazione e controllo sono protette	· **CIS CSC** 8, 12, 15 · **COBIT 5** DSS05.02, APO13.01 · **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 · **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3 · **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 5.9.1 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11

Function	Category	Subcategory	Informative References
		PR.PT-5: Sono implementati meccanismi (es. failsafe, load balancing, hot swap) che permettono di soddisfare requisiti di resilienza sia durante il normale esercizio che in situazioni avverse	· **COBIT 5** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 · **ISA 62443-2-1:2009** 4.3.2.5.2 · **ISA 62443-3-3:2013** SR 7.1, SR 7.2 · **ISO/IEC 27001:2013** A.17.1.2, A.17.2.1 · **NIST SP 800-53 Rev. 4** CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11

Function	Category	Subcategory	Informative References
DETECT (DE)	**Anomalies and Events (DE.AE):** Le attività anomale sono rilevate e il loro impatto potenziale viene analizzato.	**DE.AE-1:** Sono definite, rese note e gestite delle pratiche di riferimento (c.d. baseline) inerenti l'utilizzo della rete ed i flussi informativi attesi per utenti e sistemi	· **CIS CSC** 1, 4, 6, 12, 13, 15, 16 · **COBIT 5** DSS03.01 · **ISA 62443-2-1:2009** 4.4.3.3 · **ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4 · **Misure Minime AgID** ABSC 5.1.4, 5.5.1, 8.3.2, 13.3.1

Function	Category	Subcategory	Informative References
		DE.AE-2: Gli eventi rilevati vengono analizzati per comprendere gli obiettivi e le metodologie dell'attacco	· **CIS CSC** 3, 6, 13, 15 · **COBIT 5** DSS05.07 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 · **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple	· **CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 · **COBIT 5** BAI08.02 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4 · **Misure Minime AgID** ABSC 8.1.3
		DE.AE-4: Viene determinato l'impatto di un evento	· **CIS CSC** 4, 6 · **COBIT 5** APO12.06, DSS03.01 · **ISO/IEC 27001:2013** A.16.1.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI-4
		DE.AE-5: Vengono definite delle soglie di allerta per gli incidenti	· **CIS CSC** 6, 19 · **COBIT 5** APO12.06, DSS03.01 · **ISA 62443-2-1:2009** 4.2.3.10 · **ISO/IEC 27001:2013** A.16.1.4 · **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8 · **Misure Minime AgID** ABSC 5.5.1

Function	Category	Subcategory	Informative References
	Security Continuous Monitoring (DE.CM): I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-1:** Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity	· **CIS CSC** 1, 7, 8, 12, 13, 15, 16 · **COBIT 5** DSS01.03, DSS03.05, DSS05.07 · **ISA 62443-3-3:2013** SR 6.2 · **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4 · **D.Lgs. 18/5/2018 n. 65** Art. 14(2)-(3) · **Misure Minime AgID** ABSC 5.5.1, 8.1.2, 8.1.3, 8.5.1, 8.6.1, 8.9, 8.10.1, 13.4.1, 13.6, 13.7.1, 13.8.1
		DE.CM-2: Viene svolto il monitoraggio degli spazi fisici per rilevare potenziali eventi di cybersecurity	· **COBIT 5** DSS01.04, DSS01.05 · **ISA 62443-2-1:2009** 4.3.3.3.8 · **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2 · **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20 · **D.Lgs. 18/5/2018 n. 65** Art. 14(2)-(3)
		DE.CM-3: Viene svolto il monitoraggio del personale per rilevare potenziali eventi di cybersecurity	· **CIS CSC** 5, 7, 14, 16 · **COBIT 5** DSS05.07 · **ISA 62443-3-3:2013** SR 6.2 · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3 · **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11 · **D.Lgs. 18/5/2018 n. 65** Art. 14(2)-(3) · **Misure Minime AgID** ABSC 5.2

