Security Management: strumenti e applicazioni
- la figura del Security Manager -

Ing. Marco Pugliese, Ph. D., IEEE Sr. member
Senior Security Manager (UNI 10459:2017 cert. n. 220/PS/Vp)
Abilitato CSP/CSE
23 novembre 2022
marpug@univaq.it

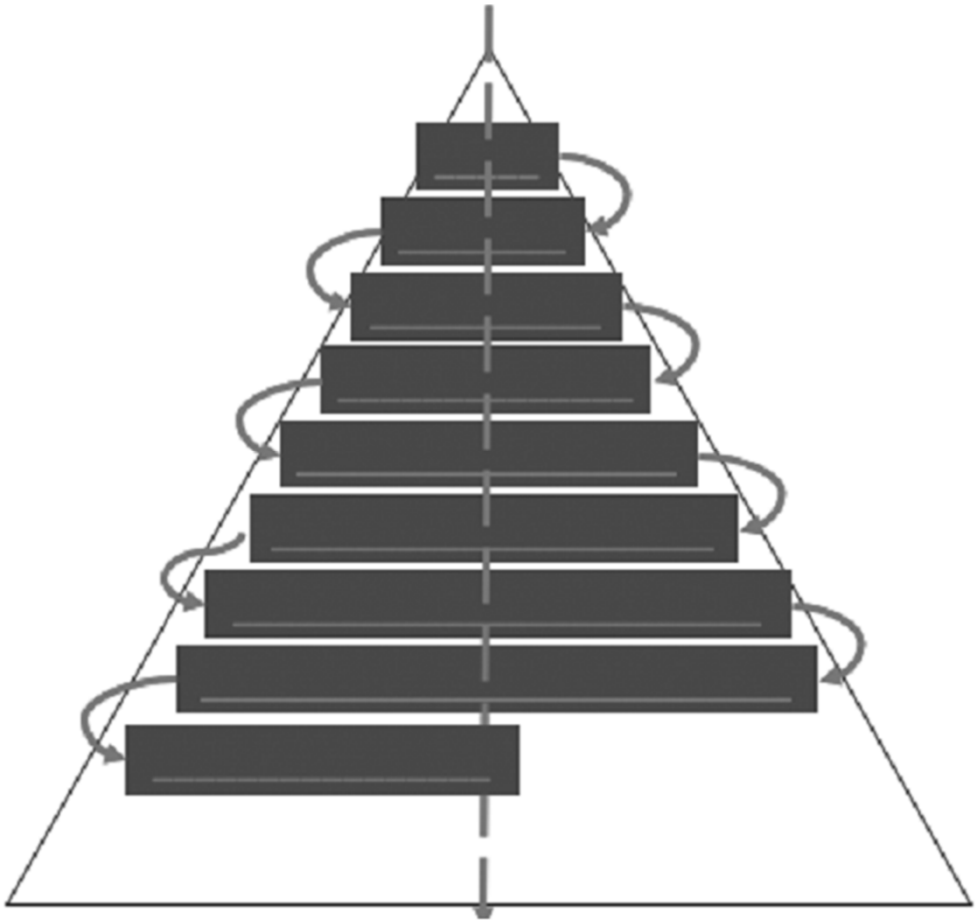
Security vs. Risk Management

- Security Management è il processo di gestione della **sicurezza integrata** finalizzato a garantire un livello di sicurezza complessiva accettabile dall'Organizzazione attraverso **strumenti** che portano a **risultati comparabili** se condotto da **professionisti qualificati (e certificati)** secondo **metodologie** riprese da **normative volontarie o cogenti.**
- **Sicurezza integrata** è l'accezione più vasta della sicurezza che "permea" tutti i processi organizzativi e produttivi di un'Organizzazione (c.d. **sicurezza liquida**). La sicurezza integrata deve prevenire e proteggere da danni riconducibili ad accadimenti:
  - **di origine interna**, legati allo svolgimento dell'attività amministrativa e produttiva dell'Organizzazione, a *responsabilità oggettiva o soggettiva per azioni dei propri dipendenti* o a *danno dei propri dipendenti* o *terzi dell'Organizzazione.*
  - **di origine esterna**, legate ad azioni compiute a *danno di beni materiali e immateriali dell'Organizzazione* o a loro conseguenze

- Pertanto se il Risk Management è il processo di gestione dei rischi, allora il **Security Management è una particolare istanza di un processo di Risk Management applicato al sotto-insieme dei rischi che comportano perdite.**

- Si dimostrerà che non si può richiedere il rischio nullo (e quindi la sicurezza "perfetta") ma solo requisiti di **rischio accettabile** (e quindi requisiti di livelli minimi di sicurezza, i c.d. **Required Security Level**).

Security vs. Risk Management



[fonte: F. Farina, M. Marrocco, Complessità di security e gestione del rischio, ed. Themis]

La genesi del concetto di rischio

Nel corso del tempo il concetto di rischio ha visto un'evoluzione notevole arrivando alla concezione moderna di rischio sia come possibilità di perdite ma anche di ricavi (il rischio come opportunità) misurabili.

- **ca. 1700 a.C.:** Codice di Hammurabi, concetto di condivisione del rischio
- **1654:** carteggio tra Pascal e Fermat su basi matematiche della teoria della probabilità.
- **1921:** l'economista F. H. Knight pubblica il libro "Risk, Uncertainty and Profit" in cui prova a dare una definizione di rischio. Knight mette in luce da subito un concetto di fondamentale importanza: **il concetto di rischio si contrappone a quello di incertezza**. **Per la prima volta si pongono in relazione i processi decisionali con le situazioni caratterizzate da rischio ed incertezza**.
- **Anni '80:** K. Popper, D. Kahneman e A. Tversky (pionieri sugli studi del bias cognitivo) propongono una visione del rischio non più basata solamente sulle metodologie di **misurazione quantitativo-statistica, ma dando valore anche alle percezioni soggettive della realtà dell'individuo (misurazione semi-quantitativa).**
- **2000:** J. W. De Loach in "Enterprise-Wide Risk Management Strategies for Linking Risk and Opportunity" (FT/Prentice Hall, 2000) per primo mette in luce un aspetto importante del concetto di rischio, ovvero **che il rischio di impresa può condurre ad effetti positivi, il rischio è una risorsa positiva**.

La genesi del concetto di rischio

- Pertanto con l'accezione "**negativa**" di rischio si inquadrano **tutti i rischi che se avverati generano perdite economiche** (quindi rischi di mancata protezione, mancata prevenzione, in genere di mancata sicurezza, di cattiva progettazione / manutenzione di sistemi, di degrado della prestazione di servizi, reputazionali per gli operatori di servizi nel caso di erogazioni sotto SLA, …).
- Con l'accezione "**positiva**" di rischio si inquadrano **tutti i rischi che se avverati generano ricavi economici** (quindi rischi di impresa, di investimento, di forecast commerciale, …).

La normativa ISO 31000:2018 "Risk Management Guidelines" raccoglie la definizione moderna e definisce il rischio come segue:

Risk is the effect of uncertainty on objectives*. An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities or threat.*

Risk is usually expressed in terms of risk sources (element which alone or in combination has the potential to give rise to risk), potential events (occurrence or change of a particular set of circumstances), their consequences (outcome of an event affecting objectives) and their likehood (chance of something happening).

Risk Management are the coordinated activities to direct and control an organization with regard to risk.

Pertanto la quantificazione di un rischio risulta proporzionale al valore del danno / opportunità pesati sulla corrispondente probabilità di accadimento.

Indice degli argomenti

- **Le precondizioni minime per un sistema "sicuro" e il Quadro normativo di riferimento**
- La cybersecurity e la direttiva UE 2016/1148 c.d. "direttiva NIS“ – L’Agenzia per la Cybersicurezza Nazionale
- Approccio Metodologico alla Gestione del Rischio secondo ISO 31000
- Il Professionista della Security (Security Manager) ai sensi della UNI 10459:2017
- Il Modello di Gestione della Sicurezza (MOGS): ambiti di applicazione
  - cybersecurity: il NIST Cybersecurity Framework (CSF) e il processo di individuazione degli RSL (Required Security Level) – il Framework Nazionale per la Cybersecurity e la Data Protection – ISMS vs. NIST CSF
  - privacy ai sensi del GDPR
  - HSE ai sensi della ISO 45001 (cenni)
  - tutela responsabilità amm. aziendale ai sensi del D. Lgs. 231/01 (cenni)

Precondizioni minime per un sistema "sicuro"

Un sistema di sicurezza (nella fattispecie un modello di gestione) è **esimente** per l'Organizzazione che lo adotta se si può dimostrare che esso è completo rispetto all'individuazione dei rischi che gravano sui processi dell'Organizzazione (produttivi, organizzativi, …) e rispetto alla definizione delle misure di mitigazione - indicate anche da leggi e normative – che rendono i rischi stessi accettabili secondo l'Organizzazione e/o secondo prescrizioni di legge.

- Quali sono le precondizioni per la costruzione di un modello di gestione esimente?

  1) **conoscenza delle basi normative** che regolano i processi produttivi e organizzativi dell'Organizzazione (*Quadro normativo di riferimento*)

  2) **conoscenza e corretta applicazione delle metodologie** a supporto del processo di Risk / Security Management che permettono la **completezza** nell'individuazione, la ponderazione e la mitigazione dei rischi identificati (*Approccio Metodologico alla Gestione del Rischio secondo ISO 31000*).

  3) **verifica dei requisiti di competenze, conoscenze e abilità** di cui devono essere in possesso coloro che sono chiamati a guidare la risposta di security e quindi a redigere i modelli di gestione (*Il Professionista della Security ai sensi della UNI 10459:2017*) o a certificarli (nella veste di auditor negli organismi accreditati).

Quadro normativo di riferimento
ISO 27001 - 27002 (ISMS)

- **ISO 27001** (*Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti*) sostituisce la ex BS 7799.2 ed è una norma internazionale che contiene i requisiti per impostare e gestire un sistema di gestione della sicurezza delle informazioni (SGSI) o ISMS (*Information Security Management System*).
- La ISO 27001 non è (unicamente) uno standard di sicurezza informatica in quanto, oltre alla sicurezza logica, include la sicurezza fisica/ambientale e la sicurezza organizzativa.
- **ISO 27002** è una raccolta di "best practices" che possono essere adottate per soddisfare i requisiti della norma ISO 27001;
- Dal momento che l'informazione è un bene che aggiunge valore all'organizzazione, e che ormai la maggior parte delle informazioni sono custodite su supporti informatici, ogni organizzazione deve essere in grado di garantire la sicurezza dei propri dati, in un contesto dove i rischi informatici causati dalle violazioni dei sistemi di sicurezza sono in continuo aumento.

Quadro normativo di riferimento
ISO 27001 - 27002 (ISMS)

- L'obiettivo dello standard è di proteggere i dati e le informazioni da minacce di ogni tipo, al fine di assicurarne **l'integrità**, la **riservatezza** e la **disponibilità** e fornire i requisiti per realizzare e adottare un adeguato SGSI.
- Applicabile a imprese operanti nella gran parte dei settori commerciali e industriali, come finanza e assicurazioni, telecomunicazioni, servizi, trasporti, settori governativi.
- L'impostazione dello standard è coerente con quella del Sistema di Gestione per la Qualità ISO 9001 ed il Risk Management ISO 31000, basandosi sull'approccio per processi, strutturato in politica per la sicurezza (il c.d. modello PDCA, Plan-Do-Check-Act):
  - Identificazione dei rischi e analisi del contesto (Plan)
  - Analisi e ponderazione dei rischi (Do)
  - Trattamento dei rischi (Check)
  - Monitoraggio e revisione (Act)

L'applicazione ciclica del modello PDCA attraverso azioni e strumenti come audit interni, analisi di non conformità, azioni correttive e preventive, monitoraggio e sorveglianza, induce necessariamente un miglioramento continuo del sistema.

Quadro normativo di riferimento
Reg. UE 2016/679 GDPR

- Il **Regolamento UE 2016/679 General Data Protection Regulation**
  https://www.privacy-regulation.eu/it/
  recepito in Italia con il D. Lgs. 10 agosto 2018 n. 101 ha doppia finalità:

  1) proteggere i **dati personali delle persone fisiche** e

  2) **consentire la circolazione degli stessi** in condizioni di **integrità**, **riservatezza** e **disponibilità**.

- Il GDPR è il nuovo regolamento europeo sulla privacy che mostra un impatto regolatorio e sanzionatorio severo, **obbliga alla adozione di misure di security finalizzate al trattamento del dato personale**, di qualsiasi tipologia e finalità.
- E' introdotta la nomina (art. 37) di un Data Protection Officer (DPO) per effettuare le valutazioni di impatto del trattamento delle tipologie di dati personali (Data Protection Impact Analysis, DPIA) basata sulle metodologie di Risk Management.
- In questo scenario si inserisce la norma **UNI 11697:2017** "*Attività professionali non regolamentate – Profili professionali relativi al trattamento e alla protezione dei dati personali – Requisiti di conoscenza, abilità e competenza*" che, nell'appendice B, in relazione alla figura del DPO, richiede in modo specifico al Professionista.

Quadro normativo di riferimento
D.Lgs. 231/2001 art. 5

- Il D.Lgs. 231/2001 "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300*" ha introdotto nel nostro ordinamento giuridico il principio della responsabilità della persona giuridica conseguente alla commissione di un reato (presupposto). Tale principio ha portato all'affermazione di una nuova forma di responsabilità oggettiva, la c.d. **colpa di organizzazione**, per la cui verificazione occorre riscontrare nell'ente un comportamento colposo che non ha evitato la perpetrazione dell'illecito penale per carenza di regole di organizzazione, gestione e controllo astrattamente idonee a prevenire l'illecito.

Art. 5. *Responsabilità dell'ente*

1. L'ente e' responsabile per i reati commessi nel suo interesse o a suo vantaggio:
   a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonchè da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso;
   b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a).
2. **L'ente non risponde se le persone indicate nel co. 1 hanno agito nell'interesse esclusivo proprio o di terzi.**

Quadro normativo di riferimento
D.lgs. 231/2001 art. 6

1. Se il reato e' stato commesso dalle persone indicate nell'articolo 5, comma 1, lettera a), l'ente non risponde se prova che:
   a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, **modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi** (che sono basati sui concetti del Risk Management, n.d.r.)
   b) il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento **e' stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo** (c.d. Organismo di Vigilanza, OdV);
   c) le persone hanno commesso il reato **eludendo fraudolentemente** i modelli di organizzazione e di gestione;
   d) non vi e' stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lettera b).
2. I modelli di cui alla lettera a) devono rispondere alle seguenti esigenze:
   a) **individuare le attività** nel cui ambito possono essere commessi reati;
   b) prevedere specifici protocolli diretti a programmare la **formazione** e **l'attuazione** delle **decisioni** dell'ente in relazione ai reati da prevenire;
   c) individuare modalità di gestione delle **risorse finanziarie** idonee ad impedire la commissione dei reati;
   d) prevedere **obblighi di informazione** nei confronti dell'OdV;
   e) introdurre un sistema disciplinare idoneo a **sanzionare** il mancato rispetto delle misure indicate nel modello.

Quadro normativo di riferimento
D.lgs 231/2001 vs. ISO 37001:2016

- La norma ISO 37001:2016, stabilisce i requisiti del sistema di gestione progettati per aiutarti a **prevenire, rilevare e rispondere alla corruzione**, nonché a rispettare le leggi anti corruzione e gli impegni volontari applicabili alle attività dell'organizzazione.
- Quindi aspetti, come la frode o il riciclaggio di denaro, possono essere inclusi nell'ambito del sistema di gestione 231/01).
- Il modello ISO 37001 è basato sui concetti del Risk Management: è un sistema di controllo focalizzato alla **prevenzione dei rischi** legati al fenomeno corruzione, a prescindere dalla provenienza di tale rischio, (organizzazione esterna, business partners, dipendenti)
- Le verifiche ed i controlli specificano i requisiti relativi a:
  - procedure e linee di condotta anti-corruzione;
  - leadership, impegno e responsabilità del Top Management;
  - supervisione della conformità ai requisiti, da parte di funzioni apposite o manager;
  - corsi di formazione anti-corruzione;
  - valutazione dei rischi e due diligence per i vari progetti e partner d'affari;
  - controlli in ambito finanziario, commerciale, contrattuale e sui processi di approvvigionamento;
  - reportistica, monitoraggio, indagini e revisioni;
  - azioni correttive e miglioramento continuo.

Quadro normativo di riferimento
D.Lgs 81/2008 vs. ISO 45001

- **Il D.Lgs. 81/2008** prevede invece obblighi in materia di tutela della salute e sicurezza nei luoghi di lavoro, imponendo in particolare al datore di lavoro di effettuare una valutazione di tutti i rischi ai fini dell'elaborazione del Documento di Valutazione dei Rischi (DVR**)** basato sui concetti del Risk Management, attività che lo stesso non può delegare, e richiamando in tal senso il modello di organizzazione, gestione e controllo di cui al D.Lgs. 231/2001. L'altra attività ad esempio che il datore di lavoro non può delegare è la designazione del Responsabile del Servizio di Prevenzione e Protezione dai rischi (RSPP).

- La **ISO 45001:2018** ˝Sistemi di gestione per la salite e sicurezza sul lavoro – Requisiti e Guida per l'uso˝ è la prima norma internazionale a definire gli standard minimi di buona pratica per la protezione dei lavoratori.
- La norma si applica a qualsiasi organizzazione, indipendentemente dalle dimensioni, dal settore di appartenenza e dalla natura delle sue attività ed è progettata per essere integrata nei processi di gestione già esistenti: adotta infatti la stessa "struttura di alto livello" (High Level Structure - HLS) delle altre norme ISO sui sistemi di gestione come la **ISO 9001** (gestione per la qualità) e la **ISO 14001** (gestione ambientale).

Quadro normativo di riferimento

D.Lgs 81/2008 art. 28 (DVR)

Il **Documento della Valutazione dei Rischi** (DVR) deve contenere:

a) una relazione sulla valutazione di tutti i rischi per la sicurezza e la salute durante l'attività lavorativa, nella quale siano specificati i **criteri adottati per la valutazione stessa**. La scelta dei criteri di redazione del documento è rimessa al datore di lavoro, che vi provvede con criteri di semplicità, brevità e comprensibilità, in modo da garantirne la completezza e l'idoneità quale strumento operativo di pianificazione degli interventi aziendali e di prevenzione;

b) l'indicazione delle misure di prevenzione e di protezione attuate e dei dispositivi di protezione individuali adottati …(omissis);

c) il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza;

d) l'individuazione delle procedure per l'attuazione delle misure da realizzare, nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere, a cui devono essere assegnati unicamente soggetti in possesso di adeguate competenze e poteri;

e) l'indicazione del nominativo del responsabile del servizio di prevenzione e protezione, del rappresentante dei lavoratori per la sicurezza o di quello territoriale e del medico competente che ha partecipato alla valutazione del rischio;

f) l'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento.

Quadro normativo di riferimento

D.Lgs 81/2008 art. 30

1. Il modello di organizzazione e di gestione (MOG) idoneo ad avere **efficacia esimente** della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica ai sensi del D.Lgs 231/01 rispetto alla sicurezza e salute dei lavoratori, deve essere adottato ed efficacemente attuato, assicurando l'adempimento di tutti gli obblighi relativi:

   a) al rispetto degli **standard tecnico-strutturali** di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;

   b) alle attività di **valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti**;

   c) alle attività di **natura organizzativa**, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;

   d) alle attività di **sorveglianza sanitaria;**

   e) alle attività di **informazione** e **formazione** dei lavoratori;

   f) alle attività di **vigilanza** con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;

   g) alla acquisizione di **documentazioni** e **certificazioni** obbligatorie di legge;

   h) alle **periodiche verifiche** dell'applicazione e dell'efficacia delle procedure adottate.

Indice degli argomenti

- Le precondizioni minime per un sistema "sicuro" e il Quadro normativo di riferimento
- **La cybersecurity e la direttiva UE 2016/1148 c.d. "direttiva NIS“ – L’Agenzia per la Cybersicurezza Nazionale**
- Approccio Metodologico alla Gestione del Rischio secondo ISO 31000
- Il Professionista della Security (Security Manager) ai sensi della UNI 10459:2017
- Il Modello di Gestione della Sicurezza (MOGS): ambiti di applicazione
  - cybersecurity: il NIST Cybersecurity Framework (CSF) e il processo di individuazione degli RSL (Required Security Level) – il Framework Nazionale per la Cybersecurity e la Data Protection – ISMS vs. NIST CSF
  - privacy ai sensi del GDPR
  - HSE ai sensi della ISO 45001 (cenni)
  - tutela responsabilità amm. aziendale ai sensi del D. Lgs. 231/01 (cenni)

La direttiva 2016/1148 (Direttiva NIS)

- La **direttiva UE 2016/1148 del 6 luglio 2016** reca misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (**c.d. direttiva NIS - Network and Information Security"**) al fine di conseguire un "*livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'UE*".
- La direttiva è stata recepita nell'ordinamento italiano con il **D. Lgs. 18 maggio 2018 n. 65**, che stabilisce la cornice legislativa delle **misure da adottare per la sicurezza delle reti e dei sistemi informativi** ed individua i soggetti competenti per dare attuazione agli obblighi previsti dalla direttiva NIS.
- A seguire, il **D. Lgs. 21 settembre 2019 n. 105** adottato per garantire un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, attraverso **l'istituzione di un perimetro di sicurezza nazionale cibernetica e con la conseguente previsione di misure volte a garantire gli standard di sicurezza ritenuti necessari per minimizzare i rischi.**

La direttiva 2016/1148 (Direttiva NIS)

In **attuazione** del decreto legge n. 105 del 2019 sono stati definiti in particolare:

A) il **DPCM 30 luglio 2020, n.131** che *stabilisce i criteri secondo i quali le apposite autorità dovranno provvedere ad* ***identificare i soggetti da includere nel perimetro****, e le* ***modalità*** *con cui questi dovranno* ***censire le proprie strutture*** *(reti, infrastrutture, sistemi informativi ed i formatici, beni ICT , ecc...) e comunicarle alle autorità. Il* ***Mise si occuperà di strutture private e la Presidenza del Consiglio di quelle pubbliche****. La lista dei soggetti interessati, circa 150, non è pubblica.*

- *L'art. 2 individua però i soggetti che svolgono funzioni essenziali per lo Stato e che quindi sono interessati dal decreto. È costituito anche un Tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica.*
- *L'art. 3 indica i settori di priorità a cui appartengono i soggetti inclusi nel perimetro: interno; difesa; spazio e aerospazio; energia; telecomunicazioni; economia e finanza; trasporti; servizi digitali; tecnologie critiche; enti previdenziali/lavoro.*

B) il **DPCM 14 aprile 2021, n. 81** che riguarda l'applicazione del perimetro cibernetico. Tale decreto, costituisce il **Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici e di misure volte a garantire elevati livelli di sicurezza***".*

C) **il DPCM 15 giugno 2021** che individua le **categorie di beni sistemi e servizi ICT destinati ad essere impiegati nel sistema di sicurezza nazionale cibernetica**.

La direttiva 2016/1148 (Direttiva NIS)

- Il 4 agosto è stato convertito in legge il **D. Lgs. 14 giugno 2021, n. 82** *"Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale".* Si tratta di 19 articoli.
  - L'art. 5 istituisce l'**Agenzia per la Cybersicurezza Nazionale (ACN),** con personalità di diritto pubblico, dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria. All'interno dell'Agenzia vi è un **Nucleo per la cybersecurity** quale supporto al Presidente del Consiglio.
  - L'art. 10 indica le modalità di gestione delle crisi che coinvolgano aspetti di cybersicurezza.

L'Agenzia per la Cybersicurezza Nazionale

- L'adozione del D.Lgs. 14 giugno 2021, n. 82 ha ridefinito l'architettura nazionale cyber e istituito **l'Agenzia per la Cybersicurezza Nazionale (ACN)** a tutela degli interessi nazionali nel campo della cybersicurezza.
- L'ACN è Autorità nazionale per la cybersicurezza e assicura il **coordinamento tra i soggetti pubblici** coinvolti nella materia.
- Promuove la **realizzazione di azioni comuni volte a garantire la sicurezza e la resilienza cibernetica** necessarie allo sviluppo digitale del Paese.
- Persegue il conseguimento **dell'autonomia strategica nazionale ed europea nel settore del digitale**, in sinergia con il sistema produttivo nazionale, nonché attraverso il coinvolgimento del mondo dell'università e della ricerca.
- Favorisce specifici percorsi **formativi per lo sviluppo della forza lavoro** nel settore e sostiene campagne di sensibilizzazione oltre che una **diffusa cultura della cybersicurezza.**

Fonte: (https://www.acn.gov.it/)

L'Agenzia per la Cybersicurezza Nazionale

Strategia Nazionale di Cybersicurezza 2022-2026

- La **Strategia Nazionale di Cybersicurezza** volta a pianificare, coordinare e attuare misure tese a **rendere il Paese più sicuro e resiliente**

  rif. doc. Strategia Nazionale di Cybersicurezza, https://www.acn.gov.it/ACN_Strategia.pdf.

- La strategia prevede il raggiungimento di **82 misure entro il 2026**

  rif. doc. Piano di Implementazione, https://www.acn.gov.it/ACN_Implementazione.pdf

  L'ACN si occuperà anche di controllare che gli obiettivi vengano raggiunti.

Fonte: (https://www.acn.gov.it/strategia-nazionale-cybersicurezza)

L'Agenzia per la Cybersicurezza Nazionale

Strategia Nazionale di Cybersicurezza 2022-2026

La Strategia Nazionale di Cybersicurezza mira ad affrontare le seguenti sfide:

- **Assicurare una transizione digitale cyber resiliente della Pubblica Amministrazione (PA) e del tessuto produttivo:** La cybersicurezza dei servizi digitali è fondamentale per incentivarne la fruibilità da parte dei cittadini, che devono essere sicuri della protezione dei loro dati.
- **Anticipare l'evoluzione della minaccia cyber:** prevedere, prevenire e mitigare il più possibile gli impatti di eventuali attività cyber offensive.
- **Contrastare la disinformazione online nel più ampio contesto della cd. minaccia ibrida:** per garantire l'esercizio delle libertà fondamentali, ad esempio, durante consultazioni elettorali oppure in situazioni di crisi internazionale.
- **Gestione di crisi cibernetiche:** coordinamento tra tutti i soggetti pubblici e privati interessati, per dare una risposta pronta in caso di eventi cyber sistemici.
- **Autonomia strategica nazionale ed europea nel settore del digitale:** avere un controllo diretto sui dati conservati, elaborati e trasmessi attraverso le moderne tecnologie.

