Rischio digitale Innovazione e Resilienza

Conoscere, affrontare e mitigare il rischio digitale

Clusit Community For Security

Digital Risk

L'unico modo di fare un salto di qualità, per noi professionisti di Information Security, è quello di parlare la lingua del business facendo l'analisi e la gestione del rischio. E' una opportunità per ottenere la giusta attenzione e le risorse necessarie a fronte di decisioni sostenibili in maniera razionale. Non investo perché è obbligatorio (GDPR). Non investo perché sennò fanno tanto male (ransomware). Investo perché è razionale farlo (considerando tutto)!

Alessandro Vallega
Founder e chairman della Clusit Community for Security

Sommario

1. Executive summary

L'obiettivo di questa pubblicazione si può riassumere con un semplice slogan: "conoscere, affrontare e mitigare il rischio digitale". Con rischio digitale intendiamo quella specifica tipologia di rischio a cui sono esposti dati e servizi digitalizzati e che generalmente si esprimono come conseguenza o attraverso l'utilizzo di tecnologie di carattere digitale.

Il testo offre una panoramica su temi quali l'analisi del rischio, la sua utilità e gli elementi normativi che la regolamentano. Particolare attenzione viene data all'importanza di procedere con un approccio integrato al rischio incentrato sui processi, in coerenza con la missione e il modello organizzativo adottato, al fine di gestire i rischi a difesa degli interessi di tutti gli stakeholder.

Il tema dell'analisi del rischio, e nello specifico del rischio digitale, è di prioritaria importanza oggi in una società ove il digitale assume una rilevanza sempre più marcata e le tipologie dei rischi evolvono nel tempo in relazione al cambiamento della società in generale, dei mercati e delle tecnologie. Le minacce di cybersecurity, secondo le più recenti statistiche, sono considerate in cima alla lista dei rischi d'impresa[1].

Nell'Introduzione, al capitolo 4, si fa un cenno alle tipologie di rischi digitali e alle relazioni fra rischi digitali e sostenibilità.
Nel capitolo 5, è quindi descritto il processo di valutazione dei rischi digitali. Le attività cardine dovranno prevedere la mappatura dei processi, assegnando importanza alla catena di fornitura, l'analisi del contesto e dei rischi, l'identificazione dei controlli di mitigazione definiti nei framework di riferimento e la realizzazione del piano di trattamento del rischio.
La valutazione del rischio può basarsi su un approccio qualitativo, quantitativo o misto. Occorre quindi scegliere l'approccio più adeguato al contesto e all'organizzazione.
Viene posto l'accento, infine, sulla necessità di comunicare in modo efficace il risultato dell'analisi, soprattutto ai vertici dell'organizzazione. È necessario il riesame periodico delle misure adottate in funzione di possibili nuove minacce, dei nuovi servizi erogati dall'organizzazione e dei cambiamenti del contesto.
Tutte queste attività vanno ripetute nel tempo per verificare l'efficacia delle azioni intraprese e tendere al miglioramento, senza dimenticare l'importanza di apprendere dall'esperienza e dagli incidenti.
Nel capitolo 6 sono citate le normative relative alla valutazione dei rischi digitali che

1 World Economic Forum. The Global Risks Report 2021, 16th Edition. S.l.: World Economic Forum, 2021. https://www.weforum.org/reports/the-global-risks-report-2021

interessano tutte le organizzazioni o solo alcuni settori, inclusi quelli regolamentati come banche, assicurazioni e sanità. Fra le normative di interesse per tutte le organizzazioni si fa riferimento a quelle relative alla privacy (GDPR e futuro regolamento ePrivacy dedicato alle comunicazioni elettroniche), ai servizi essenziali (Direttiva NIS e PNSC), all'intelligenza artificiale (Regolamento attualmente in bozza ed oggetto di discussione), alla responsabilità amministrativa degli enti (D.lgs 231/2001). Fra le normative che interessano settori specifici, sono discusse quelle relative ai dispositivi medicali, alla finanza digitale (Regolamento DORA), ai servizi di pagamento (PSD2), ai servizi fiduciari (Regolamento EIDAS), alle assicurazioni (regolamento IVASS N. 38), ai servizi digitali (Digital service ACT), al settore bancario (Circolare 285 di Bankit).
Il quadro che si presenta è assai articolato, se prendiamo in considerazione anche i rischi gestionali che ogni organizzazione deve affrontare quotidianamente. Ne deriva l'importanza di adottare un approccio integrato con soluzioni metodologiche e organizzative adeguate, di seguito indicate a livello preliminare. Per rafforzare l'importanza dell'adozione di un approccio integrato, nel capitolo 7 sono descritti alcuni dei più diffusi framework e good practice internazionali di analisi dei rischi.
Alcuni di essi non solo hanno contribuito in modo significativo a determinare un sostanziale incremento della consapevolezza da parte dei vertici delle organizzazioni, ma hanno altresì accresciuto attenzione e sensibilità nella gestione efficace dei rischi, influendo direttamente sulle capacità di raggiungere gli obiettivi stabiliti, come evidenziato nelle esperienze di adozione dei framework descritte in questa stessa pubblicazione.
Segue, nel capitolo 8 una sezione dedicata ai rischi legati a specifiche tecnologie o contesti applicativi quali per esempio intelligenza artificiale, cloud computing, Internet of things (IoT), operational technology (OT) e industriale, smart building, sanità e 5G.

Infine, il lettore potrà trovare link di approfondimento ai numerosi argomenti trattati nel testo.

2. Per chi abbiamo scritto questo libro

Questa pubblicazione nasce allo scopo di richiamare l'attenzione sulla corretta gestione del rischio digitale in tutte le organizzazioni, pubbliche e private, spesso connotate da una peculiarità di interconnessioni con soggetti diversi (una fra tutti costituisce la cosiddetta "filiera dei fornitori") che meritano di essere analizzate compiutamente.

Nell'attuale momento storico, le PA giocano un ruolo fondamentale per lo sviluppo della società, per il rilancio economico e sociale del paese e per la realizzazione di nuovi progetti e investimenti anche collegati al PNRR. Esse contribuiscono in modo determinante alla realizzazione dell'agenda digitale europea e italiana e a creare fiducia nei cittadini e nelle imprese sui servizi pubblici che devono quindi essere accessibili e sicuri.
Nonostante la grande spinta propulsiva in materia di trasformazione digitale e in materia di sicurezza informatica promossa a livello normativo negli ultimi anni dal governo, dai ministeri competenti, da AgID (Agenzia per l'Italia digitale) e dalla nuova Agenzia per la cybersicurezza nazionale (ACN), ancora oggi molte pubbliche amministrazioni mostrano debolezze, criticità e limiti nell'erogazione di servizi affidabili e sicuri a causa della mancata consapevolezza del valore delle informazioni e degli asset strategici e quindi dell'assenza di processi di gestione del rischio digitale. La diffusione della cultura della sicurezza al livello dei vertici e l'adozione all'interno delle PA di processi governati e integrati di gestione del rischio e della sicurezza digitale possono contribuire in modo fondamentale al raggiungimento degli obiettivi a cui sono chiamate le pubbliche amministrazioni nell'interesse primario del singolo cittadino.

Nel comparto privato, invece, al di là della dimensione, è necessario evitare di considerare i dati e la tecnologia solo come meri strumenti per incrementare i propri introiti: essi devono essere valutati e gestiti sistematicamente e in modo sicuro così da sfruttarne ogni beneficio senza ledere gli interessi degli stakeholder. Ad esempio, la riduzione dei rischi di sicurezza non previene solo i danni diretti e indiretti e i costi correlati a sanzioni e richieste di risarcimento, ma mette a disposizione anche tante opportunità: attrattiva per nuovi clienti, fidelizzazione di quelli già esistenti, aumento di reputazione, creazione di nuove sinergie di mercato, valorizzazione dei dati gestiti attraverso i propri sistemi informativi e l'accesso a fondi pubblici e investimenti privati (si pensi che nel 2020 il 70% delle organizzazioni che ha predisposto un modello organizzativo per la protezione dei dati personali ha ottenuto vantaggi pari al doppio degli investi-

menti iniziali[2]).

Se multinazionali e aziende di grandi dimensioni sono già strutturate e dispongono dei mezzi per fronteggiare le trasformazioni necessarie, il comparto delle startup, delle microimprese e delle PMI fatica ancora ad avere piena consapevolezza del mondo digitale (a oggi, nell'ambito dell'innovazione dell'Unione Europea, le nostre aziende sono ancora al di sotto della media degli altri Stati membri[3]).
Le cause principali? Scarsa consapevolezza e volontà nell'abbandonare i sistemi organizzativi tradizionali, mancanza di capacità specifiche nell'operare la trasformazione digitale, oltre alla frammentarietà delle soluzioni tecnologiche, offerte dai grandi fornitori, e al discontinuo supporto di finanziamenti dedicati. Lo scenario delineato è abbastanza allarmante e denota come queste lacune debbano essere colmate al più presto, visto che, in Italia, tali organizzazioni sono circa 4,5 milioni e rappresentano quasi l'80% del tessuto economico nazionale.
Trasformazione, cambiamento e tecnologia comportano senz'altro l'essere pronti ad affrontare nuove sfide, ma proprio per questo è importante comprenderne la portata, conoscerne e saperne gestire gli impatti, attraverso una piena consapevolezza di rischi ed opportunità.
A seconda della tipologia e dimensione dell'organizzazione, la gestione del rischio è strutturata in modo diverso: nelle grandi organizzazioni sono presenti processi strutturati e unità organizzative dedicate alla gestione del rischio, mentre in genere nelle piccole imprese i processi di gestione del rischio sono gestiti da gruppi informali.

Questo libro presenta una compiuta disamina degli aspetti legali, tecnici e di gestione del rischio connessi ai diversi ambiti in cui la tecnologia e il digitale sono coinvolti, con l'intento di dare supporto a più segmenti di mercato possibili.
A beneficiare della lettura di questo testo saranno i vertici delle organizzazioni, inclusi: la proprietà, il CdA, il CEO (Chief executive officer) e CFO (Chief financial officer). Essi infatti giocano un ruolo fondamentale nel perseguimento degli obiettivi e potranno sviluppare la consapevolezza sul tema e gli elementi utili per garantire e vigilare affinché la gestione del rischio sia correttamente ed effettivamente affrontata. Il vertice è chiamato a:

- identificare gli obiettivi strategici di sviluppo;
- assegnare le responsabilità nelle aree di rischio in esame;
- attribuire le risorse economiche e di personale necessarie alla gestione del rischio;

2 https://www.corrierecomunicazioni.it/privacy/data-protection-leva-di-business/.

3 IFA. La digitalizzazione delle piccole e medie imprese in Italia: Modelli per il finanziamento di progetti digitali - Relazione di sintesi. S.l.: Banca europea per gli investimenti (BEI), 2021. https://cotec.it/wp-content/uploads/2021/05/Report_digitalisation_of_smes_in_italy_summary_it.pdf.

- definire e assegnare gli indicatori di prestazione;
- assicurare la comunicazione a tutti i soggetti interessati sulle scelte effettuate e sui vantaggi attesi;
- promuovere la partecipazione e la comunicazione verso tutta l'organizzazione, in modo da contribuire a un clima di fiducia.

Il libro sarà inoltre un'utile lettura per le altre figure con responsabilità più operative e di supporto al vertice, per esempio CIO (Chief information officer), CISO (Chief information security officer), Risk manager, IT risk manager, i Data protection officer e, nell'ambito pubblico, i Responsabili per la transizione al digitale.

3. Community e licenza

Questa è la tredicesima pubblicazione della Clusit Community for Security, senza contare il blog dedicato al Regolamento europeo sulla protezione dei dati personali, con alcune centinaia di post in italiano e in inglese fatti ben prima che il testo del regolamento fosse definitivo.

Gli autori svolgono il lavoro di preparazione tramite un confronto multidisciplinare e multisettoriale. Li motiva la consapevolezza del grande bisogno di sicurezza e compliance delle organizzazioni italiane e un forte senso di responsabilità verso la nostra società. La Community opera dal 12 settembre 2007 e permette la collaborazione di alcune centinaia di professionisti che operano negli ambiti della sicurezza, dell'audit, della conformità, dell'ethical hacking, della consulenza, dell'integrazione dei sistemi e delle certificazioni basate su norme internazionali. Partecipano alla Community i responsabili della sicurezza del mondo della domanda e dell'offerta di servizi e tecnologie correlati a questi ambiti. Il lavoro verte su molteplici aspetti: culturale, organizzativo e tecnologico. La Community riceve il sostegno di prestigiose associazioni professionali e industriali che collaborano attivamente tramite i loro membri, come per esempio: ABI Lab, ACFE, AIEA, AISIS, ANDIP, ANRA, ANORC, APIHM, AUSED, BCI Italy Chapter, CSA Italy, ISACA VENICE, (ISC)².

Le pubblicazioni fatte finora sono liberamente scaricabili dal sito http://c4s.clusit.it e sono:

- ROSI - Return on Security Investments: un approccio pratico. Come ottenere Commitment sulla Security;
- Fascicolo Sanitario Elettronico: il ruolo della tecnologia nella tutela della privacy e della sicurezza;
- Privacy nel Cloud: Le sfide della tecnologia e la tutela dei dati personali per un'organizzazione italiana;
- Mobile e Privacy: Adempimenti formali e misure di sicurezza per la conformità dei trattamenti di dati personali in ambito aziendale;
- La sicurezza nei Social Media: guida all'utilizzo sicuro dei Social Media per le aziende del Made in Italy;
- I primi 100 giorni del responsabile della Sicurezza delle Informazioni: Come affrontare il problema della Sicurezza informatica per gradi;
- Le frodi nella rete: il duplice ruolo dell'ICT;
- Mobile Enterprise: sicurezza in movimento;

- SOC e Continuous Monitoring faccia a faccia con la Cybersecurity;
- Consapevolmente Cloud. Guida per l'azienda che deve affrontare l'innovazione con le idee chiare;
- IoT Security e Compliance. Gestire la complessità e i rischi;
- Intelligenza artificiale e sicurezza: opportunità, rischi e raccomandazioni.

Queste pubblicazioni sono il frutto del lavoro di almeno 50 persone e consistono in 100-200 pagine di materiale. Consci che tutto è migliorabile, e nel pieno spirito della Community, le rendiamo disponibili con una licenza "Creative Common, Attribuzione e Condividi nello stesso modo" (https://creativecommons.org/licenses/by-sa/4.0/). La licenza permette a chiunque di usare il nostro prodotto per crearne una sua evoluzione a condizione che citi gli autori originali riportando la nostra URL http://c4s.clusit.it e utilizzi a sua volta lo stesso tipo di licenza.

4. Introduzione

Spesso ci si riferisce a una definizione di rischio in termini di eventualità di subire un danno oppure di godere di un vantaggio in conseguenza di un'azione, compiuta o subita. Spesso si limita il concetto di rischio alla sola eventualità di subire un danno, e così sarà fatto nel seguito. La possibilità di godere di un vantaggio è solitamente indicata con il termine di *opportunità*. Ci alziamo la mattina, facciamo colazione e usciamo di casa. Per lavoro o nel tempo libero ci spostiamo con i mezzi pubblici, con l'auto, prendiamo un aereo, andiamo a piedi. Quasi ogni azione che compiamo comporta una scelta e, associato a questa, un rischio, piccolo o grande che sia. A volte agiamo in maniera istintiva senza neppure rendercene conto, a volte in maniera ponderata valutando le alternative. Anche le scelte economiche, gli investimenti, la decisione se aprire un mutuo comportano una scelta e un rischio.

Si potrebbe pensare che riducano il rischio scelte quali: il non agire, il restare fermi, il non far niente, l'evitare le scelte o il prendere la via più semplice che comporta meno sforzo. In casi particolari è possibile che questo approccio funzioni, ma non è una regola generale. Anche nel non scegliere e restare fermi esiste un rischio.
Ad esempio, torniamo alla nostra colazione: anche consumare o preparare del cibo ha dei rischi. Rischi alimentari se il cibo non è di buona qualità o se ha elementi allergenici fino a quel momento sconosciuti. Oppure rischi di incolumità fisica se usiamo una centrifuga montata male. Il rischio quindi è insito nella natura delle cose e ci possono essere elementi che lo aumentano o diminuiscono.

Esiste anche un altro aspetto da considerare. Spesso i cambiamenti importanti, in ambito personale come in qualsiasi altro ambito, possono comportare un vantaggio, un miglioramento, un guadagno. Però ogni cambiamento comporta un rischio. Si tratta di ponderare il rischio rispetto al potenziale vantaggio e decidere. In casi semplici possiamo basarci sull'istinto, sul sesto senso. In casi più complessi questo non è sufficiente. Esistono rischi che non dipendono dalle nostre scelte, ma che sono insiti nelle situazioni, che possono presentarsi e che in generale derivano da circostanze esterne a noi, che non possiamo controllare. Non per tutti è possibile fare una previsione ragionevole, alcuni possono essere dei cosiddetti "cigni neri", ossia presentarsi come fenomeni apparentemente non prevedibili.

Il rischio è quindi un fattore presente in ogni attività e processo, che può sfociare tanto in una situazione di crisi quanto in una svolta positiva.
L'analisi del rischio può essere sintetizzata con una semplice domanda: 'what if ...?' Chiedersi cosa può accadere a fronte di un evento (normalmente avverso, ma non

necessariamente) in modo da cercare anche delle risposte, ovverosia chiedersi cosa sia più opportuno fare al verificarsi dell'evento o per prevenirlo.
L'esempio più intuitivo è quello della continuità operativa: si valutano i potenziali eventi avversi e, conseguentemente, si progettano le relative soluzioni organizzative e tecnologiche in modo da affrontare le criticità con tranquillità e metodo, senza spreco di risorse e senza che nell'emergenza vengano compiute azioni controproducenti (in altre parole, la valutazione del rischio non porta necessariamente a una diminuzione dei costi, ma alla loro preventivazione e al loro controllo in modo che siano minimizzati).

L'analisi del rischio quindi è una disciplina importante, anzi fondamentale alla base della sicurezza e della continuità delle organizzazioni, per la quale sono disponibili strumenti, metodologie e tecniche. È ormai inserita in tutte le più importanti norme, tra cui le ISO, e in alcuni dispositivi di legge come elemento fondamentale all'interno del ciclo virtuoso del miglioramento continuo e della responsabilizzazione. Infatti, oggi è pratica comune basare le scelte e le strategie di miglioramento sui risultati di una valutazione del rischio.

4.1 Come sono cambiati i rischi negli ultimi anni

Sono nel seguito presentati i risultati di alcune indagini sulla percezione del rischio a livello globale che forniscono una panoramica di alto livello sui rischi ritenuti più significativi. I report evidenziati offrono uno spaccato estremamente utile ma rimangono pur sempre una previsione non esaustiva sul breve e medio periodo. La storia e la quotidianità insegnano drammaticamente che alcuni eventi sono imprevedibili.

4.1.1 Il Global Risk Report

Il Global Risk Report, giunto nel 2021 alla sua sedicesima edizione, viene curato da un gruppo di compagnie assicurative e viene successivamente presentato in occasione della conferenza internazionale organizzata dal World Economic Forum.

La metodologia adottata prevede la valutazione secondo una scala qualitativa delle

componenti di probabilità di accadimento e degli impatti al fine di calcolare il livello di rischio; il processo si svolge attraverso un ciclo di interviste denominato “Global Risk Perception Survey” somministrate a un gruppo di persone selezionato su base globale, composto da oltre 800 rappresentanti di primissimo livello appartenenti alle istituzioni, al mondo universitario, ad aziende multinazionali.
Ai soggetti che rappresentano il campione dell’indagine viene richiesto di indicare il livello di percezione, rispetto a un orizzonte temporale di breve, medio e lungo termine, dei rischi presentati nelle seguenti categorie: economici, ambientali, geopolitici, legati alla società, tecnologici.

Nella seguente figura è rappresentato lo spaccato specifico per i rischi tecnologici, offrendo un’indicazione di impatto, probabilità (*likelihood*).

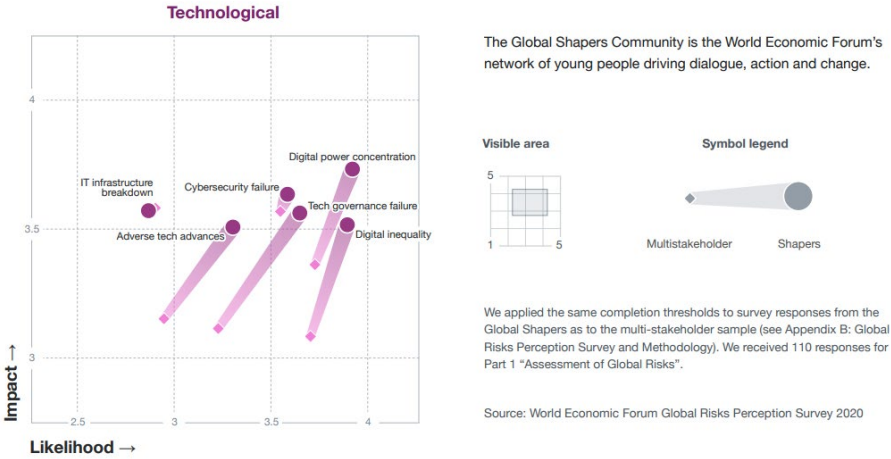

Figura 1 –Rischi tecnologici per il Global Risk Report del 2021[4]

In generale, considerando tutte le diverse categorie, si nota un ovvio balzo in avanti del rischio “Sviluppo di eventi pandemici”, precedentemente sottostimato.
Nel corso degli ultimi anni si è registrata una presenza stabile, fra i rischi ritenuti più significativi, di quelli ambientali (“Eventi naturali estremi” e “Cambiamenti climatici”) mentre si è assistito a un significativo incremento dei rischi di natura tecnologica quali gli “Attacchi di cybersecurity” e “Indisponibilità delle infrastrutture critiche”.

4 World Economic Forum. The Global Risks Report 2021, 16th Edition. S.l.: World Economic Forum, 2021. https://www.weforum.org/ reports/the-global-risks-report-2021.

4.1.2 Allianz Risk Barometer

L'Allianz Risk Barometer 2021[5] segnala, come prevedibile, la crescita dei rischi connessi a eventi pandemici, quali l'interruzione del business, i problemi operativi e organizzativi derivanti dalla pandemia, le difficoltà nello sviluppo dei mercati.

Il documento segnala la crescita di importanza dei rischi legati ad aspetti macroeconomici e di tipo politico e di violenza sociale. Rischi relativi a problemi storicamente più noti, come quelli legislativi, di catastrofi naturali, d'incendio, di esplosione e di variazioni climatiche, perdono posizione in graduatoria.

È interessante notare, a dimostrazione che il contesto è un elemento fondamentale dell'analisi del rischio, che i Paesi più orientati alla produzione di beni abbiano mediamente percepito come rischio principale quello relativo alla pandemia e alla conseguente indisponibilità di manodopera per la produzione e per i servizi logistici.

Al contrario, i Paesi più orientati al terziario hanno percepito come primario il rischio relativo alla *cybersecurity*. I Paesi industrializzati con produzione abbastanza consolidata hanno invece percepito come maggiormente critico il rischio di interruzione del business.

4.1.3 Emerging Risks Initiative (CRO Forum)

Il report "Emerging Risk Initiative – Major Trends and Emerging Risk Radar" del CRO Forum è interessante soprattutto per quanto riguarda l'attenzione ai nuovi rischi.

In particolare, nell'ultimo aggiornamento del 2020 sono stati identificati tre nuovi rischi emergenti: la mancanza di competenze su tematiche innovative, rischi ambientali e di salute legati alle materie plastiche, la disinformazione digitale, ossia il proliferare di notizie false (fake news).

Il radar sui rischi emergenti analizza varie tipologie di rischio, creando una classifica distinguendoli fra rossi, arancioni e gialli a seconda del potenziale impatto.

5 https://www.allianz.com/en/economic_research/publications/specials_fmo/2021_01_19_AllianzRiskBarometer2021.html.