Function	Category	Subcategory	Informative References
		DE.CM-4: Il codice malevolo viene rilevato	· **CIS CSC** 4, 7, 8, 12 · **COBIT 5** DSS05.01 · **ISA 62443-2-1:2009** 4.3.4.3.8 · **ISA 62443-3-3:2013** SR 3.2 · **ISO/IEC 27001:2013** A.12.2.1 · **NIST SP 800-53 Rev. 4** SI-3, SI-8 · **Misure Minime AgID** ABSC 8.1.1, 8.2.2, 8.2.3, 8.5, 8.6.1, 8.7.2, 8.7.3, 8.7.4, 8.8.1, 8.9, 8.10.1, 8.11.1
		DE.CM-5: Il codice non autorizzato su dispositivi mobili viene rilevato	· **CIS CSC** 7, 8 · **COBIT 5** DSS05.01 · **ISA 62443-3-3:2013** SR 2.4 · **ISO/IEC 27001:2013** A.12.5.1, A.12.6.2 · **NIST SP 800-53 Rev. 4** SC-18, SI-4, SC-44 · **Misure Minime AgID** ABSC 8.1.1
		DE.CM-6: Viene svolto il monitoraggio delle attività dei service provider esterni per rilevare potenziali eventi di cybersecurity	· **COBIT 5** APO07.06, APO10.05 · **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 · **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4 · **D.Lgs. 18/5/2018 n. 65** Art. 14(9)
		DE.CM-7: Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati	· **CIS CSC** 1, 2, 3, 5, 9, 12, 13, 15, 16 · **COBIT 5** DSS05.02, DSS05.05 · **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1 · **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4 · **Misure Minime AgID** ABSC 5.8.1, 8.3

Function	Category	Subcategory	Informative References
		DE.CM-8: Vengono svolte scansioni per l'identificazione di vulnerabilità	· **CIS CSC** 4, 20 · **COBIT 5** BAI03.10, DSS05.01 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** RA-5 · **Misure Minime AgID** ABSC 4.1, 4.2, 4.3, 4.4.1, 4.6.1
	Detection Processes (DE.DP): Sono adottati, mantenuti e verificati processi e procedure di monitoraggio per assicurare la comprensione di eventi anomali.	**DE.DP-1:** Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability	· **CIS CSC** 19 · **COBIT 5** APO01.02**,** DSS05.01, DSS06.03 · **ISA 62443-2-1:2009** 4.4.3.1 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14 · **Misure Minime AgID** ABSC 8.2.1
		DE.DP-2: Le attività di monitoraggio soddisfano tutti i requisiti applicabili	· **COBIT 5** DSS06.01, MEA03.03, MEA03.04 · **ISA 62443-2-1:2009** 4.4.3.2 · **ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3 · **NIST SP 800-53 Rev. 4** AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
		DE.DP-3: I processi di monitoraggio vengono testati	· **COBIT 5** APO13.02, DSS05.02 · **ISA 62443-2-1:2009** 4.4.3.2 · **ISA 62443-3-3:2013** SR 3.3 · **ISO/IEC 27001:2013** A.14.2.8 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14 · **D.Lgs. 18/5/2018 n. 65** Art. 14(2)-(3)

Function	Category	Subcategory	Informative References
		DE.DP-4: L'informazione relativa agli eventi rilevati viene comunicata	· **CIS CSC** 19 · **COBIT 5** APO08.04, APO12.06, DSS02.05 · **ISA 62443-2-1:2009** 4.3.4.5.9 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.16.1.2, A.16.1.3 · **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: I processi di monitoraggio sono oggetto di periodici miglioramenti e perfezionamenti	· **COBIT 5** APO11.06, APO12.06, DSS04.05 · **ISA 62443-2-1:2009** 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6 · **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

Function	Category	Subcategory	Informative References
RESPOND (RS)	**Response Planning (RS.RP):** Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti di cybersecurity rilevati.	**RS.RP-1:** Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente	· **CIS CSC** 19 · **COBIT 5** APO12.06, BAI01.10 · **ISA 62443-2-1:2009** 4.3.4.5.1 · **ISO/IEC 27001:2013** A.16.1.5 · **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8 · **GDPR** Art. 33

Function	Category	Subcategory	Informative References
	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).	**RS.CO-1:** Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente	· **CIS CSC** 19 · **COBIT 5** EDM03.02, APO01.02, APO12.03 · **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 · **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8 · **D.Lgs. 18/5/2018 n. 65** Art. 9(2) · **Misure Minime AgID** ABSC 8.1.3
		RS.CO-2: Sono stabiliti dei criteri per documentare gli incidenti	· **CIS CSC** 19 · **COBIT 5** DSS01.03 · **ISA 62443-2-1:2009** 4.3.4.5.5 · **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 · **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(7), 14(5)
		RS.CO-3: Le informazioni sono condivise in maniera coerente con il piano di risposta	· **CIS CSC** 19 · **COBIT 5** DSS03.04 · **ISA 62443-2-1:2009** 4.3.4.5.2 · **ISO/IEC 27001:2013** A.16.1.2, Clause 7.4, Clause 16.1.2 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: Il coordinamento con le parti interessate dell'organizzazione avviene in coerenza con i piani di risposta	· **CIS CSC** 19 · **COBIT 5** DSS03.04 · **ISA 62443-2-1:2009** 4.3.4.5.5 · **ISO/IEC 27001:2013** Clause 7.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8