L'Agenzia per la Cybersicurezza Nazionale

Strategia Nazionale di Cybersicurezza 2022-2026

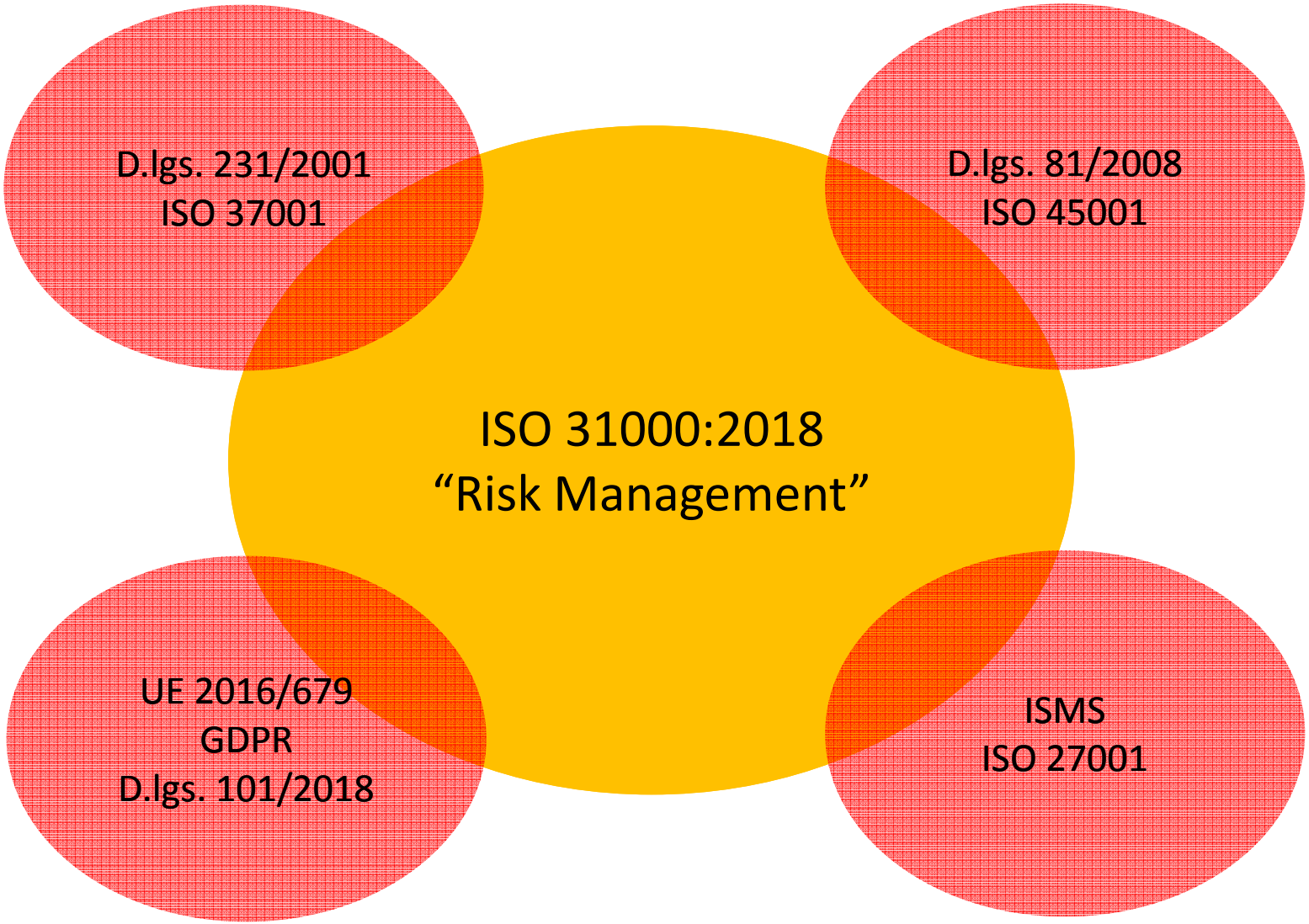
Attraverso la Strategia Nazionale di Cybersicurezza, sono stati individuati **tre obiettivi** fondamentali:

- **Protezione:** La protezione degli asset strategici nazionali, attraverso un approccio orientato alla gestione e mitigazione del rischio, formato sia da un quadro normativo che da misure, strumenti e controlli per abilitare una transizione digitale resiliente del Paese.
- **Risposta:** La risposta alle minacce, agli incidenti e alle crisi cyber nazionali, attraverso sistemi di monitoraggio, rilevamento, analisi e attivazione di processi che coinvolgano l'intero ecosistema di cybersicurezza nazionale.
- **Sviluppo:** Lo sviluppo sicuro delle tecnologie digitali, per rispondere alle esigenze del mercato, attraverso strumenti e iniziative volti a supportare i centri di eccellenza, le attività di ricerca e le imprese.

Indice degli argomenti

- Le precondizioni minime per un sistema "sicuro" e il Quadro normativo di riferimento
- La cybersecurity e la direttiva UE 2016/1148 c.d. "direttiva NIS“ – L’Agenzia per la Cybersicurezza Nazionale
- **Approccio Metodologico alla Gestione del Rischio secondo ISO 31000**
- Il Professionista della Security (Security Manager) ai sensi della UNI 10459:2017
- Il Modello di Gestione della Sicurezza (MOGS): ambiti di applicazione
  - cybersecurity: il NIST Cybersecurity Framework (CSF) e il processo di individuazione degli RSL (Required Security Level) – il Framework Nazionale per la Cybersecurity e la Data Protection – ISMS vs. NIST CSF
  - privacy ai sensi del GDPR
  - HSE ai sensi della ISO 45001 (cenni)
  - tutela responsabilità amm. Aziendale ai sensi del D. Lgs. 231/01 (cenni)

Centralità della ISO 31000:2018



Il filo logico del Rischio

- La norma ISO 31000:2018 definisce il **rischio** come il livello di incertezza nel raggiungimento di un obiettivo e può essere parimenti inteso come realizzazione di una minaccia che può portare ad una perdita (rischio puro) oppure come opportunità che può portare ad un profitto (rischio speculativo). Focalizzandosi sul rischio puro:
  - Una **minaccia** intesa come la potenzialità che venga tentato un attacco (es. attentato) o avvenga un incidente (es. malfunzionamento) o si manifesti un evento naturale (es. terremoto), che può insistere su di una …
  - **… esposizione** intesa come quantità o (superficie) misurabile di bene materiale o immateriale potenzialmente soggetto al danno e sfrutta, ovvero si avvale, della debolezza, di una o più …
  - **… vulnerabilità** di una organizzazione, inducendo il generarsi di un …
  - **… danno**, ed esponendo in tal senso l'organizzazione al rischio, riducendone la sua sicurezza.
  - oppure un **pericolo** (UNI 11230:2007) inteso come proprietà o qualità intrinseca (quindi non legata a fattori esterni) di un determinato fattore avente il potenziale di causare un **danno**.
- Il rischio non è la minaccia ma la minaccia che può realizzarsi.
- Il rischio è un parametro estrinseco (quindi legato a fattori esterni) soggetto a misura quali-quantitativa.
- **La valutazione del rischio deve essere effettuata in termini di una metodologia razionale (razionalizzare la percezione intuitiva) e quanto più possibile oggettiva (indipendente dal professionista) che produca risultati comparabili.**

Il Rischio Accettabile

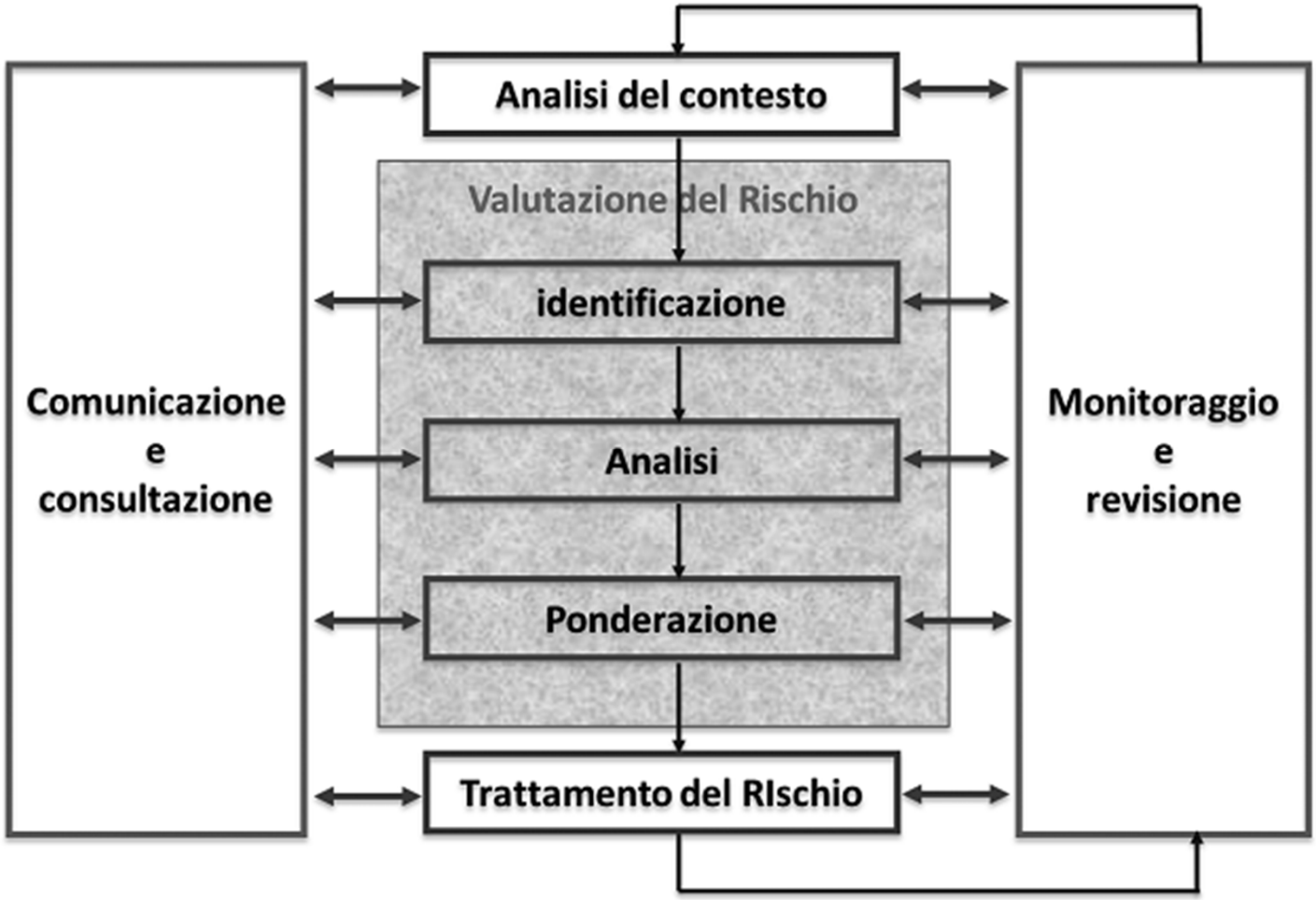
- Lo stabilisce l'Organizzazione.
- Quando il rischio residuo dopo più cicli del processo di gestione è minore o uguale al Rischio Accettabile (o rischio "TO BE"), allora la fase di trattamento è conclusa.

- Come si identifica / computa il Rischio Accettabile? Dipende dal contesto, p.es.:
  - Una possibile definizione: il rischio è ritenuto accettabile quando i controlli aggiuntivi "costano" più della risorsa da proteggere ovvero, in altre parole, quando il danno causato dall'accadimento dell'evento rischioso è inferiore al costo della misura per una ulteriore mitigazione.

    Definizione operativa, ma quando la risorsa da proteggere è la vita umana ovvero il danno in caso di accadimento dell'evento rischioso è la morte o una mutilazione ??
  - Un'altra possibile definizione (usata per i modelli di gestione secondo il D.lgs. 231/01): la soglia concettuale di accettabilità, nei casi di reati dolosi, è rappresentata da un sistema di prevenzione tale da non poter essere aggirato se non FRAUDOLENTEMENTE.

    Definizione solo formale utile per provare la non responsabilità (esimenza) dell'ente ovvero individuare il responsabile del reato.

Processo di Gestione del Rischio



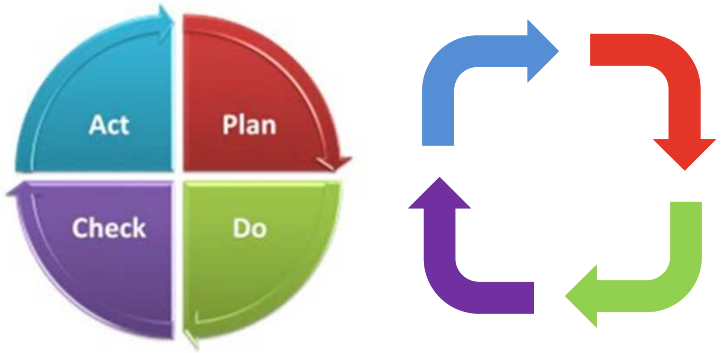
[fonte: F. Farina, M. Marrocco, Complessità di security e gestione del rischio, ed. Themis]

Processo di Gestione del Rischio

1. **Identificazione dei Rischi:** lista dei rischi sulla base delle sorgenti di rischio (risk sources) individuate sulla base di valutazioni di contesto e da diversi fonti informative., analisi del contesto (p.es. classe dei potenziali attaccanti, classe delle potenziali minacce).
2. **Analisi e Ponderazione del Rischio**: il rischio è definito come valore ponderato del danno generato in caso di accadimento. Pertanto in questa fase si analizza e si pondera la probabilità (o il livello di probabilità) di accadimento di ogni identificato e il danno corrispondente (o il livello del danno) generato in caso di accadimento.
3. **Trattamento del Rischio:** fase di progettazione e realizzazione delle misure di mitigazione del rischio (o di incremento della sicurezza). Le misure possono essere PREVENTIVE se finalizzate a ridurre la probabilità, o PROTETTIVE se finalizzate a ridurre il danno. Inoltre le misure si distinguono in PASSIVE se di deterrenza pura (protrarre nel tempo la probabilità di accadimento) dove non si ha informazione sullo stato dell'organizzazione / sistema sotto minaccia, o ATTIVE se si ha informazione per un intervento di eliminazione della minaccia in tempo utile. Le misure possono essere di natura TECNICA, PROCEDURALE, ORGANIZZATIVA. Le caratteristiche tecnico / organizzative / procedurali delle misure che portano l'organizzazione / sistema ad un livello accettabile di rischio (o di sicurezza) definiscono i requisiti dei livelli minimi di Sicurezza (**Required Security Level, RSL**) per l'organizzazione / sistema.
4. **Monitoraggio e revisione:** fase ciclica di misurazione continua dell'efficacia.

Ciclo di Deming

Il ciclo di W. E. Deming (1900-1993) o ciclo PDCA (Plan-Do-Check-Act), è uno strumento operativo alla base di qualunque sistema di gestione finalizzato al controllo e al miglioramento continuo dei processi produttivi.



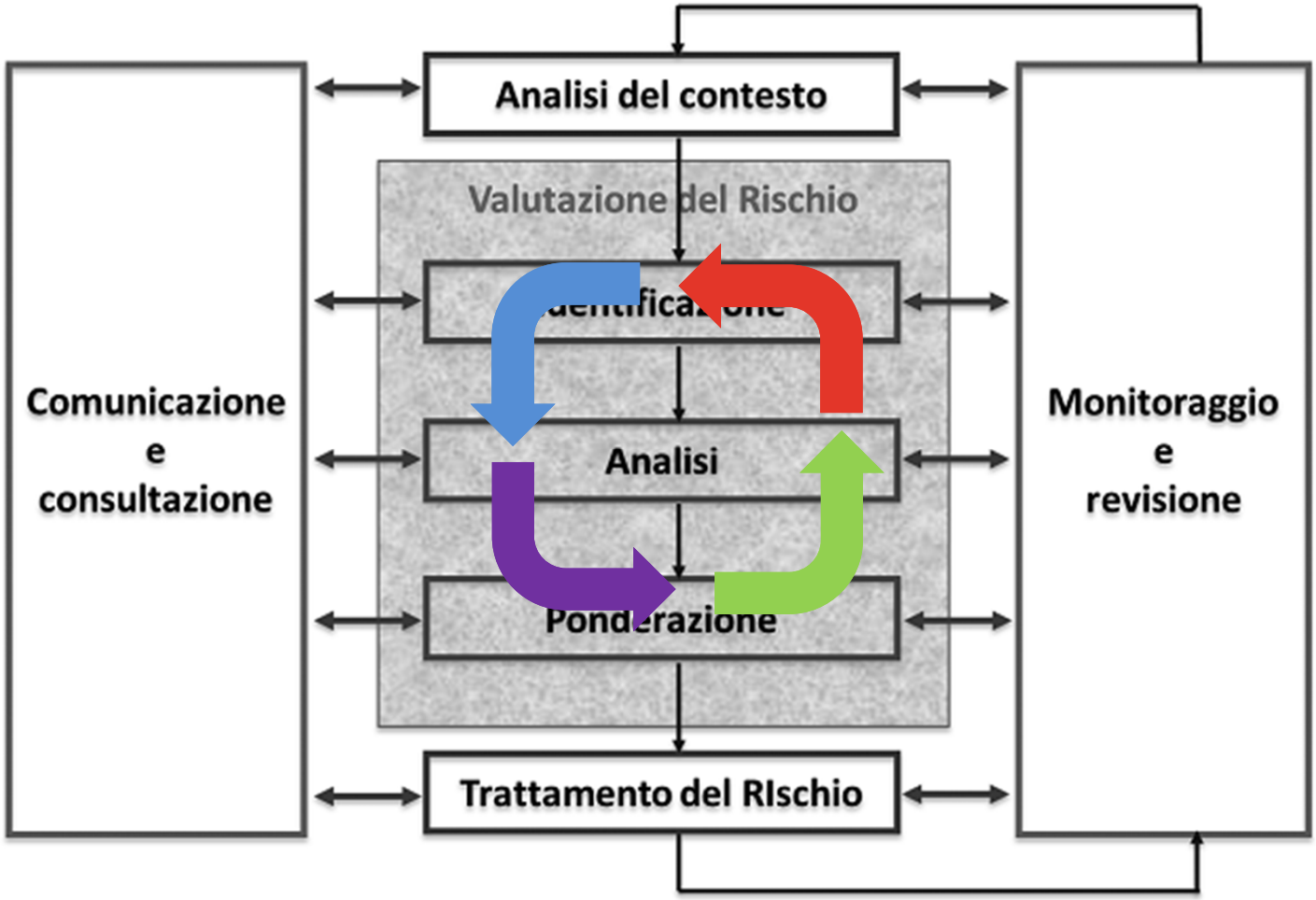
1. **PLAN – PIANIFICA: identificazione dei rischi e analisi del contesto**; definizione degli obiettivi di sicurezza; pianificazione/programmazione delle attività di sicurezza; individuazione e valutazione dei rischi a cui risultano esposte le risorse; definizione della gestione delle opzioni applicabili al rischio residuo dopo l'applicazione delle misure di riduzione;

2. **DO – IMPLEMENTA: attuazione di quanto stabilito nella fase di pianificazione**; implementazione di misure fisiche, logiche ed organizzative;

3. **CHECK – VERIFICA: confronto tra quanto emerso nella fase del DO e quanto stabilito nella fase del PLAN attraverso audit periodici**, monitoraggio dell'efficacia delle misure, nuova analisi del contesto per individuare eventuali cambiamenti;

4. **ACT – CORREGGI: standardizzazione del processo (mantenimento e perfezionamento) se non sono state riscontrate inefficienze**; azioni correttive focalizzate sugli elementi del processo che hanno dato luogo agli scostamenti tra i risultati attesi e quelli ottenuti, e quindi in caso di inefficienze.

Ciclicità del Processo di Gestione del Rischio



[fonte: F. Farina, M. Marrocco, Complessità di security e gestione del rischio, ed. Themis]

Ciclicità del Processo di Gestione del Rischio

Al fine della definizione della risposta di security, si distinguono tre tipi di rischio:

- il **Rischio Preventivo o inerente**, il rischio calcolato senza tenere conto delle contromisure adottate (o rischio "AS IS";
- il **Rischio atteso o potenziale**, il rischio calcolato a seguito di quanto definito nel Piano di trattamento del rischio, e che quindi tiene conto delle contromisure e della loro capacità attesa di riduzione del rischio;
- il **Rischio effettivo**, il rischio calcolato successivamente alle attività di monitoraggio delle stesse, che comprendono sia la misurazione di efficacia delle contromisure implementate che gli incidenti registrati.

Fase 1: Identificazione dei rischi

Attività di natura prevalentemente soggettiva dipendente dalla propria percezione dei rischi

Fase 1: Identificazione dei rischi

Attività di natura prevalentemente soggettiva dipendente dalla propria percezione dei rischi

Fase 1: Identificazione dei rischi

Attività di natura prevalentemente soggettiva dipendente dalla propria percezione dei rischi

Fase 2: Analisi e Ponderazione del Rischio

- Misurare il rischio significa determinare la sua "magnitudo", attraverso una funzione che misura la grandezza del singolo Rischio come prodotto della Probabilità che questo avvenga per il Danno che andrebbe a causare

$$\mathbf{R = P \times D}$$

- P indica la probabilità di accadimento di una minaccia che produce il danno D.
- R=0 se P=0 (ma allora non sussiste causa di rischio) e/oppure se D=0 (ma allora non è un rischio se non produce danni): quindi non esiste R=0 (q.e.d.)
- La probabilità P è funzione di diversi fattori: prevalenti la **frequenza** (F) dell'evento dannoso, la **vulnerabilità** (V) di quella specifica organizzazione rispetto a tale minaccia, l'esposizione (E), …: in generale **P= f(F, V, E, …)**.

  Frequenza: ciclicità temporale dell'accadimento, misurabile come indicatore della numerosità dell'evento osservato principalmente da evidenze documentali oggettive, ripetibili e fruibili in uguale misura da tutti.

  Vulnerabilità: caratteristica intrinseca del contesto considerato, che favorisce la concretizzazione della minaccia e quindi la generazione del rischio, in quanto criticità o debolezza nella difesa dell'obiettivo. **Può essere di natura tecnologica (V_T), procedurale (V_P) o da fattore umano (V_H).**

  Esposizione: quantità o (superficie) misurabile di bene materiale o immateriale potenzialmente soggetto al danno.

Fase 2: Analisi e Ponderazione del Rischio

- Quindi **R = P x D** con **P= f(F, V, E, …)** dove f() può assumere anche forme complesse, tipicamente dalla statistica attuariale.
- Il problema più arduo è la stima affidabile di P (o in generale di un peso W normalizzato) associata ad un rischio "complesso" ovvero in cui il c.d. "evento iniziatore" può scattare sotto diverse cause e può dare diverse conseguenze: si ricorre a tecniche qualitative o quantitative o (usualmente) semi-quantitative.
- La stima di D è "più semplice" solo nel caso di danno materiale o comunque se esistono metodi oggettivi per determinarne il costo: in casi come danno reputazionale, danno alla persona, danno all'ambiente, …, la stima diviene assai più complessa e può essere valutata:
  - Il danno reputazionale sulla base delle presumibili perdite commerciali / spese legali conseguenti.
  - Il danno alla persona, che include il danno biologico (la lesione in sé), il danno alla salute (conseguenze pregiudizievoli per la salute a causa della lesione), i danni morali (sofferenze a seguito della lesione) e i danni patrimoniali da lucro cessante (perdita di capacita lavorativa a seguito della lesione), sulla base di risarcimenti al danno biologico (da stabilirsi con criterio uniforme per qualunque persona), al danno alla salute (da stabilirsi per il singolo caso a seconda delle conseguenze pregiudizievoli), al danno da lucro cessante (da stabilirsi nella perdita patrimoniale conseguente, al danno dei pregiudizi esistenziali (pregiudizi subiti nella vita quotidiana che influiscono sulla qualità della vita)
  - Il danno ambientale sulla base dei costi sostenuti (direttamente o da ribaltare sul responsabile) per la riparazione / ripristino della situazione ante-fatto.

Fase 2: Analisi e Ponderazione del Rischio

- **Metodi qualitativi**: metodi in cui la valutazione del rischio non viene effettuata utilizzando espressioni matematiche ma risulta da un giudizio basato su documentazione, esperienze, serie storiche e quanto altro reperibile. Si adottano criteri soggettivi in cui *la probabilità di un evento è la misura del grado di fiducia che un individuo coerente attribuisce, secondo le sue informazioni e opinioni, all'avverarsi* (B. De Finetti, Sul significato soggettivo della probabilità, in *Fundamenta Mathematicae*, Warszawa, T. XVII, pp. 298–329, 1931).

- **Metodi quantitativi**: metodi in cui il rischio R=f(P,D) viene computata nel tempo, dove f() può assumere anche forme complesse dalla statistica attuariale e in cui devono essere disponibili i valori puntuali nel tempo da assegnare alla probabilità e al danno.

- **Metodi semi-quantitativi** (o semi-qualitativi): si basano su un'analisi quantitativa in cui al posto dei valori puntuali nel tempo da assegnare alla probabilità e al danno (evidentemente non disponibili), vengono assegnati alla funzione f() valori numerici pesati convenzionali per le probabilità e per il danno rappresentativi di una classe di livello di probabilità e di danno. Una classe di livello è definita (questo è l'aspetto qualitativo) da un range di valori di probabilità minima e massima per quella classe (analogamente per il danno) dove i valori agli estremi devono essere computati quantitativamente.

Fase 2: Analisi e Ponderazione del Rischio

Tecniche Qualitative

Tipicamente basate su brainstorming di gruppo con decisioni a maggioranza o sulla base della reputazione di esperienza di singoli.

Le più adottate sono:

- **Analisi storica**: consiste in una elaborazione statistica di dati che possono essere ottenuti da diverse fonti (report interni, banche dati, letteratura tecnica specializzata) ed è valido solo per prevenire tipologie di incidenti che si sono già verificati. Consente di avere una visione globale del problema, analizzando sia le cause sia le conseguenze sia eventuali modifiche organizzative e/o procedurali, strutturali e/o impiantistiche apportate dall'azienda per evitare il ripresentarsi dell'incidente.
- **Check-List**: consiste in liste di controllo, in forma di questionario (SI,NO; NON PERTINENTE), da esaminare per eseguire la rapida verifica della rispondenza alle specifiche di progettazione o agli adempimenti richiesti dalla legge.
- **HAZOP (HAZard and OPerability) analysis**: consiste in studi di gruppo sviluppati per consentire un esame formale, sistematico e critico degli intenti progettuali e processuali di un sistema attraverso il confronto diretto tra le esperienze di diverse persone con diverse funzioni aziendali (brainstorming).
- **Whatif? Analysis**: consiste in sessioni di 'brainstorming' partendo dalla domanda tipica "Cosa accade se...?". Adatto a controlli veloci.

Fase 2: Analisi e Ponderazione del Rischio

Tecniche Semi-Quantitative: FMEA

FMEA (**Failure Modes and Effects Analysis**): utilizzato nella valutazione dei rischi di impianti industriali, è una tecnica che analizza potenziali modalità di guasto, effetti e potenziali cause di un generico sistema e determina un fattore di priorità di rischio.