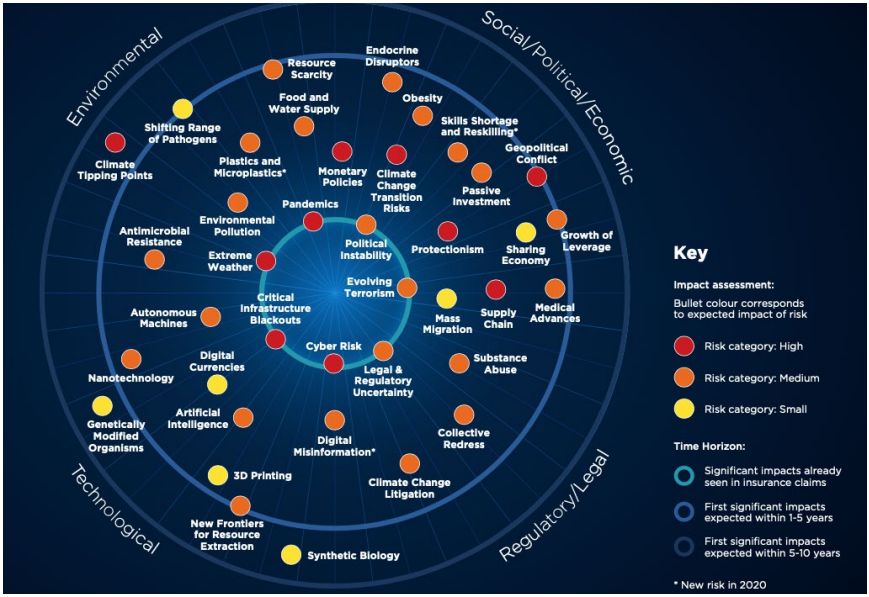

Figura 2 - Radar del "Emerging Risks Initiative" del 2020[6]

Nel rapporto sono stati evidenziati:

- i rischi legati al cambiamento climatico e alla transizione energetica, che si distinguono per la presenza di soglie di non ritorno, prossime a essere superate;
- i blackout critici delle infrastrutture, che, messe a dura prova da crescita demografica e tecnologica, potrebbero rendere le infrastrutture esistenti presto inadeguate;
- i rischi cyber;
- i conflitti geopolitici, sempre più gravi e rischiosi per l'umanità;
- i rischi legati alle politiche monetarie ed economiche, con particolare attenzione a fenomeni di ripresa inflazionistica e al ritorno a politiche protezionistiche;
- il rischio pandemico, già evidenziato a partire dal 2007 e ritenuto probabile anche in futuro;
- i rischi legati alla *supply chain*, sempre più tecnologica e globalizzata, che permette una riduzione dei costi e dei tempi, ma fragile per la dipendenza da settori e aree geografiche specifiche.

6 CRO Forum. Emerging Risks Initiative: Major Trends and Emerging Risk Radar - 2021 Update. S.l.: CRO Forum, 2021. https://www.thecroforum.org/2021/06/30/emerging-risk-initiative-major-trends-ans-emerging-risk-radar-2021-update/.

Intervista a Carlo Cosimi, Presidente ANRA, Head of Corporate Insurance and Risk Financing di Saipem S.p.A.

D. Stiamo vivendo in un mondo caratterizzato da un processo accelerato di digitalizzazione e innovazione. Inoltre assistiamo a un considerevole aumento di attacchi cyber. Pertanto diventa sempre più necessario saper gestire i rischi o, meglio, anticiparli. ANRA rappresenta, come associazione, un punto di riferimento per le organizzazioni a livello nazionale, oltre che osservatorio privilegiato. Come si è evoluta la figura del risk manager e quali caratteristiche dovrà avere in futuro per gestire al meglio il rischio cyber?

R. La figura del risk manager è in continua evoluzione e sta assumendo nelle organizzazioni un ruolo sempre più apicale e strategico. A questa evoluzione hanno sicuramente contribuito in maniera determinante le accelerazioni tecnologiche e le digitalizzazioni dei processi in atto. Tra i rischi strettamente correlati a questa trasformazione digitale quelli legati ai rischi cyber rivestono un ruolo sempre più critico e che stanno avendo una esposizione crescente, sia in termini di frequenza che di impatto.
In questo quadro il risk manager sta evolvendo e ampliando l'ambito delle proprie competenze e responsabilità supportando il presidio specialistico della funzione IT. Molte aziende hanno già separato, rispetto al passato, la funzione Operational IT dalla funzione Security IT. Con quest'ultima funzione, in particolare, la relazione con il risk manager diviene continua e indispensabile per una comune comprensione dei rischi, la loro misurazione, trattamento e trasferimento assicurativo. Si può dire che il risk manager stia acquisendo maggiori conoscenze tecnico informatiche mentre i colleghi della Security IT maggiori conoscenze sulle modalità di misurazione economica degli impatti. Il sistema di governance e di resilienza dell'azienda ne uscirà molto rafforzato.

D. Cosa sta facendo ANRA per supportare le organizzazioni in termini di diffusione della cultura del rischio e, in particolare, quello cyber?

R. ANRA, per la sua natura e finalità, si rivolge primariamente ai propri associati e non direttamente alle organizzazioni. I nostri associati sono ovviamente inseriti negli organigrammi di vertice delle principali aziende oppure operano come consulenti per le grandi, medie e piccole aziende. ANRA aiuta, dunque, i risk manager associati a formarsi, aggiornarsi, condividere le migliori pratiche ed esperienze sui diversi rischi, inclusi quelli informatici.
Nella nostra recente esperienza abbiamo visto crescere l'attenzione e l'interesse per una formazione su queste tematiche e tutte le iniziative che abbiamo organizzato come webinar hanno riscontrato un successo record, tanto da obbligarci a rimodulare questi approfondimenti sul rischio cyber con una serie di appuntamenti che è stata chiamata l'"Accademia del Cyber".

D. ANRA recentemente ha contribuito a una Cyber risk survey per analizzare la percezione e le strategie di cyber risk management adottate dalle aziende. Come stanno rispondendo le aziende, quale fotografia si sta delineando?

R. La Cyber Risk Survey 2021 è stata realizzata dall'Università di Verona con la collaborazione di Riesko e ANRA e si è focalizzata sull'analisi e valutazione dei rischi informatici percepiti dalle organizzazioni, oltre che sullo studio degli approcci manageriali adottati dalle imprese per mitigare il cyber risk nelle piccole, medie e grandi imprese italiane.

L'indagine è stata condotta attraverso un questionario con il fine di comprendere, sia da un punto di vista qualitativo che quantitativo, quali siano gli strumenti e le strategie adottate dalle imprese per mitigare il rischio informatico, quale sia lo stato di consapevolezza delle imprese stesse e il loro approccio al rischio, e infine quali siano stati i principali danni sofferti dalle imprese in termini economici, reputazionali e operativi.

L'indagine ha visto coinvolte nella risposta 247 aziende e ha visto il 61% rispondenti in ruoli apicali (Imprenditore o Ceo per il 23%) o C-Level della funzione IT e IT Security (38%), con un'anzianità media in azienda superiore, per il 79%, ai 5 anni.
Dall'analisi condotta emerge che il 64% dei rispondenti utilizza il supporto di società esterne per i servizi di sicurezza informatica e il 75% considera il rischio cyber come un rischio "chiave" nella propria realtà aziendale. In particolare, mentre il 45% lo considera un rischio IT, altri lo considerano un rischio operativo (22%) e strategico (14%) per le proprie organizzazioni.

Il 43% dei rispondenti ha dichiarato che l'impresa in cui opera adotta sistemi di protezione e tecniche di mitigazione adeguate, dato coerente con il 60% che ha dichiarato di aver subito attacchi senza conseguenze per l'attività operativa. Il 70% ammette che l'impresa ha subito almeno un attacco informatico negli ultimi 12 mesi. La fotografia che se ne ricava vede, dunque, che, a fronte dell'impennata nella frequenza degli attacchi cyber, si registra un incremento nella capacità di resilienza delle imprese dal momento che tali attacchi solo in pochissimi casi hanno prodotto danni o serie conseguenze.

Nel 50% delle imprese intervistate, la formazione dei dipendenti sui temi della sicurezza informatica è ricorrente e strutturata. Viene infine evidenziato che attualmente i budget destinati alla difesa e resilienza dal rischio informatico arrivano, al massimo, al 30% del budget annuale mentre poco più del 50% degli intervistati dichiara di ricorrere al trasferimento assicurativo per fronteggiare il rischio cyber.

4.2 L'importanza della valutazione del rischio

L'analisi del rischio porta i vertici dell'organizzazione a fare scelte e decidere dove allocare le risorse, concentrando gli sforzi in modo efficace sulle reali criticità.

L'analisi del rischio è diventata una priorità per le organizzazioni, non solo nei settori per i quali il rischio ha sempre giocato un ruolo rilevante, come nelle assicurazioni e nelle banche, ma in tutti i settori, dall'industria privata alla PA.
La rilevanza del rischio nella singola organizzazione è in funzione delle caratteristiche dei mercati in cui opera (nel caso di un'impresa) e dei servizi erogati (nel caso di una PA), delle tecnologie adottate, e, in generale, delle minacce presenti nello svolgimento dei processi e delle crescenti implicazioni di conformità.

Nel caso di un'impresa, il livello di rischio è un fattore che influisce in modo significativo sul suo valore considerato nei progetti di fusione e acquisizione[7] e che ne condiziona la sostenibilità nel tempo, come indicato nelle recenti linee guida[8] prodotte da FERMA (Federation of European risk manager association). In questo contesto, il rischio digitale, oggetto della nostra pubblicazione, assume una crescente importanza, considerando la pervasività dell'informatica nella gestione delle organizzazioni.
Al presente sono soprattutto le incombenti e crescenti implicazioni di conformità a richiamare l'attenzione dei vertici delle organizzazioni. Se diamo un veloce sguardo ai Regolamenti europei pubblicati dal 2016 e a quelli in fase avanzata di gestazione (ai quali è dato ampio spazio nel seguito), come ad esempio il regolamento ePrivacy e quello sull'intelligenza artificiale che introducono nuove categorie di rischio, ci rendiamo conto che il rischio non è un'appendice dei Regolamenti ma ne è un'asse portante.
I vertici delle organizzazioni non possono chiamarsi fuori limitandosi a delegare ai collaboratori le analisi di rischio e i relativi progetti di mitigazione, senza garantire un adeguato controllo degli stessi. Questo perché è importante soddisfare le attese degli stakeholder, degli azionisti, dei dipendenti, dei clienti, dei fornitori, delle parti sociali.
E proprio per essere responsabile, l'organizzazione deve garantire un'efficace gestione del rischio.

Questi concetti non sono nati all'improvviso per una intuizione di pochi, ma si sono progressivamente costruiti nel tempo. Un contributo molto importante l'ha dato il "Report CoSO", pubblicato nella sua prima versione nel 1992[9] e centrato sui valori di integrità e trasparenza. In altre parole il rischio è il collante dei sistemi di controllo interni, da cui scaturisce un'analisi di processi, una valutazione degli stessi e un miglioramento dell'organizzazione in un'ottica di trasparenza e di supervisione dei processi.
E' pertanto fondamentale individuare e classificare i processi che possono essere oggetto di minacce al loro funzionamento e al rispetto dei vincoli di compliance. Al riguardo è indispensabile segnalare che, da anni, per le società quotate, un Codice di autodisciplina, mutuato dal preesistente Codice Preda, richiede la costituzione di un

7 Thomas E. Copeland, Tim Koller, Jack Murrin. Il valore dell'impresa. Strategie di valutazione e gestione. Italia: Il Sole 24 Ore, 2002.

8 https://www.ferma.eu/app/uploads/2021/03/Ferma-sustainability_2021_final.pdf.

9 Price Waterhouse Coopers. Il sistema di controllo interno. Un modello integrato di riferimento per la gestione dei rischi aziendali. Italia: Il Sole 24 ore, 2004.

Comitato Rischi all'interno della società e la pubblicazione annuale dei risultati delle analisi di rischio nella relazione di Corporate Governance destinata agli azionisti. Analogo approccio è adottato dalle società appartenenti a settori regolamentati come banche e assicurazioni, che seguono regolamenti specifici pubblicati da Banca d'Italia e IVASS (l'Istituto per la vigilanza sulle assicurazioni), in coerenza con le normative internazionali di settore quali Basilea e Solvency. Per tali aziende e per le grandi imprese non quotate, si sta assistendo alla progressiva nomina di Risk manager, che coordinano le attività di gestione del rischio insieme ai responsabili di processo o di funzione, applicando la metodologia identificata come CRSA-Control risk self assessment10.

Per le altre organizzazioni non esiste una prassi formale da seguire, ma la gestione del rischio è in molti casi un adempimento normativo cogente, come per la sicurezza sul lavoro, la privacy e, in alcuni casi, la tutela ambientale e in determinate organizzazioni, come quelle che erogano i cosiddetti servizi essenziali, che adottano il modello di organizzazione e gestione richiesto dal D. Lgs. 231 del 2001 o che sono certificate secondo norme ISO (ad esempio la ISO/IEC 27001 sulla sicurezza delle informazioni, o la ISO 22301 sulla business continuity). La valutazione del rischio è necessaria anche in occasione di fusioni e acquisizioni (*merger & acquisition*) o di raccolta di finanziamenti. Si assiste, a volte, al proliferare di iniziative di gestione del rischio non integrate, mentre il rischio digitale (basti pensare alle minacce di cybersecurity) esalta invece la necessità di integrare le diverse gestioni del rischio. Tale esigenza esiste anche nelle PMI (soprattutto quelle che erogano servizi di fornitura alle grandi aziende[11]), mutuando in chiave semplificata quanto da tempo è realizzato dalle grandi aziende, assegnando una responsabilità interna di coordinamento e sensibilizzando tutti i responsabili di processo o di funzione.
L'attenzione del sistema formativo alle tematiche di rischio è un ulteriore segnale, se ce ne fosse bisogno, dell'attualità del rischio nella società, e introduce una nota di ottimismo sulla preparazione dei futuri manager su un aspetto cruciale per la gestione dell'impresa. Qualche esempio: negli USA sono disponibili 37 Master[12], in Italia le più prestigiose Università (tra cui Luiss, Bocconi, Bari, Politecnico di Milano e Università degli studi di Milano, per citarne solo alcune) propongono Master dedicati al rischio, in alcuni casi centrati sul rischio del digitale.

10 Sergio Beretta. Valutazione dei rischi e controllo interno. Italia: Università Bocconi Editore. 2004.

11 Comitato Insurance. Il risk management e le PMI. Italia: AmCham Italy, 2021. https://www.amcham.it/it/download/comitato-gruppidilavoro/38.

12 https//www.hotcoursesabroad.com/study/training-degrees/us-usa/masters/risk-management.

4.3 Il rischio digitale

La pandemia COVID-19 all'inizio del 2020 ha accelerato significativamente i processi di trasformazione digitale in atto nelle organizzazioni sia pubbliche sia private e, se possibile ancor di più, la diffusione dell'utilizzo delle stesse tecnologie nella società. Molteplici sono le considerazioni che si possono fare in proposito:

- La capacità di governare la digitalizzazione consente alle organizzazioni non soltanto di innovarsi, cogliendo le opportunità presenti nel mercato, ma anche di reagire più efficacemente a crisi improvvise, aumentando anche la propria resilienza.
- Nell'immediato, l'adozione di nuove tecnologie può portare senz'altro benefici tangibili. Spesso però, soprattutto nelle realtà tecnologicamente meno mature, non tardano a manifestarsi anche conseguenze negative. Si consideri in proposito l'esempio delle soluzioni di *smart working*:
  - a fronte del recupero di produttività da esse consentito, si è assistito ad un incremento esponenziale dei cyber attacchi
  - il cambiamento nelle modalità di collaborazione, realizzato in tempi molto brevi, ha fatto nascere un acceso dibattito sui pro e contro di questo approccio ed evidenziato la generale impreparazione culturale delle organizzazioni a riguardo.
- Il concretizzarsi di una minaccia come un'epidemia a livello mondiale, con conseguenze dirette e indirette a così ampio spettro, costituisce una prova eclatante della necessità di analizzare compiutamente l'interazione tra i diversi fattori di rischio, adottando un approccio integrato, che consideri, ad esempio, anche i rischi digitali e quelli correlati alle lunghe e complesse catene di approvvigionamento.
- L'abilità nello sfruttare appieno le tecnologie digitali per superare con successo la crisi pandemica, dimostrata da alcuni, ha portato ad ampliare il divario con "gli altri", sia a livello individuale sia a livello di organizzazioni o nazioni (si veda in proposito il The Global Risks Report 2021 del WEF[13]). Da questo punto di vista, il "digitale" si connota quindi anche come possibile causa di crescenti disuguaglianze. Recentemente, la stessa Commissione Europea si è fatta promotrice della necessità di coniugare sempre più innovazione e sostenibilità, come illustrato nel suo recente report su Industria 5.0[14], i cui principi ispiratori sono anche alla base

13 https://www.weforum.org/reports/the-global-risks-report-2021.

14 Directorate-General for Research and Innovation (European Commission). Industry 5.0 - Towards a sustainable, human-centric and resilient European industry. Brussels: European Commission, 2021. https://ec.europa.eu/info/publications/industry-50_en.

del piano Next Generation EU e del corrispondente Piano Nazionale di Ripresa e Resilienza (PNRR) italiano

In Italia, il periodo compreso tra il 2020 ed il 2021 mostra dati significativi[15] di come vi sia una maggior apertura alla tecnologia e alle soluzioni digitali (pur non trascurando alcune lacune e limiti): il 34% degli italiani ha scoperto la possibilità di acquistare restando a casa (nell'aprile 2021 in Italia vi è stata una crescita esponenziale degli e-commerce, con un +78% rispetto all'anno precedente[16]), il 32% ha effettuato per la prima volta pagamenti a distanza (home-banking) e il 25% ha potuto verificare le potenzialità del connubio vita-lavoro attraverso lo *smart-working*.
Senza dimenticare, inoltre, i netti miglioramenti in ottica di inclusione, ove, grazie all'introduzione e sviluppo di formazioni e didattiche a distanza (FAD - DAD) e allo "svecchiamento" delle maglie burocratiche, si è riusciti a garantire l'operatività delle funzioni quotidiane anche nei periodi di estrema emergenza (circa 26 milioni di italiani hanno dichiarato di essere riusciti a svolgere le proprie attività più o meno regolarmente durante i lockdown del 2020 solo grazie all'innovazione tecnologica).
Aggiungiamo poi il costante utilizzo del cloud, a scopo personale o di lavoro (nel 2021 il mercato cloud in Italia registra un introito pari a circa 3,48 miliardi di Euro e la curva non accenna a decrescere[17]), le evoluzioni di sistemi intelligenti e interconnessi (tra cui, Industria 4.0, robotica e domotica, l'Internet of Things, le applicazioni dell'intelligenza artificiale dalle smart cities ai sistemi di trasporto intelligenti) e, infine, i piani di incentivazione nazionali e sovranazionali (tra tutti citiamo il PNRR), ben può comprendersi il radicato cambiamento a cui si assiste nella nostra società e nel sistema economico. Come già accennato, le nuove tecnologie possono, a loro volta, rappresentare un rischio. Esse infatti permettono, ad esempio di:

- condurre campagne di phishing e hacking sempre più sofisticate;
- avviare cyber-war o cyber-spionaggio con attacchi indirizzati a sistemi e infrastrutture critici o ad altissimo valore;
- utilizzare botnet per influenzare l'opinione pubblica e minare l'equilibrio sociale e la democrazia nel campo della guerra dell'informazione.

Caso particolare è quello dell'intelligenza artificiale. Il rapporto WEF 2020 evidenzia come essa si presti a un uso duale (benevolo o malevolo): permette di identificare le minacce e proteggere al meglio i sistemi dell'organizzazione ma può essere utilizzata come tecnica per eludere le difese, per effettuare attacchi sempre più sofisticati e mira-

15 Deloitte Creative Team – Italia. Umanesimo digitale, stella polare dell'impresa: Innovation Summit 2020. Italia: Deloitte Italy S.p.A., 2021. https://www2.deloitte.com/content/dam/Deloitte/it/Documents/strategy/UmanesimoDigitale_Deloitte.pdf.

16 https://www.corrierecomunicazioni.it/digital-economy/ecommerce/boom-delle-commerce-il-record-e-italiano-nel-2021-crescita-a-quota-78/.

17 https://www.osservatori.net/it/ricerche/comunicati-stampa/cloud-italia-mercato.

ti a bersagli specifici (grandi e medie aziende, pubbliche o private, cittadini, Stati).
Se da un lato si riescono a cogliere i molteplici aspetti positivi del mutamento tecnologico, dall'altro ancora spesso si sottovalutano i rischi connessi al digitale e ciò anche a causa di una scarsa conoscenza degli strumenti utilizzati, ancora valutati dai vertici unicamente in ottica di opportunità per le proprie attività, senza preoccuparsi troppo delle minacce correlate, che possono cagionare importanti perdite economiche (anche per fermi operativi e conseguenti costi di ripristino, per inattività e conseguenti reclami da parte dei clienti) e reputazionali, oltre che in termini di sanzioni e responsabilità legali. Anche l'approccio basato sull'analisi dei rischi, oggi, troppo spesso non riveste carattere primario nelle organizzazioni. Ciò si verifica essenzialmente perché i vertici non riescono a percepire nell'immediato il ritorno economico correlato all'investimento. È di conseguenza difficile far comprendere, soprattutto in termini di ritorni nel medio-lungo periodo, che cosa significhi un investimento in questo ambito.
Ancora troppo spesso l'analisi dei rischi, che ai più non appare conferire risultati tangibili, è vista come l'ennesimo balzello normativo; tuttavia è importante rendersi conto che i vantaggi non si limitano all'evitare sanzioni e richieste di risarcimento, ma includono benefici effettivi.
In particolare, dal rapporto ENISA di ottobre 2021[18] emerge che le minacce e gli attacchi alla sicurezza informatica siano in costante aumento, ma anche che gli stessi continuino ad evolversi, perfezionarsi e mutare la tipologia. E così, complice anche la pandemia globale e la mancanza di una solida formazione e informazione, crescono gli attacchi al cosiddetto "fattore umano" (*phishing*, *email threat* e *disinformation* sono tra le principali minacce su cui pone l'attenzione lo studio), si consolidano i "sempreverdi" *malware* e *ransomware* e si moltiplicano a dismisura le vulnerabilità connesse a *cloud*, *supply chain* e commercio elettronico. Sono notevoli gli impatti e le conseguenze economiche: nel solo periodo COVID-19 vi è stato un +32% di attacchi *phishing* con circa 4 miliardi di perdite, oltre ai costi di ripristino della struttura, spese legali ed eventuali sanzioni delle autorità.

Il report WEF 2021 ha riconosciuto il "fallimento delle misure di cybersecurity" tra i primi 5 rischi globali (e primo fra tutti i rischi tecnologici) poiché: *"Le infrastrutture e le misure di sicurezza informatica delle imprese, del governo e delle famiglie sono superate o rese obsolete da crimini informatici sempre più sofisticati e frequenti, con conseguenti disagi economici, perdite finanziarie, tensioni geopolitiche e/o instabilità sociale".*
L'adozione delle tecnologie e la modifica dei processi organizzativi e produttivi devono quindi essere accompagnate, in particolare, da un'attenta gestione del rischio per garantire la sicurezza.
Sintetizzando, di seguito un elenco esemplificativo e non esaustivo delle possibili mi-

18 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

nacce che concorrono al rischio digitale con riferimento alla sicurezza dei processi:

- attacchi fisici con danni, per esempio, alle infrastrutture di sistemi e applicazioni e alle persone;
- eventi naturali che impattano sull'infrastruttura;
- perdita dei servizi essenziali (p.e. errori di configurazioni, eccesso di traffico sulla rete);
- compromissioni di informazioni (p.e. violazione da furto fisico dei supporti di memorizzazione o data leak da parte di un cybercriminale);
- problemi tecnici (malfunzionamenti hardware o software)
- azioni non autorizzate di soggetti interni o esterni con colpa o dolo;
- compromissione di funzioni o accessi (p.e. furto di identità, phishing, social engineering)
- attacchi di malintenzionati (p.e. zero day, ransomware).