Function	Category	Subcategory	Informative References
		RS.CO-5: È attuata una condivisione spontanea delle informazioni con le parti interessate esterne all'organizzazione (information sharing) per ottenere una maggior consapevolezza della situazione (c.d. situational awareness)	· **CIS CSC** 19 · **COBIT 5** BAI08.04 · **ISO/IEC 27001:2013** A.6.1.4 · **NIST SP 800-53 Rev. 4** SI-5, PM-15 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(5), 12(7)-(8), 14(4)-(5), 14(7)-(9) · **Misure Minime AgID** ABSC 8.11.1
		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 · **Misure Minime AgID** ABSC
	Analysis (RS.AN): Vengono condotte analisi per assicurare un'efficace riposta e supporto alle attività di ripristino.	**RS.AN-1:** Le notifiche provenienti dai sistemi di monitoraggio vengono sempre visionate e analizzate	· **CIS CSC** 4, 6, 8, 19 · **COBIT 5** DSS02.04, DSS02.07 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: Viene compreso l'impatto di ogni incidente	· **COBIT 5** DSS02.02 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 · **NIST SP 800-53 Rev. 4** CP-2, IR-4 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(5), 12(7)-(8), 14(4)-(5), 14(7)-(9)

Function	Category	Subcategory	Informative References
		RS.AN-3: A seguito di un incidente viene svolta un'analisi forense	· **COBIT 5** APO12.06, DSS03.02, DSS05.07 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 · **ISO/IEC 27001:2013** A.16.1.7 · **NIST SP 800-53 Rev. 4** AU-7, IR-4
		RS.AN-4: Gli incidenti sono categorizzate in maniera coerente con i piani di risposta	· **CIS CSC** 19 · **COBIT 5** DSS02.02 · **ISA 62443-2-1:2009** 4.3.4.5.6 · **ISO/IEC 27001:2013** A.16.1.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
		RS.AN-5: Sono definiti processi per ricevere, analizzare e rispondere a informazioni inerenti vulnerabilità rese note da fonti interne o esterne all'organizzazione (es. test interni, bollettini di sicurezza, o ricercatori in sicurezza)	· **CIS CSC** 4, 19 · **COBIT 5** EDM03.02, DSS05.07 · **NIST SP 800-53 Rev. 4** SI-5, PM-15
	Mitigation (RS.MI): Vengono eseguite azioni per prevenire l'espansione di un evento di sicurezza, per mitigare i sui effetti e per risolvere l'incidente.	**RS.MI-1:** In caso di incidente vengono messe in atto procedure atte a contenerne l'impatto	· **CIS CSC** 19 · **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.4.5.6 · **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 · **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 · **NIST SP 800-53 Rev. 4** IR-4 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(2), 14(2)-(3) · **Misure Minime AgID** ABSC 8.1.3, 8.4

Function	Category	Subcategory	Informative References
		RS.MI-2: In caso di incidente vengono messe in atto procedure atte a mitigarne gli effetti	· **CIS CSC** 4, 19 · **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 · **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 · **NIST SP 800-53 Rev. 4** IR-4 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(2), 14(2)-(3) · **Misure Minime AgID** ABSC 8.4
		RS.MI-3: Le nuove vulnerabilità sono mitigate o documentate come rischio accettato	· **CIS CSC** 4 · **COBIT 5** APO12.06 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5 · **Misure Minime AgID** ABSC 4.7, 4.9.1
	Improvements (RS.IM): Le attività di risposta sono migliorate incorporando le "lesson learned" da attività precedenti di monitoraggio e risposta.	**RS.IM-1:** I piani di risposta agli incidenti tengono in considerazione le esperienze passate (lesson learned)	· **COBIT 5** BAI01.13 · **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.IM-2: Le strategie di risposta agli incidenti sono aggiornate	· **COBIT 5** BAI01.13, DSS04.08 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8