FMEA è implementata con i seguenti passi:

- Determinare tutte le modalità di guasto in base ai requisiti funzionali e successivamente considerare l'effetto finale di ciascuna di queste. Ad ogni effetto assegnare un numero di **Gravità (G)** o **Severity (S) =** [1 nessun effetto apprezzabile, 10 critica];
- Esaminare la causa di ogni singola modalità di guasto individuata e classificare la sua frequenza di accadimento con la **Probabilità (P)** o **Occurrence (O)** = [1 rarissima, 10 estremamente probabile]. Se tale frequenza è alta (> 4) è necessario determinare delle azioni correttive;
- Ad ogni combinazione dei due passaggi precedenti viene assegnato un numero di **Rilevamento (R)** in base al quale viene stabilita l'efficienza delle azioni determinate per rimuovere i modi di guasto o **Detection Number (D) =** [1 rilevabile normalmente , 10 rilevabile solo a posteriori].
- Calcolare il **Risk Priority Number (RPN)** come **RPN = S x O x D**

Fase 2: Analisi e Ponderazione del Rischio

Tecniche Semi-Quantitative: FMEA

Probabilità (P)	Gravità (G)	Rilevamento (R)
1	1	1 - 2
quasi impossibile Probabilità circa 1 su 100.000	nessun effetto sul processo Il cliente non si accorge di nulla difettosità assolutamente tollerabili	Sicuro rilevamento nelle comuni fasi di controllo del processo
2	2-3	3-4
improbabile Probabilità circa 1 su 5.000	insignificante Il cliente potrebbe essere leggermente disturbato	Alta probabilità di Rilevamento nelle comuni fasi del processo
3	4-6	5-6
Basso Probabilità circa 1 su 1.000	Interruzioni nel processo Problemi con alcuni clienti	Scoperta solo nel contesto di test mirati
4-6	7-8	7-8
evento occasionale Probabilità circa 1: 500 - 1: 100	servizio limitato Il cliente non è assolutamente contento	Nessuna scoperta prima della consegna al cliente. Tuttavia il cliente potrebbe rilevare delle difettosità
7-8	9	9
evento frequente Probabilità circa 1:100 - 1:20	Violazione dei regolamenti danni finanziari all'organizzazione o al cliente	Molto probabilmente il cliente individuerà degli errori non tollerabili
9-10	10	10
ricorrenza costante Probabilità di circa 1:10 - 1: 20	Rischio di danno grave. Violazione dei regolamenti danni ingenti finanziari all'organizzazione o al cliente	Scoperta non possibile immediatamente, solo nel corso del tempo

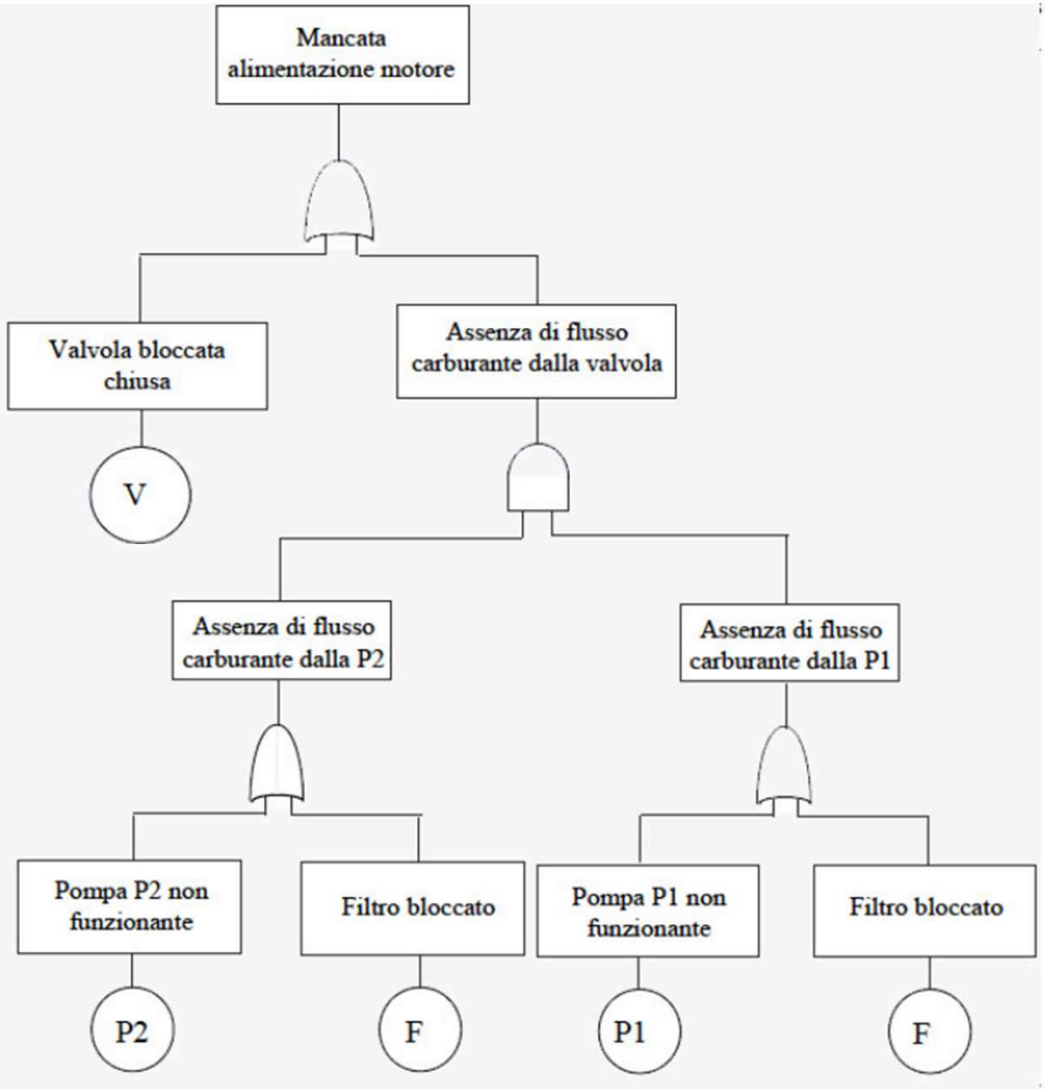
Fase 2: Analisi e Ponderazione del Rischio

Tecniche Semi-Quantitative: FTA / ETA

- **Fault Tree Analysis (FTA) o Albero dei Guasti**: albero delle relazioni di causa ed effetto dei guasti di un sistema. FTA parte da un evento incidentale (**Evento Iniziatore, EI**) e procede a ritroso, per metodo deduttivo, alla stesura di una sequenza logica fino alle cause prime (o presunte prime) che ne determinano la probabilità di accadimento .
- **Event Tree Analysis (ETA) o Albero degli Eventi:** albero delle potenziali conseguenze derivanti dal verificarsi di un EI.
- Il parametro oggetto di analisi e ponderazione è la **probabilità di accadimento di un evento** (guasto per la FTA e danno per la ETA).
- La decomposizione ad albero implica che devono essere trascurabili le probabilità condizionate tra gli eventi componenti: in caso contrario gli eventi interdipendenti devono collassare in un unico evento con probabilità pari alla probabilità congiunta (Bayes).
- Date le probabilità degli eventi componenti, FTA / ETA calcolano la probabilità di accadimento di ogni EI e di ogni conseguenza in funzione di operatori logici che definiscono i rami del FTA e dell'ETA. Dati due generici eventi A e B con probabilità di accadimento P(A) e P(B) si ha:
  - P (A **AND** B) = P(A) P(B)
  - P (A **OR** B) = P(A) + P(B) - P(A) P(B)
  - P (**NOT** A) = 1 - P(A)

Fase 2: Analisi e Ponderazione del Rischio

Tecniche Semi-Quantitative: FTA



P(EI) =
OR (**Valvola bloccata / chiusa**, Assenza di flusso carburante dalla valvola)

P(Assenza di flusso carburante dalla valvola) =
AND (Assenza di flusso carburante dalla P2, Assenza di flusso carburante dalla P1)

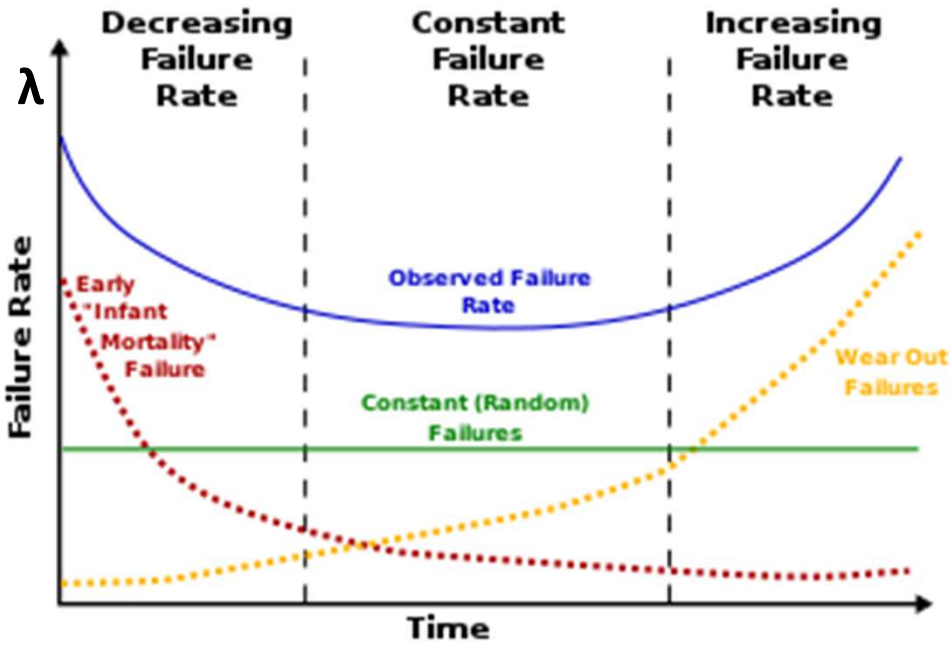
P(Assenza di flusso carburante dalla P2) =
OR (**Pompa P2 non funzionante**, **filtro bloccato**)

P(Assenza di flusso carburante dalla P1) =
OR (**Pompa P1 non funzionante**, **filtro bloccato**)

Fase 2: Analisi e Ponderazione del Rischio

Tecniche Semi-Quantitative: FTA

- Nel caso in cui l'evento è un guasto ad un apparato con parametro **λ (frequenza di guasto o failure rate) = numero di guasti per unità di tempo** (tipicamente in un anno) costante nel tempo, la distribuzione stocastica descrittiva è un processo di Poisson stazionario.
- La densità di probabilità di un guasto (senza memoria) al tempo t = $\lambda e^{-\lambda t}$
- La probabilità di un guasto (senza memoria) dall'avvio (t=0) a T anni = $1-e^{-\lambda T}$
- In realtà **λ** varia con l'età dell'apparato ed è desumibile dalle curve di guasto indicate nei manuali di manutenzione dell'apparato stesso (la c.d. curva a "vasca da bagno"): quindi esiste memoria → distribuzione di Weibull con parametro di forma opportuno.



- **Mean Time To Failure** (MTTF) = **1/λ.** Dati due apparati con λ_1 e λ_2
  - MTTF serie = $1/(\lambda_1 + \lambda_2)$
  - MTTF parallelo attivo = $1/\lambda_1 + 1/\lambda_2 - 1/(\lambda_1 + \lambda_2)$
  - MTTF parallelo passivo = $1/\lambda_1 + 1/\lambda_2$
- **Sempre MTTF parallelo passivo (entra su guasto) > MTTF parallelo attivo > MTTF serie**

Fase 2: Analisi e Ponderazione del Rischio

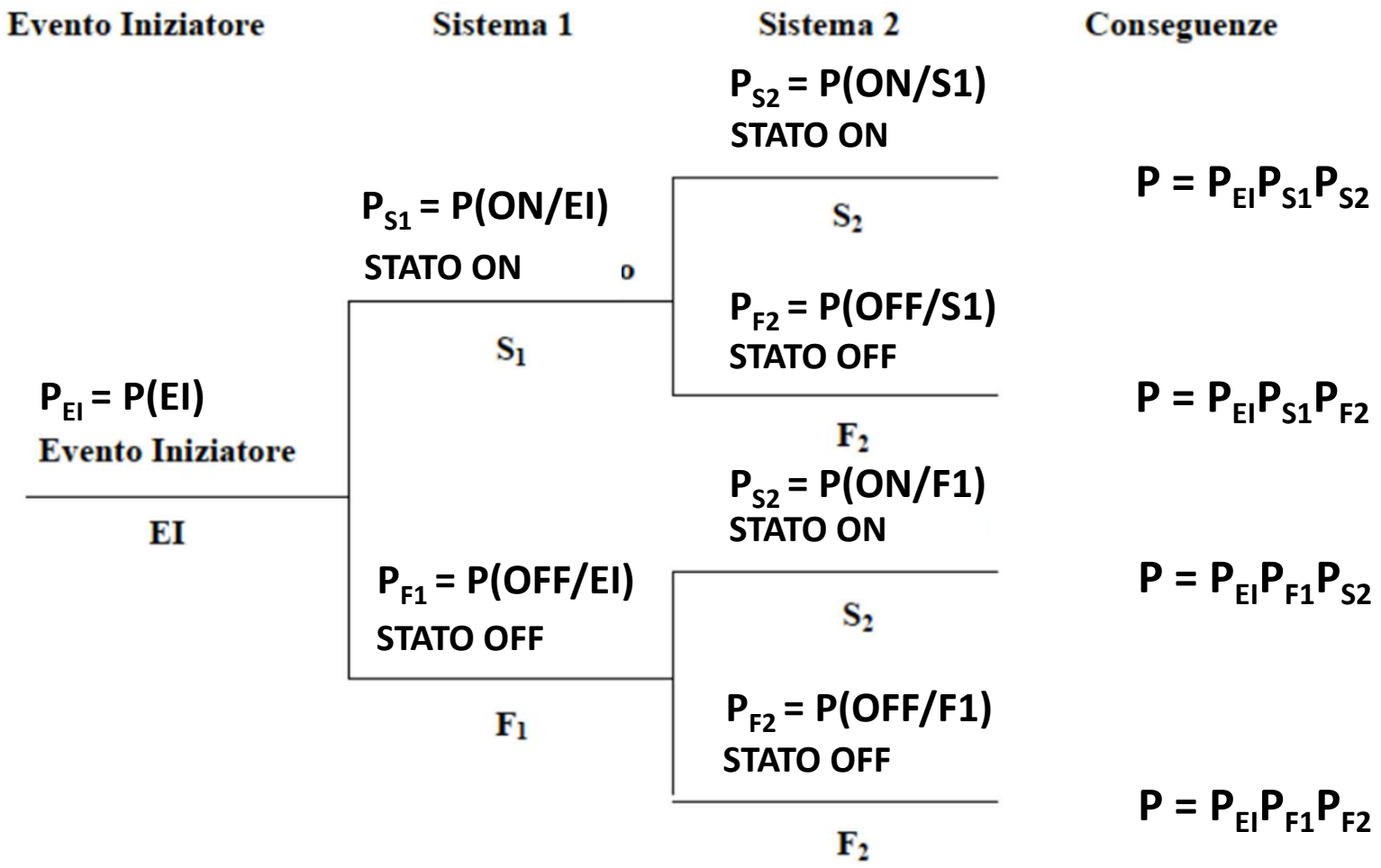
Tecniche Semi-Quantitative: FTA

Se per guasto si intende una generica disfunzione, allora la curva può risultare applicabile - almeno qualitativamente - per la probabilità di accadimento di disfunzioni, p.es. che portano a rischi sul lavoro, rischi per la salute.

- **Fase 1: la mortalità infantile**: (λ inizialmente elevata a decrescere) scarsa conoscenza del lavoro, scarsa consapevolezza del contesto aziendale se unito ad una giovane età può ulteriormente ridurre la capacità dell'individuo di rapportarsi correttamente con i rischi lavorativi. Misure: addestramento, affiancamento, sorveglianza, visite mediche preventive.
- **Fase 2: normale funzionamento**: (λ minima) il lavoratore è formato e conscio che le cose da scoprire sono ancora molte, presta generalmente attenzione a quello che fa e i riflessi lo aiutano. Misure: formazione continua e visite mediche previste secondo lo scadenziario INAIL.
- **Fase 3: usura**: (λ torna a crescere) dal punto di vista fisico è il logorio di riflessi, flessibilità muscolare e scheletrica, forza, capacità uditive, che vanno a ridurre la capacità di reagire ai rischi di malattia professionale quale rumore, vibrazioni, aumento delle fratture. Dal punto di vista psicologico, la c.d. "assuefazione al rischio“, normale processo psicologico dei lavoratori più esperti che porta a considerare con meno attenzione quei rischi ai quali sono giornalmente esposti. Misure: vigilanza ma, spesso, è svolta proprio da coloro che, più esperti, hanno assunto il ruolo di preposto ed essi stessi sono i primi a subire gli effetti di questa fase.

Fase 2: Analisi e Ponderazione del Rischio

Tecniche Semi-Quantitative: ETA



Fase 2: Analisi e Ponderazione del Rischio

Tecniche Semi-Quantitative: FTA / ETA

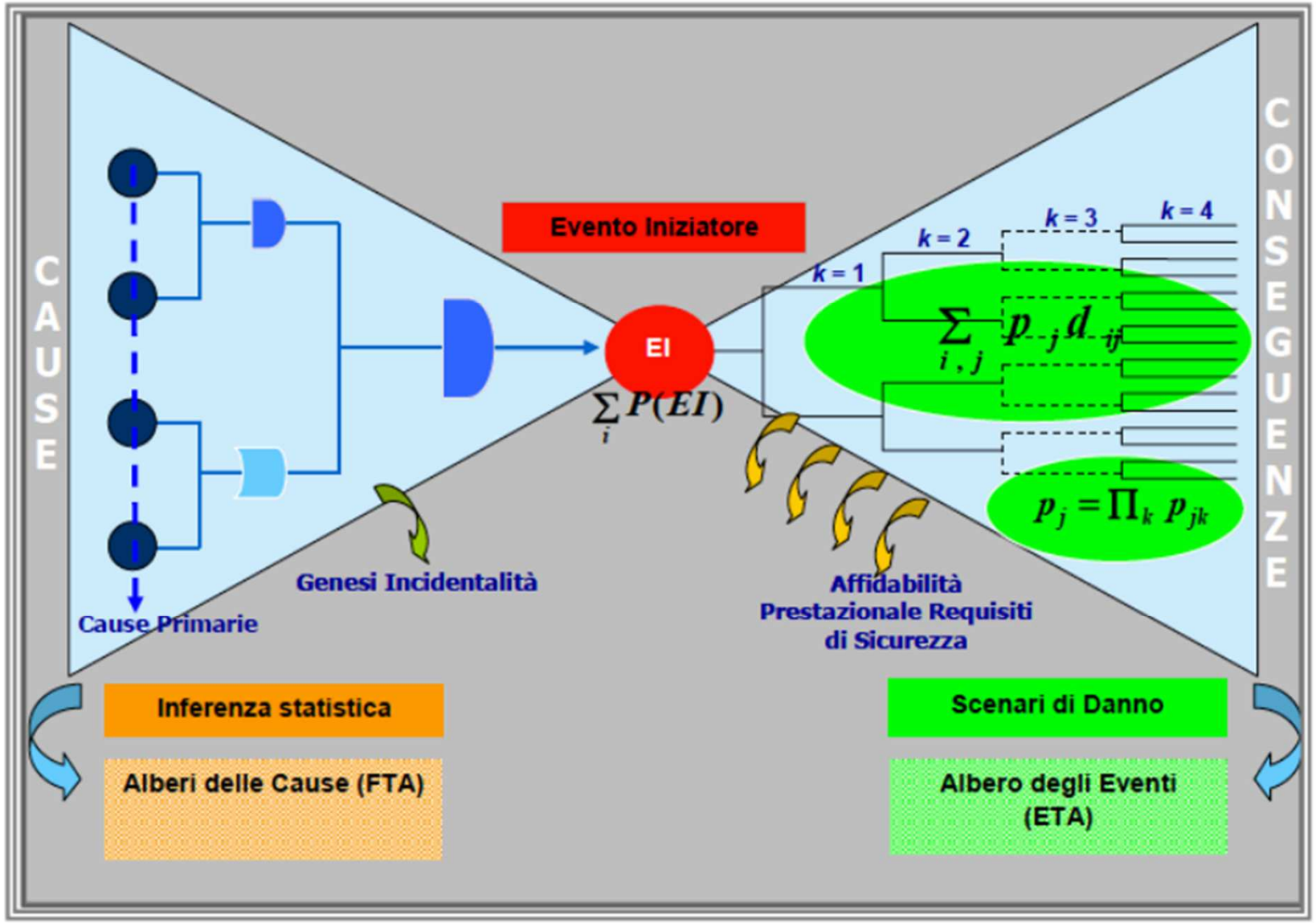
- Pertanto tramite la tecnica FTA / ETA si può ottenere la **stima della probabilità o di peso normalizzato** (puntuale o di range) di accadimento dell'EI e di tutte le conseguenze (ognuna delle quali potenzialmente EI di altri rischi!) partendo **da una stima di probabilità o di peso normalizzato** (puntuale o di range) delle cause prime.
- A questo punto si può procedere con l'assegnazione a P e a D di valori numerici convenzionali associati ai range che definiscono le varie classi di livello.

PROBABILITA'	RANGE (ESEMPIO)	CLASSE DI LIVELLO
MOLTO PROBABILE	0,7 - 1,0	4
PROBABILE	0,3 - 0,7	3
POCO PROBABILE	0,2 - 0,3	2
IMPROBABILE	0 - 0,2	1

DANNO	RANGE (ESEMPIO)	CLASSE DI LIVELLO
GRAVISSIMO	> € 1.000.000	4
GRAVE	€ 10.000 - € 1.000.000	3
MEDIO	€ 1.000 - € 10.000	2
LIEVE	€ 1 - € 1000	1

Fase 2: Analisi e Ponderazione del Rischio

Tecniche Semi-Quantitative: Bow Tie



Fase 2: Analisi e Ponderazione del Rischio

probabilità di accadimento del rischio

Livello	*Criteri di appartenenza al livello*	*Valore*
MOLTO PROBABILE	– esiste una correlazione diretta **fra** Il tipo di pericolo considerato **e** il verificarsi del danno ipotizzabile – **si sono già verificati** danni associati al tipo di pericolo considerato in azienda o in aziende simili, in situazioni operative simili – il verificarsi del danno associato al tipo di pericolo considerato **non susciterebbe stupore** in azienda – **non** sono state adottate misure di prevenzione	**4**
PROBABILE	– Il tipo di pericolo considerato può produrre un danno **anche se in modo non** automatico o diretto – è noto **qualche** caso in cui **al** tipo di pericolo considerato **è seguito un danno** in azienda o in aziende simili – il verificarsi di un danno associato al tipo di pericolo considerato **susciterebbe una moderata sorpresa** in azienda – le misure di prevenzione adottate **non** sono efficienti ed efficaci	**3**
POCO PROBABILE	– Il tipo di pericolo considerato può produrre un danno solo in circostanze sfortune di eventi – sono noti **solo rari** casi in cui al tipo di pericolo considerato **è conseguito un danno** in azienda o aziende simili – il verificarsi di un danno associato al tipo di pericolo considerato susciterebbe **una grande sorpresa** in azienda – le misure di prevenzione adottate sono efficienti ma **non sempre** efficaci	**2**
IMPROBABILE	– Il tipo di pericolo considerato può produrre un danno solo per la concomitanza di più eventi poco probabili – non sono noti casi in cui al tipo di pericolo considerato è conseguito un danno in azienda o aziende simili – il verificarsi di un danno associato al tipo di pericolo considerato susciterebbe incredulità in azienda – le misure di prevenzione adottate **sono** efficienti ed efficaci	**1**

Fase 2: Analisi e Ponderazione del Rischio

danno generato in caso di accadimento del rischio

Livello	*Criteri di appartenenza al livello*	*Valore*
GRAVISSIMO	– Il tipo di pericolo considerato in rapporto alle misure di protezione adottate può produrre un infortunio o episodio di esposizione **acuta** con **effetti letali** o di **invalidità totale** – Il tipo di pericolo considerato in rapporto alle misure di protezione adottate può produrre un'esposizione **cronica** con **effetti letali** e/o **totalmente invalidanti**	**4**
GRAVE	– Il tipo di pericolo considerato in rapporto alle misure di protezione adottate può produrre un infortunio o episodio di esposizione **acuta** con **effetti gravi** non letali o di **invalidità parziale** – Il tipo di pericolo considerato in rapporto alle misure di protezione adottate può produrre un'esposizione **cronica** con effetti **irreversibili e/o parzialmente invalidanti**	**3**
MEDIO	– Il tipo di pericolo considerato in rapporto alle misure di protezione adottate può produrre un infortunio o episodio di esposizione **acuta con effetti di inabilità reversibile** – Il tipo di pericolo considerato in rapporto alle misure di protezione adottate può produrre un'esposizione **cronica con effetti reversibili**	**2**
LIEVE	– Il tipo di pericolo considerato in rapporto alle misure di protezione adottate può produrre un infortunio o episodio di esposizione **acuta** con **effetti di inabilità rapidamente reversibile** – Il tipo di pericolo considerato in rapporto alle misure di protezione adottate può produrre un'esposizione **cronica** con **effetti rapidamente reversibili**	**1**

Fase 2: Analisi e Ponderazione del Rischio

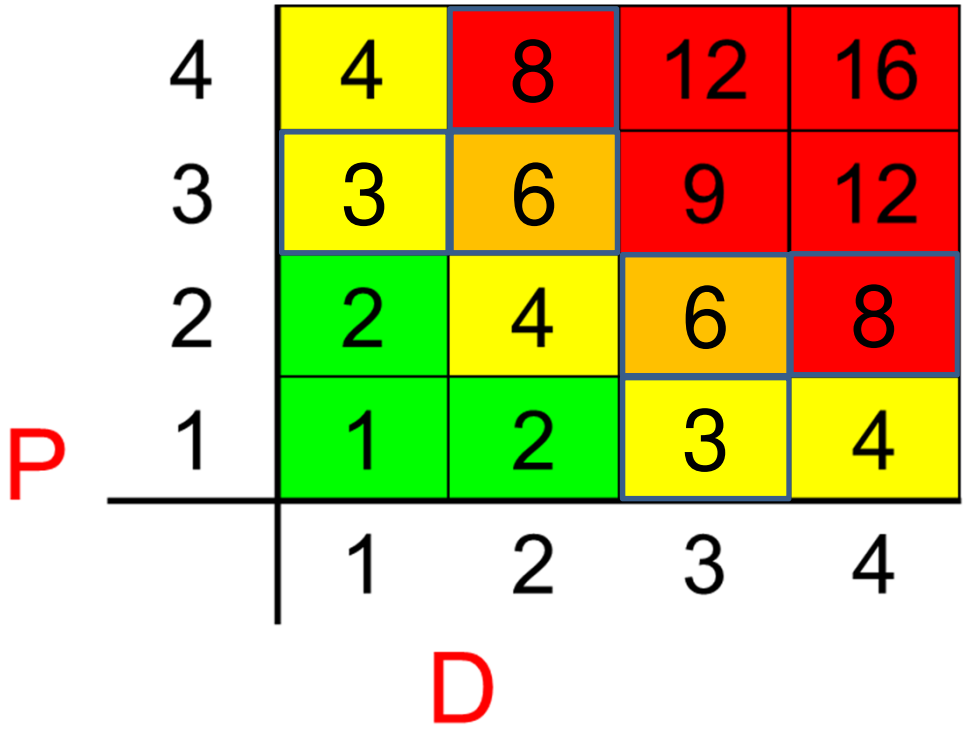
matrice del rischio

Rischio	Categoria di R	Adozione di Misure di Prevenzione e Protezione	Priorità
8 - 16	ALTO	Introduzione di misure di prevenzione e protezione per la riduzione e il controllo del rischio	Immediata o entro 3 mesi
5 - 7	MEDIO	Introduzione di misure di prevenzione e protezione necessarie per il controllo del rischio	Attuazione delle misure tra 3 e 6 mesi
3 - 4	BASSO	Garantire il mantenimento della situazione riscontrata	Attuazione delle misure entro l'anno
1 - 2	IRRILEVANTE	Non sono necessarie ulteriori misure	Prevedere una revisione di questi rischi oltre l'anno

Fase 2: Analisi e Ponderazione del Rischio

matrice del rischio

[non necessariamente quadrata]



La Valutazione del Rischio
… dipende anche dal contesto

Siamo in una giungla.

Danno: gravissimo (morte) (4)
Probabilità: probabile (3)
Rischio: 12 (ALTO)

medio (allergia) (2)
irrilevante (1)
2 (IRRILEVANTE)

La Valutazione del Rischio
… dipende anche dal contesto

Siamo in città.

Danno: gravissimo (morte) (4)
Probabilità: irrilevante (1)
Rischio: **4 (BASSO)**

medio (allergia) (2)
media (3)
6 (MEDIO)

Il Cigno Nero

- La teoria del “cigno nero" (dall'errata assunzione iniziale della sua inesistenza per poi essere scoperto) si riferisce unicamente a eventi possibili ma inaspettati di grande portata e grandi conseguenze (danni o opportunità) con un ruolo dominante nella storia. Tali eventi, considerati estremamente divergenti rispetto alla norma, giocano collettivamente un ruolo molto più importante della massa degli eventi ordinari (N. N. Taleb, “The Black Swan”, 2007), anzi di fatto sono indice che è la casualità a governare il mondo.
- Distribuzione di Taleb: caratterizzata da piccolo range di alte probabilità di basso danno / ricavo e largo range di bassissime probabilità (al limite infinitesime e comunque non quantificabili) di altissimo danno / ricavo.