4.4 Il rischio digitale e la sostenibilità

La digitalizzazione dei processi di produzione e degli stili di vita costituisce forse l'elemento che maggiormente definisce l'attuale fase di transizione verso un nuovo paradigma di organizzazione sociale imperniato sull'automazione di molte funzioni che in passato erano appannaggio esclusivo del lavoro umano.
Il concetto di sostenibilità fa riferimento alla capacità di usare una risorsa nell'ambito dei suoi limiti di capacità, perseguendo tutti gli obiettivi, non solo quelli economici.
Il rischio digitale non è dunque solo quello relativo alla sicurezza delle informazioni e degli impianti, ma anche alla capacità di coniugare nel tempo l'operatività con la sostenibilità che coinvolge tutti gli stakeholder presenti e futuri.
La trasformazione di processi, che sta avvenendo in maniera spesso non consapevole da parte delle istituzioni come del singolo individuo, è abilitata dalle tecnologie digitali che permettono la condivisione delle informazioni. Tale scambio, col concetto di producer (uno) e consumer (molti), abilita la partecipazione "istantanea" dei vari attori (persone fisiche o automi) al singolo processo. Sono stati ampiamente evidenziati i benefici della digitalizzazione per i processi industriali, i servizi alla persona e la burocrazia, ma non si è altrettanto consci del rovescio della medaglia e cioè degli

effetti transitori e permanenti della trasformazione in essere. Vanno quindi considerati diversi fattori:

- Impatto sull'occupazione - la maggiore efficienza dei processi e la partecipazione diretta dei clienti ai processi stessi sta riducendo e ridurrà la richiesta di forza lavoro tradizionale; è irrealistico pensare che i posti di lavoro guadagnati con le nuove professioni IT compensino la perdita di quelli di natura tradizionale, anche perché il fenomeno della globalizzazione sta portando alla concentrazione delle competenze (rischio strategico di natura geopolitica).
- Impatto sulla parte finale della filiera distributiva - la rapida e tumultuosa crescita dell'e-commerce, con il fenomeno COVID-19 che ha fatto da ulteriore spinta, sta minando alla radice il modello distributivo dei negozi di comunità, con impatto sull'occupazione territoriale e sulla popolazione anziana, non nativa digitale, che perde i punti di riferimento per l'approvvigionamento di beni e servizi quotidiani.
- Impatto sull'ambiente - a fronte del risparmio sul fenomeno dei rifiuti tradizionali (meno carta, minor necessità di spostamenti fisici e di conseguenza minor inquinamento da combustibili), si registra l'incremento della spazzatura tecnologica, anche perché gli attuali dispositivi sono soggetti a un ciclo di vita molto più breve del passato.
- Impatto sulla socialità - l'esperienza COVID-19, che ha forzato a un uso del digitale molto intenso, sta mostrando che si manifestano effetti psicologici negativi causati dalla riduzione delle interazioni fisiche tra persone.
- Effetti del digital divide - le aree non coperte da reti ad alta capacità e velocità diventano meno competitive e attraenti accelerando di conseguenza il processo di urbanizzazione. Inoltre le persone, tipicamente anziani, non avvezze all'uso delle tecnologie saranno sempre più isolate ed escluse dalla comunità.
- Impatto sui diritti fondamentali - oltre al digital divide, la digitalizzazione introduce (o contribuisce ad aumentare) nuovi rischi per i diritti e le libertà fondamentali e possibili discriminazioni (per esempio legate ai pregiudizi (bias) algoritmici e al non corretto funzionamento dei sistemi biometrici).

In questo contesto, è raccomandabile un approccio basato sul rischio e di valutazione della sostenibilità delle iniziative. Non è possibile individuare un approccio valido per tutte le organizzazioni. Come ricordato in precedenza, per le grandi aziende quotate in Borsa, il "Codice di autoregolamentazione" richiede specifici adempimenti di *governance*, che prevedono, ad esempio, la costituzione di un Comitato rischi che periodicamente svolga valutazioni di rischio che ormai non possono più prescindere dai rischi-opportunità del digitale.
Alcune istituzioni, come Confindustria, stanno operando per favorire una crescita della consapevolezza degli imprenditori (grandi imprese e PMI) e per fornire loro supporti

economici[19]. Non si tratta di adottare soluzioni tecnico-organizzative complesse, quanto di definire una pianificazione almeno annuale della valutazione dei rischi e della sostenibilità digitale, individuando una figura interna di coordinamento, responsabilizzando i quadri intermedi, e formalizzando i risultati delle valutazioni e dei progetti di miglioramento individuati.
Questa prassi virtuosa è sempre più importante per le PMI fornitrici di grandi aziende nazionali e internazionali verso le quali la continuità di servizio e la resilienza dei servizi aziendali assumono una dimensione strategica anche in relazione alle catastrofi ambientali e alle minacce cyber che possono condizionare le filiere produttive.

4.5 Le azioni UE a tutela dei rischi digitali

Una grande spinta alla sensibilizzazione del tema è partita dalle più recenti politiche europee per la transizione digitale con riferimenti specifici alle misure richieste nei Piani nazionali di ripresa e resilienza, nel quadro di sistema degli obiettivi di sviluppo sostenibile dell'agenda ONU 2030[20].
Si sta strutturando un quadro in cui gli aspetti d'innovazione tecnologica vanno di pari passo con un'analisi degli aspetti sociali e dei potenziali impatti negativi visti nel paragrafo precedente.
Anche se i rischi continuano a suscitare preoccupazioni, la digitalizzazione resta il mezzo con cui affrontare le sfide sociali e ambientali del nostro tempo, in cui investire per poter essere competitivi e la via europea per l'economia digitale può divenire competitiva, integrando i propri valori nei processi d'innovazione.
Con la comunicazione dal titolo "Bussola per il digitale 2030: il modello europeo per il decennio digitale"[21], la Commissione europea ha precisato la propria posizione, aggiornando il proprio programma per il decennio del digitale 2021-2030, e ha indicato che i principi del digitale europeo sono radicati nei propri trattati e come tali devono rispettare i diritti fondamentali e i suoi valori fondativi e propone dal 2021 l'adozione di una dichiarazione sui principi europei.

19 Comitato Insurance. Il risk management e le PMI. Italia: AmCham Italy, 2021. https://www.amcham.it/it/download/comitato-gruppidilavoro/38.

20 https://unric.org/it/agenda-2030/.

21 https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=COM:2021:118:FIN.

Le linee guida europee, che hanno orientato l'elaborazione dei PNRR nei diversi Stati Membri, tengono conto del quadro strategico definito dalla Commissione europea nelle sue linee d'azione generali: più precisamente dei contenuti della Comunicazione del 20 febbraio 2020 "Plasmare il futuro digitale dell'Europa"[22] le cui tematiche sono già state oggetto di diverse risoluzioni del Parlamento europeo.
Nel pacchetto di misure adottato dalla Commissione il 20 febbraio 2020, fondamentale anche il libro bianco sull'Intelligenza Artificiale (IA)[23], che integra gli orientamenti etici per una IA affidabile pubblicati nell'aprile 2019 dal Gruppo indipendente di esperti ad alto livello sull'IA, e la strategia europea per i dati, quale vera risorsa primaria dell'economia digitale. Dunque i prossimi anni saranno definiti come il decennio digitale dell'Europa con una precisa bussola concepita attorno a quattro punti cardinali:

- Cittadini dotati di competenze digitali e professionisti altamente qualificati nel settore digitale. Entro il 2030 almeno l'80% della popolazione adulta dovrebbe possedere competenze digitali di base e 20 milioni di specialisti dovrebbero essere impiegati nell'UE nel settore delle tecnologie dell'informazione e della comunicazione, con un aumento del numero di donne operanti nel settore.
- Infrastrutture digitali sostenibili, sicure e performanti. Entro il 2030 tutte le famiglie dell'UE dovrebbero beneficiare di una connettività Gigabit e tutte le zone abitate dovrebbero essere coperte dal 5G; la produzione di semiconduttori sostenibili e all'avanguardia in Europa dovrebbe rappresentare il 20% della produzione mondiale; 10.000 nodi edge, di collegamento tra i dispositivi periferici e i server centrali, a impatto climatico zero e altamente sicuri dovrebbero essere installati nell'UE e l'Europa dovrebbe dotarsi del suo primo computer quantistico.
- Trasformazione digitale delle imprese. Entro il 2030 tre imprese su quattro dovrebbero utilizzare servizi di cloud computing, big data e intelligenza artificiale; oltre il 90% delle PMI dovrebbe raggiungere almeno un livello di base di intensità digitale e dovrebbe raddoppiare il numero di imprese "unicorno" nell'UE.
- Digitalizzazione dei servizi pubblici. Entro il 2030 tutti i servizi pubblici principali dovrebbero essere disponibili online, tutti i cittadini avranno accesso alla propria cartella clinica elettronica e l'80% dei cittadini dovrebbe utilizzare l'identificazione digitale (eID).

22 https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52020DC0067.

23 https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52020DC0065.

5. La valutazione dei rischi

La valutazione dei rischi digitali è fondamentale per le organizzazioni che intendono avere la piena consapevolezza della loro situazione e desiderino affrontare un percorso di miglioramento continuo. Formalmente, l'analisi del rischio (*risk analysis*) è parte della valutazione del rischio (*risk assessment*), a sua volta parte della gestione del rischio (*risk management*). Quest'ultima è organizzata in più fasi interconnesse (vedere ISO 31000:2018):

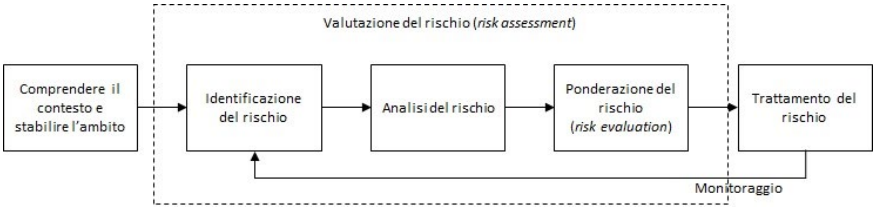

Figura 3 - Gestione del rischio[24]

Alcuni testi indicano come "gestione del rischio" la sola fase di trattamento del rischio.
L'approccio deve essere sistematico, ossia tale da rendere evidente, e quindi ripetibile, attraverso i dati, le elaborazioni e le valutazioni, il ragionamento che ha portato alle scelte fatte. Questo permette anche di verificare, validare e affinare nel tempo il proprio approccio alla gestione del rischio, riducendo conseguentemente l'aleatorietà delle valutazioni fatte.
I principali passi della gestione del rischio consistono in:

- Formazione generale sulla valutazione del rischio a tutte le persone da coinvolgere (paragrafo 5.1).
- Comprensione del contesto e identificazione dell'ambito, che includono
  - ► analisi del contesto (paragrafo 5.2);
  - ► identificazione dell'approccio da adottare e dei framework di riferimento, anche considerandone i limiti (paragrafo 5.3);
  - ► mappatura dei processi, inclusa la filiera di fornitura (paragrafo 5.4);
  - ► identificazione del perimetro da analizzare;
  - ► assegnazione delle responsabilità (paragrafo 5.5).
- Valutazione del rischio (risk assessment): identificazione e caratterizzazione dei

24 Figura degli autori.

pericoli e dell'esposizione a essi, quantificazione del rischio, in relazione alle minacce esistenti e alla probabilità che queste possano concretizzarsi, e valutazione della sua accettabilità in relazione al contesto e alle strategie dell'organizzazione; essa a sua volta si suddivide in:

- identificazione e analisi dei rischi (*risk identification* e *risk analysis* - a cui sono dedicati i paragrafi 5.6 e 5.7 per due aspetti specifici):
  - rilevazione delle minacce (attacchi cyber, eventi naturali, malfunzionamenti tecnologici, disastri ambientali, pandemie, errori umani, non ottemperanza alla compliance, ecc.) e valutazione delle stesse sulla base della loro probabilità di accadimento e del potenziale impatto per l'organizzazione;
  - individuazione delle misure tecniche e organizzative (di sicurezza, di privacy, di continuità operativa, ecc.) adottate e analisi della loro vulnerabilità, intesa come adeguatezza a ridurre gli impatti delle minacce considerate;
  - individuazione del livello di rischio "residuo" (ovvero non minimizzato dalle contromisure adottate);
- ponderazione dei rischi: confronto del livello di rischio residuo con i criteri di accettazione condivisi con i vertici dell'organizzazione;
- predisposizione del rapporto di valutazione del rischio.

- Trattamento del rischio (*risk treatment*): valutazione delle alternative disponibili per affrontare il rischio (per esempio, mitigandolo o accettandolo); di esso fanno parte:
  - attuazione, in tempi predefiniti, delle azioni stabilite;
  - verifica dell'efficacia degli interventi.
- Comunicazione del rischio (*risk communication and consultation*): attività trasversale alle due fasi precedenti, in cui vi è la condivisione delle informazioni relative agli elementi di pericolo e di rischio con tutte le parti interessate; nel paragrafo 5.8 sono descritte alcune caratteristiche dei rapporti di valutazione del rischio.
- Riesame dei rischio (*risk monitoring and review*): attività in cui sono raccolte e analizzate informazioni relative ai rischi in modo da verificare l'efficacia del loro trattamento. Di questa fase fanno parte:
  - il riesame periodico delle misure di presidio adottate in funzione di possibili nuove minacce oppure di nuovi servizi erogati dall'organizzazione a fronte del cambiamento del contesto di business; frequenza, modalità di svolgimento e livello di analisi, sono in funzione delle caratteristiche dell'organizzazione

(dimensione, settore, esigenze di certificazioni di terze parti, rilevanza per gli obiettivi, orientamento alla qualità e alle good-practices, ecc.);

- l'apprendimento delle lezioni (paragrafo 5.9);
- il monitoraggio del rischio, anche attraverso specifici indicatori, ossia i KRI (*Key risk indicator*), come descritto nel paragrafo 5.10.

Si segnala, nel paragrafo 5.11, il valore dell'approccio integrato alla valutazione dei rischi, considerando, tra gli altri, quelli relativi alla sicurezza delle informazioni, alla cybersecurity, alla privacy, alla gestione dei servizi IT e alla continuità operativa. Questo approccio integrato consente al vertice di comprendere, in modalità documentata e semplificata, i reali rischi, considerando che i rischi digitali e di compliance sono una delle componenti chiave di un'organizzazione.

5.1 Formazione preliminare

Si raccomanda, sempre nelle prime fasi del progetto, di diffondere la cultura del rischio come valore dell'organizzazione, affinché la gestione del rischio diventi "normale" operatività dell'organizzazione. Questo richiede il supporto dei vertici, che devono anche coinvolgere i responsabili ai vari livelli della struttura dell'organizzazione. Va previsto il coinvolgimento nella gestione del rischio anche dei soggetti esterni all'organizzazione, inclusi clienti, utenti, fornitori e partner.

5.2 L'analisi del contesto

Lo standard ISO 31000 ha introdotto la definizione di contesto quale attività preventiva della valutazione e del trattamento del rischio, in quanto consente di cogliere tutti gli elementi (obiettivi, ambiente, criteri di rischio, portatori d'interesse) che contribuiscono allo sviluppo di una conoscenza del rischio – atta a rivelare natura e complessità dello stesso – e di adattare il processo di analisi del rischio alle effettive esigenze del settore di attività.
È importante identificare:

- il contesto esterno, costituito dall'ambiente nel quale opera un'organizzazione

(ambiente sociale, economico, finanziario e tecnologico, gli obblighi normativi ecc.);

- il contesto interno, costituito dai fattori interni dell'organizzazione (i ruoli, le strategie, i flussi di informazione, i modelli di riferimento adottati, la complessità dell'organizzazione e il suo livello di maturità, ecc.).

5.3 Identificazione dell'approccio e dei framework

La scelta di un approccio appropriato rende la gestione del rischio pertinente e armonica, inquadrando gli elementi più significativi (responsabilità, attività da svolgere, funzioni da coinvolgere, framework da adottare, ecc.) e prendendo in considerazione tutti i tipi di rischi applicabili alle attività e funzioni.
L'adozione di un framework permette di stabilire un dizionario di termini, di misure e di pesi comprensibili e condivisi da tutti.
Quando si deve scegliere l'approccio da seguire per valutare il rischio, l'organizzazione deve tenere conto delle molteplici norme che la riguardano, il settore di mercato in cui opera e i propri obiettivi di sicurezza.
Per esempio, in settori quali sanità e produzione industriale, così diversi per tipologia di dati trattati, normative pertinenti e altri fattori, è necessario adottare approcci specifici, al fine di rappresentarli al meglio.
Differenze significative si colgono tra i diversi settori di mercato, anche a causa delle diverse culture. Si considerino per esempio i seguenti settori:

- sanitario, per cui un evento può avere conseguenze sulla vita umana;
- militare, dove è importante la sicurezza nazionale;
- amministrativo, che richiede la valutazione dell'integrità delle scritture contabili.

Un'organizzazione potrebbe usare più approcci di valutazione del rischio:

- per l'Enterprise Risk Management (ERM), che si concentra sul rischio di impresa complessivo[25];
- per i rischi digitali, vista la crescente digitalizzazione di tutte le attività;

25 Vedere, tra gli altri: NISTIR 8286A Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management. USA: 2021. https://csrc.nist.gov/publications/detail/nistir/8286a/final.

- per la protezione dei dati personali, visto che ogni organizzazione ne tratta (dipendenti, clienti, fornitori, utenti);
- specifici per le sue attività: responsabilità di impresa (D. Lgs. 231 del 2001), prevenzione della corruzione e la trasparenza, eccetera.

In alcuni settori la scelta dell'approccio di analisi trova dei vincoli più o meno stringenti nella normativa, negli standard di settore o nelle prassi imposte dalle autorità di controllo delle attività.
Fra i fattori abilitanti di un approccio efficace e integrato alla valutazione del rischio è ragionevole considerare l'orientamento all'etica, alla sostenibilità, alla comunicazione interna fra funzioni (fra loro e verso il vertice), al coinvolgimento reale dei responsabili, alla cultura di controllo interno e dell'innovazione, ecc.

5.3.1. Possibilità, probabilità e verosimiglianza

È opportuno specificare che, nella terminologia della gestione del rischio, il termine "possibilità" è utilizzato per riferirsi alla plausibilità di un accadimento, sia essa definita, misurata, determinata oggettivamente o soggettivamente, qualitativamente o quantitativamente, e descritta utilizzando termini generici o matematici come "probabilità" o "frequenza".
Il termine spesso utilizzato nelle stesure in lingua inglese della norma è "likelihood", che è spesso tradotto con "verosimiglianza". Si evita il termine "probability" perché, in inglese, ha un'accezione più legata al calcolo matematico, mentre "likelihood" ha una portata più generale e ampia.
Nel prosieguo del libro utilizzeremo in maniera intercambiabile i tre termini.

5.3.2. Impatti e conseguenze

In questo libro si usano indifferentemente i termini "impatti" e "conseguenze".
E' opportuno specificare che alcuni testi distinguono i termini e utilizzano "impatti" per gli effetti immediati di un rischio, mentre "conseguenze" include quelli a lungo termine. Questo approccio, per esempio, distingue gli impatti di un evento su un asset, che possono poi avere conseguenze per l'intera organizzazione.
In ambito privacy, si preferisce il termine "impatti" per gli effetti di un rischio su una persona fisica.

5.3.3 Metodo qualitativo e metodo quantitativo

Gli approcci di valutazione del rischio vengono raggruppati in due macro famiglie: la qualitativa e la quantitativa.
Entrambe richiedono una valutazione dei due valori tipici con cui si misura il rischio:

- probabilità o verosimiglianza che risponde alla domanda "Quale è la frequenza dell'accadimento?"
- impatto o conseguenza che risponde alla domanda "Quale è la ricaduta dell'evento?"

L'analisi qualitativa è più semplice e ampiamente utilizzata; aiuta nell'identificazione degli asset e delle risorse a rischio, delle vulnerabilità che potrebbero consentire la realizzazione delle minacce, delle tutele già in atto e quelle che possono essere implementate per raggiungere un livello di rischio accettabile e aumentare la consapevolezza generale. Questa analisi utilizza calcoli semplici e procedure in cui non è necessario determinare il valore esatto delle attività, delle frequenze di minaccia o dei costi di attuazione dei controlli.
L'analisi quantitativa richiede un maggiore impegno nel determinare i valori di costo e un impegno crescente nei calcoli. Tuttavia, presenta i suoi risultati in forma di valori monetari, percentuali e probabilità di facile interpretazione[26].
La valutazione fra quale metodo opzionare per la propria analisi del rischio dovrà tenere in considerazione diversi aspetti quali:

- Budget economico, tempo e risorse a disposizione dove una loro scarsità potrebbe suggerire di propendere per un'analisi qualitativa ed eventualmente solo per taluni fattori critici optare per un'analisi ibrida che consideri la misurazione di taluni parametri critici o incerti.
- Esperienza nella valutazione del rischio. Si potrebbe valutare di intraprendere un percorso graduale di misurazione dei parametri alla base dell'analisi del rischio, migrando gradualmente, con l'aumento dell'esperienza, dal qualitativo al quantitativo.
- Dimensione organizzativa e strutturale (con differenze tra organizzazioni piccole e medie e quelle grandi); complessità architetturale e tecnologica; articolazione e complessità del portafoglio dei servizi e prodotti offerti; natura dei rischi da contemplare.

26 James W. Meritt. A Method for Quantitative Risk Analysis. Proceedings of the 22nd National Information Systems Security Conference. https://csrc.nist.gov/publications/detail/conference-paper/1999/10/21/proceedings-of-the-22nd-nissc-1999.

- La disponibilità di serie storiche relative agli eventi avversi individuati (interne ed esterne pubbliche), di un sistema di contabilità evoluto, di strumenti di analisi o misurazione. Questi elementi potrebbero facilitare un approccio quantitativo.
- Nulla osta a immaginare un percorso di miglioramento continuo nell'attività di valutazione del rischio, che porti l'organizzazione stessa ad affinare nel tempo il metodo e di conseguenza l'affidabilità delle stime o, in alternativa, a ipotizzare un metodo ibrido, dove combinare i due metodi, massimizzando le informazioni disponibili e riducendo allo stretto necessario le metriche da raccogliere e calcolare. Le due soluzioni di graduale evoluzione o di ibridazione sono numericamente meno intensive (e meno costose) rispetto a un'analisi quantitativa approfondita ed esaustiva.

Metodo qualitativo

In una valutazione qualitativa si considerano scale di livelli con etichette descrittive, come "basso – medio – alto".

La valutazione qualitativa del rischio, nella sua rappresentazione più tipica, utilizza tabelle, che prendono il nome di "Matrice del rischio", come in rappresentazione, oppure "Mappe di calore".

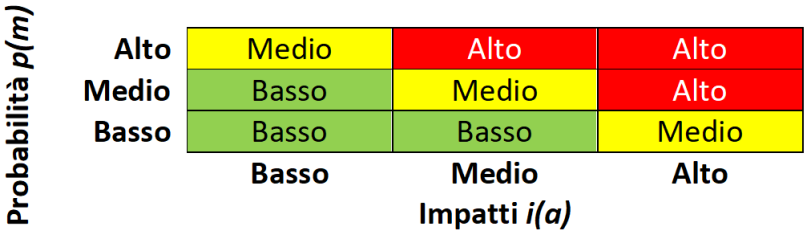

Figura 4 - Matrice del rischio[27]

In alcuni casi si utilizzano valori numerici, che però non sono direttamente riconducibili a una misurazione puntuale ma piuttosto a una stima. A titolo esemplificativo potremmo avere una valutazione dell'impatto su una scala a 4 valori (da 1 - basso, a 4 - alto) mentre la probabilità potrebbe essere posta su una scala a tre valori (da 1 poco probabile a 3 - molto probabile). Nell'esempio così descritto potremmo rappresentare in una matrice il prodotto $R = P \times I$ e valutare il rischio sulla base del valore ottenuto, dove a un rischio basso corrispondono le celle con valori da 1 a 3, ad un rischio medio le celle con valori da 4 a 6, ad un rischio alto le celle con valori da 8 a 12.