Function	Category	Subcategory	Informative References
RECOVER (RC)	**Recovery Planning (RC.RP):** I processi e le procedure di ripristino sono eseguite e mantenute per assicurare un recupero dei sistemi o asset coinvolti da un incidente di cybersecurity.	**RC.RP-1:** Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity	· **CIS CSC** 10 · **COBIT 5** APO12.06, DSS02.05, DSS03.04 · **ISO/IEC 27001:2013** A.16.1.5 · **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8 · **Misure Minime AgID** ABSC 3.2.2
	Improvements (RC.IM): I piani di ripristino ed i relativi processi sono migliorati tenendo conto delle "lesson learned" per le attività future.	**RC.IM-1:** I piani di riprisitino tengono in considerazione le esperienze passate (lesson learned)	· **COBIT 5** APO12.06, BAI05.07, DSS04.08 · **ISA 62443-2-1:2009** 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 · **Misure Minime AgID** ABSC 3.1.3
		RC.IM-2: Le strategie di recupero sono aggiornate	· **COBIT 5** APO12.06, BAI07.08 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
	Communications (RC.CO): Le attività di ripristino a seguito di un incidente sono coordinate con le parti interne ed esterne (es. le vittime, gli ISP, i proprietari dei sistemi attaccati, i vendor, i CERT/CSIRT).	**RC.CO-1:** A seguito di un incidente vengono gestite le pubbliche relazioni	· **COBIT 5** EDM03.02 · **ISO/IEC 27001:2013** A.6.1.4, Clause 7.4
		RC.CO-2: A seguito di un incidente viene ripristinata la reputazione	· **COBIT 5** MEA03.02 · **ISO/IEC 27001:2013** Clause 7.4
		RC.CO-3: Le attività di ripristino condotte a seguito di un incidente vengono comunicate alle parti interessate interne ed esterne all'organizzazione, inclusi i dirigenti ed i vertici dell'organizzazione	· **COBIT 5** APO12.06 · **ISO/IEC 27001:2013** Clause 7.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4

Appendice B. Prototipo di contestualizzazione per il GDPR

Function	Category	Subcategory	Classe	Livello di Priorità
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.	**ID.AM-1:** Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	**Libera**	
		ID.AM-2: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	**Libera**	
		ID.AM-3: I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati	**Libera**	

Function	Category	Subcategory	Classe	Livello di Priorità
		ID.AM-4: I sistemi informativi esterni all'organizzazione sono catalogati	**Libera**	
		ID.AM-5: Le risorse (es: hardware, dispositivi, dati, allocazione temporale, personale e software) sono prioritizzate in base alla loro classificazione (e.g. confidenzialità, integrità, disponibilità), criticità e valore per il business dell'organizzazione	**Libera**	
		ID.AM-6: Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	**Libera**	
		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)	**Obbligatoria**	**ALTA**

Function	Category	Subcategory	Classe	Livello di Priorità
		DP-ID.AM-8: I trattamenti di dati personali sono identificati e catalogati	**Obbligatoria**	**ALTA**
	Business Environment (ID.BE): La mission dell'organizzazione, gli obiettivi, le attività e gli attori coinvolti sono compresi e valutate in termini di priorità. Tali informazioni influenzano i ruoli, le responsabilità di cybersecurity e le decisioni in materia di gestione del rischio.	**ID.BE-1:** Il ruolo dell'organizzazione all'interno della filiera produttiva è identificato e reso noto	**Libera**	
		ID.BE-2: Il ruolo dell'organizzazione come infrastruttura critica e nel settore industriale di riferimento è identificato e reso noto	**Libera**	
		ID.BE-3: Sono definite e rese note delle priorità per quanto riguarda la missione, gli obiettivi e le attività dell'organizzazione	**Libera**	
		ID.BE-4: Sono identificate e rese note interdipendenze e funzioni fondamentali per la fornitura di servizi critici	**Libera**	
		ID.BE-5: Sono identificati e resi noti i requisiti di resilienza a supporto della fornitura di servizi critici per tutti gli stati di esercizio (es. sotto stress/attacco, in fase di recovery, normale esercizio)	**Libera**	