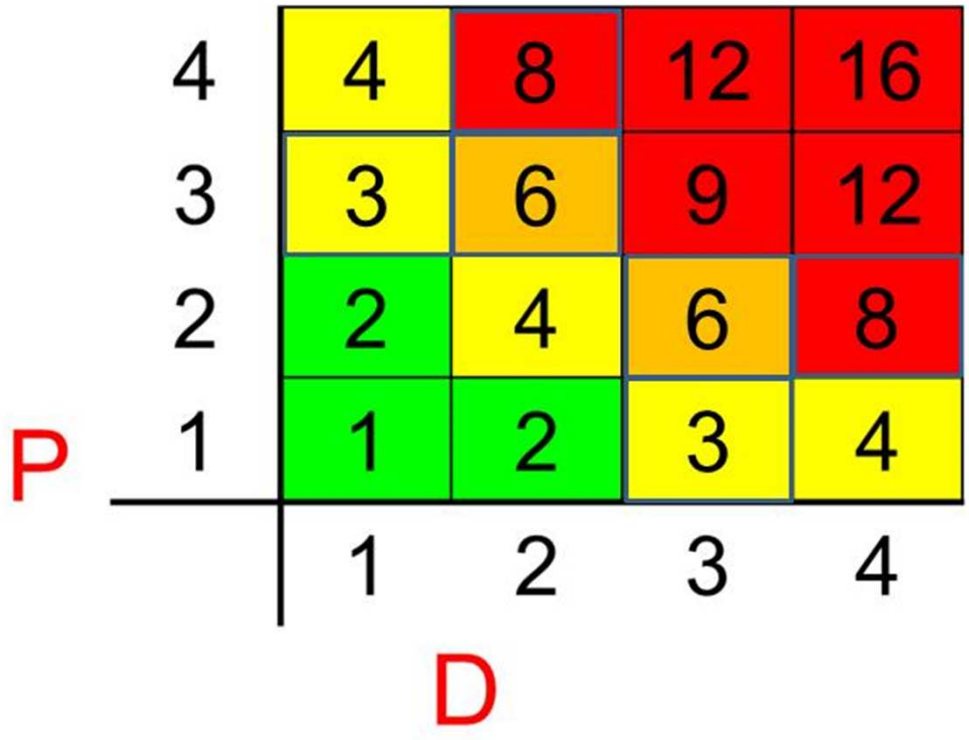
- Tuttavia si dimostra che se un evento è possibile per quanto sia bassa la probabilità di occorrenza è comunque destinato a verificarsi prima o poi.

  Se p è la probabilità di occorrenza di un evento e k è il numero di fallite realizzazioni prima della sua effettiva occorrenza, la probabilità di occorrenza dell’evento dopo k fallimenti è $P(p,k) = p(1-p)^k$ (distribuzione geometrica).

  Ma la somma per k→ inf (quindi prima o poi …) è convergente ed è pari a 1 (… si verifica) per qualsiasi p. C.V.D.

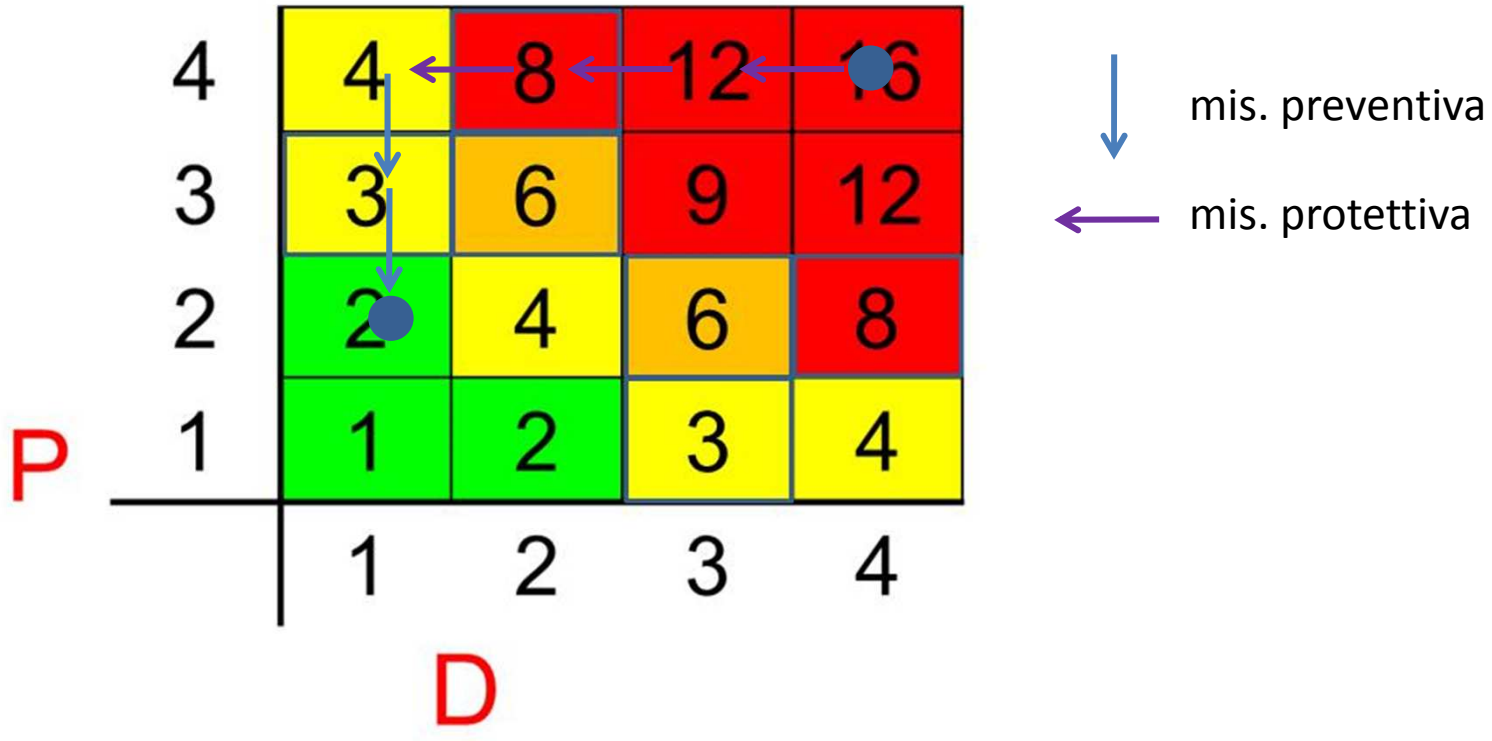
Fase 3: Il Trattamento del Rischio

- **Misure di Prevenzione (o di tutela)**: misure tecniche organizzative e procedurali mirate alla riduzione della probabilità di realizzazione della minaccia.
- **Misure di Protezione**: misure tecniche organizzative e procedurali mirate alla riduzione del danno provocato dalla realizzazione della minaccia.



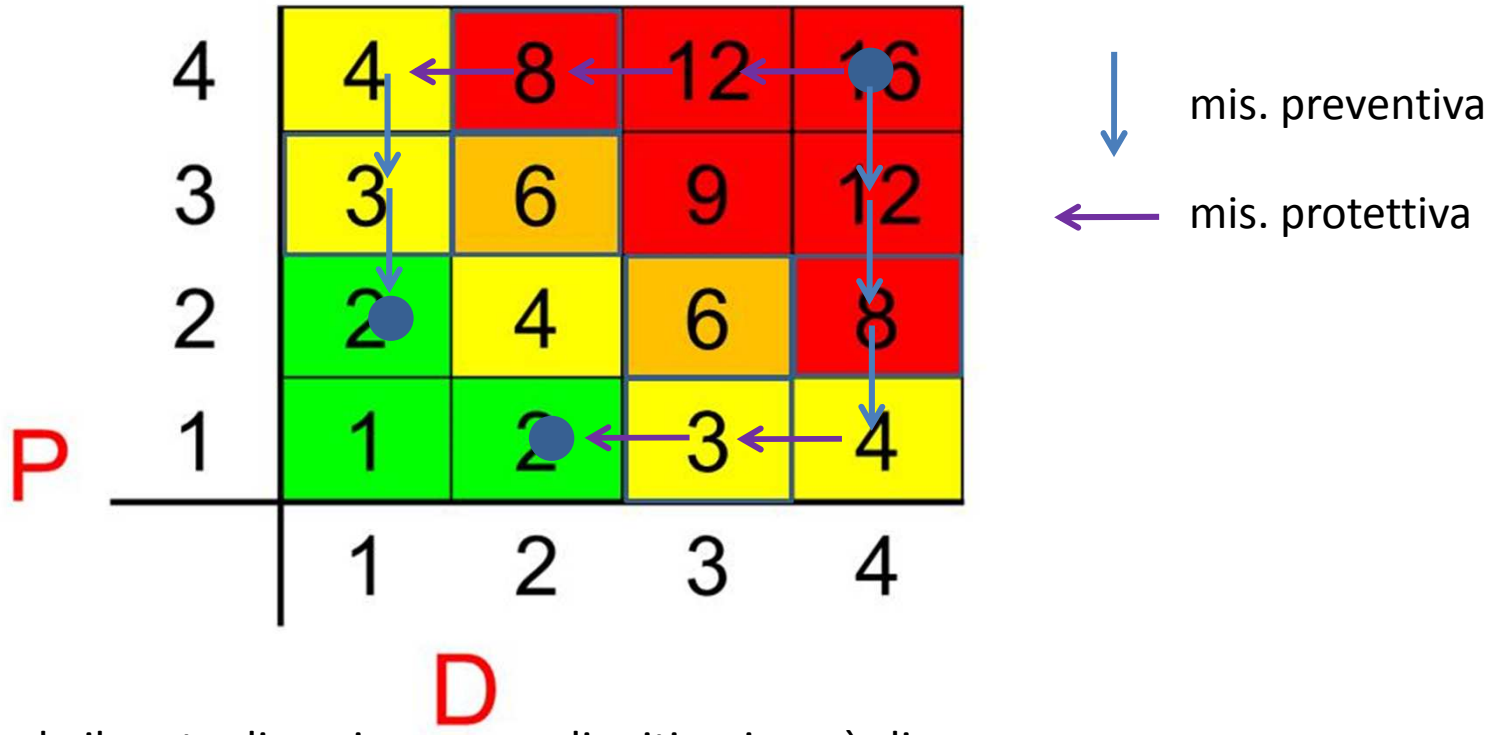
Fase 3: Il Trattamento del Rischio

- **Misure di Prevenzione (o di tutela)**: misure tecniche organizzative e procedurali mirate alla riduzione della probabilità di realizzazione della minaccia.
- **Misure di Protezione**: misure tecniche organizzative e procedurali mirate alla riduzione del danno provocato dalla realizzazione della minaccia.



Fase 3: Il Trattamento del Rischio

- **Misure di Prevenzione (o di tutela)**: misure tecniche organizzative e procedurali mirate alla riduzione della probabilità di realizzazione della minaccia.
- **Misure di Protezione**: misure tecniche organizzative e procedurali mirate alla riduzione del danno provocato dalla realizzazione della minaccia.



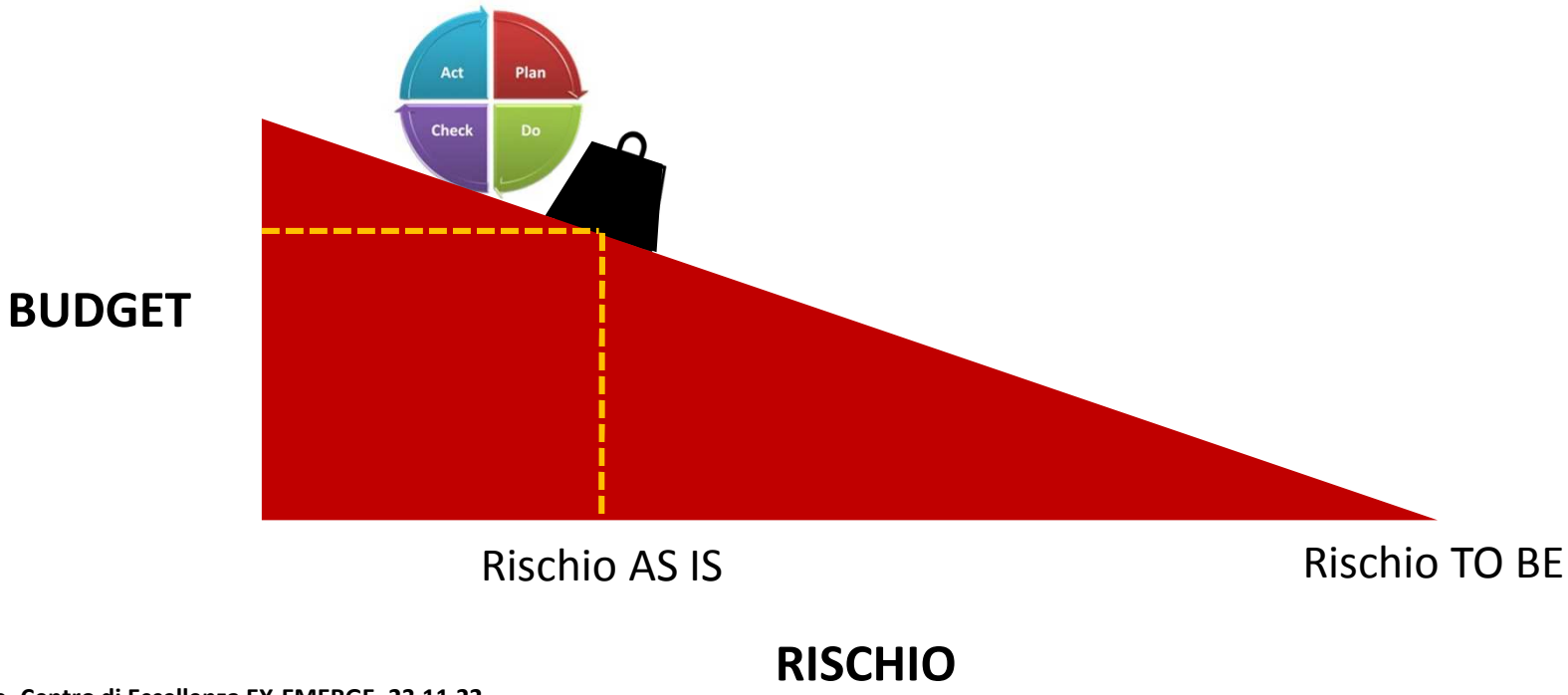
- In generale il costo di ogni percorso di mitigazione è diverso.
- In linea di principio il percorso ottimo è quello a costo minimo.

Fase 3: Il Trattamento del Rischio

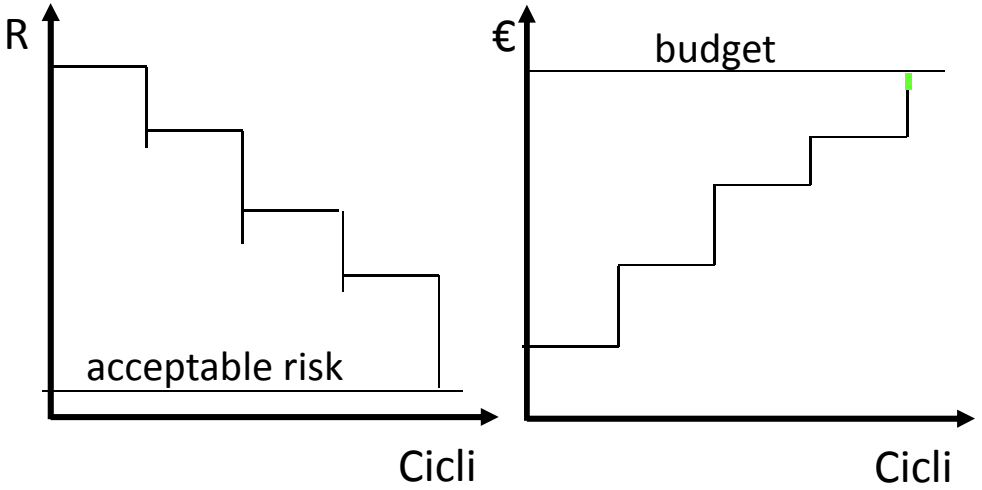
- **Elusione o eliminazione del rischio**, ovvero non iniziare o non continuare l'attività che dà origine ad esso, oppure, ove possibile, rimuovere la fonte (minaccia) del rischio. Solo in questi casi si può porre R=0 in quanto diventa P=0.
- **Trasferimento del Rischio**, ovvero trasferire o condividere tutto o parte del rischio con altra(e) parte(i) (contratti e finanziamento del rischio, assicurazioni, esternalizzazioni, ecc.)
- **Trattamento Operativo del Rischio**, investire in attività che permettano di ricondurre il rischio ai livelli ritenuti accettabili, attraverso l'individuazione di contromisure (misure di riduzione preventive e/o protettive) atte ad abbassare corrispondentemente le probabilità di accadimento o le conseguenze (danni/impatti).
- **Accettazione o Ritenzione del Rischio**, con una decisione formale ed informata nei casi in cui ciò non è escluso dalle leggi, dai regolamenti o dalle obbligazioni assunte.

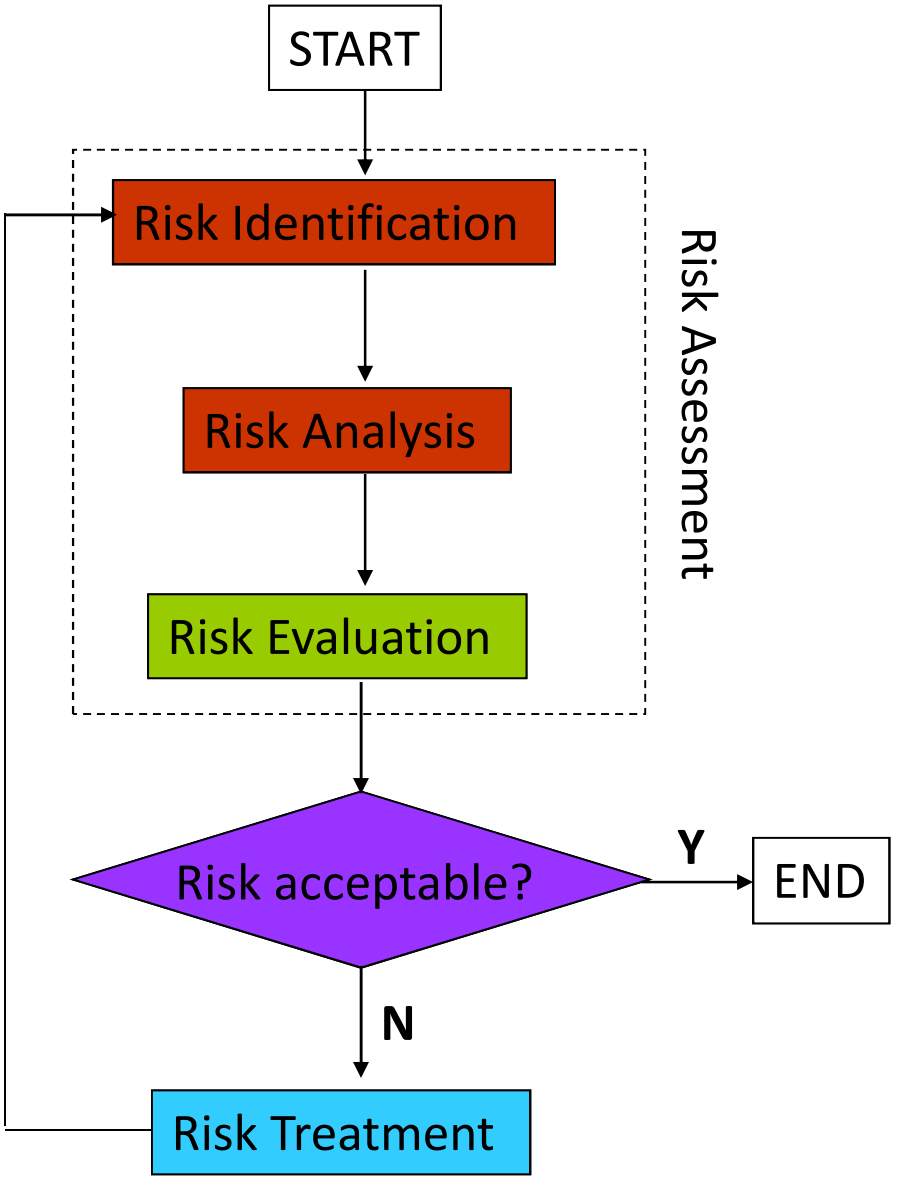
Fase 3: Il Trattamento del Rischio

- In linea di principio, il costo delle misure per rendere il rischio AS IS minore o uguale al rischio TO BE deve essere contenuto nel budget allocato.
- Se il costo del trasferimento del rischio (tramite coperture assicurative) è inferiore al costo delle corrispondenti misure, si può trasferire il rischio residuo TO BE – AS IS.



Fase 3: Il Trattamento del Rischio





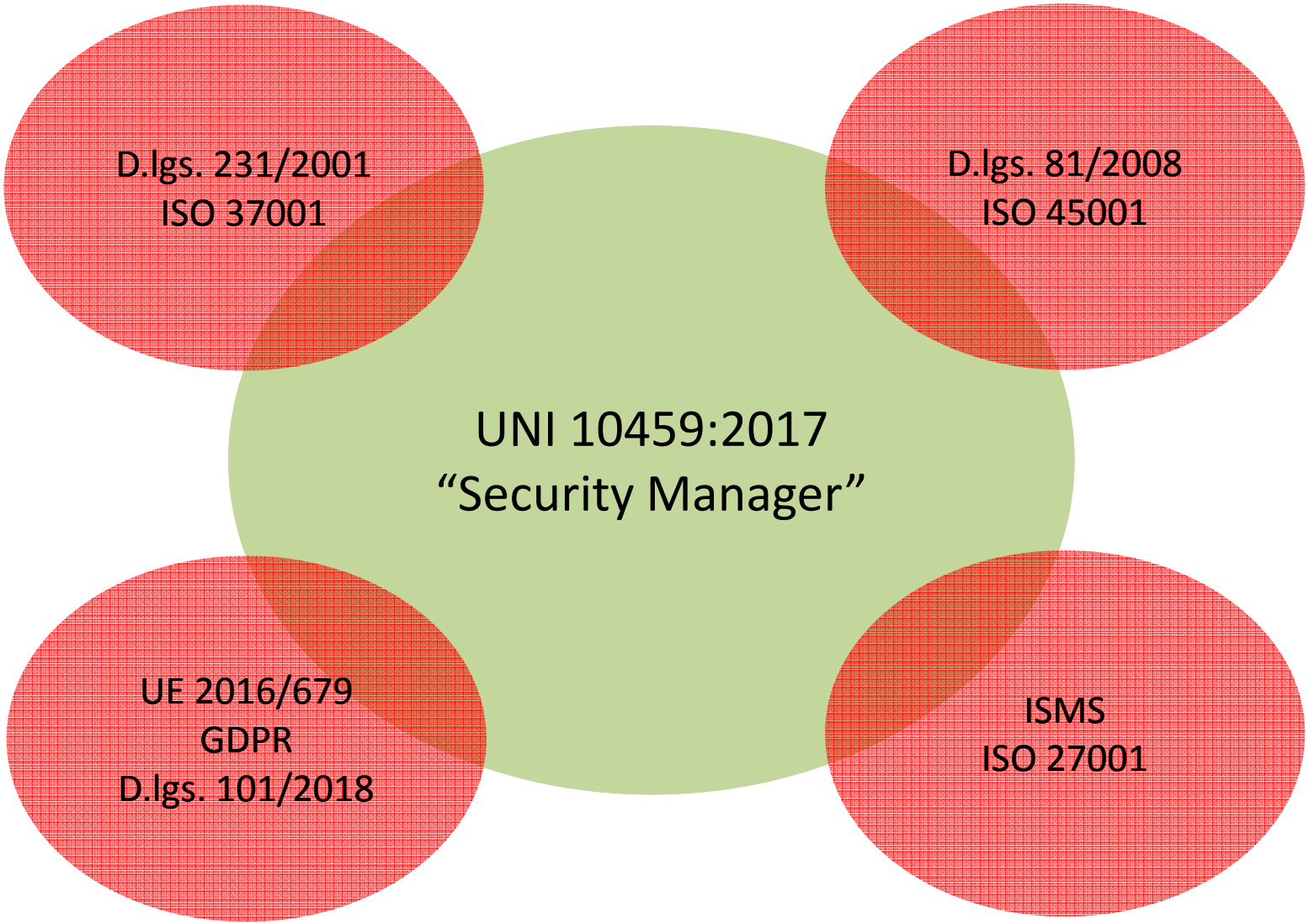
Fase 4: Monitoraggio e Revisione

- La progettazione e la realizzazione di misure tecniche deve avvenire in conformità con le norme dello stato dell'arte (normative cogenti, raccomandazioni, certificazioni).
- In condizioni di assenza di interferenze, l'approccio "compliancy-based" della progettazione e della realizzazione di misure garantisce di per sè il raggiungimento del rischio accettabile (ovvero della sicurezza accettabile) TO BE rispetto al rischio AS IS di partenza in quanto garantito dalla normativa stessa.
- In ogni caso è necessaria un'attività ciclica di misurazione continua dell'efficacia (e dell'efficienza) delle misure applicate sia per aggiornamento normativo e sia per mutati contesti operativi.

Indice degli argomenti

- Le precondizioni minime per un sistema "sicuro" e il Quadro normativo di riferimento
- La cybersecurity e la direttiva UE 2016/1148 c.d. "direttiva NIS“ – L’Agenzia per la Cybersicurezza Nazionale
- Approccio Metodologico alla Gestione del Rischio secondo ISO 31000
- **Il Professionista della Security (Security Manager) ai sensi della UNI 10459:2017**
- Il Modello di Gestione della Sicurezza (MOGS): ambiti di applicazione
  - cybersecurity: il NIST Cybersecurity Framework (CSF) e il processo di individuazione degli RSL (Required Security Level) – il Framework Nazionale per la Cybersecurity e la Data Protection – ISMS vs. NIST CSF
  - privacy ai sensi del GDPR
  - HSE ai sensi della ISO 45001 (cenni)
  - tutela responsabilità amm. aziendale ai sensi del D. Lgs. 231/01 (cenni)

Centralità della UNI 10459:2017



Il Professionista della Security

- La norma **UNI 10459:2017** "Attività professionali non regolamentate – Professionista della security – Requisiti di conoscenza, abilità e competenza" è lo standard di riferimento per il "Professionista della Security" (codice PS).