27 Figura degli autori.

Esempi di approcci qualitativi

Molti degli approcci di valutazione del rischio utilizzati comunemente prevedono valutazioni di tipo qualitativo. Tra di essi vi sono quelli descritti dalla NIST SP 800-31, dalla ISO/IEC 29134 per la *privacy impact assessment* (PIA) e il Magerit. Nel seguito sono brevemente approfonditi questi ultimi due.

ISO/IEC 29134

L'ISO/IEC 29134 è uno standard pubblicato nel 2017 per la *privacy impact assessment* (PIA) nell'ambito del trattamento di dati personali.

In tabella l'evidenza di come lo standard definisce i parametri per valutare l'impatto di un accadimento.

Valore	Impatto	Criterio
1	Trascurabile	Nessuna conseguenza o alcuni inconvenienti che possono essere superati senza alcun problema (tempo impiegato per reinserire informazioni, fastidi, irritazioni, ecc.).
2	Limitato	Notevoli disagi che potranno essere superati con alcune difficoltà (costi aggiuntivi, diniego di accesso ai servizi, paure, incomprensioni, stress, lievi disturbi fisici, ecc.).
3	Significativo	Conseguenze significative, che dovrebbero essere superate seppur con gravi difficoltà (appropriazione indebita di fondi, blacklist da parte delle banche, danni materiali, perdita del posto di lavoro, citazione in giudizio, peggioramento dello stato di salute, ecc.).
4	Massimo	Conseguenze significative, o addirittura irreversibili, che non possono essere superati (disagio finanziario come debiti inservibili o incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).

Nella tabella successiva è riportato come la ISO/IEC 29134 suggerisce di valutare la verosimiglianza (ossia la probabilità) di un evento.

Valore	Verosimiglianza	Criterio
1	Trascurabile	Un attacco che sfrutta le proprietà degli asset non sembra possibile per le sorgenti di rischio selezionate (p.e. furto di documenti cartacei da una stanza protetta con lettore di badge e codice di accesso).
2	Limitato	Un attacco che sfrutta le proprietà degli asset sembra difficile per le sorgenti di rischio selezionate.
3	Significativo	Un attacco che sfrutta le proprietà degli asset sembra possibile per le sorgenti di rischio selezionate (p.e. furto di documenti da uffici controllati da una reception)
4	Massimo	Un attacco che sfrutta le proprietà degli asset sembra molto facile per le sorgenti di rischio selezionate (p.e. furto di documenti da un luogo pubblico).

Magerit

Magerit[28], richiede di identificare innanzitutto gli asset principali o essenziali del sistema informativo (le informazioni gestite dal sistema informativo e i servizi forniti) e quindi le loro dipendenze o "asset di supporto" (asset e strumenti utilizzati per l'erogazione dei servizi principali).

Magerit, descrive la probabilità di accadimento o verosimiglianza attraverso un modello qualitativo basato sulla scala nominale descritta in tabella.

Vantaggi e svantaggi di un metodo qualitativo

Il vantaggio principale dell'approccio qualitativo è la sua facilità di implementazione da parte di organizzazioni che hanno esperienze limitate, che dispongano di poco tempo per effettuare la valutazione, oppure che non abbiano a disposizione quantità significative di dati a supporto delle valutazioni. Altro vantaggio è quello di produrre risultati facilmente confrontabili, dando la possibilità di mettere in ordine i valori o di effettuare facilmente simulazioni di tipo "*what-if*" sull'applicazione di eventuali contromisure. Il principale svantaggio dell'approccio qualitativo è rappresentato dalla soggettività delle valutazioni, con il rischio di introdurre pregiudizi (*bias*) da parte di chi

28 https://www.pilar-tools.com/doc/magerit e https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=en.

effettua la valutazione o di produrre risultati non condivisibili da altre persone.
Per ovviare agli inconvenienti di soggettività dell'approccio qualitativo è molto importante definire e descrivere in maniera chiara i criteri con i quali vengono effettuate le assegnazioni, precisando che cosa rappresentano i valori previsti nelle varie valutazioni. In questo modo la valutazione sarà il più possibile oggettiva e ripetibile.
In merito alle criticità delle matrici del rischio è interessante l'analisi effettuata da Cox, nel suo articolo "*What's Wrong with Risk Matrices?*"[29], nel quale si evidenzia come solo "*poca ricerca convalida rigorosamente le loro prestazioni nel migliorare effettivamente le decisioni di gestione del rischio*". Analizzando alcune delle proprietà matematiche delle matrici del rischio, l'autore dimostra come queste abbiano varie limitazioni, tra cui: risoluzione scadente, errori, assegnazione delle risorse tutt'altro che ottimale e ambiguità sia in ingresso che in uscita.
A titolo esemplificativo si consideri la figura sottostante dove in una matrice del rischio 2x2 sono rappresentate delle curve iso-risk caratterizzate dal possedere una pendenza negativa e dall'avere un valore del rischio identico su tutti i punti della stessa curva.

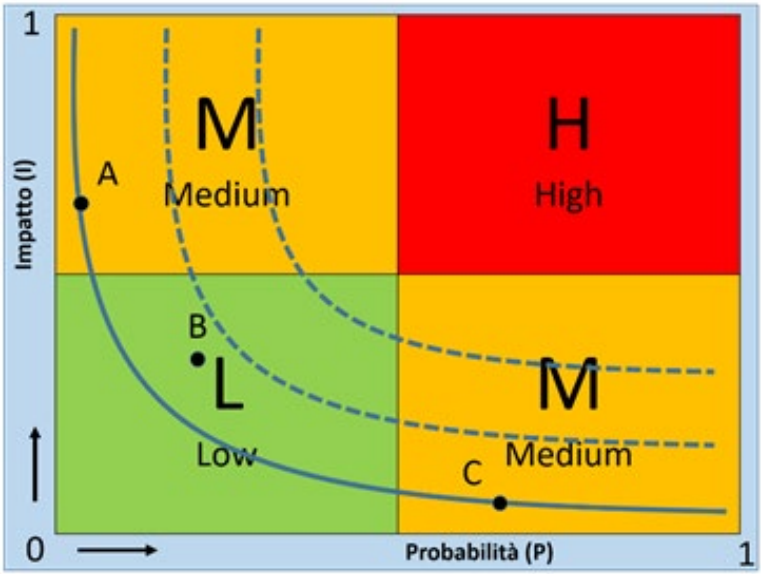

Figura 5 - Matrici del rischio (qualitative) e curve iso-risk (quantitative)[30]

29 I. Anthony Cox. What's wrong with risk matrices?. Risk Analysis, vol. 28 n. 2. 2008, 497-512. doi: 10.1111/j.1539-6924.2008.01030.x. https://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2008.01030.x.

30 Francesco Ciclosi. La protezione dei dati e la gestione del rischio nella Pubblica Amministrazione. Italia: Maggioli Editore, 2019.

Se consideriamo la funzione di rischio R=PxI, con la correlazione negativa P=(0,75 -I), sarà possibile ottenere i seguenti valori:

Punto A: I=0,65 e P=0,1, con rischio R= 0,65x0,1=0,065

Punto B: I=0,4 e P=0,35, con rischio R= 0,4x0,35=0,14

Punto C: I=0,1 e P=0,65, con rischio R= 0,1x0,65=0,065

Si osserva quindi che, con un approccio qualitativo, il rischio B è "Basso", mentre A e C sono "Medi", mentre con un approccio quantitativo B ha valore superiore ad A e C.

Metodo quantitativo

Un'analisi quantitativa presuppone che ognuna delle variabili abbia un valore numerico puntuale, stimato o misurato.

Il vantaggio di avere misurazioni quantitative, seppur con un loro intervallo di confidenza, è dato dalla loro:

- Oggettività: una misurazione è solitamente oggettiva, un'etichetta (p.e. "medio-alto") è soggettiva;
- analiticità: l'inserimento dei valori nei fogli di calcolo rende semplice e rapida l'analisi dei valori;
- rappresentabilità: la rappresentazione analitica, fatta di curve, istogrammi, costi e ROI, è meglio comprensibile per coloro che dovranno avallare decisioni economiche su tali analisi;
- confrontabilità anche a distanza di tempo e anche da soggetti diversi, come conseguenza dell'oggettività;
- modificabilità: attraverso i fogli di calcolo si possono inserire i valori in maniera puntuale, anche in analisi costi-benefici, intervenendo per riparametrare valori o correggere errori;
- comunicabilità: la quantificazione economica della perdita è immediatamente comprensibile;
- storicità: con il passare del tempo il valore migliora per una maggiore efficacia e attitudine alla misurazione, e per la creazione di serie storiche.

In conclusione l'analisi quantitativa è oggettiva e strutturata su misurazioni. La statistica permette di individuare scarti medi e probabilità di accadimento[31].

Open Group[32], un consorzio per la promozione di standard tecnologici, ha redatto una specifica tassonomia[33], atta ad approfondire la computazione del rischio, usando la

31 https://www.cybersecurity360.it/soluzioni-aziendali/misurare-il-rischio-metodi-e-approcci-per-un-corretto-risk-management/.

32 https://www.opengroup.org/.

33 The Open Group. Risk Taxonomy (O-RT), Version 3.0.1. UK: The Open Group, 2021.

formula classica per calcolare il rischio (R = P x I).
La tassonomia offre interessanti spunti di riflessione e comprensione.

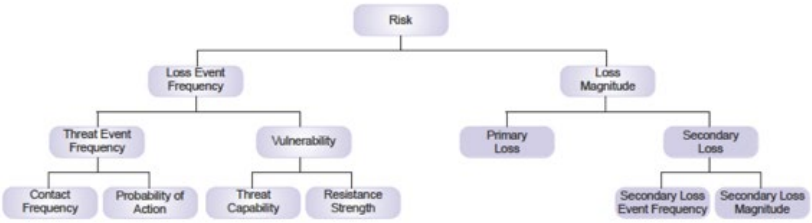

Figura 6 - I parametri per l'analisi del rischio[34]

La probabilità P (LEF o frequenza dell'evento di perdita, secondo la tassonomia) è un valore compreso fra 0 (non accadimento) e 1 (accadimento certo) ed è definita all'interno di un intervallo di tempo. La probabilità si basa sempre su un intervallo di tempo (l'evento X ha il 10% di probabilità di verificarsi nel prossimo Y), poiché nel lungo periodo tutto può accadere. A sua volta la probabilità è data da due fattori: frequenza della minaccia e vulnerabilità, a loro volta condizionati da sottovalori.
La magnitudo della perdita o impatto I è data dalla somma di perdite primarie e secondarie. Le perdite primarie sono direttamente riconducibili all'impatto (p.e. fermo produttivo con connesse perdite operative e costi di ripristino), mentre le secondarie sono derivabili (p.e. danno d'immagine, reclami, contenziosi per inadempimento contrattuale).

Strumenti e metodi di misurazione

Per raccogliere dati è possibile adottare alcune tecniche:

- *root cause analysis,* per esplorare le relazioni causa-effetto e individuare l'oggetto della misurazione[35];
- sfruttare le Ricerche Secondarie, ossia identificare ricerche accademiche o svolte da centri di ricerca, che abbiano già sviscerato il problema e definito parametri e metodi standard di misurazione;
- usare strumenti di misurazione tecnologici, per esempio software applicativi di monitoraggio o sensoristica e sondaggi online;
- l'osservazione diretta, da sempre alla base di qualsiasi metodo scientifico, validata

34 FAIRE. Risk Tassonomy.

35 https://www.riskmanagement360.it/risk-analysis/lillusione-dellintangibile-nellanalisi-del-rischio-come-misurare-aspetti-apparentemente-immisurabili/

anche con esperimenti (p.e. mandare una mail di phishing al personale per testare la capacità di riconoscerla);

- campionamento, per ridurre gli sforzi e da considerarsi una sorta di primo passo in un percorso di misurazione più approfondito; si può fare riferimento ad analisi quali quella sul "catch-recatch"[36] o la "regola del 5"[37];
- il Metodo Montecarlo[38], usato in moltissimi campi.

Le debolezze del metodo quantitativo

I metodi quantitativi hanno il vantaggio di possedere una solida base teorica, utile alla dimostrazione di specifiche proprietà o alla disamina dei differenti profili di rischio. Va comunque rilevato come spesso la corretta valutazione dei parametri sia troppo dispendiosa e complessa, costringendo l'analista a optare per un più gestibile risultato approssimato, ma concretamente ottenibile, tipico dell'utilizzo dei metodi qualitativi.
Bisogna dire che solitamente i dati su cui basare il metodo quantitativo sono scarsi. Si può comunque avviare un percorso di misurazione per iniziare a raccoglierli ed evitare il circolo vizioso per cui a fronte della scarsità di dati non si inizia a misurare e quindi non si avranno a disposizione dati.

Parimenti si evidenzia come a volte, al fine di comprendere se un dato risultato sia certo o meno, sia più utile essere in grado di ricostruire il ragionamento effettuato, piuttosto che limitarsi a una semplice verifica matematica di quanto ottenuto.

Si evidenzia infine che la letteratura scientifica ha più volte evidenziato come "spesso l'analisi di uno stesso problema ripetuta più volte, utilizzando in un'occasione un metodo quantitativo e in un'altra un metodo qualitativo, determini due risultati tra di loro contraddittori".

5.3.4 Valutazione basata sugli asset o sui processi

La valutazione del rischio può essere basata sui processi (*process driven*) oppure sugli asset (*asset driven*).
La valutazione basata sui processi identifica e valuta gli scenari di rischio a partire dai

36 https://www.usgs.gov/centers/eesc/science/capture-mark-recapture-science?qt-science_center_objects=0#qt-science_center_objects

37 http://nsfconsulting.com.au/rule-of-five-reduce-uncertainty/

38 https://www.ibm.com/cloud/learn/monte-carlo-simulation

processi organizzativi (p.e. HR, Contabilità, IT).
La valutazione basata sugli asset identifica e valuta gli scenari partendo da beni, risorse e strumenti, dando particolare rilievo agli asset tecnologici che costituiscono l'infrastruttura a supporto dei processi di business.
L'approccio per processi ha il vantaggio di partire da una percezione chiara e immediata di quali siano gli impatti sull'organizzazione all'avverarsi di un evento avverso ed è quindi più facile stabilire le priorità di intervento per il trattamento del rischio (investimenti per la mitigazione o la condivisione, ecc.).

Quello che parte dalla valutazione di rischio del singolo asset (solitamente informatico, incluse le applicazioni software) è invece un approccio più analitico che può contare su una forte conoscenza tecnica delle minacce che si possono concretizzare in base alla tipologia e all'utilizzo dell'asset stesso. Esso richiede di stabilire il valore di ciascun asset e permette quindi di stimare l'impatto dell'evento considerando il coinvolgimento degli elementi dell'infrastruttura IT. Di contro non sempre risulta agevole risalire ai processi che il singolo asset supporta e risulta difficile stimare l'impatto sul business al verificarsi di uno scenario di rischio.

I due approcci vanno quindi considerati come complementari e possono essere utilizzati insieme correlandone i risultati attraverso la definizione di una tassonomia dei rischi. In questo modo si realizza un approccio ibrido che considera sia gli aspetti tecnici dell'infrastruttura IT che gli aspetti di processo. Per esempio, se un'organizzazione ha mappato la dipendenza dei processi di business dagli asset IT, è possibile utilizzare i processi per valutare gli impatti (in caso di perdita di riservatezza, integrità e disponibilità) e gli asset IT per valutare le probabilità di accadimento delle minacce, le vulnerabilità e le misure di sicurezza applicate. Il calcolo del rischio terrebbe quindi conto dell'impatto sui processi e delle minacce e vulnerabilità sugli asset IT.

La futura edizione della ISO/IEC 27005 (che non sarà pronta prima di fine 2022), ora in redazione, segnala la possibilità di utilizzare, oltre al classico approccio *asset-based*, anche un approccio *scenario-based*. Quest'ultimo approccio prevede che, invece di esaminare minacce e vulnerabilità a cui è soggetto uno specifico asset o una classe di asset, vengano identificati alcuni scenari di rischio e valutati gli impatti e le probabilità di accadimento di questi scenari. Gli scenari di rischio, come le minacce, possono essere identificati a partire da possibili eventi, utilizzando a tale scopo database pubblici di eventi con l'indicazione delle possibili conseguenze, oppure a partire da eventi specifici che possono capitare o sono capitati alla propria organizzazione. Si tratta di un approccio che permette di identificare più facilmente i rischi.

5.3.5 Le caratteristiche dell'approccio di analisi dei rischi

Lo standard ISO/IEC 27001:2013 richiede che l'approccio di valutazione dei rischi garantisca che i risultati di ripetute valutazione dei rischi siano coerenti, validi e confrontabili tra loro.
Nel seguito sono descritti quindi gli aspetti richiamati dalla norma (coerenza, validità e confrontabilità dei risultati), a cui se ne aggiungono altri.

Coerenza
L'approccio di analisi deve tenere conto del livello di rischio accettabile deciso dall'organizzazione e in linea con i requisiti di business e con il contesto in cui la stessa opera.
Per quanto riguarda l'algoritmo usato, a fronte di valori più alti di probabilità o di impatto, il livello di rischio deve essere più alto.

Validità
Per la ISO/IEC 27001, la validità si ha quando l'approccio è coerente e ripetibile.
Bisogna anche assicurare che i risultati cambino, se opportuno, in occasione di modifiche del contesto o di eventi significativi (p.e.: incidenti occorsi).

Confrontabilità
L'analisi dei rischi deve essere confrontabile e condivisa con tutte le funzioni coinvolte. Un buon sistema di "*orchestration*" (regia) dei rischi e delle relative analisi può rendere più efficiente il lavoro, rendendo le informazioni raccolte più precise e quindi meglio valutabili in fase di analisi e di trattamento.

Per esempio, capita spesso che le analisi del rischio vengano elaborate per singole aree e analizzate senza confronti con altre aree sui criteri e sulla metodologia seguita. La necessità di condividere, confrontare e comparare le informazioni di rischio sta alla base del processo stesso. Tale azione è senza dubbio fondamentale affinché si possano poi intraprendere tutte le opportune azioni di mitigazione.

Le informazioni devono anche essere confrontabili in caso di ripetizione dell'analisi. Per esempio, se si analizza il rischio nella stessa area dopo un certo periodo di tempo, deve essere possibile capire se è aumentato o diminuito o se le azioni pianificate sono state efficaci.

Ripetibilità
L'analisi deve fornire risultati uguali se le condizioni sono le medesime (contesto, minacce analizzate, probabilità e conseguenze uguali).
Questo richiede anche che l'approccio sia formalmente definito e approvato dagli attori coinvolti e regolarmente riesaminato.

Oggettività
Uno degli aspetti più complicati nell'effettuare qualunque tipo di valutazione dei rischi risiede nell'oggettività dell'analisi. Nessuno strumento o metodologia potrà garantirla in quanto sarà sempre influenzata dalla soggettività dell'analista che effettua la valutazione. La valorizzazione di impatto e probabilità risulta condizionata dall'analista che valuta ogni rischio in funzione della sua percezione, della conoscenza dell'organizzazione e alla sua esperienza.

Indipendenza
È necessario garantire l'indipendenza dell'analista, sia egli esterno o interno all'organizzazione, dal punto di vista economico, tecnico e operativo in modo che non sia condizionabile nella sua mansione.

Imparzialità
Per garantire l'imparzialità, che è un attributo derivante dall'indipendenza, l'analisi deve essere condotta senza pregiudizi e, in particolare, deve essere possibile dimostrare che coloro che la effettuano non hanno interessi economici dipendenti dall'esito dell'analisi stessa. Stesso discorso vale per gli aspetti psicologici.

Sistematicità
Per garantire la sistematicità bisogna seguire i passi previsti per le analisi del rischio: sviluppare la funzione di calcolo con i parametri di probabilità e impatto, identificare i rischi nel perimetro di analisi e identificarne i responsabili, comparare i risultati con i livelli di accettabilità e individuare quali rischi li superano.
La sistematicità è una caratteristica essenziale affinché si verifichi anche la ripetibilità. Infatti per garantire che un'analisi sia ripetibile, va utilizzata la stessa metodologia di analisi dei rischi, condivisa all'interno dell'organizzazione.

Manutenibilità
L'attività di analisi del rischio è un processo iterativo e periodico e deve essere costantemente aggiornato in funzione dell'evoluzione dell'organizzazione (ad esempio

l'introduzione di una nuova tecnologia) e del suo contesto (p.e. cambiamenti normativi o l'intensificazione degli attacchi da parte di cybercriminali). Per tale ragione l'approccio di analisi del rischio di un'organizzazione deve essere flessibile per poter modificare facilmente i parametri previsti per il calcolo del rischio, deve prevedere la possibilità di aggiungere, eliminare o modificare l'elenco delle minacce e di cambiare la soglia di accettabilità del rischio.

Riservatezza

L'analisi del rischio permette di identificare il rischio residuo. Ogni rischio residuo è legato a una o più vulnerabilità e, pertanto, è necessario mantenere un adeguato livello di riservatezza in merito alle vulnerabilità residue per evitare che un attaccante le possa sfruttare.

Semplicità

Il costo complessivo della gestione del rischio deve essere inferiore al valore del bene che si deve proteggere. Inoltre, applicando il principio di Pareto dell'80/20, si ha che il 20% degli eventi è causa dell'80% dei danni. Per questi motivi, non è necessario adottare approcci eccessivamente sofisticati di analisi del rischio, che fanno perdere di vista i rischi realmente importanti. Iterazioni successive delle analisi possono permettere di contemplare altri aspetti, ma, soprattutto la prima volta, è bene evitare di eccedere nel livello di dettaglio.
La semplicità permette solitamente di soddisfare anche il principio di manutenibilità.

Intervista a Sofia Scozzari, CEO & Founder Hackmanac, Direttivo Women For Security e Comitato Scientifico Clusit.

D. Visto che da anni analizzi per Clusit tutti gli incidenti pubblici di sicurezza informatica, quali sono i trend globali? Le tecniche di attacco, i bersagli e gli attaccanti di oggi sono sostanzialmente diversi da quelli di 3 o 4 anni fa?

R. I cyber attacchi sono in continua evoluzione e in aumento.
Classifichiamo ormai 176 attacchi in media al mese, la più alta media mensile mai registrata. Le tecniche e le modalità con cui i cyber criminali cercano di violare i sistemi sono costantemente aggiornate ed adeguate a quelle che sono le tendenze mondiali.
In piena pandemia, ad esempio, siamo stati immediatamente bombardati da phishing e social engineering a tema COVID-19 o con attacchi mirati ai lavoratori in smart working.
Diverse entità governative, inoltre, sono state colpite da BEC scam (business email compromise) nel momento in cui dovevano rifornirsi di apparati medicali e protezioni contro il COVID-19, cosa che ha causato perdite ingenti e ha influito sulle strategie difensive messe in

atto per gestire l'emergenza.
I ransomware sono in questo momento la minaccia prevalente, utilizzata in più di un terzo degli attacchi noti.
Minacce come vulnerabilità note, 0-day, phishing e social engineering restano sempre tra le più utilizzate. Diminuisce invece la frequenza di attacchi web e DDoS.
Le motivazioni degli attacchi sono sostanzialmente sempre le stesse da 10 anni, ma sono cambiate le proporzioni: il cybercrime rappresenta a questo punto oltre l'80% degli attacchi, mentre espionage e information warfare rappresentano percentuali minori, anche perché per loro natura meno soggetti a divenire di pubblico dominio. È quasi sparito invece il fenomeno dell'hacktivism.
Le categorie più colpite negli ultimi anni sono in particolare Gov / Mil / Law Enforcement, Healthcare, Education, ICT e Finance / Insurance.

D. Secondo te, quanti incidenti non diventano di dominio pubblico, ovvero quanta parte dell'iceberg non è visibile?

R. Purtroppo, la parte dell'iceberg che non vediamo è difficile da stimare.
Da una parte, le normative stanno finalmente obbligando le organizzazioni colpite da attacchi alla disclosure anche in Europa, e questo ci aiuta ad avere più visibilità su cosa sta succedendo.
Il fenomeno ha avuto una ripercussione anche sui dati che classifichiamo: quest'anno un quarto degli attacchi si sono verificati in Europa e, per la prima volta, gli attacchi in America sono scesi sotto il 50%. In America, infatti, dove hanno obbligo di disclosure ormai da tempo, negli anni precedenti si concentravano normalmente la metà degli attacchi noti.
Inoltre, è molto difficile ottenere informazioni in merito a ciò che avviene in America Latina, Asia e Africa, e ciò che riusciamo a classificare relativamente a queste zone è certamente una frazione del totale.
Restano certamente sottostimati gli attacchi con finalità di spionaggio o di intelligence che sono volutamente condotti con molta cautela.