Function	Category	Subcategory	Classe	Livello di Priorità
	Governance (ID.GV): Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity.	**ID.GV-1:** È indetificata e resa nota una policy di cybersecurity	**Libera**	
		ID.GV-2: Ruoli e responsabilità inerenti la cybersecurity sono coordinati ed allineati con i ruoli interni ed i partner esterni	**Libera**	
		ID.GV-3: I requisiti legali in materia di cybersecurity, con l'inclusione degli obblighi riguardanti la privacy e le libertà civili, sono compresi e gestiti	**Obbligatoria**	**ALTA**

Function	Category	Subcategory	Classe	Livello di Priorità
		ID.GV-4: La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity	**Libera**	
	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.	**ID.RA-1:** Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate	**Libera**	
		ID.RA-2: L'organizzazione riceve informazioni su minacce e vulnerabilità da fonti esterne (e.g. CERT, fonti aperte, forum di information sharing)	**Libera**	

Function	Category	Subcategory	Classe	Livello di Priorità
		ID.RA-3: Le minacce, sia interne che esterne, sono identificate e documentate	**Libera**	
		ID.RA-4: Sono identificati i potenziali impatti sul business e le relative probabilità di accadimento	**Libera**	
		ID.RA-5: Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio	**Libera**	
		ID.RA-6: Sono identificate e prioritizzate le risposte al rischio	**Libera**	

Function	Category	Subcategory	Classe	Livello di Priorità
		DP-ID.RA-7: Viene effettuata una valutazione di impatto sulla protezione dei dati personali	**Obbligatoria**	**ALTA**
	Risk Management Strategy (ID.RM): Le priorità e i requisiti dell'organizzazione e la tolleranza al rischio sono definiti e utilizzati per supportare le decisioni sul rischio operazionale.	**ID.RM-1:** I processi di risk management sono stabiliti, gestiti e concordati tra i responsabili dell'organizzazione (c.d. stakeholder)	**Libera**	
		ID.RM-2: Il rischio tollerato dall'organizzazione è identificato ed espresso chiaramente	**Libera**	
		ID.RM-3: Il rischio tollerato è determinato tenendo conto del ruolo dell'organizzazione come infrastruttura critica e dei rischi specifici presenti nel settore industriale di appartenenza	**Libera**	

Function	Category	Subcategory	Classe	Livello di Priorità
	Supply Chain Risk Management (ID.SC): Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-1:** I processi di gestione del rischio inerenti la catena di approvvigionamento cyber sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione	**Libera**	
		ID.SC-2: I fornitori e i partner terzi di sistemi informatici, componenti e servizi sono identificati, prioritizzati e valutati utilizzando un processo di valutazione del rischio inerente la catena di approvvigionamento cyber	**Libera**	
		ID.SC-3: I contratti con i fornitori e i partner terzi sono utilizzati per realizzare appropriate misure progettate per rispettare gli obiettivi del programma di cybersecurity dell'organizzazione e del Piano di Gestione del Rischio della catena di approvvigionamento cyber	**Libera**	
		ID.SC-4: Fornitori e partner terzi sono regolarmente valutati utilizzando audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali	**Libera**	

Function	Category	Subcategory	Classe	Livello di Priorità
		ID.SC-5: La pianificazione e la verifica della risposta e del ripristino sono condotti con i fornitori e i partner terzi	**Libera**	
	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	**Consigliata**	
		DP-ID.DM-2: Sono definiti, implementati e documentati i processi riguardanti l'informazione dell'interessato in merito al trattamento dei dati	**Obbligatoria**	**ALTA**
		DP-ID.DM-3: Sono definiti, implementati e documentati i processi di raccolta e revoca del consenso dell'interessato al trattamento di dati	**Obbligatoria**	**ALTA**

Function	Category	Subcategory	Classe	Livello di Priorità
		DP-ID.DM-4: Sono definiti, implementati e documentati i processi per l'esercizio dei diritti (accesso, rettifica, cancellazione, ecc.) dell'interessato	**Obbligatoria**	**ALTA**
		DP-ID.DM-5: Sono definiti, implementati e documentati i processi di trasferimento dei dati in ambito internazionale	**Obbligatoria**	**ALTA**

Function	Category	Subcategory	Classe	Livello di Priorità
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi, ed è gestito in maniera consistente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-1:** Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza	**Consigliata**	**ALTA**