  Essa inquadra il "contesto soggettivo" del Professionista su tre livelli differenziandoli anche per il loro operato in aziende di media, medio/alta e massima security con un crescendo di requisiti quali competenze, conoscenze e abilità, (rif. UNI 10459:2017 all. A) delineando figure con compiti non meramente esecutivi, con ruolo e complessità crescenti fino all'apice manageriale di azienda complessa che è il "Senior Security Manager".
- La norma richiama esplicitamente la ISO 31000 come metodologia di riferimento per tutte le attività riconducibili al Professionista della Security.
- Pertanto il Professionista della Security:
  - **non** è una qualsiasi persona che opera nel campo della security e ha frequentato un corso di laurea o un master o un corso di formazione che rispetta i requisiti previsti dalla UNI 10459;
  - **non** è un manager di azienda per il solo fatto che l'azienda si occupa di security;
  - **non** è annoverata tra le professioni ordinistiche e non esiste un Albo professionale a vigilare e a validarne requisiti professionali e deontologici: pertanto il suo riconoscimento "certificato" avviene, come per le norme volontarie da parte di enti terzi indipendenti **con criteri predefiniti e standardizzati**;

Il Professionista della Security

Estratto dalla norma UNI 10459:2017: "*Fattori di natura sia economica-competitiva sia socio-politica, determinano dinamismi e complessità sempre crescenti alimentati dal convergere e dell'intrecciarsi di fenomeni quali l'instabilità sociale, i mutamenti politici ed economici, il rapido ed incessante sviluppo tecnologico, i continui processi di ristrutturazione, la progressiva dematerializzazione delle attività dell'Organizzazione, la crescente apertura geografica alla competitività, l'intensificarsi dei rapporti internazionali ed il continuo proliferare di norme e leggi a livello locale, nazionale ed internazionale. La conseguenza è il* ***costante moltiplicarsi dei fronti verso cui le organizzazioni sono costrette ad impegnarsi al fine di conservare la competitività e di mantenere integra nel tempo la capacità di ottenere soddisfacenti risultati economici****.*

Si è acquisita la consapevolezza che, indipendentemente dall'ambito di attività, l'equilibrio gestionale può essere alterato, se non addirittura definitivamente compromesso, da una serie di eventi di diversa natura. ***Ogni tipo di Organizzazione è costantemente esposta a minacce di natura dolosa, colposa o accidentale; ciò in relazione ai processi produttivi, alle azioni dei dipendenti, ai rapporti con l'esterno e, più in generale, dall'essere parte di un mondo globalizzato caratterizzato dall'incertezza e dalla conflittualità****. Accanto, quindi, all'efficacie gestione delle variabili competitive tradizionali, le organizzazioni hanno come obiettivo la tutela del patrimonio tangibile e intangibile, inteso nell'accezione più vasta del termine e quindi anche, e non in modo secondario, delle persone che sia dell'Organizzazione sia di quelle che con questa interagiscono, che si pone alla base dei processi di creazione del valore, assicurando così il mantenimento della capacità reddituale nel tempo.*

Questa attività si realizza anche attraverso il ricorso alle tecniche di gestione per la qualità, per il contributo che esse possono dare sia alla riduzione dei costi sia alla qualità di prodotti e servizi."

Il Professionista della Security

- **Formazione Specifica:** Superamento di un Master I° o II° livello in materia di security oppure un corso di formazione in materia di Security della durata di **almeno 120 ore**, erogato da Università riconosciute dal Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR) oppure da Enti di formazione accreditati presso le Regioni.
- Il corso è finalizzato al trasferimento di conoscenze riferite a (UNI 10459:2017 all. A4):
  - Analisi scenari e contesto: analisi scenari di riferimento (geopolitici, sociali, economici, ambientali, tecnologici), analisi settore di competenza, analisi organizzativa interna
  - Criminologia applicata
  - Legislazione: sicurezza nella costituzione e sicurezza pubblica, responsabilità giuridiche e aziendali, elementi di diritto penale, responsabilità amministrativa degli enti, sicurezza sul lavoro, sicurezza privata, elementi di sicurezza delle informazioni, codice di tutela della proprietà industriale, tutela del know-how e del segreto industriale, statuto dei lavoratori, elementi di protezione dei dati personali
  - Gestione del Rischio
  - Security Management
  - Il sistema di gestione dei rischi per la security (Security Risk Management): progetto, sistema di gestione, intelligence e security intelligence, strumenti di sicurezza, servizi di sicurezza e altri servizi, sicurezza delle informazioni e delle risorse intangibili, continuità operativa e gestione delle emergenze (business continuity & emergency management), elementi di management.

Il Professionista della Security
estensione alla Sicurezza Sussidiaria

- **Riferimento normativo: UNI 10459:2017** Attività professionali non regolamentate - Professionista della Security - Requisiti di conoscenza, abilità e competenza, **D.M. 4 giugno 2014 n.115, D.M. 1 dicembre 2010 n.269, Disciplinare del Capo della Polizia - Direttore Generale della Pubblica Sicurezza - del 24 febbraio 2015.**
- Il Professionista della Security è la persona le cui conoscenze, abilità e competenze sono tali da garantire la **gestione complessiva del processo di security**. A seconda della diversa complessità dei contesti organizzativi in cui opera, tale figura professionale può ricoprire tre diversi livelli: **operativo** (Security Expert), **manageriale** (Security Manager), **alto manageriale** (Senior Security Manager).
- Obbligatorio per ottenere la titolarità di licenza per servizi di Sicurezza Sussidiaria (codice Vp)
- La certificazione è rilasciata da organismi di certificazione accreditati secondo la ISO/IEC 17024:2012 “Requisiti generali per gli organismi che eseguono la certificazione delle persone”

Il Professionista della Security

Si possono identificare le seguenti aree di responsabilità che rientrano nella funzione del professionista della security

- Analisi di scenario e del contesto esterno
- Analisi del contesto interno (settore, attività, processi e risorse critiche)
- Analisi dei rischi di security
- Gestione dei rischi di security
- Elaborazione e attuazione piano di security
- Elaborazione struttura organizzativa e budget di funzione,
- Attività formativa / informativa al personale dell'Organizzazione sui rischi di security
- Antifrode
- Antintrusione
- Conformità alle prescrizioni legali e alle altre prescrizioni sottoscritte che riguardano la security
- Coordinamento dei sistemi integrati di sicurezza delle strutture
- Coordinamento della continuità operativa (Business Continuity e Disaster Recovery)
- Gestione e/o coordinamento delle risorse umane ed economiche di security
- Gestione della vigilanza privata e dei servizi di sicurezza privati
- …… (continua)

Il Professionista della Security

Si possono identificare le seguenti aree di responsabilità che rientrano nella funzione del professionista della security

- Gestione delle crisi (Crisis Management)
- Gestione delle investigazioni private affidate a terzi
- Gestione della protezione delle informazioni, incluso il coordinamento e supporto alle attività relative alla sicurezza delle informazioni
- Investigazioni
- Business / Competitive Intelligence
- Audit tecnico di security
- Monitoraggio e reporting di security
- Tutela del know-how, segreto industriale e delle risorse immateriali
- Protezione da spionaggio industriale
- Protezione di infrastrutture critiche
- Protezione e tutela del Management dell'Organizzazione
- Rapporti con le forze di Polizia e Forse Armate, agenzie e istituzioni pubbliche
- Supervisione della gestione di contratti afferenti alla security
- Supporto al datore di lavoro per la tutela dei lavoratori dai rischi di origine criminosa

Il Professionista della Security

LIVELLO PROFESSIONISTA SECURITY/REQUISITI – LIVELLO MANAGERIALITÀ – COMPLESSITA' SECURITY	REQUISITI			LIVELLO MANAGERIALITÀ	COMPLESSITÀ SECURITY
	DIPLOMA	LAUREA	LAUREA MAGISTRALE O DIPLOMA DI MASTER UNIVERSITARIO (I O II LIVELLO)		
SECURITY EXPERT	8 anni di esperienza di security di cui	4 anni di esperienza di security di cui	2 anni di esperienza di security in incarichi con responsabilità e autonomia coerenti con il livello	OPERATIVO	MEDIA
(I LIVELLO)	4 anni in incarichi con responsabilità e/o autonomia coerenti con il livello	2 anni in incarichi con responsabilità e autonomia coerenti con il livello			
SECURITY MANAGER (II LIVELLO)	12 anni di esperienza di security di cui	8 anni di esperienza di security di cui	5 anni di esperienza di security di cui	MANAGERIALE	MEDIO-ALTA
	6 anni in incarichi con responsabilità e autonomia coerenti con il livello	4 anni in incarichi con responsabilità e autonomia coerenti con il livello	3 anni in incarichi con responsabilità e autonomia coerenti con il livello		
SENIOR SECURITY MANAGER	20 anni di esperienza di security di cui	18 anni di esperienza di security di cui	10 anni di esperienza di security di cui 6 anni in incarichi con responsabilità e autonomia coerenti con il livello	ALTO MANAGERIALE	MASSIMA
(III LIVELLO)	8 anni in incarichi con responsabilità e autonomia coerenti con il livello	5 anni in incarichi con responsabilità e autonomia coerenti con il livello			

Fonte: UNI 10459:2017

La Struttura di Riferimento dell'Organizzazione

Il miglioramento continuo della struttura di riferimento dell'Organizzazione
in un contesto generalmente variabile
è l'oggetto di intervento del Professionista.

- La struttura di riferimento dell'Organizzazione è come una macchina industriale a produzione ciclica messa a disposizione dell'Organizzazione cui il Professionista deve garantire manutenzione ordinaria e straordinaria con la sua "cassetta degli attrezzi" fatta di strumenti, conoscenze, esperienze e competenze.
- La struttura di riferimento pone le fondamenta per tutte le componenti di quella organizzazione ed i suoi stakeholders, identificando ed esplicitando la policy aziendale, gli obiettivi, il mandato, l'impegno e le disposizioni organizzative che l'organizzazione mette in atto rispetto a Piani, Relazioni, Responsabilità, Risorse, Processi, Attività.

Il Ruolo dell'Organizzazione

- Nel proprio framework di riferimento, l'organizzazione deve definire le sue politiche di gestione del rischio, i criteri di valutazione e di accettazione dei rischi, ovvero i parametri di riferimento per valutarne i possibili Danni/Impatti.
- I criteri di valutazione e di accettazione definiti sono quelli che si andranno ad utilizzare nell'implementazione dei processi di valutazione e nella ponderazione dei rischi, rappresentando l'aspetto quanti/qualitativo della propensione al rischio dell'organizzazione.
- La definizione degli obiettivi e dei criteri di accettazione è fondamentale perché sulla base di questi saranno effettuate le scelte strategiche di gestione del rischio da parte dell'amministrazione in merito a:

  a) Elusione o eliminazione del rischio, decidendo di non iniziare o non continuare l'attività che dà origine ad esso, oppure, ove possibile, rimuovere la fonte (minaccia) del rischio.

  b) Trasferimento del Rischio, decidendo di trasferire o condividere tutto o parte del rischio con altra(e) parte(i) (contratti e finanziamento del rischio, assicurazioni, esternalizzazioni, ecc.)

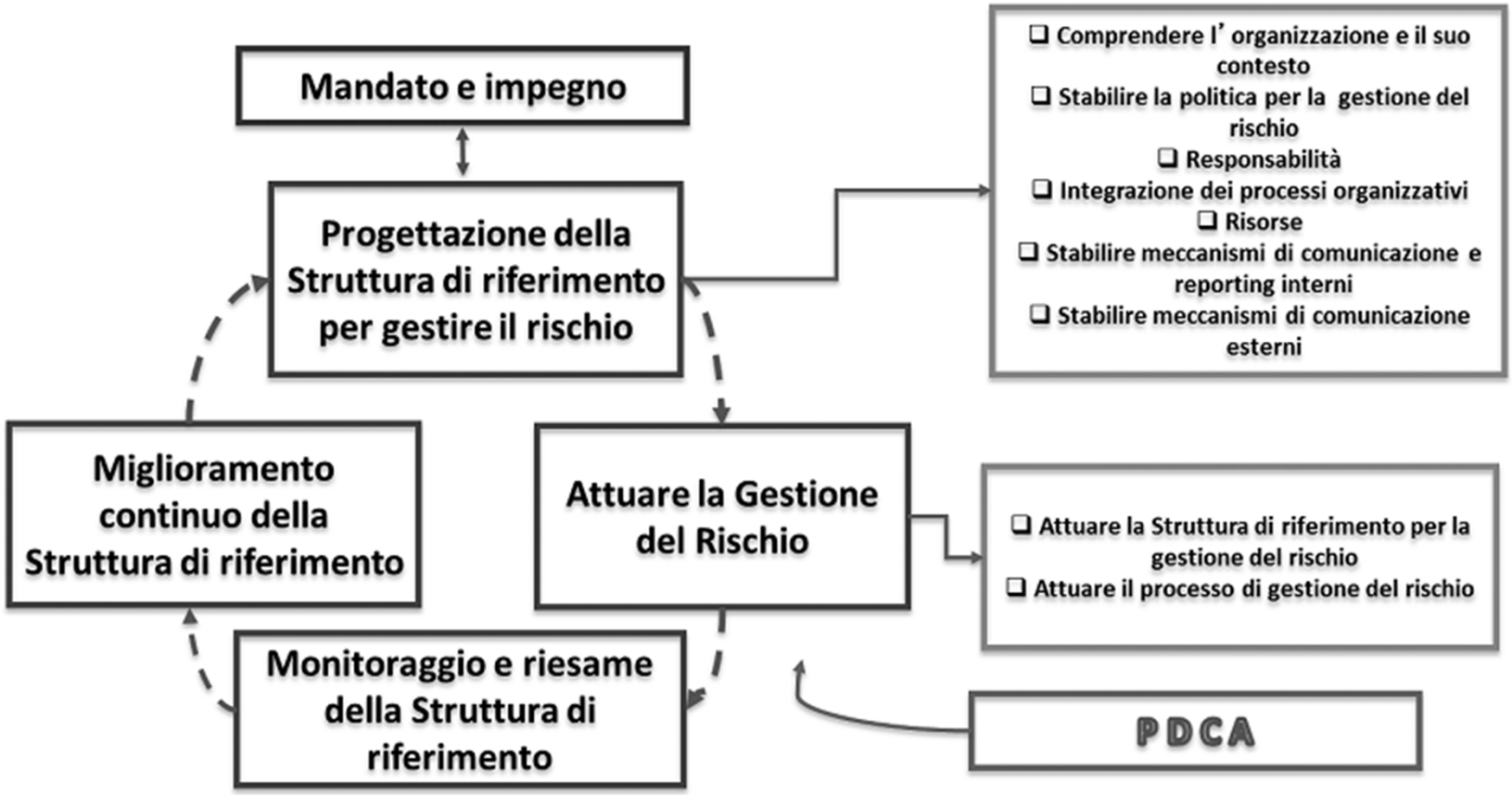
  c) Trattamento del Rischio, decidendo di investire in attività che permettano di ricondurre il rischio ai livelli ritenuti accettabili, attraverso l'individuazione di contromisure (misure di riduzione) atte ad abbassare le probabilità di accadimento o le conseguenze (danni/impatti).

  d) Accettazione o Ritenzione del Rischio, con una decisione formale ed informata nei casi in cui ciò non è escluso dalle leggi, dai regolamenti o dalle obbligazioni assunte.

Il Ruolo del Professionista

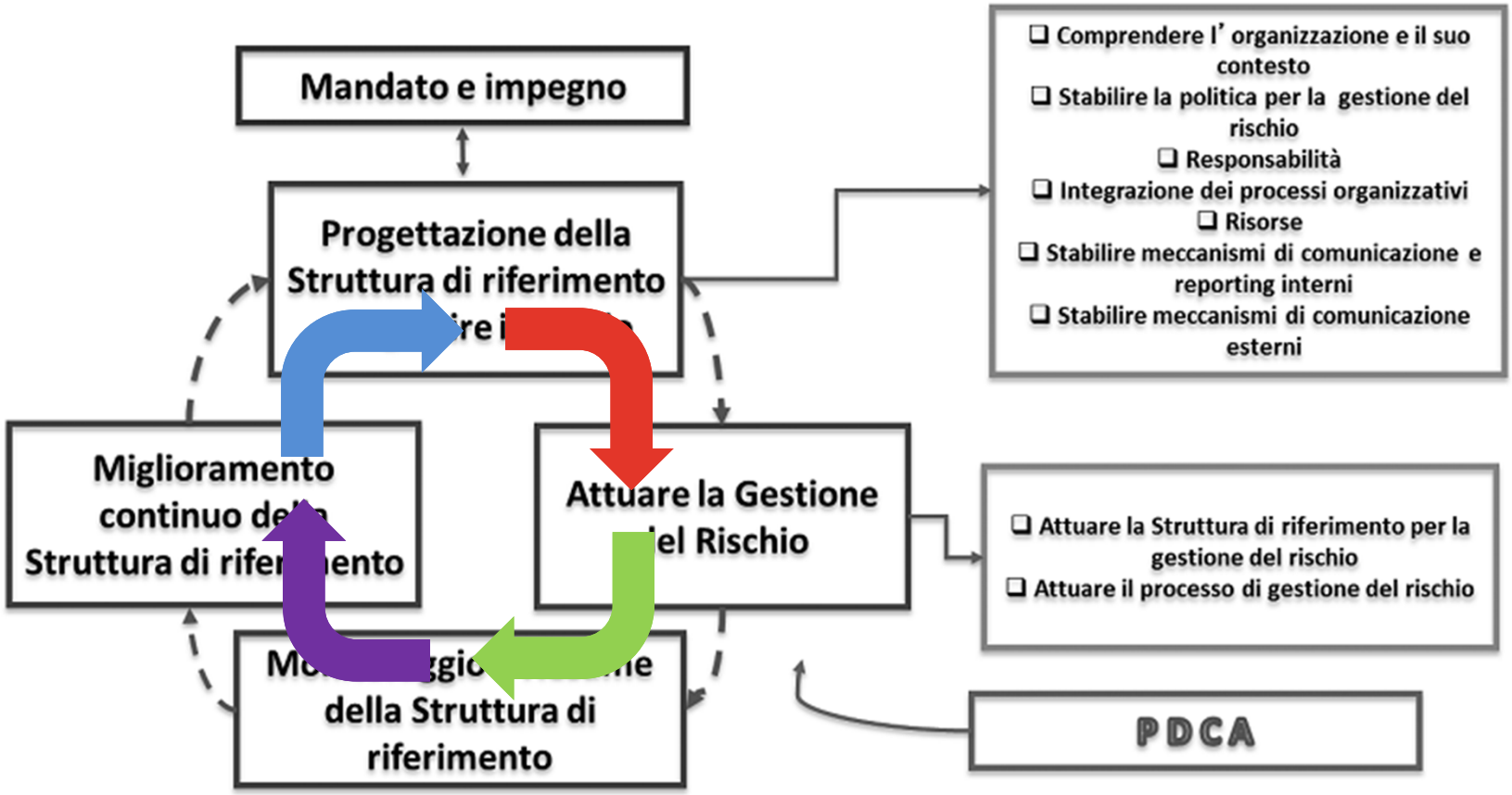
- Si può partire dal presupposto che, nel rispetto dei rispettivi ruoli, l'organizzazione ed il suo management hanno la responsabilità ed il compito della gestione dei rischi.
- **Il Professionista è la figura chiamata a proporre soluzioni e a dare risposte di security per il trattamento dei rischi.**
- Il suo ruolo acquisisce ragion d'essere con il mandato che riceve dall'organizzazione, con il quale questa dà atto di impegnare parte delle risorse economiche a disposizione per la gestione dei rischi di Security, a supporto e tutela dello svolgimento delle normali attività caratteristiche.
- Il suo compito è quello di dare una risposta di security alle minacce che imperversano sull'organizzazione, secondo un percorso logico di cui lo standard ISO 31000 ha saputo inquadrare i passaggi essenziali, perché chiunque ed in qualsiasi contesto abbia dei criteri di riferimento per implementare la propria risposta per la gestione del rischio.
- La ISO 31000 non fa distinzioni di complessità o di tipologia di rischio, o distinzioni di organizzazione pubblica, privata, non profit: propone un modello unico e integrato applicabile a tutti i processi operativi ed organizzativi, secondo un'unica metodologia di approccio al rischio, sia esso strategico, operativo, finanziario, valutario, di mercato, di compliance, paese, ecc.

Il Ruolo del Professionista



[fonte: F. Farina, M. Marrocco, Complessità di security e gestione del rischio, ed. Themis]

Il Ruolo del Professionista



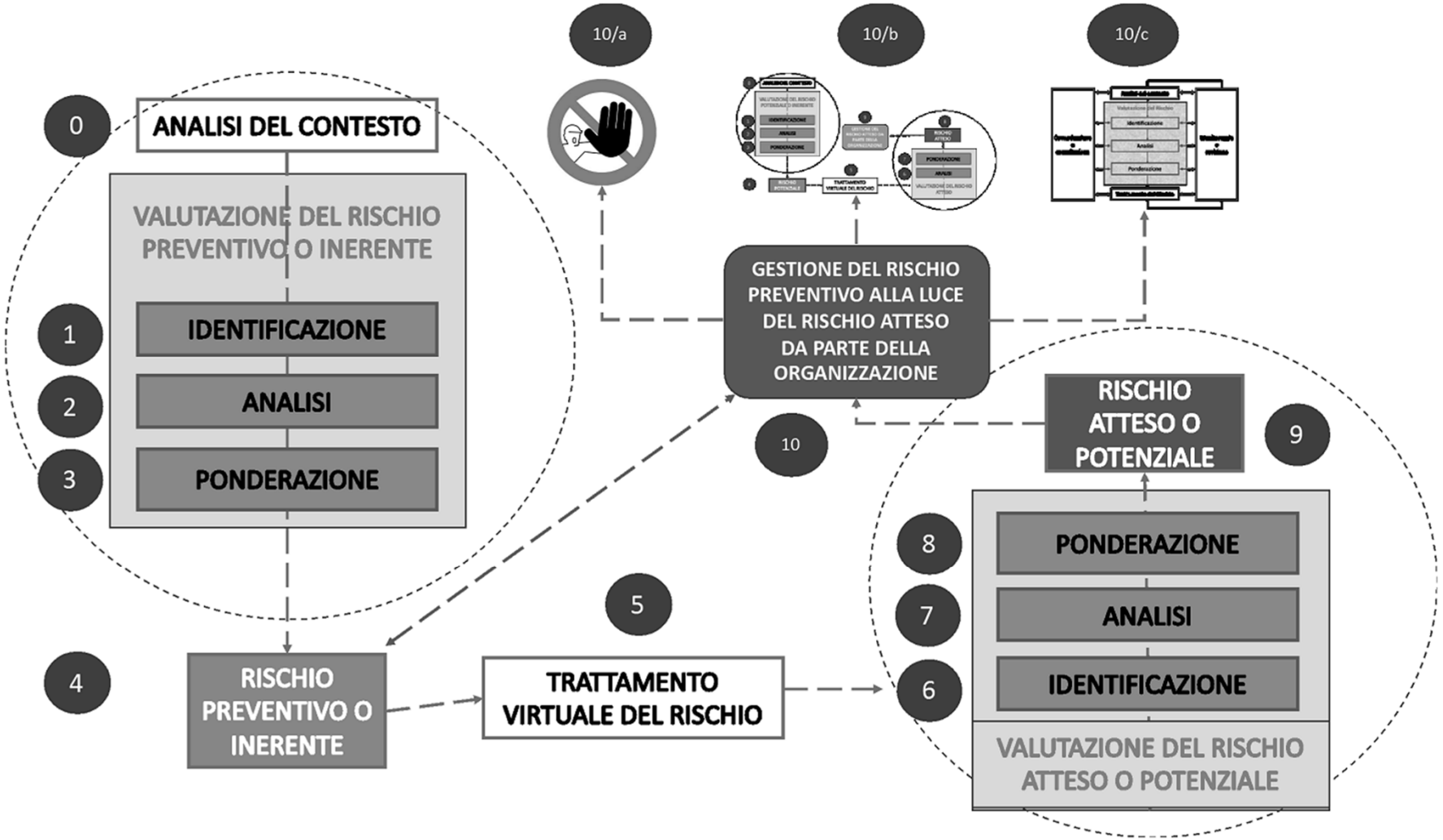
[fonte: F. Farina, M. Marrocco, Complessità di security e gestione del rischio, ed. Themis]

Modello di Misurazione Continua dell'Efficacia

Al fine della definizione della risposta di security, il Professionista distingue tre tipi di rischio:

- il **Rischio Preventivo o inerente**, il rischio calcolato senza tenere conto delle contromisure adottate;
- il **Rischio atteso o potenziale**, il rischio calcolato a seguito di quanto definito nel Piano di trattamento del rischio, e che quindi tiene conto delle contromisure e della loro capacità attesa di riduzione del rischio;
- il **Rischio effettivo**, il rischio calcolato successivamente alle attività di monitoraggio delle stesse, che comprendono sia la misurazione di efficacia delle contromisure implementate che gli incidenti registrati.

Modello di Misurazione Continua dell'Efficacia



[fonte: F. Farina, M. Marrocco, Complessità di security e gestione del rischio, ed. Themis]

Modello di Misurazione Continua dell'Efficacia

- Fasi 1-4 : **il Professionista misura il rischio "preventivo o inerente",** al tempo "T0" della condizione esistente e precedente al suo intervento.
- Fasi 5-9: **il Professionista misura il rischio "atteso o potenziale",** al tempo "T1", la cui stima è, come abbiamo visto, direttamente correlata all'efficacia prevista delle misure implementate e presenta all'Organizzazione la propria risposta di security.
- Fase 10: **l'Organizzazione riscontra la risposta di security elaborata dal Professionista in**:

  (10.a) non procedere all'implementazione della risposta perché non ci sono le condizioni per la gestione dei rischi generati, neppure alla luce del trattamento potenziale che ha portato al rischio "atteso o potenziale";

  (10.b) non gestire il rischio "preventivo" diffidando del rischio "atteso", ritenendo che la risposta di "security" possa essere ulteriormente ottimizzabile (richiesta di una nuova risposta e combinazione di misure che portino ad un nuovo rischio "atteso");

  (10.c) gestire il rischio e implementare concretamente le misure di riduzione previste.

Indice degli argomenti

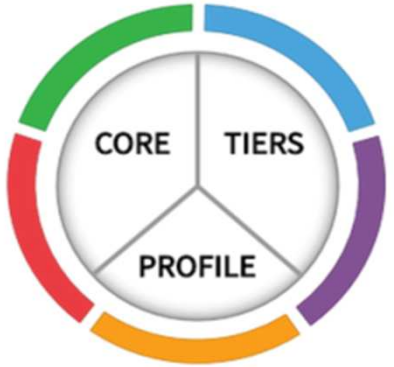
- Le precondizioni minime per un sistema "sicuro" e il Quadro normativo di riferimento
- La cybersecurity e la direttiva UE 2016/1148 c.d. "direttiva NIS“ – L’Agenzia per la Cybersicurezza Nazionale
- Approccio Metodologico alla Gestione del Rischio secondo ISO 31000
- Il Professionista della Security (Security Manager) ai sensi della UNI 10459:2017
- **Il Modello di Gestione della Sicurezza (MOGS): ambiti di applicazione**
  - **cybersecurity: il NIST Cybersecurity Framework (CSF) e il processo di individuazione degli RSL (Required Security Level) – il Framework Nazionale per la Cybersecurity e la Data Protection – ISMS vs. NIST CSF**
  - privacy ai sensi del GDPR
  - HSE ai sensi della ISO 45001 (cenni)
  - tutela responsabilità amm. aziendale ai sensi del D. Lgs. 231/01 (cenni)

NIST Cybersecurity Framework (CSF)

- NIST CSF è strutturato secondo i principi della ISO 31000:2018 e si riferisce alla famiglia ISO 27000 e alla NIST Special Publication 800-53

  https://www.nist.gov/cyberframework/framework-documents
- Suddiviso in tre componenti:
  - Framework Core
  - Implementation Tiers
  - Profiles
- **Framework Core:** Il Core è la griglia delle funzioni di "cybersecurity risk management" il cui livello di applicazione che l'Organizzazione intende misurare e confrontare rispetto ai propri target. Intuitivo ed in termini non tecnici per permettere una migliore comunicazione inter-disciplinare.

  Il Core consiste di tre parti: **Funzioni (5)**, **Categorie (23)** e **Subcategorie**. Il Core include 5 funzioni di alto livello: **Identify**, **Protect**, **Detect**, **Respond**, and **Recover**.