D. Rispetto al totale, quanti incidenti sono di semplice criminalità organizzata e quanti sono invece sponsorizzati da stati sovrani?

R. Nel primo semestre 2021 quasi il 90% degli attacchi ha finalità di cybercrime, una percentuale inaudita, mai vista prima e cresciuta negli anni con un trend molto netto (era intorno all'80% negli anni precedenti).
In questo caso le tecniche maggiormente utilizzate sono malware, in particolare ransomware, vulnerabilità note, phishing e social engineering.
Solo l'11% degli attacchi noti hanno invece finalità di spionaggio, information warfare o operazioni di intelligence.
Le tecniche utilizzate in questo caso sono di norma multiple e complesse, ma c'è la tendenza

a fare maggiormente affidamento ad exploit di bug noti, 0-day e Malware, in particolare RAT (remote access trojan).
Bisogna anche tenere conto del fatto che alcune attività cyber criminali sono svolte anche con finalità di intelligence e che alcuni gruppi che svolgono di norma attività di spionaggio, si possono autofinanziare con attacchi di cybercrime.

5.4 La mappatura dei processi

Per svolgere una corretta analisi dei rischi e il relativo monitoraggio, la rappresentazione dei processi assume un'importanza fondamentale. Costituisce il punto di partenza per una descrizione dettagliata dell'attività dell'organizzazione e, quindi, per l'identificazione delle aree e attività più critiche.
Un'analisi della struttura complessiva di un'organizzazione (detta da alcuni "*enterprise architecture*") parte dai suoi servizi e processi consente di:

- avere una visione condivisa;
- identificare e caratterizzare tutti gli elementi che la costituiscono e come questi sono posti in relazione tra loro;
- identificare i servizi critici per l'organizzazione;
- determinare i livelli di rischio a cui sono esposti;
- identificare le misure tecnologiche, organizzative e procedurali necessarie per mantenere il rischio sotto la soglia ritenuta accettabile dall'organizzazione.

I processi sono legati alla missione dell'organizzazione e quindi ai suoi obiettivi globali. Vanno mappati tutti i processi e non solo quelli critici e ad alto rischio. I processi possono essere di varia natura: quelli fondamentali per la missione dell'organizzazione e quelli di supporto e di gestione dell'organizzazione. Per ciascun processo dovrebbe essere identificata la criticità che riveste per l'organizzazione e i servizi a cui è correlato.

Esistono varie modalità e strumenti per rappresentare i processi. Gli strumenti possono essere basati sui dati e sui flussi dei dati e i documenti coinvolti nell'esecuzione delle attività (*data flow diagram*), sulle comunicazioni e l'interazione tra agenti con enfasi sulle fasi di negoziazione (per esempio, *UML interaction diagram*), sulle attività e le loro sequenze e le interazioni (p.e. *Workflows on an Intelligent and Distributed database Environment* – WIDE e *UML activity diagram*). In quest'ultimo caso i processi sono

visti come insiemi di attività tra loro collegate da vincoli di precedenza e punti di sincronizzazione.
Di seguito un esempio di workflow per la prenotazione di un viaggio.

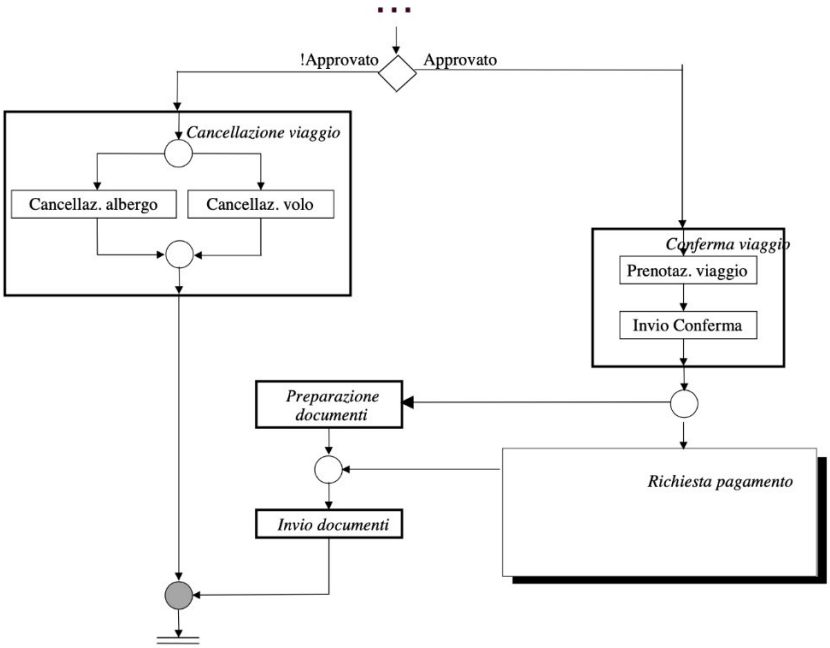

Figura 7 - Esempio di workflow di attività per la prenotazione di un viaggio[39]

Si può rappresentare ogni task svolto nel processo e gli input e gli output di cui è composto. Uno dei principali metodi per i diagrammi di flusso è il *Business Process Modeling Notation* (BPMN), che illustra graficamente la sequenza delle attività e i flussi di informazioni necessari per completare il processo.

Per ogni processo risulta fondamentale identificare le dipendenze, ossia i processi ai quali è correlato. Un processo non critico che produce, ad esempio, input per un processo critico potrebbe comportare un effetto a catena rilevante nel caso di interruzioni, rallentamenti, indisponibilità, compromissione del patrimonio informativo.

È indispensabile, inoltre, un'assegnazione chiara dei ruoli e delle responsabilità

39 Università di Bologna dipartimento DISI, slide corso Reti di Calcolatori. http://www-db.disi.unibo.it/courses/RCPG/workflow.pdf.

all'interno dei processi. Tali ruoli andrebbero rappresentati in matrici RACI delineando per ciascuna attività: chi esegue e assegna l'attività (responsible), chi ha la responsabilità sul risultato dell'attività (accountable), chi collabora per l'esecuzione dell'attività (consulted), chi deve essere solo informato (informed).

Un processo a sua volta può essere composto da sotto-processi e concorrere da solo o con altri processi all'erogazione di servizi. Una mappatura tra servizi, processi, risorse impiegate, dati trattati, tecnologia e sedi consente di avere tutte le informazioni necessarie per una corretta analisi dei rischi. Sapere se un servizio e il relativo processo tratta dati riservati o di dominio pubblico, se il parco macchine è in un data center in disaster recovery o meno, se è ubicato in Europa o fuori dall'Unione, se è legato a un servizio critico, se utilizza applicativi obsoleti o innovativi ci consente di valutare correttamente i rischi.

5.5 Responsabilità per la valutazione del rischio

Il responsabile ultimo della gestione del rischio è sempre il vertice dell'organizzazione.
Il modello che determina chi ha le responsabilità operative varia invece da organizzazione a organizzazione.

Fondamentale è l'individuazione puntuale dei *risk owner* intesi come persone responsabili dell'analisi delle minacce e delle vulnerabilità in specifici ambiti e, conseguentemente, della gestione del rischio anche nelle attività quotidiane. Devono avere i necessari poteri per attuare le adeguate misure di mitigazione dei rischi e interagire con i vertici e le persone incaricate del coordinamento complessivo della gestione dei rischi.

Negli ambienti finanziari la figura di *Chief risk officer* (CRO) ha spesso un ruolo di controllo. Esso potrebbe essere presente anche in organizzazioni in altri settori.
Per la sicurezza delle informazioni, è spesso presente un CISO (*Chief information security officer*) che ha la responsabilità di supervisione della gestione del rischio per la sicurezza delle informazioni, mentre la responsabilità operativa è assegnata al *Chief information officer* (CIO) o *Chief digital officer* (CDO).
Per valutare il rischio è necessario coinvolgere anche il referente privacy.
La figura del CISO è fondamentale nella gestione del rischio digitale. Secondo una

ricerca di Deloitte[40], ci sono quattro ambiti che un CISO deve presidiare, anche per la valutazione del rischio:

- In qualità di tecnologo, il CISO deve guidare nella scelte di tecnologie sicure e diffondere gli standard di sicurezza.
- Nel ruolo di tutore, monitorare l'efficacia dei programmi di miglioramento della sicurezza.
- In qualità di stratega, il CISO deve allineare la sicurezza con la strategia dell'organizzazione per determinare in che modo gli investimenti in sicurezza possono portare valore.
- In quanto consulente, il CISO aiuta le persone a comprendere i rischi relativi alla sicurezza informatica in modo che possano prendere decisioni corrette sulla base delle informazioni ricevute.

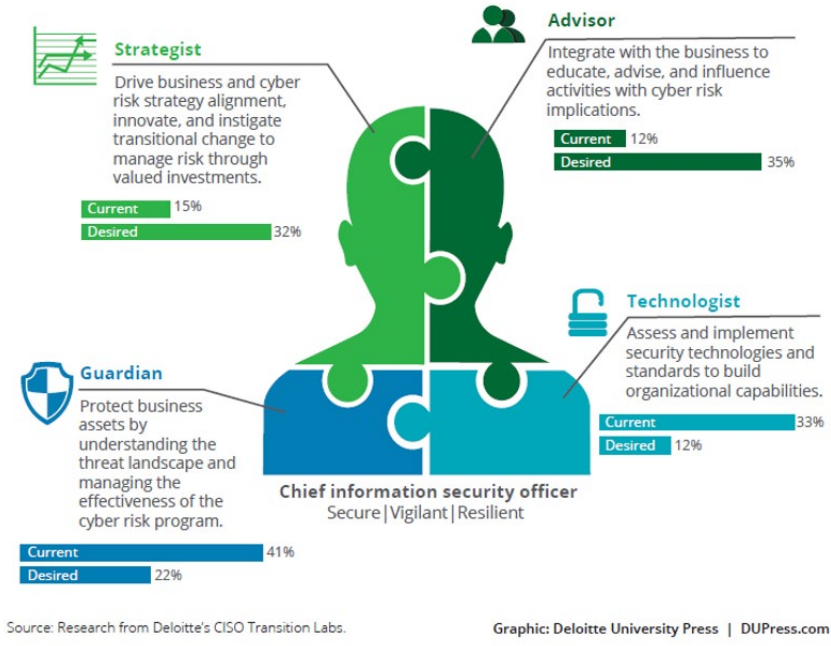

Figura 8 - I ruoli del CISO[41]

40 https://www2.deloitte.com/content/dam/insights/us/articles/ciso-next-generation-strategic-security-organization/DR19_The-NewCISO.pdf.

41 https://www2.deloitte.com/content/dam/insights/us/articles/ciso-next-generation-strategic-security-organization/DR19_The-NewCISO.pdf

Sono richieste competenze specifiche su:

- minacce, tecniche di attacco e normative;
- gestione delle organizzazioni, per comprendere quali sono le priorità della propria e perché si sono prese determinate decisioni; è utile anche approfondire le caratteristiche del settore della propria organizzazione per avere una prospettiva più ampia;
- gestione del rischio;
- comunicazione, per discutere con personale tecnico, partecipare a riunioni direzionali o presentare al vertice dell'organizzazione.

5.6 Valutazione dei rischi e vulnerabilità

L'identificazione e la valutazione delle vulnerabilità è componente necessaria per il calcolo del rischio, come previsto dalla maggior parte dei framework di analisi del rischio. Le vulnerabilità possono essere di due tipi:

- la mancata attuazione dei controlli; di conseguenza le vulnerabilità vengono identificate attraverso la valutazione dello stato di applicazione di liste di controlli, come ad esempio quelli della ISO/IEC 27001;
- le debolezze intrinseche delle componenti che potrebbero essere sfruttate da attaccanti. In merito alle vulnerabilità i sistemi di classificazione più significativi emersi negli ultimi anni sono due. Questi sono:
  - quello proposto da OWASP, decisamente buono ma, per alcuni, sorpassato dal framework della MITRE;
  - il sistema di classificazione, un vero e proprio framework, della Mitre che mette a confronto le debolezze del software (CWE) con le vulnerabilità proprie di un prodotto (CVE) che potrebbero essere sfruttate da attaccanti (vedere il successivo paragrafo su ATT&ACK); esso è ritenuto particolarmente autorevole per completezza, aggiornamento e per la sua capacità di mettere a sistema i fattori citati.

Nel seguito saranno prese in considerazione solo le vulnerabilità di cui al punto 2.

5.6.1 Vulnerabilità note

Si elencano alcune classificazioni utili al fine dell'enumerazione delle vulnerabilità note.

Common Vulnerabilities and Exposures (CVE)

Il CVE, "*Common Vulnerabilities and Exposures*", è un dizionario di vulnerabilità pubblicamente note. Nello *US National Vulnerability Database*, mantenuto dalla MITRE Corporation, sono elencati gli identificativi di ogni CVE[42]:

- CVE Id: composto da CVE, anno e numero sequenziale (es. CVE-2021-38088);
- breve descrizione della vulnerabilità;
- ogni altro riferimento utile[43].

Mitre è l'autorità primaria per l'assegnazione delle CVE (*CVE Numbering Authority*, CNA). Al di sotto di questa vi sono varie autorità subordinate (Microsoft, Red Hat, Oracle, ecc.), alle quali vengono assegnati blocchi di numeri da impiegare per i propri prodotti. Vi sono poi altre autorità come il CERT Coordination Center che può assegnare dei CVE Id.

Common Vulnerability Scoring System (CVSS)

Il CVSS, "*Common Vulnerability Scoring System*", è uno standard di settore per la valutazione della gravità delle vulnerabilità della sicurezza dei sistemi informatici[44].
Mentre la CVE permette di avere elementi sulla singola vulnerabilità, il CVSS permette di contestualizzarla. Infatti non ha molto senso parlare di gravità di una CVE senza avere calcolato gli effetti che questa vulnerabilità può avere sullo specifico sistema in un determinato contesto.
Il CVSS è molto importante ed efficace perché permette di valutare la gravità di ogni singola vulnerabilità conosciuta e la priorità da dare, in base alle risorse, alle risposte nei confronti delle minacce. Ciò porta, nel processo di trattamento del rischio, ad associare a ciascun valore di vulnerabilità il percorso decisionale più efficace.

Common Weakness Enumeration (CWE)

Il CWE, ovvero "Common Weakness Enumeration"[45], è un elenco sviluppato dalla comunità di utenti di tipi di debolezze del software (commerciale o open source) e dell'hardware. Serve come linguaggio comune, metro per gli strumenti di sicurezza del software e base per l'identificazione delle debolezze, le mitigazioni e gli sforzi

42 https://cve.mitre.org/.

43 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38088.

44 http://www.first.org/cvss/.

45 http://cwe.mitre.org/.

di prevenzione. Il CWE offre una tassonomia delle vulnerabilità suddividendole in circa 700 categorie tra cui: *buffer overflow*, *path/directory tree traversal error*, *race condition*, *cross-site scripting*, *hard-coded password* e *insecure random number*.

È destinato a strumenti e servizi di sicurezza atti a trovare punti deboli nel codice sorgente e nei sistemi operativi e aiuta a comprendere e gestire meglio le carenze del software legate all'architettura e allo sviluppo facendo riferimento a sistemi noti[46] come CWE Top 25 e OWASP Top Ten.

Common Weaknesses Scoring System (CWSS)

Analogamente al sistema CVSS, anche per le CWE esiste un sistema analogo noto come CWSS[47]. In questo caso, a ogni "CWE id" è assegnato un punteggio da 0 a 100 (dove 0 è l'impatto nullo e 100 sono le conseguenze catastrofiche).

La tabella seguente consente di mettere a confronto il sistema CWSS con il CVSS.

CVSS	CWSS
Assume che una vulnerabilità sia già stata scoperta e verificata	Può essere utilizzato prima che una nuova debolezza sia già stata scoperta
Non dà la possibilità di utilizzare risposte standard	Può fornire una risposta più accurata grazie a una migliore conoscenza
	Cataloga un solo aspetto per volta

CAPEC

CAPEC, ovvero il "*Common Attack Pattern Enumeration and Classification*", è un dizionario di modelli di attacco utilizzati per sfruttare le vulnerabilità note nei sistemi informatici (p.e. SQL Injection, XSS, Session Fixation, Clickjacking). Vi sono due visualizzazioni diverse:

- Meccanismi di attacco;
- Domini di attacco.

Entrambe le viste contemplano 541 tipi di modelli, ognuno identificato da un ID univoco.

46 https://cwe.mitre.org/data/index.html.

47 https://cwe.mitre.org/cwss/

ATT&CK

L'*Adversarial Tactics, Techniques & Common Knowledge* (ATT&CK)[48] è della Mitre. Questa base di conoscenza è dedicata alla difesa della rete, presenta un modello per comprendere il comportamento degli attaccanti prima e dopo l'attacco (ad esempio persistenza, movimento laterale, esfiltrazione) e dettaglia le tattiche, tecniche e procedure specifiche (TTP) che gli *advanced persistent threat* (APT) impiegano per raggiungere i propri obiettivi. L'uso di TTP permette, tra le altre cose, di fare attività di indagine individuando i possibili autori (cioè permette la cosiddetta *attribution*) di un attacco attraverso una selezione rapida e contestualizzata dell'evento.
Molti modelli di attacco elencati da CAPEC sono impiegati con tecniche descritte da ATT&CK.

CAPEC	ATT&CK
Consente di mappare le minacce alle applicazioni	Consente di valutare le capacità di difesa della rete informatica
Agevola la formazione degli sviluppatori	È un ausilio alla difesa dalle APT e alla ricerca di nuove minacce
È una guida per i test di penetrazione	Migliora la threat intelligence
	Consente di esercitarsi emulando un attaccante

5.6.2 Ricerca e identificazione delle vulnerabilità

Il metodo per identificare le vulnerabilità, conosciute (ed elencate nel CVE) e sconosciute, di un sistema è il cosiddetto *Vulnerability Assessment* (VA).
Seguendo le indicazioni della ISO/IEC 27005 e della ISO/IEC 18045 (CEM o manuale di valutazione dei Common Criteria di cui alla ISO/IEC 15408) si evince che il processo di *vulnerability assessment* si articola in quattro fasi di complessità ed efficacia crescenti:

48 https://attack.mitre.org/.

- La prima fase prevede un vulnerability scanning, eseguito con strumenti automatici di scansione delle vulnerabilità (tra i più diffusi vi sono Nessus e OpenVAS); esso permette di individuare una buona parte delle vulnerabilità già note (solitamente non più del 50% delle CVE presenti).
- La seconda fase prevede un security test evaluation (STE), con il quale si svolgono dei test di base tesi alla ricerca delle vulnerabilità più semplici. Ad esempio, se i requisiti di sistema dicono che la password deve essere di almeno 8 caratteri il test consiste nel provare password con lunghezza minore.
- Successivamente si eseguono penetration test (PT) effettuati da persone con elevate competenze tecniche. Questi test normalmente mancano della caratteristica della riproducibilità, infatti due diversi penetration tester difficilmente attueranno le stesse procedure di attacco e anche i risultati sono spesso diversi. Secondo i Common Criteria, il PT può limitarsi alla sola Proof of Concept (PoC).
- Il metodo più efficace per l'individuazione delle vulnerabilità è quello del riesame del codice sorgente (code review), attività solitamente molto complessa (e pertanto richiesta dai Common criteria dal livello EAL 4 in su).

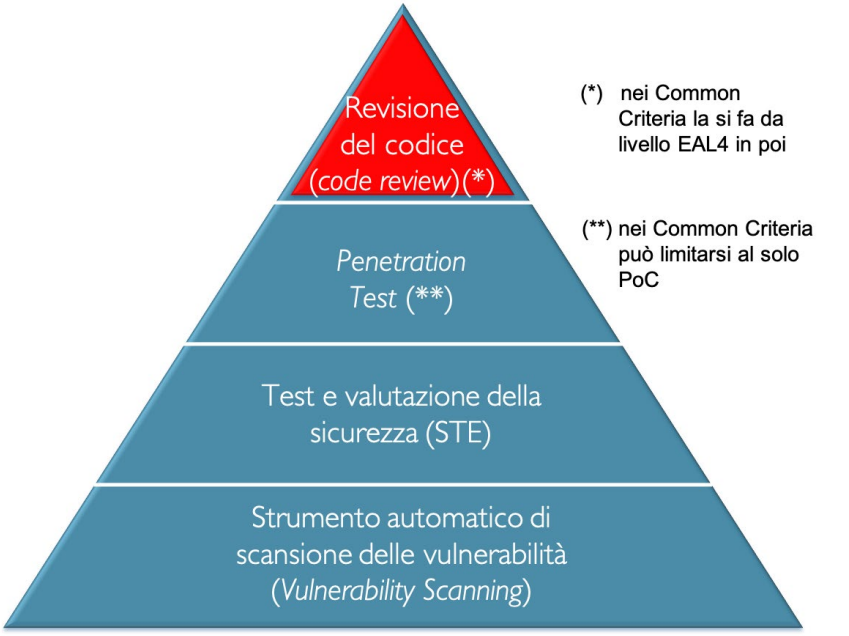

Figura 9 - VA & PT per ISO/IEC 18045 e 27005[49]

49 Figura degli autori.

5.6.3 Utilizzo delle vulnerabilità tecniche nella valutazione del rischio

L'utilizzo nella valutazione del rischio delle vulnerabilità tecniche, anche facendo riferimento a un sistema di tracciamento e punteggio (*scoring*), permette di prendere le decisioni più adeguate in merito alle modalità e ai tempi di risoluzione delle vulnerabilità tecniche. Poiché nuove vulnerabilità vengono rilevate in continuazione, questo tipo di approccio richiede di attuare un processo automatizzato per la valutazione del rischio.
A titolo di esempio, il tool software Pilar, che implementa Magerit, utilizza le informazioni relative alle vulnerabilità tecniche associate agli asset per il calcolo del rischio[50].

5.7 Il rischio dell'analisi del rischio

L'esecuzione di un'analisi dei rischi è un'attività ricca di incognite, sia per quanto concerne la sua conduzione, sia per quanto attiene i risultati ottenuti. È quindi particolarmente importante che si abbia consapevolezza di questi limiti.
Per la ISO 31010, l'analisi dei rischi è caratterizzata da una serie di incertezze, fra le quali:

- gli errori negli approcci utilizzati;
- il fatto che gli eventi futuri non necessariamente saranno simili al quelli del passato;
- la conoscenza imperfetta o incompleta delle minacce;
- le vulnerabilità ancora da scoprire;
- le dipendenze non riconosciute, che possono portare a impatti imprevisti.

Per la NIST SP 800-30 Rev.1 un'analisi del rischio non è uno strumento preciso ed è condizionata da:

- gli strumenti e le tecniche di valutazione impiegati;

50 https://www.pilar-tools.com/doc/CVE_73.pdf

- la soggettività, la qualità e l'affidabilità dei dati utilizzati;
- l'interpretazione dei risultati della valutazione;
- le capacità e le competenze di chi effettua le valutazioni.

Per tale motivo dovrebbero essere adeguatamente documentate:

- le scelte effettuate;
- l'approccio scelto;
- il momento in cui è stata condotta l'analisi;
- il perimetro di indagine;
- la giustificazione di completezza;
- la giustificazione di accuratezza con cui si è svolta l'analisi dei rischi.