Function	Category	Subcategory	Classe	Livello di Priorità
		PR.AC-2: L'accesso fisico alle risorse è protetto e amministrato	**Consigliata**	**ALTA**
		PR.AC-3: L'accesso remoto alle risorse è amministrato	**Consigliata**	**ALTA**
		PR.AC-4: Gli accessi alle risorse e le autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni	**Consigliata**	**ALTA**
		PR.AC-5: L'integrità di rete è protetta (es. segregazione di rete, segmentazione di rete)	**Consigliata**	**ALTA**
		PR.AC-6: Le identità sono comprovate, associate a credenziali e verificate durante le interazioni	**Consigliata**	**ALTA**
		PR.AC-7: Le modalità di autenticazione (es. autenticazione a singolo o multi fattore) per gli utenti, i dispositivi e altri asset sono commisurate al rischio della transazione (es. rischi legati alla sicurezza e privacy degli individui e altri rischi dell'organizzazione)	**Consigliata**	**ALTA**

Function	Category	Subcategory	Classe	Livello di Priorità
	Awareness and Training (PR.AT): Il personale e le terze parti sono sensibilizzate e formate in materia di cybersecurity e ricevono adeguata preparazione, coerente con le politiche, le procedure e gli accordi esistenti, per svolgere correttamente i compiti e le responsabilità legate alla cybersecurity	**PR.AT-1:** Tutti gli utenti sono informati e addestrati	**Libera**	
		PR.AT-2: Gli utenti privilegiati (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità	**Libera**	
		PR.AT-3: Tutte le terze parti (es. fornitori, clienti, partner) comprendono i loro ruoli e responsabilità	**Libera**	
		PR.AT-4: I dirigenti ed i vertici aziendali comprendono i loro ruoli e responsabilità	**Libera**	
		PR.AT-5: Il personale addetto alla sicurezza fisica e alla cybersecurity comprende i suoi ruoli e responsabilità	**Libera**	

Function	Category	Subcategory	Classe	Livello di Priorità
	Data Security (PR.DS): I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-1:** I dati e le informazioni memorizzate sono protetti	**Consigliata**	**ALTA**
		PR.DS-2: I dati sono protetti durante la trasmissione	**Consigliata**	**ALTA**
		PR.DS-3: Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale	**Consigliata**	**ALTA**
		PR.DS-4: I sistemi hanno adeguate risorse a disposizione per poter garantire la disponibilità	**Consigliata**	**MEDIA**
		PR.DS-5: Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak).	**Consigliata**	**ALTA**
		PR.DS-6: Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni	**Consigliata**	**ALTA**

Function	Category	Subcategory	Classe	Livello di Priorità
		PR.DS-7: Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione	**Libera**	
		PR.DS-8: Sono impiegati meccanismi di controllo dell'integrità per verificare l'integrità del hardware	**Consigliata**	**BASSA**
	Information Protection Processes and Procedures (PR.IP): Sono attuate e adeguate nel tempo politiche di sicurezza (che indirizzano scopo, ambito, ruoli e responsabilità, impegno da parte del management e coordinamento tra le diverse entità organizzative), processi e procedure per gestire la protezione dei sistemi informativi e degli assets.	**PR.IP-1:** Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)	**Libera**	
		PR.IP-2: Viene implementato un processo per la gestione del ciclo di vita dei sistemi (System Development Life Cycle).	**Consigliata**	**BASSA**
		PR.IP-3: Sono attivi processi di controllo della modifica delle configurazioni	**Consigliata**	**MEDIA**
		PR.IP-4: I backup delle informazioni sono eseguiti, amministrati e verificati	**Consigliata**	**ALTA**
		PR.IP-5: Sono rispettate le policy ed i regolamenti relativi agli ambienti fisici in cui operano le risorse dell'organizzazione	**Consigliata**	**MEDIA**

Function	Category	Subcategory	Classe	Livello di Priorità
		PR.IP-6: I dati sono distrutti in conformità con le policy	**Consigliata**	**ALTA**
		PR.IP-7: I processi di protezione sono sottoposti a miglioramenti	**Consigliata**	**MEDIA**
		PR.IP-8: L'efficacia delle tecnologie di protezione viene condivisa	**Consigliata**	**BASSA**
		PR.IP-9: Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro	**Consigliata**	**ALTA**
		PR.IP-10: I piani di risposta e recupero a seguito di incidenti/disastri sono verificati nel tempo	**Consigliata**	**MEDIA**
		PR.IP-11: Le problematiche inerenti la cybersecurity sono incluse nei processi di gestione del personale (es: screening, deprovisioning)	**Consigliata**	**MEDIA**
		PR.IP-12: Viene sviluppato e implementato un piano di gestione delle vulnerabilità	**Consigliata**	**ALTA**