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Fonte: (https://www.nist.gov/cyberframework/online-learning/components-framework)

NIST Cybersecurity Framework (CSF)

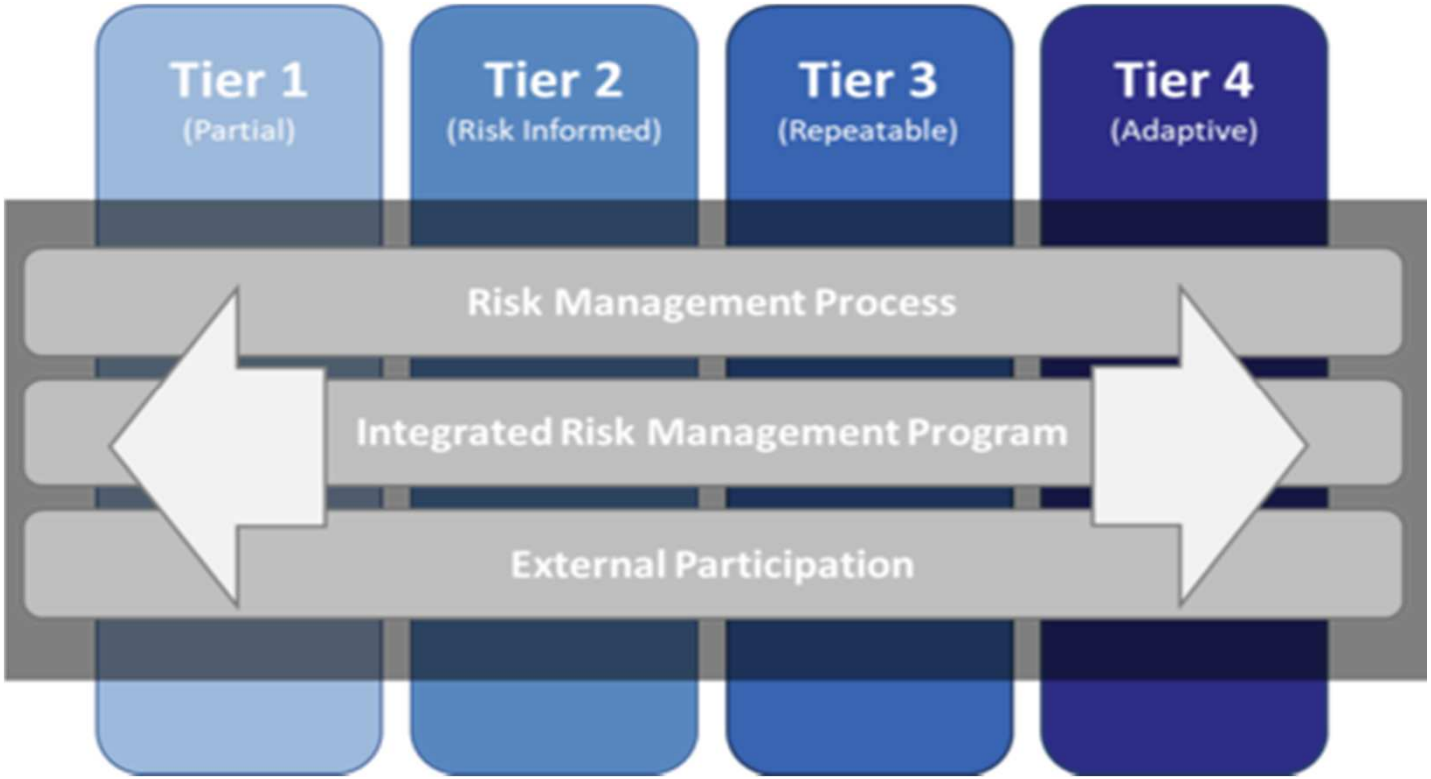
Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**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: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**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: Dependencies and critical functions for delivery of critical services are established	**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: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** 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-14

Fonte: (https://www.nist.gov/cyberframework/online-learning/components-framework)

Implementation Tier

- Gli **Implementation Tiers** servono per classificare il rigore nell'applicazione delle pratiche di "cybersecurity risk management" da parte dell'Organizzazione e il livello di integrazione fra le decisioni. I livelli vanno da Partial (Tier 1) ad Adaptive (Tier 4) in modo crescente.



Fonte: (https://www.nist.gov/cyberframework/online-learning/components-framework)

Profiles

- I **Profile** racchiudono al loro interno:
  - Il livello delle misure attuali (c.d. rischio AS IS)
  - I requisiti e gli obiettivi organizzativi di un'organizzazione;
  - La propensione al rischio dell'Organizzazione (livello di rischio accettabile);
  - Il livelo target delle misure da attuare (c.d. rischio TO BE)
- Quantitativamente i profile target sono rappresentati dall'insieme dei livelli minimi di prestazione di sicurezza, i c.d. **Required Security Level**.

Subcategory	Priority	Gaps	Budget	Activities (Year 1)	Activities (Year 2)
1	Moderate	Small	$$$		X
2	High	Large	$$	X	
3	Moderate	Medium	$	X	
...	...	...	...		
98	Moderate	None	$$		Reassess

Target Profile

Fonte: (https://www.nist.gov/cyberframework/online-learning/components-framework)

Processo di Individuazione dei RSL

- I Required Security Level identificano i requisiti di quelle misure PREVENTIVE di cybersicurezza che mitigano i rischi di sicurezza del sistema ad un livello di accettabilità.

  Le misure si distinguono in:
- Misure di sicurezza PASSIVE (PSM) se di deterrenza pura (l'obiettivo è protrarre nel tempo la probabilità di accadimento) quindi **senza informazione** sullo stato dell'organizzazione / sistema.
  - Tipicamente tecniche di **cifratura** e di **autenticazione**, **hashing**, **pseudonomizzazione**, ….
  - Parametro di prestazione caratterizzante è il tempo di resistenza del sistema a partire dall'inizio dell'attacco fino alla sua finalizzazione (**tempo di deterrenza**).
- Misure di sicurezza ATTIVE (ASM) se **si ha informazione** sullo stato dell'organizzazione / sistema finalizzato ad un intervento di eliminazione della minaccia **in tempo utile**.
  - Tipicamente IDS ovvero **stimatori del comportamento** di un sistema (tramite tecniche di AI, ML, …), controllo accessi, …
  - Parametri di prestazione caratterizzanti possono essere (senza perdita di generalità) il FPR (False Positive Rate) e il FNR (False Negative Rate). Le curve ROC (Receiver Operating Characteristics) sono grafici TPR (True Positive Rate, o probabilità di detection) vs. FPR. Si dimostra che TPR = 1 – FNR.

Processo di Individuazione dei RSL

- Sicurezza PERFETTA (o sicurezza incondizionata)
  - Per le PSM **tempo di deterrenza infinito**
  - Per le ASM i valori di FPR e FNR **pari a zero**
- Sicurezza REALE (o sicurezza condizionata)
  - Per le PSM **tempo di deterrenza finito**
  - Per le ASM i valori di FPR e FNR **superiori a zero**
- Il tempo di deterrenza si può assumere direttamente proporzionale all'entropia associata ai flussi di dati cifrati: infatti se l'entropia per binit = 1, allora i flussi cifrati sarebbero assimilabili a stringhe binarie puramente random ed il tempo di deterrenza sarebbe infinito in quanto il problema inverso (algoritmo deterministico) dello schema crittografico risulterebbe di complessità infinita (non esistono algoritmi deterministici per la generazione di sequenze puramente random). Realisticamente, entropia per binit < 1, il problema inverso di complessità finita e tempo di deterrenza è finito.
- FPR e FNR si possono assumere inversamente proporzionali alla capacità di rappresentazione del comportamento del sistema attraverso una macchina a stati (ogni comportamento è associabile ad una determinata sequenza di stati e si dimostra dalla teoria dell'informazione che è questa capacità, non quella di classificazione, che pone il limite massimo prestazionale di uno stimatore di comportamento). FPR=0 e FNR=0 se ogni comportamento del sistema è rappresentabile, ovvero se la macchina associata è a stati infiniti. Realisticamente, i modelli di comportamento sono macchine a stati finiti, quindi non ogni comportamento sarà rappresentabile, quindi FPR > 0 e FNR > 0.

Processo di Individuazione dei RSL
computo del tempo di deterrenza

Capacità di Computazione (CC): indicatore di prestazione di un processore in milioni di istruzioni al secondo (MIPS, Million Instructions Per Second). Per convenzione si pone come riferimento unitario CC = 1 MIPS la prestazione del (mitico) VAX-11/780 (DEC, 1977).

T_P: **tempo di deterrenza** di una PSM. Dato un problema inverso di complessità minima O(f(x)) con x fattore predominante dell'algoritmo (p.es. la lunghezza della chiave o dell'input, numero di chiavi, …), allora deve essere: **$T_P \geq f(x) / CC$**.

Per esempio:

Un moderno mainframe si può porre a CC ≈ 20.000 MIPS ≈ 2 10^{10} operazioni /sec

Per uno schema RSA si ha $f(n) \sim \exp((\ln n)^{1/3} \cdot (\ln \ln n)^{2/3})$ dove $n = 2^k$ e k è la lunghezza della chiave. Se k=2048 bit, quindi $n=2^{2048}$, $f(n) \approx 10^{18}$ operazioni, si computa:

$T_p \geq 10^8$ secondi ≈ **1,4 anni**;

Assumendo una rete di 1000 mainframes, si ottiene **$T_p \approx$ 14 ore.**

Nelle reti ad hoc, dove adottano schemi ECC (Elliptic Curve Cryptography), si ottiene ancora $T_p \approx 14$ ore ma con chiavi di lunghezza k ≈ 256 bit.

Processo di Individuazione dei RSL
vincoli temporali

T_P: **tempo di deterrenza** di una PSM.

T_A: **latenza di reazione** di una ASM (latenza tra classificazione e notifica).

T_O: **latenza di intervento** di una ASM (latenza tra notifica ed eliminazione della minaccia: dipende anche da misure organizzative e procedurali).

T_{ATT}: durata dell'attacco.

T_{OP}: durata in esercizio del sistema.

Le **equazioni dei tempi (vincoli temporali)** per le PSM e le ASM sono:

$$\begin{cases} T_P > T_{OP} \\ T_{ATT} < T_P \\ T_A + T_O < T_{ATT} \end{cases}$$

tempo di deterrenza > durata in esercizio

durata dell'attacco < **tempo di deterrenza**

latenza di reazione + **latenza di intervento** < durata dell'attacco

Processo di Individuazione dei RSL

RSL vs. OSL

Il **Required Security Level (RSL)** associato ad un rischio del sistema è definito dalle minime caratteristiche tecnico / organizzative / procedurali delle misure che portano l'organizzazione / sistema ad un livello accettabile di sicurezza**.**

Per esempio:

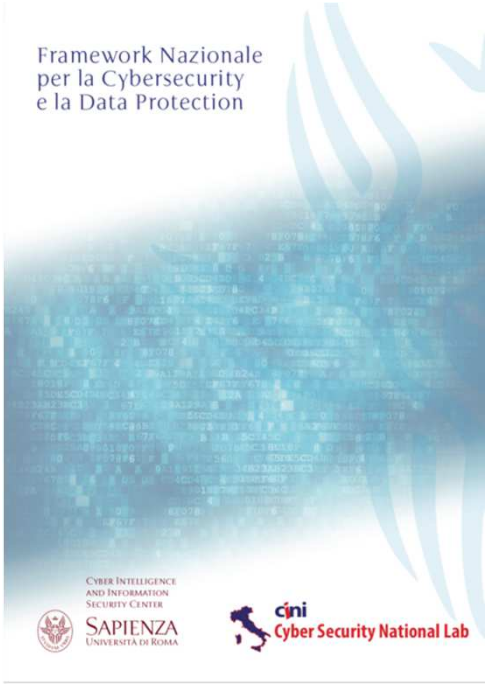
- Minimo Tempo di Deterrenza (mDT)
  mDT = MAX(durata in esercizio, durata stimata dell'attacco)
- Latenza Massima di Reazione (MRT), Latenza Massima di Intervento (MIT)
  MRT + MIT = durata stimata dell'attacco
- FPR Massimo (MFPR), FNR Massimo (MFNR)

La **Offered Security Level (OSL)** definisce le caratteristiche tecnico / organizzative / procedurali delle misure adeguate allo scopo secondo i seguenti vincoli.

- $(\text{Tempo di Deterrenza})_{PSF} \geq \text{mDT}$
- $(\text{Tempo di Reazione})_{ASF} \leq \text{MRT}$
- $(\text{Latenza di Intervento})_{SOC} \leq \text{MIT}$ (dipende anche da altre misure organizzative e procedurali)
- $FPR_{ASF} \leq \text{MFPR}$
- $FNR_{ASF} \leq \text{MFNR}$

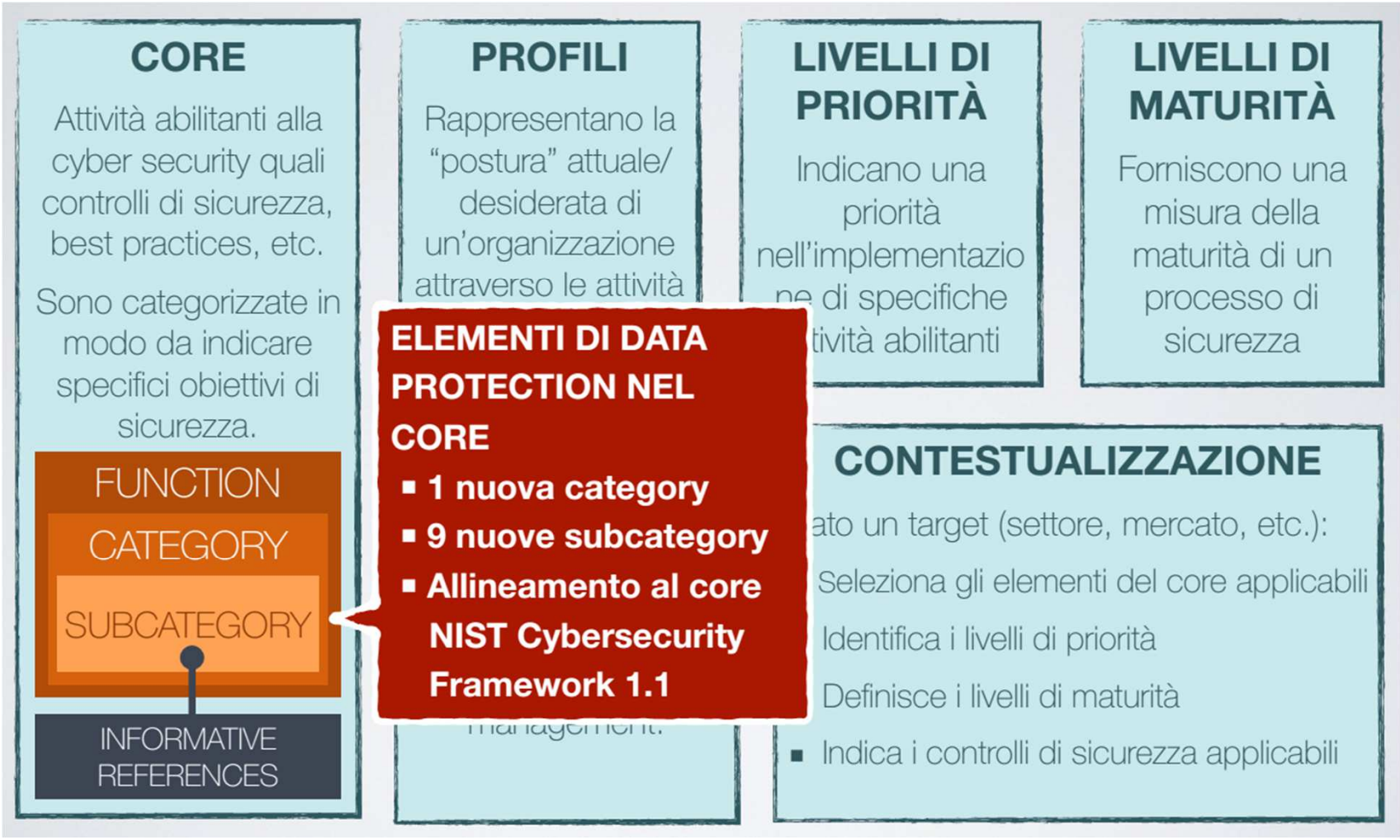
Framework Nazionale per la Cybersecurity

- Il Framework Nazionale per la Cybersecurity e la Data Protection è frutto della collaborazione tra accademia, enti pubblici, e imprese private ed è ispirato al NIST CSF.
- **Strumento operativo di supporto alle organizzazioni che necessitano di strategie e processi volti alla protezione dei dati personali e alla sicurezza cyber.**
- Infatti alla luce delle norme previste dal GDPR e i rischi connessi con i **data breach** che sottraggono in modo fraudolento dati, anche sensibili, dalle banche dati di industrie, enti pubblici ed organizzazioni di ogni genere e che, in caso di accadimento, rappresentano un danno spesso ingente per le organizzazioni, viene introdotta la nuova versione 2.0 del *Framework Nazionale per la Cybersecurity e la Data Protection*.
- 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.



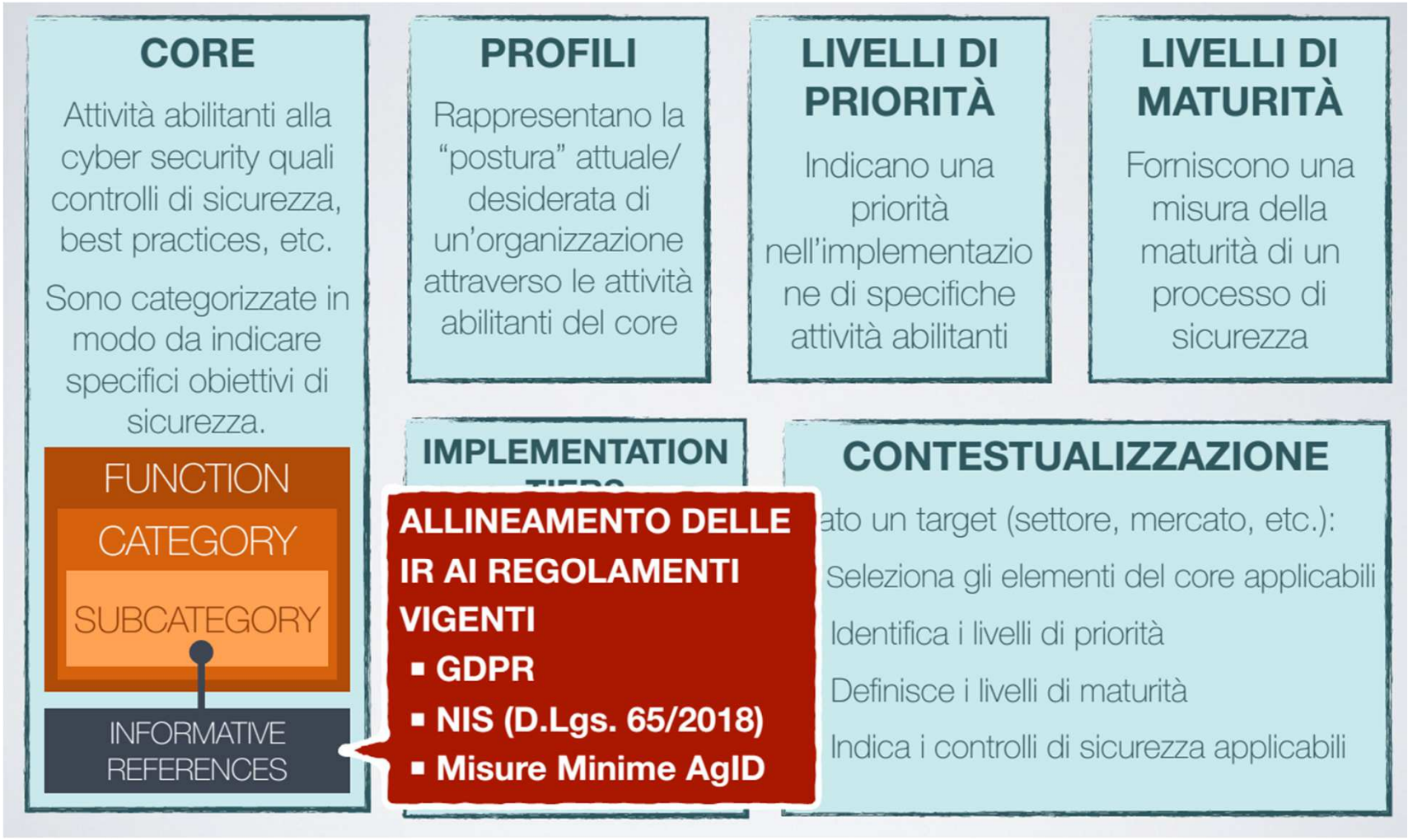
Fonte: (https://www.cybersecurityframework.it/framework2)

Framework Nazionale per la Cybersecurity



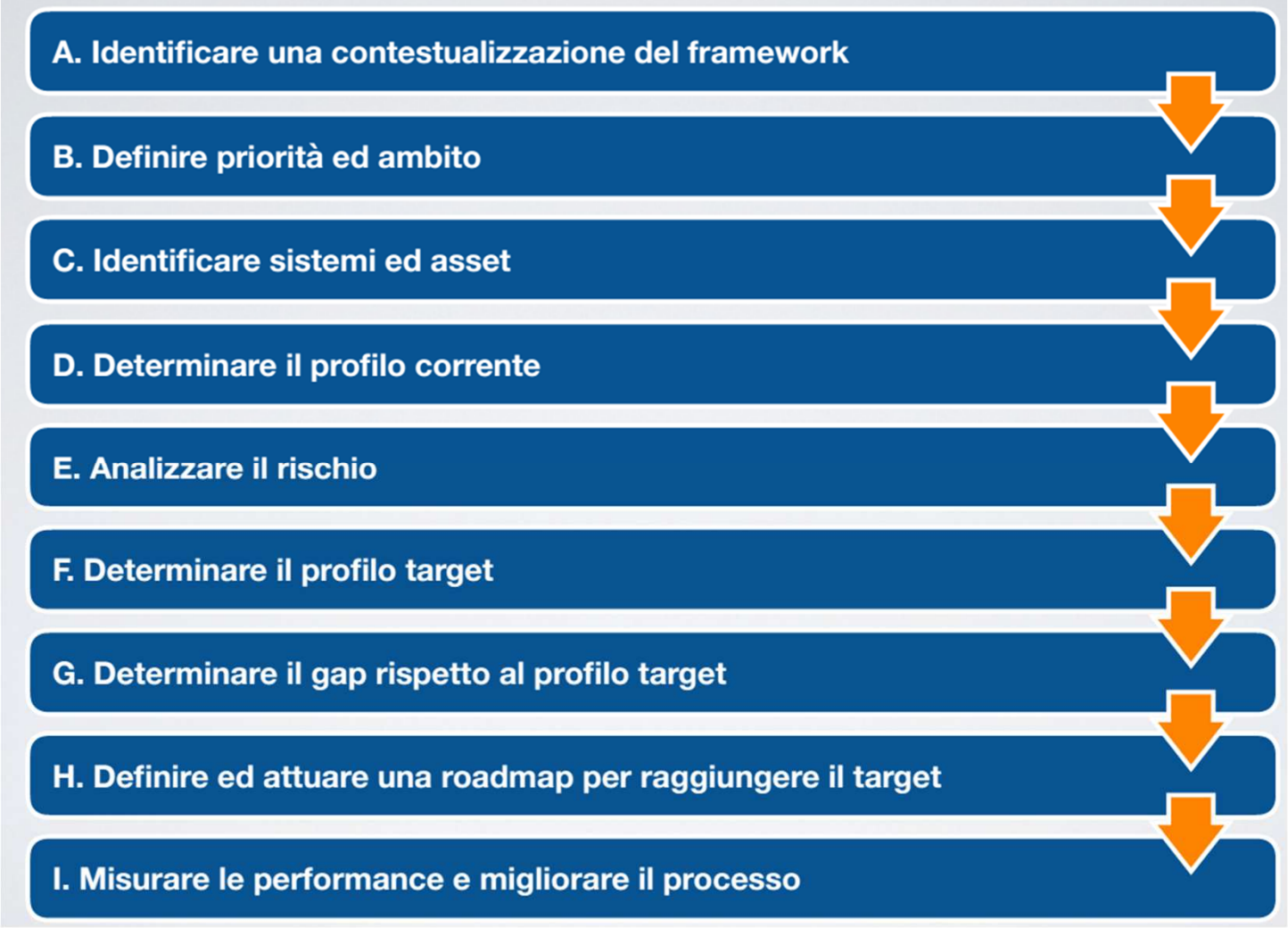
Fonte: (https://www.cybersecurityframework.it/framework2)

Framework Nazionale per la Cybersecurity



Fonte: (https://www.cybersecurityframework.it/framework2)

Framework Nazionale per la Cybersecurity



Fonte: (https://www.cybersecurityframework.it/framework2)

Information Security Management System

Information Security Management System (ISMS) definita dalla ISO/IEC 27001, è una norma volontaria per la gestione della sicurezza dei dati e dei sistemi informatici applicabile a organizzazioni di differenti dimensioni e operanti in qualsiasi settore. I benefici più evidenti di un modello di ISMS sono i seguenti:

- consentono di avere una visione complessiva e centrale della sicurezza aziendale che spazia oltre il perimetro della sicurezza IT includendo anche persone e processi secondo un approccio olistico;
- è un modello adattativo che si adegua all'evoluzione temporale delle minacce e quindi ai rapidi cambiamenti tipici degli odierni sistemi informativi;
- restituisce una corretta visione sullo stato della security e diventa quindi lo strumento fondamentale per l'ottimizzazione dell'allocazione del budget indirizzandolo verso le iniziative che restituiscono un maggior ritorno in termini di riduzione del rischio;
- implementare questo modello di controlli permette in molti casi di rispondere anche a vincoli normativi esterni che normalmente richiedono una serie di misure che altro non sono che un sottoinsieme dei possibili controlli del framework.
- l'applicazione dei controlli consente un'efficace strumento per il governo della sicurezza aziendale.

Information Security Management System

Information Security Management System

- L'Annex A dell'ISO 27001 contiene gli obiettivi ed i controlli da applicare (le 14 aree tematiche che sono poi scomposte in controlli più di basso livello, più specifici nella ISO 27002):
- A.5: information security policy
- A.6: organization of information security
- A.7: human resource security
- A.8: assett management
- A.9: access control
- A.10: cryptography
- A.11: physical and environmental security
- A.12: operation security
- A.13: communications security
- A.14: system acquisition, development and maintenance
- A.15: supplier relationships
- A.16: information security incident management
- A.17: information security aspects of business continuity management
- A.18: compliance

Information Security Management System

- **Plan**: stabilire il piano di ISMS definendone il perimetro e gli obiettivi, si effettua il risk assessment, si stabilisce il piano e le procedure per il trattamento dei rischi;
  - identificazione del rischio: è la fase in cui devono emergere i possibili rischi che se si materializzassero condurrebbero ad una compromissione in termini di integrità, riservatezza o disponibilità dei dati;
  - misurazione del rischio: una volta identificati i possibili rischi questi devono essere soppesati in funzioni dell'impatto che questi avrebbero sull'organizzazione: essi possono essere sia impatti monetari quantificabili (di solito nel caso di perdite materiali) che immateriali come nel caso di perdite reputazionali;
  - ponderazione del rischio: in questo step si confrontano i risultati della fase precedente con i criteri di rischio stabiliti per stabilire le priorità e modalità di trattamento del rischio.
- **Do**: attuazione del piano di ISMS, si rende operativa la procedura;
- **Check**: fase di monitoraggio e correzione del piano di ISMS che viene eseguito tramite audit interni e i risultati vengono riportati all'alta direzione;
- **Act**: mantenere e migliorare il piano attraverso azioni correttive.