5.7.1 Gli errori degli approcci

Relativamente all'approccio, fra i possibili errori si riscontrano:

- l'utilizzo di operatori matematici non corretti (la moltiplicazione presente nella formula è corretta se i parametri di probabilità e impatto sono espressi con scale lineari; se viceversa vengono espressi con scala logaritmica è invece necessario utilizzare la somma);
- la mancata documentazione del significato attribuito a valori espressi in forma qualitativa (ad esempio che cosa si intende per Alto, quando si parla di impatto, probabilità e rischio);
- la mancata documentazione della motivazione che ha portato alle valutazioni dei parametri di probabilità e impatto e dei soggetti che hanno partecipato alla valutazione;
- la mancata indicazione, allorquando si valuta l'impatto, di quale sia l'impatto al quale ci si riferisce (valore dell'asset interessato dall'evento avverso, costo del suo ripristino, mancato guadagno, perdita di clienti, legale, reputazionale, sanzionatorio);
- la mancata indicazione della profondità temporale da considerare per la valutazione dell'impatto (le conseguenze di un evento sono sia immediate sia protratte nel tempo e dovrebbe pertanto essere definito un tempo limite entro quando stimare gli impatti);
- la mancata indicazione circa il fatto che si stia considerando nella valutazione dell'impatto un valore medio o il caso peggiore;

- la mancata indicazione sul fatto che si stia parlando di rischio inerente o di rischio residuo;
- l'uso del rischio inerente (ossia senza prendere in considerazione le strategie di mitigazione e i controlli di sicurezza attuati), senza considerare che l'adozione di contromisure è endemica a ciascuna organizzazione, anche quando destrutturata o non rivolta specificatamente al contenimento del rischio oggetto di analisi (ci possono essere controlli posti in essere per gestire un rischio diverso da quello oggetto d'analisi, ma che comunque lo altera);
- l'eccessiva semplificazione del modello che non tiene conto della correlazione esistente fra gli asset (un dato è registrato su un disco fisso che è presente in un pc che è in un edificio...), le probabilità, gli impatti e i rischi (ad esempio, la stessa minaccia potrebbe avere effetti sia sull'asset, sia sull'eventuale contromisura).

5.7.2 Aspetti psicologici e pregiudizi (bias) nella percezione del rischio

Negli ultimi anni gli sforzi continui per definire e classificare scientificamente e matematicamente il rischio attraverso processi e metriche standardizzati, nei vari campi applicativi, hanno permesso di migliorare le decisioni, in ambito privato e pubblico.

Ma l'approccio tecnico-scientifico non sembra considerare tutte le variabili in gioco: troppe volte abbiamo assistito o assistiamo a decisioni (di rilevanza strategica) prese senza avere considerato o, avendo perlomeno sottovalutato, anche i rischi più evidenti.[51] Cos'è allora che "distorce" gli indicatori di valutazione del rischio, cos'è che fa sottovalutare o, in antitesi, sopravvalutare un rischio?

Secondo gli psicologi, la percezione del rischio è un processo cognitivo utilizzato dalla mente umana in diverse attività abituali che orienta i comportamenti di fronte a decisioni che possono implicare potenziali rischi. Il rischio è percepito considerando varie dimensioni come, per esempio, le conseguenze immediate e future e le loro implicazioni tanto su un piano razionale e oggettivo quanto su un piano emozionale e soggettivo. Studi approfonditi hanno indicato che molto frequentemente esiste una sostanziale differenza tra la percezione soggettiva del rischio e la valutazione oggettiva. [52]

51 L. Savadori, R. Rumiati. Nuovi rischi e vecchie paure. Bologna: Il Mulino, 2005.

52 P. Slovic. The Perception of Risk. London, UK: Earthscan Publications Ltd, 2001.

In poche parole, le persone a volte temono attività in realtà non pericolose e non temono, invece, attività che potrebbero avere conseguenze molto drammatiche.

Esistono meccanismi generali che sottendono al modo in cui le persone elaborano le informazioni provenienti dall'ambiente e anche quelle che hanno in memoria. I principali processi sono le *euristiche cognitive* ed i *bias cognitivi*, entrambi hanno un ruolo sostanziale nel modo in cui le persone valutano il rischio di un'attività. In particolare, si tratta di strategie di pensiero che agiscono generalmente a livello inconsapevole.

Le euristiche cognitive

Le euristiche (dal greco *heurískein*: trovare, scoprire) sono procedimenti mentali intuitivi e sbrigativi, delle specie di scorciatoie mentali, che permettono di costruire un'idea generica su un argomento senza troppi sforzi cognitivi. Sono strategie utilizzate di frequente per giungere rapidamente a delle conclusioni, anche se spesso, inconsciamente, ci si dimentica che si tratta di semplificazioni.

Nel 2002 Kahneman e Frederick[53] teorizzarono che l'euristica cognitiva funzionasse per mezzo di un sistema chiamato "sostituzione dell'attributo", che avviene senza consapevolezza. In base a questa teoria, quando qualcuno esprime un giudizio complesso da un punto di vista inferenziale, risulta essere sostituito da un'euristica che è un concetto affine a quello precedente, ma formulato più semplicemente. Le euristiche sono, dunque, trucchi mentali che portano a conclusioni veloci con il minimo sforzo cognitivo.

I pregiudizi (bias) cognitivi

I bias cognitivi sono costrutti fondati, al di fuori del giudizio critico, su percezioni errate o deformate, su pregiudizi e ideologie; utilizzati spesso per prendere decisioni in fretta e senza fatica. Si tratta, il più delle volte di errori cognitivi che impattano nella vita di tutti i giorni, non solo su decisioni e comportamenti, ma anche sui processi di pensiero.

Quindi, i bias sono particolari euristiche usate per esprimere giudizi, che alla lunga diventano pregiudizi, su cose mai viste o di cui non si è mai avuto esperienza. Mentre le euristiche funzionano come una scorciatoia mentale e permettono di avere accesso a informazioni immagazzinate in memoria.

In sintesi, se le euristiche sono scorciatoie comode e rapide estrapolate dalla realtà che portano a veloci conclusioni, i bias cognitivi sono euristiche inefficaci, pregiudizi astratti che non si generano su dati di realtà, ma si acquisiscono a priori senza critica o giudizio.

53 Daniel Kahneman, Shane Frederick. Heuristics and Biases: The Psychology of Intuitive Judgment. New York, USA: Cambridge University Press, 2002.

Activity or Technology	League of Women Voters	Collee students	Active club members	Experts
Nuclear power	1	1	8	20
Motor vehicles	2	5	3	1
Handguns	3	2	1	4
Smoking	4	3	4	2
Motorcycles	5	6	2	6
Alcoholic beverages	6	7	5	3
General (private) aviation	7	15	11	12
Police work	8	8	7	17
Pesticides	9	4	15	8
Surgery	10	11	9	5
Fire fighting	11	10	6	18
Large construction	12	14	13	13
Hunting	13	18	10	23
Spray cans	14	13	23	26
Mountain climbing	15	22	12	29
Bicycles	16	24	14	15
Commercial aviation	17	16	18	16
Electric power (non nuclear)	18	19	19	9
Swimming	19	30	17	10
Contraceptives	20	9	22	11
Skiing	21	25	16	30
X-rays	22	17	24	7
Hig school and college football	23	26	21	27
Railroads	24	23	29	19
Food preservatives	25	12	28	14
Food coloring	26	20	30	21
Power mowers	27	28	25	28
Prescription antibiotics	28	21	26	24
Home applicances	29	27	27	22
Vaccinations	30	29	29	25

Figura 10 - Tabella di percezione del rischio per 30 attività e tecnologie[54].
L'ordine è basato sulla media geometrica dell'indice di rischio dentro ciascun gruppo.
Il valore 1 rappresenta l'attività o tecnologia a maggior rischio.

Una sintetica selezione di bias che potrebbero parzialmente inficiare un'analisi del rischio[55]:

- Il **zero risk bias** che digrada verso il risk aversion bias, sono caratterizzati da emozioni negative quali apprensione e ansia. L'analista, soggetto a tali bias, sovrastimerebbe i fattori di rischio o cercherebbe un rischio vicino allo zero

54 P. Slovic. The Perception of Risk. London, UK: Earthscan Publications Ltd, 2001.

55 Gilberto Montibeller, Detlof von Winterfeldt. "Cognitive and Motivational Biases in Decision and Risk Analysis". Risk Analysis, Vol. 35, No. 7. 2015. DOI: 10.1111/risa.12360.

incrementando in maniera non giustificata i costi.

- Il **risk neutrality** bias o insensibilità al fattore di rischio, potrebbe comportare una incapacità o scarsa sensibilità da parte del soggetto di comprendere appieno il fattore di rischio.
- Il **risk appetite bias** e il **risk lovers bias**, dove le emozioni legate al fattore di rischio sono persino positive, quasi adrenaliniche, potrebbero indurre a sottostime o trascuratezza nella valutazione.
- **Omitted variable bias** e **myopic problem** per cui l'analista potrebbe non essere sufficientemente meticoloso o semplicemente omettere talune variabili, soggettivamente ritenute poco significative. Il risultato sarà un'analisi del rischio incompleta, che enfatizzi verosimiglianza e impatto dei soli elementi individuati.
- Il **confirmation bias** rappresenta la naturale propensione a confermare scelte precedenti, sottovalutando nuove variabili che potrebbero smentirle. L'incapacità di trovare difetti nelle proprie argomentazioni non è una prova di giustezza, ma un sintomo del confirmation bias.
- Il **bandwagon** bias è la naturale tendenza a "salire sul carro del vincitore" e inconsciamente conformarsi al pensiero precostituito. Anche in termini di analisi del rischio questo potrebbe essere un problema poiché limita il pensiero critico.
- L'**availability bias** è la propensione a esaltare la significatività di eventi recenti o emotivamente impattanti, particolarmente vividi nella memoria. Tuttavia questa è suggestionata dalla rilevanza mediatica, dalla sua vicinanza o da altri elementi soggettivi.
- L'**equalizing bias** è la tendenza dell'analista ad appiattire i valori, attribuendo valori eccessivamente omogenei. Questo bias è tipico delle analisi qualitative, soprattutto se le categorie sono a soli quattro fattori; la naturale tendenza porta ad escludere o sotto utilizzare la categoria "Alto" e concentrarsi sulle sole etichette "Basso" e "Medio basso".
- Il **desirability bias** porta inconsciamente ad assegnare probabilità più elevate a eventi e risultati per noi desiderabili, o ad assegnare probabilità inferiori agli indesiderabili.
- **Overconfidence bias** o underconfidence bias per cui, per eccesso o scarsità di fiducia, l'analisi del rischio viene falsata dalla fiducia o sfiducia dell'analista in determinate contromisure.
- L'**anchor bias** rappresenta l'incapacità dell'analista di allontanarsi troppo dal primo numero a cui pensa o con cui entra in contatto, quasi fosse una barca all'ancora.
- Il **pseudo-certainty effect** o **effetto di pseudo-certezza** è la tendenza a

percepire un risultato incerto come certo. Ciò si osserva principalmente nei processi decisionali a più fasi, in cui ci si dimentica che i valori stimati comportano sempre in sé uno scarto probabilistico. L'intervallo di confidenza per una probabilità infatti è sempre + o - uno scarto d'errore. Lo scarto d'errore, in quanto probabile e non certo, viene trascurato e, soprattutto nelle analisi quantitative, non più computato.

L'elemento ulteriormente complicante è dato dal fatto che analista e destinatari dell'analisi potrebbero avere diverse tolleranze al rischio o essere affetti da bias differenti.

Percezione del rischio in ambito personale

Ciò che rende questi stili di pensiero disfunzionali non è la loro presenza, ma la loro rigidità e inflessibilità, specialmente se conduce a interpretare gli eventi, e noi stessi, in modo irrealisticamente negativo.

Le distorsioni cognitive possono essere riconosciute e modificate allo scopo di riformulare pensieri più realistici, adattivi e funzionali in modo da migliorare il nostro processo decisionale e, per quanto indicato sopra, migliorare il nostro benessere.

Alcuni studi hanno dimostrato che esistono diversi fattori che influenzano la percezione che le persone hanno della pericolosità di un'attività. Tra i fattori principali ci sono:

- quanto controllo è possibile esercitare sugli eventi che possono generare pericolo (per esempio, si pensa di poter esercitare molto controllo nel caso della guida e molto poco nel caso dei cataclismi naturali);
- quanto volontariamente la gente ha deciso di affrontare una situazione rischiosa;
- quanto gravi sono le possibili conseguenze[56].

Altri fattori[57] possono essere l'ampiezza del rischio (p.e. basata su quante persone sono esposte), la diversità (p.e. le differenze di sfera sociale), fiducia nelle autorità[58].

Utilizzando l'analisi di tipo fattoriale, le variabili in gioco possono essere raggruppate in fattori, per esempio: "rischio terrificante" e "rischio sconosciuto". Il primo fattore indica il livello di quanto catastrofico è il rischio associato a una certa attività, mentre il secondo fattore indica quanto è osservabile e controllabile quel rischio. Utilizzando questi fattori è possibile costruire una *mappa cognitiva* della rischiosità che ciascuna persona associa a una determinata attività. In questo modo è possibile comprendere

56 P. Slovic. Perception of risk. Science. 1987, 236, 280-285.

57 P. Vermigli, S. Raschielli, E. Rossi, Antonio Roazzi. Gravità e probabilità nella percezione del rischio: Influenza delle caratteristiche individuali sesso, genitorialità ed expertise. Giornale di Psicologia, Vol. 3, No. 1. 2009. ISSN 1971-9558.

58 M. Siegrist, G. Cvetkovich, Perception of hazards: The role of social trust and knowledge. Risk Analysis. 2000, 20, 713-720. doi: 10.1111/0272-4332.205064

come mai le persone possono associare rischi differenti ad attività che hanno la stessa probabilità di produrre conseguenze negative[59].

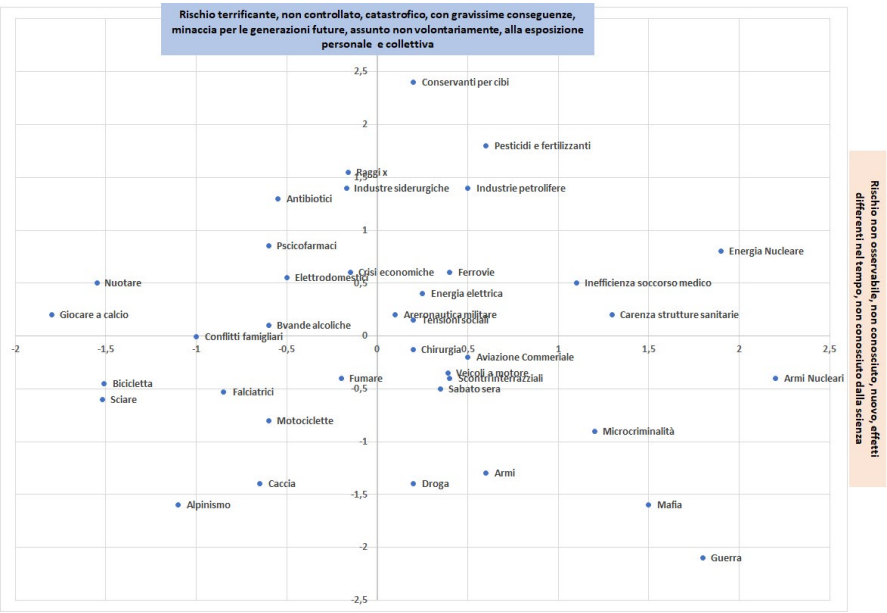

Figura 11 - Rappresentazione mentale del rischio in un campione di soggetti non esperti[60]

La percezione del rischio in ambito lavorativo

Euristiche e bias cognitivi possono influenzare molto anche i processi decisionali in ambito professionale e lavorativo. In un'organizzazione, se da un lato si lavora molto per rendere "oggettivo" il rischio, dall'altro si fa ancora molto poco per contrastare gli errori introdotti dagli aspetti psicologici e le sensibilità (o mancanza di sensibilità) individuali.

Queste derive nella corretta percezione del rischio possono incidere in situazioni complesse, in cui il "contatto" con la realtà è fortemente indiretto (immaginiamo le decisioni basate sull'analisi del rischio digitale). Con i criteri dell'analisi fattoriale indicati sopra è possibile capire quanto sia complessa la valutazione dei rischi digitali, vista la variabilità della minaccia e la quantità e qualità dei dati che devono essere analizzati.

59 E. Mullet, C. Lazreg, C. Candela, F. Neto. The Scandinavian way of perceiving societal risks. Journal of Risk Research. 2005, 8, 19 – 30.

60 Lucia Savadori et al. Expertise and regional differences in risk perception : the case of Italy. Swiss Journal of Psychology. 1998, 57, 101-113.

In un'organizzazione, le esperienze e le sensibilità individuali non dovrebbero essere trascurate. Si supponga di analizzare la percezione del rischio informatico di due figure professionali che devono decidere o supportare nel processo decisionale legato a possibili investimenti in ambito IT:

- Il vertice quasi mai ha competenze tecniche informatiche approfondite, anzi, raramente vuole avere a che fare direttamente con questioni di questo tipo; l'informatica è un servizio (percepito come costoso) che, probabilmente, serve ma non è indispensabile per le proprie attività. Difficile possa immaginarsi conseguenze "catastrofiche", soprattutto se non ci sono stati dei precedenti significativi.
- Il consulente informatico basa l'analisi sugli aspetti tecnologici, ma non conosce approfonditamente il contesto e i processi dell'organizzazione. Il consulente ha probabilmente molto chiaro il rischio legato alle apparecchiature informatiche ma ha certamente difficoltà nel convincere il suo interlocutore sulle possibili implicazioni disastrose per l'organizzazione.

Debiasing

Daniel Kahneman (uno psicologo israeliano, vincitore, insieme a Vernon Smith, del Premio Nobel per l'economia nel 2002 «per avere integrato risultati della ricerca psicologica nella scienza economica, specialmente in merito al giudizio umano e alla teoria delle decisioni in condizioni d'incertezza») fornisce una soluzione per combattere i bias: imparare a non fidarsi delle proprie impressioni e riconoscere lo schema fallace che mettiamo in atto.
Le tecniche di *debiasing* includono:

- formarsi per analizzare le situazioni in cui agiscono i bias e avere un riscontro immediato sul risultato che essi provocano;
- consider the opposite: porsi delle domande sull'efficacia dell'attribuzione sistematica;
- utilizzare approcci quantitativi abbinati a quelli qualitativi, in modo da avere riscontri oggettivi attraverso misurazioni o test derivanti da studi o esperienze analoghi;
- adottare strumenti di supporto informatico alle decisioni e, per le analisi qualitative, scale di valutazione prive di valori centrali;
- confrontare le decisioni con altre persone in modo da diminuire il rischio di errore e di aumentare il numero delle informazioni raccolte; nessuno può permettersi di rinchiudersi nella torre ma si deve curare lo scambio di informazioni, la condivisione di esperienze e l'approfondimento continuo;

- annotare considerazioni, esperienze e processi decisionali che hanno contribuito all'assegnazione dei valori e alle scelte.

5.8 Il rapporto di valutazione del rischio

L'attività di analisi giunge a conclusioni e offre indicazioni, che dovranno essere valutate opportunamente. Vediamo in cosa consiste il rapporto (o report) di valutazione del rischio e la sua comunicazione.
Da una parte vengono evidenziate le istanze di carattere puramente tecnico che possono essere risolte direttamente in tale contesto; altre, invece, possono mettere in evidenza rischi di tipo strutturale e organizzativo che necessitano di un intervento decisionale di respiro più ampio (per esempio, la scelta di trasferire il rischio di un intero processo ad altro fornitore specializzato). Deve essere quindi previsto in anticipo un piano di comunicazione dei risultati.

Si deve evitare che il processo di analisi del rischio sia un'attività fine a se stessa che non abbia ben chiaro un destinatario preciso, o che, per contro, ecceda l'obiettivo che ci si pone, distribuendo in modo incontrollato le informazioni emerse da questo tipo di attività.

Prima di iniziare un'analisi del rischio devono essere chiari i soggetti a cui è destinata l'analisi del rischio stessa. Tra questi devono essere inclusi il vertice dell'organizzazione, i responsabili tecnici, i clienti che possono richiedere informazioni sul livello di rischio delle attività svolte dall'organizzazione per conto loro, i fornitori che, facendo parte della catena del valore, possono essere fonti di rischio per l'organizzazione, il mercato e gli investitori. Ognuno di questi soggetti ha sensibilità e necessità informative differenti (e in alcuni casi la comunicazione errata potrebbe costituire essa stessa un rischio). Queste necessità informative devono essere la guida per identificare i modelli di report da produrre e i canali di comunicazione attraverso cui trasmetterli. Per esempio: verso i clienti dovrà essere veicolata dai commerciali, verso i vertici dall'audit interno, verso il mercato dal marketing.

Il processo di comunicazione dei rapporti deve anche assicurarne la riservatezza.

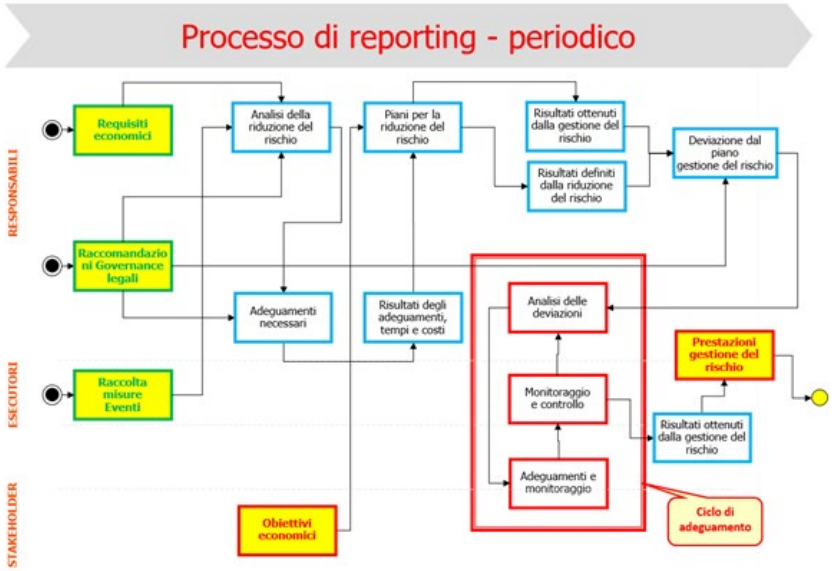

Figura 12 - Il processo di reporting[61]

Il rapporto tecnico deve permettere l'identificazione, da parte delle strutture tecniche, delle possibili soluzioni per il trattamento del rischio e mettere in luce i relativi controlli sui quali bisogna focalizzare l'attenzione.

Il rapporto per i tecnici deve fornire evidenze di vulnerabilità tecniche. Il rapporto dovrebbe anche indicare tutti gli eventi che potrebbero verificarsi a causa dello sfruttamento di una vulnerabilità. È opportuno notare che alcune vulnerabilità non sono tanto dipendenti da istanze tecnologiche (aspetti tecnici) ma quanto da una loro errata, incompleta o superficiale modalità di uso (processo).

Il rapporto per il vertice potrà includere cruscotti di sintesi (*dashboard*), le situazioni di rischio più critiche opportunamente filtrate per famiglie di rischi, analisi specifiche per divisione organizzativa o per processo, lo stato effettivo della risposta al rischio e tendenze di rischio emergenti.

Nell'Appendice B della pubblicazione COBIT 5 for Risk, "Detailed Risk Governance and Management Enablers" all'Enabler Information di Cobit5, sono descritte le caratteristiche di un rapporto di rischio.

61 Figura degli autori.

5.9 Far tesoro delle lezioni apprese

Al termine di un processo di analisi del rischio, in un'ottica di miglioramento continuo, è fondamentale incorporare le lezioni apprese, dare valore all'esperienza maturata e ovviamente evitare di ripetere errori commessi in precedenza.
Il *Lesson Identified* è un processo formale di apprendimento.
Qui di seguito si mostra uno schema esemplificativo del ciclo di vita del processo così come rappresentato nel "NATO Lessons Learned Handbook"[62].