Function	Category	Subcategory	Classe	Livello di Priorità
	Maintenance (PR.MA): La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-1:** La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati	**Libera**	
		PR.MA-2: La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati	**Libera**	
	Protective Technology (PR.PT): Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-1:** Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi	**Consigliata**	**MEDIA**
		PR.PT-2: I supporti di memorizzazione removibili sono protetti ed il loro uso è ristretto in accordo alle policy	**Consigliata**	**ALTA**
		PR.PT-3: Viene adottato il principio di minima funzionalità configurando i sistemi in modo che forniscano solo le funzionalità necessarie	**Consigliata**	**MEDIA**
		PR.PT-4: Le reti di comunicazione e controllo sono protette	**Consigliata**	**ALTA**
		PR.PT-5: Sono implementati meccanismi (es. failsafe, load balancing, hot swap) che permettono di raggiungere i requisiti di resilienza sia durante il normale esercizio che in situazioni avverse	**Consigliata**	**ALTA**

Function	Category	Subcategory	Classe	Livello di Priorità
DETECT (DE)	**Anomalies and Events (DE.AE):** Le attività anomale sono rilevate e il loro impatto potenziale viene analizzato.	**DE.AE-1:** Sono definite, rese note e gestite delle pratiche di riferimento (c.d. baseline) inerenti l'utilizzo della rete ed i flussi informativi attesi per utenti e sistemi	**Libera**	
		DE.AE-2: Gli eventi rilevati vengono analizzati per comprendere gli obiettivi e le metodologie dell'attacco	**Libera**	
		DE.AE-3: Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple	**Libera**	
		DE.AE-4: Viene determinato l'impatto di un evento	**Libera**	
		DE.AE-5: Vengono definite delle soglie di allerta per gli incidenti	**Libera**	
	Security Continuous Monitoring (DE.CM): I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-1:** Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity	**Libera**	
		DE.CM-2: Viene svolto il monitoraggio degli spazi fisici per rilevare potenziali eventi di cybersecurity	**Libera**	

Function	Category	Subcategory	Classe	Livello di Priorità
		DE.CM-3: Viene svolto il monitoraggio del personale per rilevare potenziali eventi di cybersecurity	**Libera**	
		DE.CM-4: Il codice malevolo viene rilevato	**Libera**	
		DE.CM-5: Il codice non autorizzato su dispositivi mobili viene rilevato	**Libera**	
		DE.CM-6: Viene svolto il monitoraggio delle attività dei service provider esterni per rilevare potenziali eventi di cybersecurity	**Libera**	
		DE.CM-7: Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati	**Libera**	
		DE.CM-8: Vengono svolte scansioni per l'identificazione di vulnerabilità	**Libera**	

Function	Category	Subcategory	Classe	Livello di Priorità
	Detection Processes (DE.DP): Sono adottati, mantenuti e verificati processi e procedure di monitoraggio per assicurare la comprensione di eventi anomali.	**DE.DP-1:** Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability	**Libera**	
		DE.DP-2: Le attività di monitoraggio soddisfano tutti i requisiti applicabili	**Libera**	
		DE.DP-3: I processi di monitoraggio vengono testati	**Libera**	
		DE.DP-4: L'informazione relativa agli eventi rilevati viene comunicata	**Libera**	
		DE.DP-5: I processi di monitoraggio sono oggetto di periodici miglioramenti e perfezionamenti	**Libera**	

Function	Category	Subcategory	Classe	Livello di Priorità
RESPOND (RS)	**Response Planning (RS.RP):** Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti di cybersecurity rilevati.	**RS.RP-1:** Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente	**Consigliata**	**ALTA**

Function	Category	Subcategory	Classe	Livello di Priorità
	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).	**RS.CO-1:** Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente	**Libera**	
		RS.CO-2: Sono stabiliti dei criteri per documentare gli incidenti	**Libera**	
		RS.CO-3: Le informazioni sono condivise in maniera coerente con il piano di risposta	**Libera**	
		RS.CO-4: Il coordinamento con le parti interessate dell'organizzazione avviene in coerenza con i piani di risposta	**Libera**	
		RS.CO-5: È attuata una condivisione spontanea delle informazioni con le parti interessate esterne all'organizzazione (information sharing) per ottenere una maggior consapevolezza della situazione (c.d. situational awareness)	**Libera**	
		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	**Obbligatoria**	**ALTA**