ISMS vs. Privacy

- La conformità alla ISO 27001 non solleva l'organizzazione dal rispetto delle misure minime di sicurezza e dalla produzione della documentazione richiesta dalla legge sulla privacy;
- il controllo A.18.1.4 richiede infatti che "La protezione dei dati e della privacy deve essere garantita come richiesto nella legislazione, nelle norme e, se applicabile, nelle clausole contrattuali".
- La differenza sostanziale tra legge sulla privacy e la norma ISO 27001 è che la legge sulla privacy tutela dati personali, sensibili e non, mentre la ISO 27001 pur richiedendo che ciò sia fatto, s'interessa anche dei dati di *business* dell'organizzazione che devono essere salvaguardati per l'interesse stesso dell'organizzazione.
- Pertanto il soddisfacimento dei requisiti di legge non è condizione sufficiente al test della ISO 27001.

ISMS vs. NIST CSF

- Alcune stime stabiliscono che il 100% di compliance alla ISO 27001 equivalga a circa il 60% di compliance al NIST CSF e che il 100% di compliance al NIST CSF equivalga a circa l'80% di compliance alla ISO 27001!
- Quindi tra il 60 e il 80 % di sovrapposizione.

- NIST CSF è stato creato a supporto delle agenzie federali statunitensi per la gestione del rischio mentre ISO 27001 è un approccio riconosciuto a livelo internazionale
- ISO 27001 coinvolge figure di auditing e organismi di certificazione mentre NIST CSF è volontario, ovvero NIST CSF è auto-certificato.
- NIST CSF ha 5 funzioni per la personalizzazione dei controlli di cybersecurity controls, mentre ISO 27001 Annex A fornisce 14 categorie di controlli con 114 controlli.
- ISO 27001 è meno tecnica con enfasi sull'approccio risk-based management che fornisce delle best practices per creare l'ISMS.

Indice degli argomenti

- Le precondizioni minime per un sistema "sicuro" e il Quadro normativo di riferimento
- La cybersecurity e la direttiva UE 2016/1148 c.d. "direttiva NIS“ – L’Agenzia per la Cybersicurezza Nazionale
- Approccio Metodologico alla Gestione del Rischio secondo ISO 31000
- Il Professionista della Security (Security Manager) ai sensi della UNI 10459:2017
- **Il Modello di Gestione della Sicurezza (MOGS): ambiti di applicazione**
  - cybersecurity: il NIST Cybersecurity Framework (CSF) e il processo di individuazione degli RSL (Required Security Level) – il Framework Nazionale per la Cybersecurity e la Data Protection – ISMS vs. NIST CSF
  - **privacy: ai sensi del GDPR**
  - HSE ai sensi della ISO 45001 (cenni)
  - tutela responsabilità amm. aziendale ai sensi del D. Lgs. 231/01 (cenni)

Reg. UE 2016/679 GDPR art. 4 definizioni

Fonte: https://www.privacy-regulation.eu/it/

1) **dato personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata direttamente o indirettamente, con particolare riferimento a un identificativo come
   - Dati anagrafici
   - Codici di identificazione (codice fiscale, codice sanitario)
   - Targa del proprio veicolo
   - Indirizzo email
   - dati relativi all'ubicazione
   - un identificativo on-line,
   - a uno o più elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale e sociale.

   Per una persona giuridica, sono dati personali quelli inerenti il proprio Legale Rappresentante o del personale di contatto all'interno della persona giuridica con cui si intrattengono rapporti. Rientrano anche i c.d. dati sensibili dal D.lgs 196/2003 che rivelano origine razziale, etnica, …, convinzioni religiose, filosofiche, …, relativi alla salute e all'orientamento sessuale.

Reg. UE 2016/679 GDPR art. 4 definizioni

2) **trattamento**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

4) **profilazione**: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

5) **pseudonimizzazione**: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

12) **violazione dei dati personali**: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

Reg. UE 2016/679 GDPR art. 4 definizioni

7) **titolare del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, **determina le finalità e i mezzi del trattamento di dati personal**i; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

8) **responsabile del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali **per conto del titolare del trattamento**;

11) **consenso dell'interessato**: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

Reg. UE 2016/679 GDPR art. 5

Principi applicabili al trattamento di dati personali

- Principio di **liceità, correttezza e trasparenza**: nei confronti dell'interessato (art. 5.1.a)
- Principio di **limitazione delle finalità**: determinate, esplicite e legittime (art. 5.1.b)
- Principio di **minimizzazione**: parsimonia massima nel ricorrere ai dati personali (art. 5.1.c)
- Principio di esattezza: **dati esatti e aggiornati** (art. 5.1.d)
- Principio di limitazione delle conservazione: tempo di conservazione coerente con le finalità (art. 5.1.e)
- Principio di **sicurezza dei dati personali**: integrità e riservatezza (art. 5.1.f).
- Principio di responsabilizzazione: Il titolare del trattamento è competente per il rispetto e in grado di comprovarlo.

Reg. UE 2016/679 GDPR art. 6
liceità del trattamento

Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti istituzionali.

Reg. UE 2016/679 GDPR art. 9

Trattamento di categorie particolari di dati personali

1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi:
   a) l'interessato ha prestato il **proprio consenso esplicito** al trattamento di tali dati personali per una o più finalità specifiche, ….
   b) il trattamento è necessario per **assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale**, ….;
   c) il trattamento è necessario per **tutelare un interesse vitale dell'interessato** o di un'altra persona fisica qualora l'interessato si trovi **nell'incapacità fisica o giuridica di prestare il proprio consenso**;
   d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;

Reg. UE 2016/679 GDPR art. 9

Trattamento di categorie particolari di dati personali

2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi:

e) il trattamento riguarda dati personali **resi manifestamente pubblici dall'interessato**;

f) il trattamento è necessario **per accertare, esercitare o difendere un diritto in sede giudiziaria** ….;

g) il trattamento è necessario **per motivi di interesse pubblico rilevante** sulla base del diritto dell'Unione o degli Stati membri, ….;

h) il trattamento è necessario **per finalità di medicina preventiva o di medicina del lavoro**, ….;

i) il trattamento è necessario per motivi **di interesse pubblico nel settore della sanità pubblica**, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, …

j) il trattamento è necessario **a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'art. 89 co. 1** (Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici) sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Reg. UE 2016/679 GDPR art. 25

Privacy by design

Il principio di *privacy by design* (protezione per progettazione) prevede che fin dalla progettazione di un sistema / organizzazione la realizzazione di una adeguata protezione dei dati personali sia tra gli obiettivi della progettazione stessa. Quindi **prevenire per non correggere**:

- privacy **incorporata nel progetto** (ad esempio, l'utilizzo di tecniche di pseudonomizzazione);
- massima **funzionalità**, in maniera da rispettare tutte le esigenze (rifiutando le false dicotomie quali più privacy = minor prestazione);
- **visibilità** e **trasparenza** del trattamento, cioè tutte le fasi operative devono essere trasparenti in modo che sia verificabile la tutela dei dati;
- **centralità dell'utente**, quindi rispetto dei diritti, tempestive e chiare risposte alle sue richieste di accesso.

Reg. UE 2016/679 GDPR art. 25

Privacy by default

Il principio di *privacy by default* (protezione per impostazione predefinita) prevede che per impostazione predefinita le imprese dovrebbero trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini.

- Occorre, quindi, progettare il sistema di trattamento di dati garantendo la **non eccessività dei dati raccolti**. in modo che l'interessato riceva un alto livello di protezione anche se non si attiva per limitare la raccolta dei dati.
- Il principio in questione ovviamente tocca tutti gli aspetti del trattamento, non solo la quantità e qualità dei dati, ma anche il periodo di trattamento e le persone che possono accedere ai dati.

Reg. UE 2016/679 GDPR art. 30
Registri delle attività di trattamento

1. Ogni **titolare del trattamento** e, ove applicabile, il suo rappresentante tengono un **registro delle attività di trattamento** svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

   a) **il nome e i dati di contatto del titolare del trattamento** e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;

   b) **le finalità del trattamento;**

   c) una **descrizione delle categorie di interessati e delle categorie di dati personali**;

   d) le **categorie di destinatari** a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

   e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale, …;

   f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

   g) ove possibile, una **descrizione generale delle misure di sicurezza tecniche e organizzative** di cui all'art. 32

Reg. UE 2016/679 GDPR art. 30
Registri delle attività di trattamento

2. Ogni **responsabile del trattamento** e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

a) **il nome e i dati di contatto del responsabile o dei responsabili del trattamento,** di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;

b) le **categorie dei trattamenti** effettuati per conto di ogni titolare del trattamento;

c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale, ….;

d) ove possibile, **una descrizione generale delle misure di sicurezza tecniche e organizzative** di cui all'art. 32.

3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.

4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento **mettono il registro a disposizione dell'autorità di controllo.**

5. ….

Reg. UE 2016/679 GDPR art. 32
Sicurezza del Trattamento

L'art. 32 stabilisce l'adozione di misure tecnico-organizzative da parte del titolare e del responsabile per il trattamento dei dati personali commisurata al rischio per gli interessati finalizzate alla

- **Riservatezza per i dati digitali**: credenziali di accesso, cifratura degli storage, password robuste, cancellazione sicura ante dismissione / vendita / rottamazione / cessione del server, aggiornamento periodico del S.O.,
- **Riservatezza per i documenti cartacei**: custodia in armadi chiusi a chiave, distruzione con apparati distruggi-documenti, nelle comunicazioni: e-mail crittografate, pseudonomizzazione,
- **Riservatezza per la rete interna**: firewall perimetrali, cambio password, WIFI cifrato, …),
- **Integrità** (correttezza e completezza del trasferimento file, tracciatura accessi al sistema, …)
- **Disponibilità** (continuità operativa del sistema con backup, dischi in RAID, procedure di recovery, disaster recovery. …)
- **Resilienza** (qualità elastica del sistema di operare sia in condizioni previste che impreviste).

Violazione dei dati personali (data breach)
Notifica all'autorità di controllo

- La violazione dei dati personali (data breach) è l'evento conseguente al fallimento delle misure tecnico-organizzative messe in atto per il trattamento con danno (normalmente grave) sugli interessati. Esempi di tali danni sono la discriminazione, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione.
- Art. 33 co. 1: in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'art. 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile (rischio basso) che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo. La notifica di cui al co. 1 deve almeno (art. 33 co. 3):
  a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
  b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
  c) descrivere le probabili conseguenze della violazione dei dati personali;
  d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Violazione dei dati personali (data breach)

Comunicazione agli interessati

- Art. 34 co. 1: quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
- Art. 34 co. 2: la comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'art. 33 co. 3, lettere b), c) e d)
- Art. 34 co. 3: Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:
  a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
  b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
  c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Violazione dei dati personali (data breach)

- Per la valutazione della gravità della violazione si utilizza la metodologia FMEA-like elaborata da ENISA (rif. “Linee Guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento UE 2016/679”) per cui **G = DCP x IE x CB** dove:

– Contesto di elaborazione dei dati (DCP): valutato sulla base del tipo di dati coinvolti nei data breach e di fattori di correzione relativi al contesto, che aumentano la criticità della violazione anche nel caso di dati “semplici”: $1 \leq DCP \leq 4$

– Facilità di Identificazione (IE): valutato sulla base dei dati personali coinvolti nei data breach, è un fattore correttivo del DCP: $0{,}25 \leq IE \leq 1$

– Circostanze della Violazione (CB): valutato sulla base alle tipologie di data breach e alla eventuale intenzionalità della violazione , è un fattore additivo del DCP: $0 \leq CB \leq 2$

GRAVITÀ	RISCHIO	DESCRIZIONE
G < 2 Minore di 2	Basso	Gli interessati non incontreranno inconvenienti o potrebbero incontrare alcuni inconvenienti che supereranno senza alcun problema (tempo passato a reinserire informazioni, fastidio, irritazione, ecc...)
2 =< G < 3 Compreso tra 2 e meno di 3	Medio	Gli interessati potrebbero incontrare inconvenienti significativi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici lievi, ecc...)
3 =< G < 4 Compreso tra 3 e meno di 4	Alto	Gli interessati potrebbero incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, lista nera da parte delle banche, danni alla proprietà, perdita di posti di lavori, citazione, peggioramento della salute, ecc...)
4 =< G Uguale o maggiore di 4	Molto Alto	Gli interessati potrebbero incontrare conseguenze significative o addirittura irreversibili non superabili (difficoltà finanziare come debito sostanziale o incapacità al lavoro, disturbi psicologici a lungo termine o disturbi fisici, morte, ecc...)

Reg. UE 2016/679 GDPR art. 35
DPIA (Data Protection Impact Analysis)

- La DPIA è un'analisi rischi che va svolta prima di procedere ad un trattamento che comporti impatto sugli interessati.
- E' uno strumento importante per la responsabilizzazione in quanto sostiene il Titolare nel garantire e dimostrare la conformità al GDPR.
- Non è obbligatorio effettuarla per ciascun trattamento ma soltanto quando questo (art. 35 co.1) ˝*… allorchè prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche*˝

- In particolare la DPIA è uno strumento utilissimo quando si tratta di valutare l'impatto di un **nuovo dispositivo tecnologico**, HW o SW che sia, p.es. interconnesso in una IoT.

- Effettuare una DPIA significa quindi implementare un'analisi del rischio.
- Il nostro GPDP pubblicizza un softare messo a disposizione dal CNIL (GPDP francese): https://www.cnil.fr/en/privacy-impact-assessment-pia
- Metodo di ponderazione usato è tipicamente **FMEA** (Failure Mode and effect Analysis).

Reg. UE 2016/679 GDPR art. 35
DPIA (Data Protection Impact Analysis)

- Art. 35 co. 3: La valutazione d'impatto sulla protezione dei dati è richiesta in particolare in determinate casistiche

- Al fine di decidere il grado di esposizione al rischio del trattamento e conseguente, ente l'opportunità di svolgere una DPIA si può consultare il documento WP248 dello European Data Protection Board emissione del 4.10.17: https://ec.europa.eu/newsroom/document.cfm?doc_id=47711

- Ripreso e ulteriormente chiarito dal Garante della Protezione dei Dati Personali (GPDP) nel documento "Elenco delle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 co. 4 reg. 2016/679" emissione 11.10.18: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9058979

  https://www.garanteprivacy.it/documents/10160/0/ALLEGATO+1+Elenco+delle+tipologie+di+trattamenti+soggetti+al+meccanismo+di+coerenza+da+sottoporre+a+valutazione+di+impatto

Reg. UE 2016/679 GDPR art. 35
DPIA (Data Protection Impact Analysis)

1) *Trattamenti valutativi di scoring:* includono la **profilazione** e le **attività predittive**, in particolare quando si parla di aspetti riguardanti il **rendimento professionale**, la **situazione economica**, la **salute**, le **preferenze** o gli **interessi personali**, l'**affidabilità** o il **comportamento**, l'**ubicazione** e gli **spostamenti** dell'interessato. Si pensi per esempio agli screening fatti in ambito finanziario ricorrendo a DB di rischio creditizio; ai test genetici effettuati per predire eventuali patologie; alla creazione di profili comportamentali ai fini marketing, …

2) *Decisioni automatizzate che producono significativi effetti giuridici o di analoga natura:* quali per esempio trattamenti che possano **escludere l'interessato da determinati benefici** (erogazione di un mutuo o di una copertura assicurativa) o la sua discriminazione.

3) *Monitoraggio sistematico:* trattamenti utilizzati per **osservare**, **monitorare** o **controllare** gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di luoghi pubblici, situazioni nelle quali spesso l'interessato non si rende conto di essere soggetto a monitoraggio e facilmente non può sottrarvisi.

4) *Dati sensibili o di natura estremamente personale:* che possono riguardare ad esempio **ospedali**; **investigatori privati**; **informazioni relative a vita familiare o privata**; dati sull'**ubicazione** o gli **spostamenti**, …, informazioni la cui violazione può comportare un grave impatto sulla vita quotidiana dell'interessato.

Reg. UE 2016/679 GDPR art. 35
DPIA (Data Protection Impact Analysis)

5) *Trattamenti di dati su larga scala:* in sintesi prende in considerazione il numero di soggetti interessati al trattamento, il volume dei dati trattati; la durata o persistenza dell'attività e l'ambito geografico dell'attività.

6) *Combinazione o raffronto di insiemi di dati:* per esempio derivanti da due o più trattamenti, svolti per diverse finalità e/o da titolari distinti, motivo per il quale probabilmente l'interessato **non sa di essere oggetto del confronto**.

7) *Dati relativi a interessati vulnerabili:* che portano con sè uno squilibrio fra interessato e titolare del trattamento e che includono ad esempio il trattamento di dati relativi a **minori**, **dipendenti**, **categorie affette da patologie psichiatriche**, ….

8) *Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative:* il ricorso ad una nuova tecnologia può generare forme innovative di raccolta e utilizzo dei dati cui può associarsi un rischio elevato per i diritti e le libertà dell'interessato.

9) *Tutti quei trattamenti che impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o contratto:* cosa che include tutti i trattamenti finalizzati a consentire, modificare o negare l'accesso degli interessati a un servizio o contratto.

Reg. UE 2016/679 GDPR art. 35
DPIA (Data Protection Impact Analysis)

- Concetto di **larga scala**: non esiste ancora una quantificazione di cosa è definibile con "larga scala". I criteri da tenere in considerazione per ora sono questi: il numero dei soggetti interessati; il volume e il range di informazioni trattati; la durata del trattamento; l'estensione geografica del trattamento. Ad esempio **rientrano in questa definizione** gli ospedali, chi elabora statistiche sulla base della geolocalizzazione, chi elabora i dati dei clienti di banche o assicurazioni, chi elabora in modo automatizzato i dati per marketing mirato, chi gestisce i dati per conto dei provider internet o telefonici. Sono invece **esclusi** gli studi medici o legali in cui opera un unico professionista.
- Concetto di **regolare e sistematico monitoraggio dei dati** : ci si riferisce a tutti i sistemi di profilazione e tracciamento automatico dell'utente che, per esempio, possono essere effettuati tramite: i network di telecomunicazioni; la profilazione del cliente per scopi assicurativi, bancari; la geolocalizzazione tramite mobile app; i programmi fedeltà; il marketing comportamentale (tipico di google e dei social media), i **wearable devices** per il monitoraggio dello stato di salute e delle performance fisiche nonchè **l'elaborazione delle informazioni derivanti dagli oggetti interconnessi IoT**. I criteri su cui basarsi per valutare la sistematicità e regolarità del trattamento sono: la periodicità e la durata con cui questo viene effettuato, se è svolto in modo metodico, organizzato, sistematico, inserito all'interno di un progetto di raccolta ed elaborazione dei dati e all'interno di una specifica strategia aziendale.

Reg. UE 2016/679 GDPR art. 35
DPIA (Data Protection Impact Analysis)

Art. 35 co. 7. La valutazione contiene almeno:

a) una **descrizione sistematica dei trattamenti previsti e delle finalità del trattamento**, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione della necessità e proporzionalità dei trattamenti** in relazione alle finalità;

c) una **valutazione dei rischi per i diritti e le libertà degli interessati**;

d) le **misure previste per affrontare i rischi**, includendo le garanzie, le **misure di sicurezza** e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Processo di Certificazione GDPR

- Art. 42 co. 1. Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano, in particolare a livello di Unione, l'**istituzione di meccanismi di certificazione della protezione dei dati** nonché di sigilli (uno schema di certificazione valido in tutti gli Stati membri dell'Unione Europea) e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento.
- La certificazione è volontaria e accessibile tramite una procedura trasparente (art. 42 co. 3) ma non riduce la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al GDPR …. (art. 42 co. 4).
- Art. 42 co. 5. La certificazione ai sensi del presente articolo è rilasciata dagli organismi di certificazione di cui all'art. 43 ….
- Art. 43 co. 1 lett. b) dall'organismo nazionale di accreditamento designato in virtù del regolamento (CE) n. 765/2008 del Parlamento europeo ….. conformemente alla norma ISO 17065:2012 che dà i requisiti per gli **organismi che certificano prodotti, processi e servizi**" - diversamente dalla ISO 17024:2012 che dà i requisiti per gli **organismi che certificano le persone**.
- In merito, il nostro Garante ha predisposto il provvedimento n. 148 del 20 luglio 2020 in cui ha indicato i Requisiti di accreditamento "aggiuntivi" dell'Autorità di controllo italiana con riguardo alla norma ISO 17065:2012. Tali requisiti aggiuntivi se soddisfatti dall'Organismo di Certificazione, possono ritenersi validi a livello europeo ai fini dell'utilizzo di un sigillo europeo per la protezione dei dati personali.

Processo di Certificazione GDPR
ISO 27701

- Tuttavia il GDPR prescrive cosa fare ma non come fare ovvero **non dà istruzioni operative**.
- La **ISO 27701:2019 "Security techniques - Extension to ISO 27001 and ISO 27002 for privacy information management - Requirements and guidelines"** fornisce i requisiti per estendere gli ISMS al perimetro della gestione della Privacy.
- La certificazione accreditata secondo la ISO 27701:
  - attesta a clienti e stakeholder che l'azienda utilizza **sistemi efficaci per supportare la conformità al GDPR** e ad altre normative sulla privacy correlate.
  - **riduce i rischi legati alla violazione della privacy** delle persone e dell'organizzazione migliorando un sistema di gestione della sicurezza delle informazioni esistente.

Processo di Certificazione GDPR
ISO 27701 vs. ISO 27001

- Le organizzazioni che hanno già implementato un ISMS (Information Security Management System) secondo la ISO 27001 saranno in grado di utilizzare la ISO/IEC 27701 per estendere la copertura dell'information security alla gestione della privacy, comprendendo anche i trattamenti di dati personali (PII - Personally Identifiable Information), in modo da poter dimostrare la conformità con le legislazioni cogenti in materia di protezione dei dati personali come il GDPR
- Per quanto riguarda la ISO 27001, la norma prevede
  - la sua estensione alla "sicurezza delle informazioni e privacy", dove i dati personali sono indicati come Personal identifiable information (PII);
  - l'analisi del contesto in quanto titolare o responsabile di trattamenti;
  - l'inclusione, tra le parti interessate, degli interessati ai trattamenti dei dati personali;
  - l'inclusione, tra i controlli da considerare per la Dichiarazione di applicabilità (Statement of Applicability o SOA) di quelli proposti dalla stessa ISO 27552 nelle appendici A (per i titolari) e B (per i responsabili).

Processo di Certificazione GDPR
ISO 27701 vs. ISO 27002

- Per quanto riguarda la ISO/IEC 27002, la norma prevede l'estensione dei suoi controlli nel caso in cui l'organizzazione sia titolare (cap. 7) o responsabile dei trattamenti (cap. 8). Nel cap. 6 sono riportate alcune considerazioni aggiuntive ai controlli già esistenti. Tra di esse, l'aggiunta:
  - tra le politiche, di impegni a soddisfare la legislazione vigente in materia di privacy;
  - tra i ruoli e le responsabilità, di persone di riferimento per quanto attiene alla privacy (alcuni punti riprendono quelli previsti per il DPO, nelle organizzazioni dove questa figura è presente; nelle altre è possibile prevedere un unico ruolo o ruoli distinti per il controllo e per la gestione);
  - tra la classificazione, di elementi relativi alle categorie di dati personali;
  - tra la gestione degli utenti, di considerazioni in merito ai servizi cloud in cui il cliente può autonomamente gestire i propri utenti; manca una relazione tra assegnazione delle autorizzazioni e istruzione e formazione, come invece previsto dal GDPR;
  - tra le misure relative al logging, di dettagli in merito agli accessi ai dati personali, alla messa a disposizione del titolare dei log da parte del responsabile e alla protezione dei log in quanto dati personali;
  - tra le misure relative allo sviluppo, di richiami all'importanza della privacy;
  - tra la gestione degli incidenti, della gestione delle violazioni dei dati personali (*data breach*).

Processo di Certificazione GDPR
ISO 27701 vs. ISO 27002

- Ulteriori misure sono incluse, ma si tratta principalmente di precisazioni in merito alle misure già presenti nella ISO/IEC 27002.
- Il capitolo 7 presenta controlli aggiuntivi per i titolari del trattamento.
  - identificazione delle basi legali;
  - registro dei trattamenti;
  - DPIA;
  - contratti con i responsabili;
  - informative;
  - gestione dei diritti degli interessati;
  - minimizzazione e limitazione dei trattamenti;
  - conclusione dei trattamenti;
  - tempi di conservazione;
  - trasferimenti in altri Paesi o organizzazioni internazionali.
- Il capitolo 8 presenta controlli aggiuntivi per i responsabili del trattamento. Tra di essi, similmente a quelli per i responsabili, ci sono controlli relativi a:
  - registro dei trattamenti;
  - accordi con i clienti;
  - contratti con i sub-responsabili;
  - gestione dei diritti degli interessati;
  - conclusione dei trattamenti;
  - trasferimenti in altri Paesi o organizzazioni internazionali.

Processo di Certificazione GDPR
ISO 27701

- Sono inoltre presenti 6 allegati (Annex) che riportano sia controlli (cioè misure tecnico/organizzative di mitigazione del rischio privacy), sia riferimenti alle altre normative ISO/IEC vigenti. Nel dettaglio:
- **Annex A**: riporta i controlli che devono essere implementati da un'organizzazione che si configuri come Titolare del Trattamento;
- **Annex B**: riporta i controlli che devono essere implementati da un'organizzazione che si configuri come Responsabile del Trattamento;
- **Annex C**: riporta la mappatura rispetto alla normativa ISO/IEC 29100 *Information Technology – Privacy Techniques – Privacy Framework*;
- **Annex D**: **riporta il mapping delle clausole ISO 27701 rispetto agli adempimenti ed ai concetti chiave del GDPR**; L'allegato è strutturato sottoforma di tabella che riporta nella prima colonna le clausole della ISO 27701 e nella seconda colonna l'articolo GDPR di riferimento indicando anche il paragrafo e la lettera.
- **Annex E**: contiene la mappatura rispetto alle normative ISO 27018 *Information Technology – Security Techniques – Code of Practice for Protection of Personally Identifiable Information (PII) in public clouds acting as PII* ed alla ISO/IEC 29151 *Information Technology – Security Techniques – Code of Practice for Personally Identifiable Information Protection*;
- **Annex F**: descrive ulteriori modalità per applicare la ISO 27001 ed ISO 27002 all'ambito privacy laddove vengano trattati dati personali.

Processo di Certificazione GDPR ISO 27701

Dimostrare che il modello adottato è completo rispetto a:

- **Identificazione dei trattamenti svolti** → registro delle attività di trattamento.
- **Individuazione delle finalità e basi giuridiche del trattamento** → informative al trattamento, modulo di consenso al trattamento, richieste di conferma del consenso per i dati già raccolti che sono trattati con finalità diverse a quella per la quale sono stati raccolti o si è perso traccia della finalità di trattamento
- **Valutazione d'impatto sulla protezione dei dati personali (DPIA) ovvero l'analisi dei rischi da svolgersi prima di procedere al trattamento che comporti un rischio per interessato** → valutazione d'impatto sulla protezione dati personali per nuovi trattamenti critici, misure di sicurezza organizzative e tecniche aggiuntive da adottare sul nuovo trattamento.
- **Protezione dei dati personali** → analisi dei rischi, misure di sicurezza organizzative e tecniche adottate, politica di "data protection by design" e "by default" (art. 25) ovvero l'attuazione di misure tecnico-organizzative già in fase di progettazione ed esecuzione del trattamento, no a posteriori (rif. "Linee guida per lo sviluppo del software sicuro", AgID e "Privacy and Data Protection by Design", ENISA).
- **Identificazione e gestione delle violazioni dei dati personali (data breach)** → procedura di escalation interna per la valutazione delle violazioni, di notifica all'Autorità Garante (entro 72 ore se rischio>basso), di comunicazione agli interessati.
- **Gestione dei diritti degli interessati** → processo / procedura da seguire a seguito di una richiesta di esercizio dei diritti da parte degli interessati.