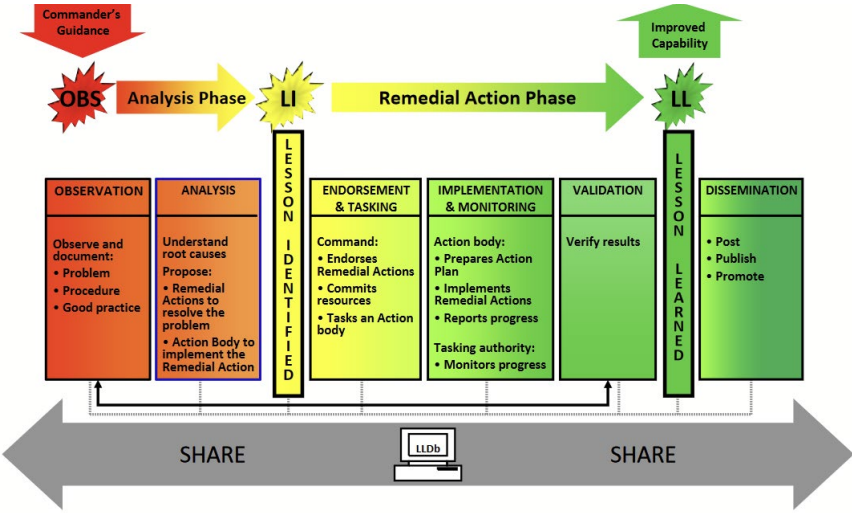

Figura 13 - Processo di apprendimento delle lezioni[63]

5.9.1 Identificare le lezioni

Nel corso di qualsiasi attività, che ci coinvolga quotidianamente, si è costantemente alla ricerca di un sistema, che ci permetta di fare le cose in modo più semplice o più efficiente, e che possa essere, una volta acquisito per noi stessi, trasmesso agli altri per aiutarli ad evitare di ripetere gli errori e migliorarsi.

62 https://nllp.jallc.nato.int/iks/sharing%20public/nato%20lessons%20learned%20handbook%202016%203rd%20edition.pdf.

63 NATO Lessons Learned Handbook, third edition. USA: NATO, Joint Analysis and Lessons Learned Centre, 2016

In una fase iniziale questa attività assume la veste di *Lesson Identified* (LI), definita come un'osservazione opportunamente approfondita relativamente alla radice del problema osservato. Le LI vanno documentate con: la sequenza degli eventi, le condizioni in cui gli eventi sono avvenuti e altri dettagli.
Le LI, se accettate, vanno seguite da azioni correttive da pianificare (con tempi e responsabilità). Un'azione correttiva è "l'attività o l'insieme di attività che corregge un problema identificato per il miglioramento o per facilitare l'attuazione di *best practice*".

5.9.2 Apprendere le lezioni

Dopo il completamento dell'azione correttiva e la convalida con successo da parte del vertice, la *Lesson Identified (LI)* viene considerata una *Lesson Learned* (LL) e il processo formale si conclude. La LL viene catalogata in un apposito registro, cui possano attingere gli utenti per un miglioramento continuo delle operazioni.
La NATO definisce le LL come: "migliori capacità o aumento di prestazioni, confermate se necessario da una convalida, risultanti dall'attuazione di una o più azioni correttive per una *lesson identified*". È fondamentale che la LL sia diffusa e le informazioni relative condivise e comprese.
Le singole *lesson identified* possono essere associate una o più *lesson learned* (una stessa LI può dare luogo ad azioni in differenti unità organizzative, ognuna con la sua LL) o viceversa (es. due LI relative ad acquisti possono concretizzarsi in una sola LL da parte del CFO).

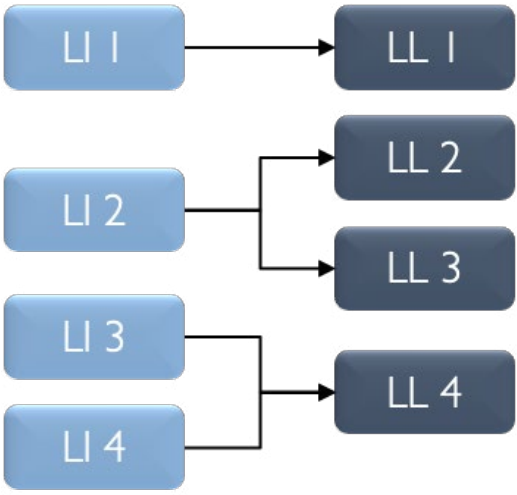

Figura 14 - Relazioni tra lesson identified e lesson learned

5.9.3 Incidenti e lezioni apprese

Un caso particolare di impiego delle *lesson learned* è contemplato nella SP 800-61 del NIST dal titolo "Computer Security Incident Handling Guide". Essa individua, nella fase di post-incidente, la necessità di tenere una riunione per determinare quali sono le lezioni apprese. Ciò al fine di impiegarle come strumento che possa consentire al team di risposta agli incidenti di evolvere, di migliorare le misure di sicurezza e tutto il processo di gestione degli incidenti.
Anche in questo caso si sottolinea il fatto che le lezioni apprese e le conseguenti azioni concordate, che potrebbero comportare l'attuazione di misure di sicurezza aggiuntive o la modifica alle politiche e procedure di gestione degli incidenti, devono essere ben documentate e comunicate alle parti interessate. Tale documentazione sarà molto utile per la formazione di nuovi membri del team di risposta agli incidenti e come base di conoscenza per la gestione di incidenti futuri.

5.10 Key risk indicator e key impact indicator

L'identificazione di metriche permette di migliorare la valutazione del rischio. Ogni indicatore deve avere soglie predeterminate, all'interno delle quali le oscillazioni saranno ritenute normali o accettabili.

- **I KPI - key performance** indicator sono parametri di misurazione di prestazioni, singoli processi o attività, spesso relativi alle attività primarie a sostegno dei processi critici o strategici dell'organizzazione. Essi offrono una visione in tempo reale o su base giornaliera, settimanale o mensile; misurano le carenze di prestazione e spesso alimentano cruscotti interattivi.
- **I KRI - key risk indicator** sono misurazioni o metriche, utilizzate da un'organizzazione per gestire l'esposizione attuale e potenziale ai rischi operativi, finanziari, reputazionali, di conformità e strategici. L'individuazione dei KRI varia a seconda del rischio che si vuole monitorare e, analogamente ai KPI, questi agiscono come un sistema di allerta precoce per avvisare l'organizzazione di eventuali oscillazioni del fattore di rischio.

Di seguito alcuni esempi KRI in ambito IT:

- tempo medio (misurato in giorni) fra la rimessa in servizio di un sistema e il successivo fermo;
- tempo di fermo dovuto ad attività di manutenzione pianificata;
- tempo medio di risoluzione dei ticket di assistenza;
- numero di volte in cui l'hardware ha superato le soglie di capacità;
- numero di progetti IT annullati dopo il lancio negli ultimi 6 mesi;
- percentuale di risorse IT interessate dalla fine del ciclo di vita o dal supporto di un prodotto.

La pubblicazione di ISACA "Risk Scenarios Using COBIT 5 for Risk" offre una rappresentazione di possibili scenari e minacce, fornendo al contempo dei KRI di riferimento. Il documento, per ogni scenario di minaccia descritto, fornisce due diversi insiemi di KRI: quelli relativi agli obiettivi IT e quelli relativi agli obiettivi di processo.

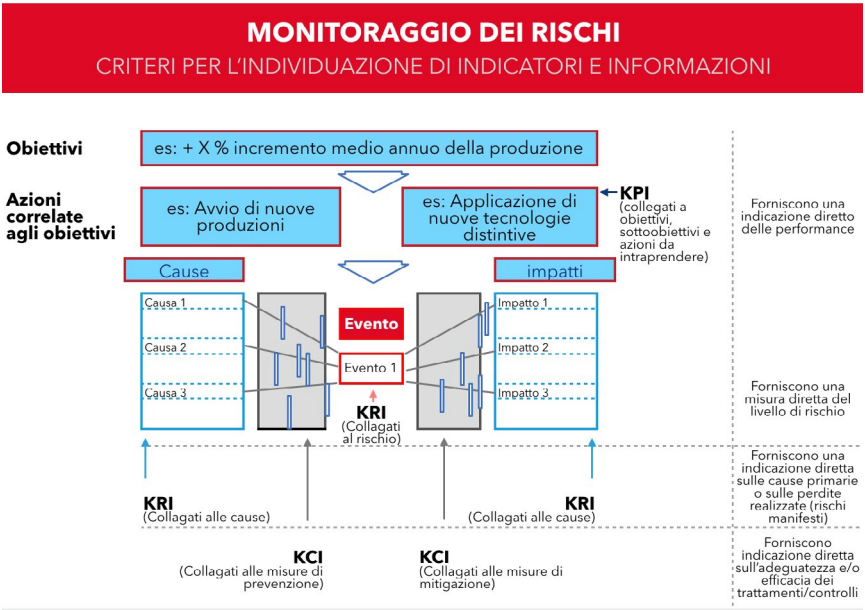

Figura 15 - Relazioni tra obiettivi, KPI e KRI[64]

64 Immagine degli autori.

Il Modello rappresentato in figura è un esempio di gestione degli indicatori per il monitoraggio delle prestazioni e del rischio sotto diversi aspetti.
Il KRI (*key risk indicator*) è la metrica associata prevalentemente alla cause del fattore di rischio e può essere facilmente individuata e personalizzata a seconda delle specifiche esigenze. Il KII (*key impact indicator*) è la metrica associata agli impatti consequenziali. Alcuni esempi[65]:

- perdite (p.e. profit loss; EBITDA loss);
- danno reputazionale;
- danno emergente;
- spese legali, sanzioni e contenziosi;
- tempi medi di ripristino (MTTR);
- costi di ripristino e sostituzione di tecnologie e apparecchiature;
- costi di fermo operativo (sia del personale che degli impianti);
- perdita di valore del patrimonio informatico (es. dati, brevetti);
- costi diretti e indiretti legati all'incidente.

Infine i KCI (*key cost indicator*) rappresentano i costi associati alle misure di prevenzione e di mitigazione.
Il Ponemon Institute, con IBM, ha adottato una metodologia di analisi dei costi chiamata *activity-based costing* (ABC), già conosciuta e diffusa nelle pratiche del *project management*, per calcolare il costo medio di una violazione dei dati, imputando sia costi diretti, quali attività forensi o risarcimenti, e costi diretti quali *detection, response* e *recovery* post incidente.

5.11 La gestione integrata dei rischi

La gestione del rischio digitale può essere favorita da un approccio integrato. Il termine «rischio integrato» non significa svolgere un'unica analisi valida per tutte le aree di rischio presenti in un'organizzazione, quanto pianificare e mettere a fattor comune le analisi svolte per le diverse aree, evitando duplicazioni e massimizzando l'efficacia della

65 https://www.ictsecuritymagazine.com/articoli/key-impact-indicator-e-key-risk-indicator-per-la-cyber-risk-evaluation/

comunicazione verso il vertice , con ricadute positive sull'efficacia e sull'efficienza del processo di valutazione del rischio, per il tramite di:

- approcci omogenei per le diverse aree di rischio, con le necessarie personalizzazioni;
- pianificazione condivisa delle diverse analisi di rischio (ambiti, responsabilità, risorse coinvolte, ecc.);
- visibilità su un'ampia gamma di rischi tra processi e funzioni;
- decisioni strategiche migliori basate su valutazioni complete del rischio;
- produzione di un rapporto formale destinato al vertice e agli stakeholder.

Si tratta, quindi, di anticipare i rischi e ottimizzare i controlli e gli investimenti.
Si suggerisce, al riguardo, di svolgere una pianificazione annuale per l'intera organizzazione e di sviluppare piani analitici per le diverse aree di rischio, con indicazione di ambiti, obiettivi, criteri di integrazione con altre analisi, priorità, ruoli e responsabilità, ecc.

Si raccomanda di basare la valutazione del rischio integrata sui controlli (o contromisure) presenti negli standard ISO, dove disponibili, dedicati alle diverse aree di rischio (sicurezza delle informazioni, alla cybersecurity, alla privacy, alla gestione dei servizi IT e alla continuità operativa) e sulla valutazione delle minacce pertinenti.

La gestione integrata dei rischi può essere concepita come un insieme di pratiche e processi supportati da una cultura consapevole del rischio e da tecnologie abilitanti. Per svilupparla, l'organizzazione deve definire questi aspetti fondamentali:

- **Strategia** - abilitazione e attuazione di un quadro d'insieme, compreso il miglioramento delle prestazioni attraverso una governance efficace e la titolarità del rischio;
- **Risposta** - identificazione e implementazione di meccanismi per mitigare il rischio;
- **Comunicazione e rendicontazione** - utilizzo delle modalità più appropriate per tracciare e informare le parti interessate;
- **Monitoraggio** - identificazione e implementazione di processi atti a tracciare gli obiettivi di governance, le responsabilità del rischio, la conformità alle politiche e alle decisioni stabilite attraverso il processo di governance unitamente ai rischi per tali obiettivi e l'efficacia della mitigazione e dei controlli del rischio.

I risultati di uno studio Forrester[66] hanno indicato che la gestione integrata del rischio può diventare uno strumento di supporto decisionale strategico, attraverso una visione

66 https://www.tenable.com/analyst-research/forrester-cyber-risk-report-2020.

completa del rischio.

Intervista a Valentina Paduano, Chief Risk & Sustainability Officer Sogefi Group - FERMA Board Member

D. FERMA, in questi ultimi anni, ha supportato operatori assicurativi del settore e risk manager dando vita ad iniziative e report mirati e ha rafforzato il suo rapporto con l'OCSE sui rischi informatici per stabilire indicatori statistici internazionali per misurare la gestione del rischio digitale nelle imprese. Tale lavoro si è tradotto in un documento dal titolo "Measuring Digital Risk Management Practices in Businesses" Ce ne può parlare?

R. Il paper trae origine dalla Security Recommendation del 2015 dell'OECD (Organization for Economic Co-operation and Development o Organizzazione per la cooperazione e lo sviluppo economico) che invita le organizzazioni ad approcciare al digital risk al pari di altri rischi di tipo economico e pertanto integrarlo all'interno dei processi di risk management e decisionali dell'organizzazione.

FERMA, attraverso una survey che ha coinvolto l'intera community, ha cercato infatti di fornire una chiara visione di come e quanto integrata ed efficace sia la gestione dei digital security risk all'interno delle organizzazioni.

Ciò che emerge è che, sebbene diverse siano le tipologie di metriche riconosciute utili a misurare i digital security risk, non è possibile trarre delle statistiche rappresentative sulle pratiche di gestione di tali rischi applicate dalle organizzazioni. Inoltre, poiché il panel dei rispondenti è principalmente composto da grandi imprese, tali risultati non possono essere generalizzati e considerati validi anche per le PMI.

In particolare, la mancanza di dati di qualità nell'area dei rischi digitali determina la difficoltà di definire quanto i business siano esposti agli attacchi cyber e qual è il grado di protezione fornito dalle forme di trasferimento del rischio esistenti. Il progetto Lucy, lanciato dall'associazione francese AMRAE (Association pour le Management des Risques et des Assurances de l'Entreprise) cerca proprio di colmare questo gap informativo e, pertanto, FERMA lo ripropone nel 2022, estendendo il perimetro a livello EU.

Occorre tuttavia precisare che il lavoro è stato svolto nel 2017-18 e gli eventi successivamente accaduti, quali l'entrata in vigore della normativa GDPR, l'attacco cyber Wanna Cry, nonché le conseguenze della pandemia sul mondo digitale, hanno ulteriormente modificato la percezione del rischio cyber, mi sentirei di dire, rafforzando positivamente la consapevolezza.

Infatti, l'attenzione della OECD sul tema del digital security risk management è sempre elevata e diverse sono le iniziative proposte, sebbene la strada per individuare le statistiche internazionali per misurare il digital risk nelle aziende è ancora molto lunga.

D. Ci può parlare della proposta di FERMA e l'European Confederation of Institutes of Internal

Auditing (ECIIA) in termini di gestione del rischio cyber, atta ad aumentare la resilienza e l'efficienza delle organizzazioni?

R. La proposta di FERMA e ECIIA, pubblicata nel 2017 attraverso il report intitolato "At the junction of corporate governance and cybersecurity"[67], si focalizza sulla necessità per le organizzazioni di dotarsi di una cyber risk governance quale elemento primario e fondamentale per rafforzare la consapevolezza e la cultura aziendale sui cyber risk e, pertanto, indirizzare una efficace gestione. Gli attacchi cyber avvenuti negli ultimi anni, come il Wanna Cry, confermano effettivamente questa mancanza all'interno delle organizzazioni.

In particolare, FERMA e ECIIA ribadiscono che il rischio cyber è un problema che influenza anche alcuni aspetti strategici del vertice, quali stima, reputazione e fiducia e che pertanto deve essere gestito primariamente a livello di governance. A tal supporto, ad esempio, si raccomanda la costituzione di comitati interni di cyber risk governance o gruppi di lavoro, presieduti dal risk manager e composti dai principali attori aziendali coinvolti nella gestione dei rischi digitali (p.e. IT, HR, finance, legal, DPO, CISO), con il compito di determinare i potenziali costi derivanti dai rischi cyber e proporre le relative misure di mitigazione al comitato di cyber risk governance e al vertice.

D. Avete in programma iniziative ad hoc per migliorare la sinergia tra Risk Manager e assicurazioni a livello EU a supporto delle PMI?

R. Diverse sono le iniziative portate avanti da FERMA già da diversi anni.

Nel 2018, FERMA ha collaborato con ECIIA sulla definizione di modelli di governance che prevedesse l'allineamento tra le strategie di business ed il cyber risk. Attività che si è basata principalmente sulla raccolta delle best practice delle grandi aziende, utili a indirizzare le azioni indipendentemente dalla dimensione dell'organizzazione.

Nel 2019, FERMA, BIPAR e Insurance Europe, in collaborazione con Aon e Marsh, hanno pubblicato la linea guida "Preparing for cyber insurance", volta a supportare le organizzazioni nella comprensione dei rischi cyber, nonché nel prepararne il dialogo con intermediari e assicuratori. Tale guida fornisce anche gli strumenti necessari per valutare le coperture assicurative cyber offerte e il loro risvolto pratico. Il tutto secondo una prospettiva utile anche alle PMI.

Infine, il Digital Committee di FERMA, partendo dal successo del progetto Lucy di AMRAE, ha di recente avviato uno studio a livello europeo sul mercato assicurativo cyber dal punto di vista degli insurance buyer, con l'obiettivo di fornire informazioni pratiche in termini di premi e claim, al fine di incoraggiare una conversazione più ampia e pragmatica sui rischi cyber fronteggiati dalle aziende e indirizzare il settore assicurativo su come mitigare e trasferire tali rischi.

67 https://www.ferma.eu/publication/ferma-eciia-cyber-risk-governance-report/.

6. I rischi secondo la normativa EU e italiana

L'obbligatorietà dell'analisi del rischio, presente oggi in diverse discipline e ambiti giuridici, ha origine nell'adozione del "principio di precauzione", emerso per la prima volta negli anni '70 nel diritto tedesco e presente in alcuni trattati internazionali come il Trattato di Maastricht del 1992 e il Trattato sul funzionamento dell'Unione europea (TFUE) sempre in riferimento alla materia ambientale.

Il principio nasce per garantire un adeguato livello di protezione dell'ambiente, grazie all'individuazione preventiva di azioni da intraprendere per la mitigazione degli scenari di rischio. Il suo campo di applicazione è oggi molto più vasto di quello per il quale era stato inizialmente ideato e si estende anche alla politica dei consumatori, alla legislazione europea sugli alimenti, alla salute umana, animale e vegetale.

Il principio di precauzione è strettamente legato alla gestione del rischio (valutazione e trattamento del rischio), poiché vanno applicate misure precauzionali a seguito di una decisione "politica", per controllare e gestire le principali minacce al raggiungimento degli obiettivi, a seguito di una ponderata valutazione delle probabilità di accadimento e delle possibili conseguenze.

Negli ultimi anni, quindi, si sta delineando il graduale passaggio da un approccio basato sulla normativa e i diritti, dove i rischi sono gestiti una volta per tutte imponendo un sistema ordinato di comportamenti, a uno basato sulla gestione del rischio determinato dal contesto di ciascuno[68], che consente di prevedere e applicare misure flessibili proporzionali alla natura dei rischi a cui si è esposti.

È importante sottolineare che il secondo approccio non si pone come rigida alternativa ai diritti e ai principi consolidati attraverso il primo approccio; piuttosto è condivisibile la commistione delle due anime per garantire al meglio i diritti fondamentali degli individui[69].
La contrapposizione tra i due approcci è da ricercare nella storica classificazione e distinzione tra sistemi giuridici di civil law e sistemi di common law.

68 Malcolm K. Sparrow. The Regulatory Craft: Controlling Risks, Solving Problems, and Managing Compliance. Washington DC, USA: Brookings Institutions Press, 2011.

69 Malcolm K. Sparrow. The Character of Harms: Operational Challenges in Control. UK: Cambridge University Press, 2008.

Civil law e common law

La separazione tra i sistemi civil law e common law nasce anzitutto per motivi geografici. Mentre la civil law si sviluppa nel continente europeo, la common law nasce in Inghilterra, che ne è l'unico centro promotore.

Gli ordinamenti di civil law riconoscono il ruolo preminente della legge nel guidare le decisioni delle corti, che devono attenersi al rispetto della normativa vigente nell'ordinamento e applicarla al caso concreto. La disciplina normativa è dunque costruita mediante "codificazione" delle disposizioni di legge, accessibili a tutti. Il modello giuridico del civil law è, attualmente, il più diffuso al mondo. Ad aderire a tale modello sono la maggior parte dei Paesi dell'Europa continentale e dell'Asia orientale ma anche Paesi ex colonie o protettorati francesi, olandesi, tedeschi, spagnoli o portoghesi, inclusa gran parte dell'America centrale e meridionale.

Diversamente, il modello common law si basa sulle decisioni dei giudici ed è caratterizzato dall'assenza di una costituzione scritta o di leggi codificate. Le decisioni giudiziarie sono vincolanti e vi è un'ampia libertà contrattuale. L'applicazione di tali regole comporta due conseguenze. La prima è che anche il giudice stesso è vincolato da tale precedente salvo che non disponga diversamente (principio dello stare decisis). Quindi il tribunale è libero di cambiare opinione ma, fino a quando non lo fa, questa è la regola che si applicherà. In secondo luogo questo dà una sorta di prevedibilità e di stabilità in tali sistemi legali. La certezza del diritto è, infatti, un principio che ispira tutti gli ordinamenti giuridici. I Paesi che seguono un sistema di common law sono in genere le ex colonie o protettorati britannici, compresi gli Stati Uniti.

Un grande vantaggio del modello di common law si manifesta in particolare quando si manifestano nuovi sviluppi tecnici o sociali. Il giudice può, infatti, reagire abbastanza prontamente agli stessi e modulare la decisione conseguentemente, non dovendo aspettare che il legislatore si esprima o emetta una legge.
Nell'approccio common law emerge con forza il concetto di accountability, termine che contiene e rimanda a tre significati:

- dare conto delle decisioni assunte e dei riflessi economici (trasparenza),
- rispondere del risultato delle azioni compiute o autorizzate (efficacia),
- essere conformi alle norme (legalità).

Volendo salvare del Diritto romano almeno una espressione linguistica, si potrebbe dire che l'accountability è la responsabilità (praestatio) ex ante ed ex post di quanto compiuto dall'attore.

L'approccio legislativo basato sul rischio

Il legislatore europeo, dunque, ha fatto proprio il concetto di "*risk-based thinking*", come si evince nel richiamo all'analisi dei rischi all'interno di interventi normativi comunitari, quali il Regolamento Europeo 2016/679 (GDPR) e le normative dell'UE riferite all'intelligenza artificiale. Lo stesso orientamento si rinviene nella normativa nazionale con particolare riferimento al Perimetro di sicurezza cibernetica italiano.

Queste discipline presentano un analogo schema normativo: definiscono in maniera puntuale il bene giuridico che si intende proteggere e il soggetto chiamato a garantire questa protezione; per quanto riguarda invece il "come" deve essere raggiunta questa protezione, non vengono stabiliti adempimenti precisi ma si chiede invece di analizzare il contesto operativo in cui vengono posti in essere gli atti oggetto di protezione (o gli atti che possono influenzare la protezione del bene), valutando in concreto i rischi connessi a tale contesto e decidendo infine le misure di protezione idonee a mitigare o eliminare tali rischi.
L'approccio si porta poi dietro un altro elemento di assoluto rilievo: l'onere della prova.