Function	Category	Subcategory	Classe	Livello di Priorità
	Analysis (RS.AN): Vengono condotte analisi per assicurare un'efficace riposta e supporto alle attività di ripristino.	**RS.AN-1:** Le notifiche provenienti dai sistemi di monitoraggio vengono sempre visionate e analizzate	**Libera**	
		RS.AN-2: Viene compreso l'impatto di ogni incidente	**Libera**	
		RS.AN-3: A seguito di un incidente viene svolta un'analisi forense	**Libera**	
		RS.AN-4: Gli incidenti sono categorizzate in maniera coerente con i piani di risposta	**Libera**	
		RS.AN-5: Sono definiti processi per ricevere informazioni, analizzare e rispondere a vulnerabilità rese note all'organizzazione da fonti interne o esterne (es. test interni, bollettini di sicurezza, o ricercatori in sicurezza)	**Libera**	

Function	Category	Subcategory	Classe	Livello di Priorità
	Mitigation (RS.MI): Vengono eseguite azioni per prevenire l'espansione di un evento di sicurezza, per mitigare i sui effetti e per risolvere l'incidente.	**RS.MI-1:** In caso di incidente vengono messe in atto procedure atte a contenerne l'impatto	**Libera**	
		RS.MI-2: In caso di incidente vengono messe in atto procedure atte a mitigarne gli effetti	**Libera**	
		RS.MI-3: Le nuove vulnerabilità sono mitigate o documentate come rischio accettato	**Libera**	
	Improvements (RS.IM): Le attività di risposta sono migliorate incorporando le "lesson learned" da attività precedenti di monitoraggio e risposta.	**RS.IM-1:** I piani di risposta agli incidenti tengono in considerazione le esperienze passate (lesson learned)	**Libera**	
		RS.IM-2: Le strategie di risposta agli incidenti sono aggiornate	**Libera**	

Function	Category	Subcategory	Classe	Livello di Priorità
RECOVER (RC)	**Recovery Planning (RC.RP):** I processi e le procedure di ripristino sono eseguite e mantenute per assicurare un recupero dei sistemi o asset coinvolti da un incidente di cybersecurity.	**RC.RP-1:** Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente	**Libera**	

Function	Category	Subcategory	Classe	Livello di Priorità
	Improvements (RC.IM): I piani di ripristino ed i relativi processi sono migliorati tenendo conto delle "lesson learned" per le attività future.	**RC.IM-1:** I piani di riprisitino tengono in considerazione le esperienze passate (lesson learned)	**Libera**	
		RC.IM-2: Le strategie di recupero sono aggiornate	**Libera**	
	Communications (RC.CO): Le attività di ripristino a seguito di un incidente sono coordinate con le parti interne ed esterne (es. le vittime, gli ISP, i proprietari dei sistemi attaccati, i vendor, i CERT/CSIRT).	**RC.CO-1:** A seguito di un incidente vengono gestite le pubbliche relazioni	**Libera**	
		RC.CO-2: A seguito di un incidente viene ripristinata la reputazione	**Libera**	
		RC.CO-3: Le attività di ripristino condotte a seguito di un incidente vengono comunicate alle parti interessate interne ed esterne all'organizzazione, inclusi i dirigenti ed i vertici dell'organizzazione	**Libera**	

Bibliografia

[1] Presidenza del Consiglio dei Ministri, «Quadro strategico nazionale per la sicurezza dello spazio cibernetico,» Dicembre 2013. [Online]. Available: https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/quadro-strategico-nazionale-cyber.pdf.

[2] Presidenza del Consiglio dei Ministri, «Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica,» Marzo 2017. [Online]. Available: https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf.

[3] CIS Sapienza, 2015 Italian Cyber Security Report - Un Framework Nazionale per la Cyber Security, R. Baldoni e L. Montanari, A cura di, 2015.

[4] CIS Sapienza, 2016 Italian Cybersecurity Report - Controlli Essenziali di Cybersecurity, 2016.

[5] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, vol. v1.1, 2018.