Processo di Certificazione GDPR
Il Data Protection Officer (DPO)

- Il DPO ha principalmente una **funzione consulenziale nei confronti del titolare** e deve pertanto raccogliere tutte le informazioni necessarie ad identificare trattamenti e dati trattati, analizzare e verificare il grado di conformità dei vari processi e fornire indicazioni e consigli al titolare, che resta ultimo responsabile della conformità normativa. Nel caso il titolare debba effettuare una valutazione di impatto del trattamento, è opportuno che tale valutazione sia realizzata con l'ausilio del DPO.
- Deve svolgere poi il suo compito sulla base di una valutazione dei rischi che gli permetta di individuare le aree maggiormente a rischio e fornire al titolare una priorità di intervento che gli consenta di allocare correttamente e sensatamente budget e risorse.
- **Autonomia del DPO**: il DPO che deve operare sulla base della propria esperienza e non su istruzioni impartite dal titolare, fermo restando che non ha potere decisionale ma può solo riferire al titolare che rimane l'unico responsabile delle decisioni prese e della conformità ai requisiti del decreto. Il DPO inoltre non può in alcun modo essere penalizzato o sanzionato per la sua attività o per le indicazioni fornite, in particolare per quanto riguarda figure all'interno all'azienda che non devono subire discriminazioni per il lavoro svolto. Come anche per i membri dell'organismo di vigilanza 231, è opportuno evitare conflitti di interesse in capo al DPO.

Processo di Certificazione GDPR

Decalogo del DPO

Il DPO deve **periodicamente** effettuare le seguenti verifiche:

1) Verifica liceità del trattamento
2) Verifica che i dati raccolti siano adeguati, pertinenti, e limitati rispetto alla finalità del trattamento
3) Trattamento dei dati esclusivamente per le finalità per i quali sono stati raccolti
4) Definire la durata della conservazione dei dati compatibilmente con la legislazione in vigore
5) Fornire l'informativa agli interessati e quando previsto raccogliere il consenso
6) Applicare i principi di Data Protection by Design e by Default
7) Documentare ogni violazione dei dati personali e comunicare al Titolare
8) Mantenere un registro (censimento) delle attività di trattamento
9) Valutare i rischi del trattamento e l'attuazione di misure tecniche organizzative (misure di sicurezza) adeguate con riesame periodico
10) Provvedere a nomine di eventuali organizzazioni esterne con comunicazione delle misure di sicurezza da adottare

Indice degli argomenti

- Le precondizioni minime per un sistema "sicuro" e il Quadro normativo di riferimento
- La cybersecurity e la direttiva UE 2016/1148 c.d. "direttiva NIS“ – L’Agenzia per la Cybersicurezza Nazionale
- Approccio Metodologico alla Gestione del Rischio secondo ISO 31000
- Il Professionista della Security (Security Manager) ai sensi della UNI 10459:2017
- **Il Modello di Gestione della Sicurezza (MOGS): ambiti di applicazione**
  - cybersecurity: il NIST Cybersecurity Framework (CSF) e il processo di individuazione degli RSL (Required Security Level) – il Framework Nazionale per la Cybersecurity e la Data Protection – ISMS vs. NIST CSF
  - privacy ai sensi del GDPR
  - **HSE ai sensi della ISO 45001 (cenni)**
  - tutela responsabilità amm. aziendale ai sensi del D. Lgs. 231/01 (cenni)

Salute e Sicurezza sui luoghi di lavoro

BS OHSAS 18001

- Acronimo di Occupational Health and Safety Assessment Series.
- Lo standard internazionale OHSAS 18001 ha una storia quasi ventennale, con il quale sono stati introdotti i principi anglosassoni sul concetto di rischio, l'evoluzione di tutti i sistemi di gestione negli ultimi anni ha reso necessario **uniformare la norma per il sistema SSL** alle altre norme di certificazione più comuni come quella sulla qualità, ambiente, dati, sicurezza alimentare, ecc.
- La norma BS OHSAS 18001:1999 è stata emanata dal BSI (British Standard Institute) nel 1999, rivista nel 2007 (**BS OHSAS 18001:2007**), così da poter disporre di uno standard per il quale potesse essere rilasciata una certificazione di conformità. La certificazione OHSAS attesta l'applicazione volontaria, all'interno di un'organizzazione, di un sistema che permette di garantire un adeguato controllo riguardo alla sicurezza e la salute dei lavoratori, oltre al rispetto delle norme cogenti.
- **Il sistema di gestione regolato dalla norma OHSAS è integrato con il sistema di gestione ambientale, ispirato alla norma 14001**: la sicurezza e l'ambiente sono infatti strettamente collegati tra loro. Inoltre, solitamente il Sistema di Gestione della Sicurezza e Salute dei Lavoratori (SGSL) è costruito a partire da un sistema ISO 9001, rivolto alla qualità, già esistente. Sebbene la norma sia inglese, essa, di fatto, è divenuta uno standard internazionale utilizzato in tutto il mondo per la certificazione di un SGSL.

Salute e Sicurezza sui luoghi di lavoro
La normativa ISO 45001

- La ISO 45001:2018 ("*Occupational Health and Safety Management Systems – Requirements with guidance for use*") è la prima norma internazionale per la salute e la sicurezza nei luoghi di lavoro; con la pubblicazione della ISO 45001, nel marzo del 2018, la BS OHSAS 18001 è stata ritirata.
- La norma si applica a qualsiasi organizzazione, indipendentemente dalle dimensioni, dal settore di appartenenza e dalla natura delle sue attività ed è progettata per essere integrata nei processi di gestione già esistenti: adotta infatti la stessa "struttura di alto livello" (High Level Structure - HLS) delle altre norme ISO sui sistemi di gestione come la **UNI EN ISO 9001** (gestione per la qualità) e la **UNI EN ISO 14001** (gestione ambientale).
- I potenziali benefici derivanti dall'applicazione della norma includono:
  - la **riduzione** degli incidenti sul lavoro, dell'assenteismo e del turnover e quindi una più alta produttività, dei costi dei premi assicurativi.
  - l'**incremento** di una cultura della prevenzione, della salute e della sicurezza che incoraggi i lavoratori a svolgere un ruolo attivo, un miglioramento del morale dei lavoratori, il maggiore impegno dei vertici aziendali a migliorare le performance di salute e sicurezza sul lavoro, la capacità di soddisfare gli obblighi legali e normativi dell'organizzazione e un miglioramento dell'immagine e della reputazione.

Sistema di Gestione della Sicurezza e Salute dei Lavoratori (SGSL)

- D.lgs 81/08 art. 2 lett. s) "rischio": probabilità di raggiungimento del livello potenziale di danno nelle condizioni di impiego o di esposizione ad un determinato fattore o agente oppure alla loro combinazione;
- D.lgs 81/08 art. 2 lett. dd) "modello di organizzazione e di gestione" ovvero il "Sistema di Gestione della Sicurezza e Salute dei Lavoratori" (abbreviato in **SGSL)** è il modello organizzativo e gestionale per la definizione e l'attuazione di una politica aziendale per la salute e sicurezza, ai sensi dell'articolo 6, comma 1, lettera a), del D.lgs 231/2001 idoneo a prevenire i reati di cui agli articoli 589 e 590, terzo comma, del codice penale, commessi con violazione delle norme antinfortunistiche e sulla tutela della salute sul lavoro;
- L'SGSL pertanto non è altro che uno **strumento documentale ed operativo** che permette di tenere i processi di safety sotto controllo.

Sistema di Gestione della Sicurezza e Salute dei Lavoratori (SGSL)

- L'SGSL attuato in base alla ISO 45001 recepisce i requisiti legislativi cogenti del nostro ordinamento, quelli cioè previsti a carico del datore di lavoro e li trasforma in criteri utili a disciplinare processi e risorse.
- L'SGSL (punto 6.1.3 ISO 45001) deve essere determinato nei suoi requisiti legali e negli altri requisiti. **I requisiti legali cui fa riferimento la ISO 45001:2018 in Italia sono gli articoli del D.Lgs.81/2008 che disciplina la salute e la sicurezza in azienda**.
- L'integrazione dei requisiti cogenti all'interno del SGSL deve assicurare che questi siano conosciuti ed applicati nell'organizzazione secondo quanto prevede la ISO 45001:2018.
- Il capo III del D.Lgs.81/2008 è dedicato interamente alla gestione della prevenzione nei luoghi di lavoro: l'art.15 disciplina le misure generali di tutela e fornisce le indicazioni che vengono acquisite dal SGSL nel momento in cui si sviluppa il programma per la sicurezza.
- Gli articoli che vanno dal 16 al 26 istituiscono una serie di obblighi per le figure previste quali il DL, i dirigenti, il preposto, i lavoratori, il medico competente, …

SGSL: Misure di tutela (D.Lgs 81/08 art. 15)

Le misure generali di tutela della salute e della sicurezza dei lavoratori nei luoghi di lavoro sono:

a) la valutazione di tutti i rischi per la salute e sicurezza;

b) la programmazione della prevenzione, mirata ad un complesso che integri in modo coerente nella prevenzione le condizioni tecniche produttive dell'azienda nonché l'influenza dei fattori dell'ambiente e dell'organizzazione del lavoro;

c) l'eliminazione dei rischi e, ove ciò non sia possibile, la loro riduzione al minimo in relazione alle conoscenze acquisite in base al progresso tecnico;

d) il rispetto dei principi ergonomici nell'organizzazione del lavoro, nella concezione dei posti di lavoro, nella scelta delle attrezzature e nella definizione dei metodi di lavoro e produzione, in particolare al fine di ridurre gli effetti sulla salute del lavoro monotono e di quello ripetitivo;

e) la riduzione dei rischi alla fonte;

f) la sostituzione di ciò che è pericoloso con ciò che non lo è, o è meno pericoloso;

g) la limitazione al minimo del numero dei lavoratori che sono, o che possono essere, esposti al rischio;

h) l'utilizzo limitato degli agenti chimici, fisici e biologici sui luoghi di lavoro;

i) la priorità delle misure di protezione collettiva (DPC) rispetto alle misure di protezione individuale (DPI);

… (continua)

SGSL: Misure di tutela (D.Lgs 81/08 art. 15)

Le misure generali di tutela della salute e della sicurezza dei lavoratori nei luoghi di lavoro sono:

l) il controllo sanitario dei lavoratori;

m) l'allontanamento del lavoratore dall'esposizione al rischio per motivi sanitari inerenti la sua persona e l'adibizione, ove possibile, ad altra mansione;

n) l'informazione e formazione adeguate per i lavoratori;

o) l'informazione e formazione adeguate per dirigenti e i preposti;

p) l'informazione e formazione adeguate per i rappresentanti dei lavoratori per la sicurezza;

q) le istruzioni adeguate ai lavoratori;

r) la partecipazione e consultazione dei lavoratori;

s) la partecipazione e consultazione dei rappresentanti dei lavoratori per la sicurezza;

t) la programmazione delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza, anche attraverso l'adozione di codici di condotta e di buone prassi;

u) le misure di emergenza da attuare in caso di primo soccorso, di lotta antincendio, di evacuazione dei lavoratori e di pericolo grave e immediato;

v) l'uso di segnali di avvertimento e di sicurezza;

z) la regolare manutenzione di ambienti, attrezzature, impianti, con particolare riguardo ai dispositivi di sicurezza in conformità alla indicazione dei fabbricanti

SGSL: DPC vs. DPI

- **Dispositivi di Protezione Collettiva (DPC):** si intendono quei sistemi che **intervengono direttamente sulla fonte del rischio**, riducendolo o eliminandolo. **L'intero ambiente lavorativo beneficia di tali sistemi** che riducono per tutti i soggetti operanti in esso il rischio sul quale agiscono (es. rivelatori di incendi, sistemi di monitoraggio, gruppi di continuità, cappe chimiche, depuratori d'aria, ponteggi, corrimano, parapetti, …)
- **Dispositivi di Protezione Individuale (DPI):** si intendono invece quelle dotazioni personali che **hanno la funzione di proteggere il lavoratore** che ne fa uso, nel corso della sua attività. **I DPI agiscono sul singolo individuo**, non estendendo la loro protezione ad altri soggetti esposti alla fonte di rischio (es. protezione testa, udito, occhi, pelle , vie respiratorie, indumenti di protezione, …)
- La **normativa di riferimento** (D.Lgs. 81/2008 art. 15, art. 75 e art. 111) **sancisce che DPC e DPI debbano sottostare ad una logica gerarchica**. L'adozione dei dispositivi di protezione collettiva debba essere necessariamente **prioritaria** rispetto all'utilizzo di dispositivi di protezione individuale.
- L'idea alla base di questo ordine gerarchico segue il principio secondo cui il datore di lavoro debba agire, laddove possibile, con **priorità sui rischi interessanti la globalità dell'ambiente lavorativo**, riducendoli o eliminandoli. I DPI in dotazione, invece, devono essere considerati come **difesa ultima del lavoratore** che ne fa uso e non come unica fonte di protezione.

Costruzione del SGSL

- Questi obblighi costituiscono un punto di riferimento nel momento in cui l'impresa sviluppa il SGSL al punto **5.3 Ruoli, responsabilità ed autorità nell'organizzazione**.
- **La valutazione dei rischi** prevista dal D.Lgs.81/2008 all'art. 28 e all'art.29 è recepita dal sistema di gestione ISO 45001:2018 attraverso lo sviluppo dei punti 6.1 **Azioni per affrontare rischi e opportunità** e 6.2 **Obiettivi per la SSL e pianificazione** per il loro raggiungimento.
- **Il servizio di prevenzione e protezione** indicato dal D.Lgs.81/2008 negli articoli che vanno dal 31 al 34 è la parte legislativa (cogente) che può interessare lo sviluppo delle **attività operative** del sistema disciplinate dalla ISO 45001:2018 al punto 8 della norma.
- L'art.35 del D.Lgs.81 che **prevede la riunione periodica** può essere recepito dal sistema ISO attraverso il **riesame di direzione** previsto al punto 9.3.
- I punti della norma relativi alla **competenza, alla consapevolezza e all'informazione** trattati nel punto 7 dedicato al supporto, possono essere sviluppati anche in base agli articoli 36 e 37 del D.lgs. 81/08 dedicati rispettivamente **all'informazione ai lavoratori e alla formazione dei lavoratori e dei loro rappresentanti.**
- Il D.Lgs.81/2008 non esaurisce tutti i requisiti cogenti che un'azienda è tenuta a rispettare, altri requisiti cogenti vanno ricercati a seguito dello svolgimento di altre attività specialistiche che trovano normazione in altre fonti nazionali ed internazionali come ad esempio **le norme CEI.**

Costruzione del SGSL

- Il **responsabile del sistema di gestione per la sicurezza sul lavoro** non è una figura espressamente prevista dalla norma ISO 45001:2018. Dalla lettura della norma e dall'analisi dei requisiti cogenti posti dal D.Lgs. 81/08 una certa **responsabilità finale, assoluta,** cade sempre **in capo all'Alta Direzione (nella Norma) e al Datore di lavoro (nel Decreto).**
- Il sistema tuttavia è un insieme complesso di documenti ed attività il cui funzionamento richiede sicuramente molta attenzione ed il dovuto tempo. Il funzionamento del sistema perciò di solito è affidato ad una persona interna all'azienda che provvede:
  - Alla somministrazione della documentazione
  - All'organizzazione della formazione e dell'addestramento
  - All'organizzazione delle riunioni e delle comunicazioni
  - Al rapporto con gli enti e le istituzioni della sicurezza e della salute sul lavoro
  - Alla distribuzione dei dispositivi di protezione individuale
  - All'organizzazione delle simulazioni di emergenza.
- Con il D.Lgs. 81/08 assume particolare importanza il **Servizio di Prevenzione e Protezione (SPP)** previsto dagli artt. 31,32 e 33. **Il responsabile SPP (RSPP) è la figura che viene ritenuta maggiormente idonea dalle aziende a svolgere il ruolo di responsabile del SGSL della ISO 45001:2018**.

RSPP vs. HSE Manager

- La figura del **Manager HSE** (**Health Security Environment**) sta prendendo sempre più piede all'interno delle aziende come figura di supporto per le tematiche Salute, Sicurezza e Ambiente.
- Si tratta di un'attività professionale che, ad oggi, non risulta essere regolamentata dalla normativa cogente. La norma **UNI 11720:2018** (attiva dal 19 luglio 2018) delinea i requisiti di conoscenza, abilità e competenza del Manager HSE.
- L'importanza della figura del Manager HSE emerge a partire dall'esigenza delle organizzazioni di garantire il rispetto dei requisiti e, al tempo stesso, puntare al miglioramento continuo in ambito HSE.
- In quest'ottica, assume particolare rilevanza l'**integrazione** tra le aree della **prevenzione** e **tutela** della sicurezza sul lavoro e della **protezione** dell'ambiente.
- Vi sono analogie tra il **ruolo** svolto dal **Manager HSE** ed il Responsabile del Servizio di Prevenzione e Protezione (**RSPP**) ma…
- *il **RSPP**, a differenza del Manager HSE , è un soggetto **istituito** dalla normativa cogente. In secondo luogo, svolge un ruolo di natura **consulenziale.***
- *il **Manager HSE**, svolge un ruolo di **carattere gestionale**, in riferimento alle tematiche HSE dal punto di vista degli aspetti legali, normativi, tecnici e relazionali. Inoltre, possiede caratteristiche riferite alla **leadership** e alla **managerialità.***

Efficacia esimente del SGSL

- Nell'ambito della gestione della sicurezza suoi luoghi di lavoro, il datore di lavoro può **incorrere in alcuni reati** in occasione del verificarsi di infortuni.
- Il datore di lavoro infatti deve proteggere la salute e la vita dei suoi lavoratori e per farlo è tenuto a rispettare tutto quello che gli impone la legislazione vigente. Se però accade che un lavoratore subisce un danno a causa di una mancata osservanza dei **requisiti cogenti** da parte del datore di lavoro o del dirigente allora si aprono ipotesi di: **lesioni, lesioni gravissime ed omicidio colposo.**
- In realtà tale individuazione ed attribuzione della colpa è spiegata dal nostro ordinamento attraverso questo ragionamento: se il datore di lavoro avesse fatto tutto quanto previsto dalla normativa cogente allora l'incidente non sarebbe avvenuto.
- L'imprenditore quindi in caso di giudizio deve provvedere con i suoi legali a dimostrare di aver rispettato i requisiti cogenti. Il sistema ISO 45001:2018 tuttavia ha un enorme potere, quello cioè di ribaltare l'onere della prova in capo al pubblico ministero.
- Un **sistema di gestione SGSL** efficacemente attuato e mantenuto, **secondo il D.Lgs. 231/01 che istituisce la responsabilità amministrativa delle imprese**, può costituire un motivo esimente per l'imprenditore accusato di lesioni o di omicidio colposo.
- L'**SGSL** può quindi **esimere l'imprenditore** poiché fornisce evidenza oggettiva che questi ha adempiuto a tutti i requisiti cogenti e il lavoratore invece ha aggirato fraudolentemente il sistema.

Efficacia esimente del SGSL

- Se ad esempio un lavoratore è stato formato, addestrato e motivato all'uso degli otoprotettori in occasione dell'impiego del martello pneumatico e questi non indossa gli otoprotettori eludendo la vigilanza, allora la colpa non cade sul datore di lavoro. Il sistema in questo caso dovrebbe già dimostrare che il datore di lavoro ha fatto tutto quanto possibile affinché il lavoratore non subisse alcun infortunio e non contraesse alcuna malattia professionale.
- **L'efficacia esimente non dipende dalla certificazione ISO del sistema ma dalla scrupolosità con la quale il sistema è stato concepito.** Il consulente che implementa il sistema deve prevedere di dare luce, attraverso la modulistica, a tutti i passaggi che avvengono nello svolgimento delle attività.
- Un sistema documentale ben fatto permette di tracciare le attività e di identificare eventuali responsabilità, non soltanto, ma consente anche di dare evidenza della propria estraneità ai fatti.
- Le **non conformità** più rilevanti che spesso portano ad un coinvolgimento da parte del datore di lavoro nelle vicende legate all'infortunio e alle sue conseguenze sono:
  - Il mancato impiego dei dispositivi di protezione individuale
  - La mancata formazione per i lavoratori a rischio
  - L'assenza della valutazione dei rischi
  - L'impiego di sostanze e tecnologie non più lecite perché ritenute pericolose per l'uomo
  - L'assenza di istruzioni di lavoro in condizioni critiche quali ad esempio il lavoro in solitario

Asseverazione MOG-SSL

- UNI/TR 11709:2018 ”Adozione ed efficace attuazione dei Modelli di Organizzazione e Gestione della salute e sicurezza – Modalità di asseverazione da parte di Organismi Paritetici”
- Gli Organismi Paritetici sono organismi che rappresentano sia le organizzazioni dei Lavoratori che dei Datori di Lavoro comparativamente più rappresentative sul piano nazionale, quali sedi privilegiate per (art. 51):
  - La programmazione di attività formative e l’elaborazione e la raccolta di buone prassi a fini prevenzionistici;
  - Lo sviluppo di azioni inerenti alla salute e alla sicurezza sul lavoro;
  - L’assistenza alle imprese finalizzata all’attuazione degli adempimenti in materia;
  - Ogni altra attività o funzione assegnata loro dalla legge o dai contratti collettivi di riferimento.
- Gli organismi paritetici comunicano annualmente all'Ispettorato nazionale del lavoro e all'INAIL i dati relativi al rilascio delle asseverazioni

Asseverazione MOG-SSL
vantaggi

- **Autotutela delle aziende** che possono essere completamente esonerate dalla responsabilità amministrativa di cui al D.Lgs. n. 231/2001, dal versante reati in materia di salute e sicurezza sul lavoro, in caso di reati commessi da propri collaboratori apicali e/o subordinati in violazione delle regole interne (Modelli Organizzativi conformi a quanto richiesto dalla normativa);
- **Semplificazione organizzativa**, in quanto di fatto implica l'adozione della norma ISO 45001:2018 (e dunque favorisce la realizzazione di un'impostazione organizzativa unitaria e omogenea, col superamento della contemporanea presenza di procedure spesso contrastanti tra loro e non allineate;
- **Limitazione dei rischi** (permette una significativa razionalizzazione dei processi ai fini della riduzione dei rischi);
- **Aumento dell'efficienza aziendale** (agevola la condivisione delle informazioni, rafforzando i flussi informativi interni, e la definizione di attività di controllo sempre più avanzate);
- **Creazione di vantaggi competitivi** (migliora l'immagine dell'azienda nei rapporti con i clienti e con tutti i portatori d'interesse, con conseguente generazione di nuove opportunità di affari, contrattuali, e appalti pubblici);
- **Facilitazione dell'accesso al credito bancario** (la presenza di un efficace Modello Organizzativo è un parametro importante di valutazione per la concessione del credito in base a "Basilea II".

Indice degli argomenti

- Le precondizioni minime per un sistema "sicuro" e il Quadro normativo di riferimento
- La cybersecurity e la direttiva UE 2016/1148 c.d. "direttiva NIS“ – L’Agenzia per la Cybersicurezza Nazionale
- Approccio Metodologico alla Gestione del Rischio secondo ISO 31000
- Il Professionista della Security (Security Manager) ai sensi della UNI 10459:2017
- **Il Modello di Gestione della Sicurezza (MOGS): ambiti di applicazione**
  - cybersecurity: il NIST Cybersecurity Framework (CSF) e il processo di individuazione degli RSL (Required Security Level) – il Framework Nazionale per la Cybersecurity e la Data Protection – ISMS vs. NIST CSF
  - privacy ai sensi del GDPR
  - HSE ai sensi della ISO 45001 (cenni)
  - **tutela responsabilità amm. aziendale ai sensi del D. Lgs. 231/01 (cenni)**

Il modello 231

1. Premesse

- L'art. 6, comma 2, del D.lgs. 231/01 indica le caratteristiche essenziali per la costruzione di un modello di organizzazione, gestione e controllo (MOG).
- Le fasi principali in cui il MOG dovrebbe articolarsi sono le seguenti:

  a) l'identificazione dei rischi potenziali: ossia l'analisi del contesto aziendale per individuare in quali aree o settori di attività e secondo quali modalità si potrebbero astrattamente verificare eventi pregiudizievoli per gli obiettivi indicati dal D.lgs. 231/01. *Per "rischio" si intende qualsiasi variabile o fattore che nell'ambito dell'azienda, da soli o in correlazione con altre variabili, possano incidere negativamente sul raggiungimento degli obiettivi indicati dal D.lgs. 231/01* (in particolare all'art. 6, comma 1, lett. a); pertanto, a seconda della tipologia di reato, gli ambiti di attività a rischio potranno essere più o meno estesi.

  Per esempio, in relazione al rischio di omicidio colposo o lesioni colpose gravi o gravissime commessi con violazione delle norme in materia di salute e sicurezza sul lavoro, l'analisi dovrà verosimilmente estendersi alla totalità delle aree ed attività aziendali;

[fonte: Confindustria, Linee Guida per la costruzione dei Modelli di Organizzazione , Gestione e Controllo]

Il modello 231

b) la progettazione del sistema di controllo (cd. "protocolli" per la programmazione della formazione e attuazione delle decisioni dell'ente), ossia la valutazione del sistema esistente all'interno dell'ente per la prevenzione dei reati ed il suo eventuale adeguamento, in termini di capacità di contrastare efficacemente, cioè ridurre ad un livello accettabile, i rischi identificati.

Sotto il profilo concettuale, ridurre un rischio comporta di dover intervenire - congiuntamente o disgiuntamente - su due fattori determinanti:

i) la probabilità di accadimento dell'evento e

ii) l'impatto dell'evento stesso.

- Il sistema delineato, per operare efficacemente, deve tradursi in un processo continuo o comunque svolto con una periodicità adeguata, da rivedere con particolare attenzione in presenza di cambiamenti aziendali (apertura di nuove sedi, ampliamento di attività, acquisizioni, riorganizzazioni, modifiche della struttura organizzativa, ecc.), ovvero di introduzione di nuovi reati presupposto della responsabilità dell'ente in via normativa.

[fonte: Confindustria, Linee Guida per la costruzione dei Modelli di Organizzazione , Gestione e Controllo]

Il modello 231

2. La definizione di "rischio accettabile"

- **Nel caso del decreto 231 del 2001 la logica economica dei costi non può però essere un riferimento utilizzabile in via esclusiva**. È pertanto importante che ai fini dell'applicazione delle norme del decreto sia definita una soglia effettiva che consenta di porre un limite alla quantità/qualità delle misure di prevenzione da introdurre per evitare la commissione dei reati considerati. In assenza di una previa determinazione del rischio accettabile, la quantità/qualità di controlli preventivi istituibili è, infatti, virtualmente infinita, con le intuibili conseguenze in termini di operatività aziendale.
- Del resto, il generale principio, invocabile anche nel diritto penale, dell'esigibilità concreta del comportamento rappresenta un criterio di riferimento ineliminabile anche se, spesso, appare difficile individuarne in concreto il limite.

[fonte: Confindustria, Linee Guida per la costruzione dei Modelli di Organizzazione , Gestione e Controllo]

Il modello 231

- Riguardo al sistema di controllo preventivo da costruire in relazione al rischio di commissione delle fattispecie di reato contemplate dal D.lgs. 231/01, la soglia concettuale di accettabilità, nei casi di reati dolosi, è rappresentata da un:

sistema di prevenzione tale da non poter essere aggirato se non FRAUDOLENTEMENTE

- Questa soluzione è in linea con la logica della "elusione fraudolenta" del modello organizzativo quale esimente espressa dal decreto 231 ai fini dell'esclusione della responsabilità amministrativa dell'ente (art. 6, comma 1, lett. c, "le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione").

[fonte: Confindustria, Linee Guida per la costruzione dei Modelli di Organizzazione , Gestione e Controllo]