Ove infatti il legislatore emana discipline precettive, è l'autorità di controllo che deve dimostrare la violazione dell'obbligo legislativo ai fini dell'applicazione della sanzione; al contrario, ove la disciplina stabilisce solo l'obiettivo da raggiungere (la protezione del bene), senza indicare i mezzi da adottare, ma rimettendo tale decisione a valle di una valutazione del rischio, sarà il soggetto chiamato a proteggere il bene che dovrà dimostrare come ha effettuato la sua valutazione, quali mezzi ha deciso di porre in essere per proteggere il bene, l'adeguatezza e l'efficacia dei mezzi stessi e, in caso del verificarsi di un evento avverso, l'imprevedibilità e l'inevitabilità dell'evento stesso.

Tale rovesciamento dell'onere della prova pone un peso molto rilevante in capo al soggetto chiamato a tutelare il bene: lo chiama a predisporre (in situazioni di operatività fisiologica) tutte le prove - preferibilmente documentali – per dimostrare come è stato valutato il rischio e il perché delle scelte fatte. L'assetto documentale sarà poi cardine per una possibile difesa di fronte all'autorità giudiziaria.

Intervista all'avv. Valentina Frediani, CEO di Colin & Partners

D. Oggi ogni nuova iniziativa a livello Europeo, che sia una direttiva o un regolamento a livello comunitario o una guideline di qualche autorità, posizionano in primo piano il tema dell'analisi dei rischi. Da cosa è motivata secondo te questa evoluzione delle norme?

R. Dobbiamo dire che gli ultimi due anni hanno visto incrementare in modo esponenziale gli attacchi finalizzati a danneggiare economicamente le organizzazioni bloccandone spesso l'operatività. Tale aumento non ha però stimolato sufficientemente gli organi decisionali ad implementare l'analisi dei rischi ignorandone la portata e soprattutto le eventuali azioni da

intraprendere nell'immediato di un attacco.

È proprio a fronte di questa mancanza di sensibilità, e direi di "visione", che i legislatori europei, così come le autorità, hanno sempre più ritenuto necessario intervenire sul tema dell'analisi dei rischi.

L'entrata in vigore del Regolamento Europeo per la protezione dei dati personali doveva già rappresentare un momento di forte riflessione e confronto interno per le aziende che nel rispetto del principio di accountability avrebbero dovuto procedere a una formale valutazione dei rischi rispetto all'impatto sui dati di cui sono titolari, analizzando lo status della sicurezza e valutando i correlati rischi informatici; ma purtroppo, ancora una volta, in gran parte delle realtà imprenditoriali nazionali ed europee, questo obbligo normativo è stato tradotto più come un mero adempimento e non è stato vissuto come una spinta oggettiva a valorizzare le scelte sul fronte degli investimenti e della razionalizzazione delle modalità operative per evitare rischi provenienti sia dall'interno dell'organizzazione che dall'esterno.

D. In sintesi, senza entrare nel merito dei singoli articoli, cosa raccomandano oggi le norme con riferimento al trattamento dei rischi informatici?

R. Ad oggi tutte le norme che prendono in considerazione l'analisi dei rischi sotto il profilo informatico si basano sulla necessità di valutare misure tecniche ed organizzative: questi gli elementi posti a fattor comune, dimostrando così come la sicurezza delle informazioni, dei dati e quindi della funzionalità e l'operatività delle organizzazioni non possa che passare attraverso non solo le misure di sicurezza logiche e fisiche ma anche – e forse in maggior misura - attraverso l'elemento umano, nella sua organizzazione e gestione dei rischi legati all'esecuzione delle attività.

È impensabile poter effettuare una valutazione dei rischi basandosi esclusivamente sul prendere atto dello status tecnologico di una realtà e trascurando completamente l'elemento umano, peraltro non solo sotto il profilo organizzativo ma anche nell'eventuale reattività che si manifesterà nell'ipotesi in cui si verifichino determinati eventi.

L'analisi dei rischi, inoltre, non può vivere di staticità: non può prevedere esclusivamente una fotografia della situazione attuale e una proiezione di quelli che possono essere miglioramenti atti a ridurre al minimo i rischi, ma deve necessariamente prendere in considerazione tutte le possibili evoluzioni al fine di poter effettuare un'analisi veritiera.

D. In base alla tua esperienza, qual è il migliore approccio che dovrebbero oggi seguire le organizzazioni, e quali sono ancora i limiti che lo frenano?

R. Sicuramente oggi le organizzazioni dovrebbero partire da una valutazione dei rischi che non coinvolga in maniera passiva le risorse interne; spesso vengono assunte le informazioni sulla base delle evidenze senza approfondire in maniera concreta le modalità operative e le problematiche gestite dagli utenti interni, ignorandone le potenziali reazioni a determinati

eventi. Questo rappresenta, a mio parere, uno dei limiti maggiori che incontriamo oggi nelle organizzazioni, ossia, un'analisi dei rischi completamente avulsa dalla percezione effettiva dei rischi che hanno le risorse interne.

Un limite decisamente forte è quello rappresentato dall'approccio psicologico che i vertici hanno rispetto all'analisi dei rischi: c'è un timore sempre molto diffuso di analizzare per poi scoprire l'entità dell'eventuale soluzione da adottare. Questo diviene impeditivo e, in qualche modo, pregiudica anche l'evoluzione dell'azienda stessa. Infine, dovrebbe far parte dell'approccio metodologico la ripetitività nel tempo dell'analisi dei rischi: che oggi invece appare sempre più "statica", come se, una volta effettuata, permanesse lo status rilevato per sempre! La periodicità dell'analisi dei rischi è fondamentale anche per consentire all'intera organizzazione di evolvere sulla base dei cambiamenti interni ed esterni.

6.1 Il GDPR

Il Regolamento UE 679/2016 (noto come GDPR, acronimo di "General Data Protection Regulation") ha introdotto una disciplina uniforme e armonizzata a livello comunitario per la protezione delle persone fisiche nel trattamento dei dati.
Seppure si parli comunemente di "protezione dei dati", il bene giuridico protetto è la persona fisica. Quindi tutta la disciplina va letta, interpretata e applicata tenendo conto che l'obiettivo è proteggere le persone (e i diritti attinenti alla sfera giuridica delle persone stesse) dai danni che potrebbero derivare da un non corretto trattamento dei dati.

L'ulteriore obiettivo che si pone il GDPR è quello di favorire la libera circolazione dei dati: quindi l'applicazione pratica della disciplina rappresenta il frutto del bilanciamento di interessi tra la protezione dei diritti della persona fisica e la libera circolazione dei dati.

6.1.1 A chi è rivolto il GDPR

Il GDPR deve essere applicato da coloro che trattano dati personali, con solo alcune eccezioni riportate nell'articolo 2 del Regolamento medesimo.

6.1.2 La rilevanza giuridica dell' analisi del rischio

Diversamente dalla precedente Direttiva 95/46/CE che conteneva principi prescrittivi, il GDPR chiede al titolare del trattamento di analizzare il rischio a cui i dati sono sottoposti e di identificare le misure di gestione e sicurezza idonee a eliminarlo o mitigarlo; ciò allo scopo di proteggere le persone fisiche da eventuali danni derivanti da una non corretta protezione dei dati.
Il GDPR non parla mai di "analisi dei rischi", ma con gli artt. 24, 25, 32 e 35 richiede di valutare i rischi per i diritti e le libertà delle persone fisiche, considerando probabilità e gravità diverse.

6.1.3. Gli adempimenti per l'analisi del rischio

L'analisi dei rischi in ambito GDPR (che non deve essere confusa con la valutazione di impatto richiesta dall'art. 35 del Regolamento medesimo) presenta alcune particolarità:

- non si tratta di una valutazione del rischio relativo all'organizzazione, ma relativo ai diritti delle persone fisiche;
- l'analisi dei rischi non riguarda solo gli interessati (i soggetti di cui si trattano i dati), ma tutte le persone fisiche, che oltre agli interessati comprendono un numero non ben definibile di soggetti;
- non riguarda i soli aspetti di sicurezza.

Per quanto riguarda le valutazioni d'impatto (che mirano a valutare gli impatti che un trattamento comporta sui diritti degli interessati), l'articolo 35 del GDPR richiede che contengano:

- una valutazione dei rischi per i diritti e le libertà degli interessati;
- 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 GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati.

Al riguardo sono stati presentati differenti approcci da autorità ed istituzioni euro-

pee quali: ENISA[70] (per la valutazione del rischio relativo alla privacy), AEPD[71] (per la valutazione del rischio relativo alla privacy e la valutazione d'impatto) e CNIL[72] (per la valutazione d'impatto).

Da osservare che:

- l'identificazione della probabilità è complessa in quanto molto spesso il pregiudizio ai diritti e libertà delle persone fisiche non è il reale oggetto della violazione, ma ne costituisce solo un effetto secondario;
- è difficile valutare un impatto perché non sempre sono evidenti i possibili danni ai diritti e libertà delle persone fisiche in seguito a un evento avverso.

Una valutazione basata su una scala qualitativa (per esempio Alto, Medio e Basso rischio) appare più che sufficiente e gli approcci segnalati propongono linee guida per assegnare i valori.
Per quanto riguarda le opzioni di trattamento, il rischio da valutare non è quello relativo all'organizzazione, ma quello per gli interessati. Pertanto, il titolare, in caso di rischio elevato, deve rinunciare al trattamento o rivolgersi all'autorità garante attraverso la consultazione preventiva prevista dall'art. 36.
Le misure di sicurezza sono indicate in più di un articolo: in particolare l'art. 25 del GDPR sulla protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (*privacy-by-design* e *privacy-by-default*) indica, fra le altre cose, che sia effettuata una valutazione anche per limitare il numero dei soggetti che accedono ai dati personali: in altri termini devono essere previste misure tecniche per la gestione delle autorizzazioni all'accesso ai dati. Nell'Art.32 si richiede di mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio e, per esempio, al §4 prescrive l'obbligo di istruzione dei soggetti che accedono ai dati.

6.1.4 Il regime sanzionatorio

L'art. 83 del GDPR riporta le sanzioni amministrative applicabili nel caso di violazione del Regolamento medesimo. Esse, a seconda della tipologia di violazione, possono arrivare fino a 20.000.000 EUR (o, per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente).
Per completezza si precisa che, oltre al rischio sanzionatorio derivante dal mancato

70 https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing.

71 https://www.aepd.es/es/guias-y-herramientas/herramientas/evalua-riesgo-rgpd.

72 https://www.cnil.fr/en/privacy-impact-assessment-pia.

rispetto della normativa, il titolare e il responsabile possono essere chiamati al risarcimento dei danni materiali ed immateriali derivanti dal mancato rispetto della normativa. Inoltre qualunque impatto sui dati personali può avere ulteriori conseguenze per l'organizzazione, per esempio mancati guadagni, perdita di clienti, danni di immagine, cause legali.

6.2 Il Regolamento sulle comunicazioni elettroniche

La Commissione europea nel 2017 presentò una proposta, non ancora approvata, di Regolamento sul rispetto della vita privata e la tutela dei dati personali nelle comunicazioni elettroniche (il cosiddetto "Regolamento e-privacy") destinato a sostituire la Direttiva 2002/58/CE ("Direttiva e-Privacy"). La proposta del Regolamento e-privacy e il GDPR si integrano, costituendo i pilastri del quadro giuridico complessivo per la tutela del diritto alla protezione dei dati personali e dei diritti e libertà fondamentali della persona, in linea con la Carta dei diritti fondamentali dell'Unione europea.
La proposta di Regolamento e-privacy tutela i diritti e libertà fondamentali delle persone (non solo persone fisiche, ma anche giuridiche, a differenza del GDPR) nel contesto dei servizi di comunicazione elettronica, attraverso la protezione dei dati personali nella fase di trattamento e della riservatezza delle comunicazioni.

6.2.1 La rilevanza giuridica dell'analisi del rischio

Come nel GDPR, il rischio per la proposta di Regolamento e-privacy non attiene ai dati personali e alle informazioni (i contenuti delle comunicazioni elettroniche) in sé considerati, ma ai diritti e libertà delle persone (qui, anche giuridiche) che possono subire nocumento a causa di un trattamento illecito, cioè contrario alle norme.
La Proposta di Regolamento e-privacy richiede di garantire la sicurezza dei dati, mitigare il rischio di violazione e compiere azioni in funzione della possibilità che un dato trattamento comporti rischi elevati per i diritti e le libertà delle persone fisiche e delle persone giuridiche.

6.2.2 Gli adempimenti per l'analisi del rischio

La proposta di Regolamento e-privacy non indica misure di sicurezza minime né specifiche azioni di mitigazione del rischio obbligatorie, ma fornisce suggerimenti ed esempi di misure utili in funzione di specifici trattamenti. Le misure sono sia tecniche, quali la crittografia, la pseudonimizzazione e l'uso di dati aggregati, sia di altro tipo, come indicare nell'informativa l'esistenza di misure che l'utente dell'apparecchio terminale può prendere per minimizzare o escludere la raccolta dei suoi dati.
In ogni caso, dato il ruolo integrativo e di specificazione rispetto al GDPR, dovranno essere prese tutte le misure richieste da quest'ultima normativa, inclusa la valutazione del rischio.

6.2.3 Il regime sanzionatorio

Le sanzioni sono analoghe a quelle previste dal GDPR: l'art. 23 del Regolamento e-privacy infatti richiama espressamente l'applicazione - "*mutatis mutandis*" - dell'art. 83 del GDPR. Anche questa normativa lascia ai singoli ordinamenti nazionali la facoltà di stabilire altre sanzioni, con l'unica condizione che esse siano efficaci, proporzionate e dissuasive. Non va inoltre dimenticato il sistema della responsabilità risarcitoria, che richiama integralmente e direttamente quello del GDPR mediante il riferimento espresso al suo articolo 82.

6.3 La direttiva NIS

Tra le disposizioni più rilevanti dell'Unione Europea in materia di cyber security troviamo la Direttiva (UE) 2016/1148[73] del Parlamento Europeo e del Consiglio, nota come "Direttiva NIS - Network and Information Security".
Essa reca misure per un livello comune di sicurezza delle reti e dei sistemi informativi nell'Unione, dal momento che le stesse svolgono sempre di più un ruolo vitale nella società (sempre più digitalizzata) e occorre che siano affidabili per garantire le attività

73 https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016L1148.

economiche e sociali e il funzionamento del mercato interno (*digital trust*).
La Direttiva NIS rappresenta un elemento importante dell'approccio alla cybersicurezza nell'Unione europea, con il quale per la prima volta è stato imposto agli Stati membri di adottare un modello di governo in questa materia. In Italia è stata recepita con il Decreto Legislativo 18 maggio 2018, n. 65 (Decreto NIS)[74].

La pervasività della trasformazione digitale, insieme alle minacce informatiche in continua evoluzione, ha recentemente indotto la Commissione europea ad avviare un processo di revisione e aggiornamento della Direttiva NIS, al momento in corso. Tra le principali novità ci sarà sicuramente l'ampliamento del perimetro dei soggetti interessati dalla normativa come, ad esempio, il settore dei rifiuti, quello aerospaziale, dell'alimentazione, dei servizi postali e altri ancora; anche l'impianto sanzionatorio sarà inasprito, almeno rispetto a quello adottato in Italia.

6.3.1 A chi è rivolta la Direttiva NIS

I soggetti a cui è rivolta la Direttiva NIS sono i cosiddetti operatori di servizi essenziali (OSE) e fornitori di servizi digitali (FSD); i primi sono tutti i soggetti che forniscono un servizio essenziale per il mantenimento delle attività economiche e sociali, la cui fornitura dipende proprio dalla rete e dai sistemi informativi, i secondi sono invece quelli che forniscono servizi di e-commerce, cloud computing e motori di ricerca.
In Italia l'identificazione degli OSE e degli FSD è demandata all'Agenzia per la cybersicurezza nazionale (ACN) e alle autorità di settore.

6.3.2 La rilevanza giuridica dell'analisi del rischio

Gli OSE e FSD sono chiamati ad adottare misure tecniche e organizzative adeguate e proporzionate per gestire i rischi attraverso processi e tecnologie in grado di garantire la resilienza delle reti e dei sistemi informatici.

74 https://www.gazzettaufficiale.it/eli/id/2018/06/09/18G00092/sg.

6.3.3 Gli adempimenti per l'analisi del rischio

La Direttiva NIS definisce il rischio come la circostanza o l'evento ragionevolmente individuabile con potenziali effetti pregiudizievoli per la sicurezza della rete e dei sistemi informatici. Al riguardo, il Dipartimento delle informazioni per la sicurezza (DIS), ha rilasciato le linee guida per la gestione dei rischi e la prevenzione, mitigazione e notifica degli incidenti[75]. Le linee guida sono basate sul Framework nazionale per la cyber security (paragrafo 7.5) e sono condivise con i soli operatori di servizi essenziali interessati dal provvedimento (più di 450 soggetti).

Analoghi obblighi in materia di sicurezza sono previsti a carico dei fornitori di servizi digitali, i quali sono tenuti ad adottare anch'essi misure tecniche e organizzative per la gestione dei rischi e per la riduzione dell'impatto di eventuali incidenti informatici. Gli elementi che i fornitori di servizi digitali devono prendere in considerazione ai fini della gestione dei rischi informatici sono indicati nel Regolamento di esecuzione (UE) 2018/151 della Commissione.

Enisa, per supportare gli OSE e i FSD (in inglese, *digital service provider* o DSP) ha pubblicato un rapporto con anche un'analisi degli standard e framework disponibili[76].

6.3.4 Il regime sanzionatorio

La definizione dell'impianto sanzionatorio per l'inadempimento degli obblighi previsti nella Direttiva NIS è lasciata agli Stati membri.

In Italia con il Decreto NIS e il DL 82 del 2021, l'accertamento delle violazioni spetta all'Agenzia per la cybersicurezza nazionale; le sanzioni amministrative possono arrivare, a seconda dei casi, fino a 150.000 euro per chi non rispetterà gli obblighi previsti.

75 https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/nis-al-via-le-linee-guida-su-gestione-rischio-e-notifica-incidenti.html.

6.4 Il perimetro di sicurezza nazionale cibernetica (PSNC)

Con la normativa in materia di Perimetro di sicurezza nazionale cibernetica (PSNC) il legislatore ha inteso istituire nell'ordinamento giuridico italiano un presidio dal rischio che incidenti informatici possano minare l'indipendenza, l'integrità e la sicurezza della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento, ossia gli interessi politici, militari, economici, scientifici e industriali del Paese.

Con il DL 105 del 2019 (con Legge di conversione 133 del 2019) si è dato impulso ad un corpus di norme giuridiche e tecniche, organismi e sinergie istituzionali, abilitanti per il conseguimento di un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici di quei soggetti da cui dipende l'esercizio di una funzione essenziale dello Stato, ossia la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato. Nella pratica si sono riprese alcune disposizioni della Direttiva NIS per applicarle a soggetti che esercitano funzioni e servizi essenziali non considerati dalla Direttiva NIS. L'attuazione degli adempimenti del PSNC si basa su DPCM (vedere la figura seguente).

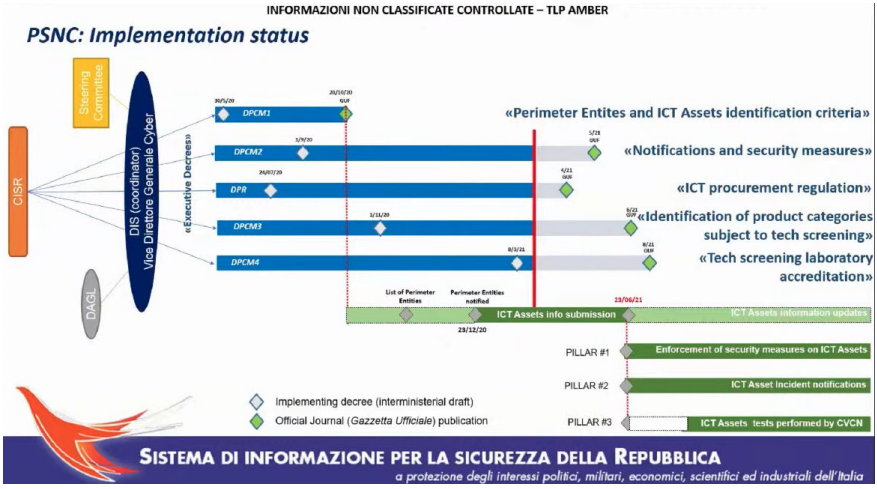

Figura 16 – Stato di implementazione del PSNC[77]

77 Roberto Baldoni. National Security Perimeter for Cyber. Presentazione a ITASEC21.

Più precisamente, i DPCM sono i seguenti:

- DPCM 131 del 30 Luglio 2020 (DPCM1), che tratta dell'analisi del rischio e dell'elenco dei beni ICT;
- DPR 54 del 5 Febbraio 2021, che tratta dell'affidamento di forniture di beni, sistemi e servizi ICT e più precisamente di:
  - procedure da seguire ai fini delle valutazioni da parte del Centro di Valutazione e Certificazione nazionale (CVCN) e dei centri di valutazione;
  - criteri di natura tecnica per l'individuazione delle categorie a cui si applica la procedura di valutazione;
  - procedure con cui le autorità competenti effettuano le attività di verifica e ispezione;
- DPCM 81 del 14 Aprile 2021 (DPCM2), che tratta della notifica degli incidenti e delle misure di sicurezza;
- DPCM 198 del 15 Giugno 2021 (DPCM3), che individua le categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel PSNC;
- un ulteriore DPCM in via di pubblicazione (DPCM4), ritardato rispetto a quanto riportato in Figura 16 per il passaggio di competenze all'Agenzia per la cybersicurezza nazionale (ACN) a seguito dell'approvazione del DL 82 del 2021.

6.4.1 A chi è rivolta la normativa PNSC

I soggetti chiamati ad attuare le protezioni previste sono quelli che esercitano una funzione essenziale dello Stato o erogano servizi essenziali per il mantenimento di attività civili, sociali o economiche, fondamentali per gli interessi dello Stato; in particolare:

- soggetti operanti nel settore governativo, concernente le attività del Comitato Interministeriale per la Sicurezza della Repubblica (CISR);
- soggetti, pubblici o privati, operanti nei seguenti settori di attività, ove non ricompresi in quello governativo: interno, difesa, spazio e aerospazio, energia, telecomunicazioni, economia e finanza, trasporti, servizi digitali, tecnologie critiche, enti previdenziali e per il lavoro.

L'identificazione dei soggetti è demandata all'Agenzia per la cybersicurezza nazionale e alle autorità di settore.

6.4.2 La rilevanza giuridica dell' analisi del rischio

L'analisi del rischio è richiamata da:

- articolo 7 comma 2 e seguenti del DPCM 131 del 2020;
- articolo 3 comma 3 e seguenti del DPCM 81 del 2021.

Alcuni aspetti dell'analisi del rischio richiesta dai DPCM citati sono descritti nel seguito.

6.4.3 Gli adempimenti per l'analisi del rischio

Nel seguito sono indicati gli elementi più significativi della normativa che stiamo considerando.

Elenco dei beni ICT
Il DPCM 131 stabilisce che ciascun soggetto deve trasmettere l'elenco dei beni ICT (reti, sistemi informativi e servizi informatici di rispettiva pertinenza), comprensivo della descrizione dell'architettura e della componentistica, ritenuti necessari, a seguito di un'analisi del rischio, a svolgere la funzione essenziale o il servizio essenziale.

Notifica degli incidenti e misure di sicurezza
Il DPCM 81 del 2021 stabilisce che i soggetti inclusi nel perimetro, al verificarsi di uno degli incidenti aventi impatto su un bene ICT individuato secondo quanto previsto dal DPCM 131, devono procedere alla notifica al CSIRT Italia secondo le modalità previste dal regolamento.
Gli incidenti da notificare sono quelli con impatti sui beni ICT identificati come previsto dal DPCM 131 e sui sistemi informativi che, sulla base dell'analisi del rischio, condividono con essi funzioni di sicurezza o risorse.

Misure di sicurezza
Il DPCM 81 stabilisce anche le misure di sicurezza da adottare e i tempi richiesti. Le misure di sicurezza previste dal PSNC sono un estratto dei controlli già previsti nel FNCS (paragrafo 7.5).

Affidamento di forniture
Il DPR 54 del 2021 richiede che i soggetti, fatto salve alcune eccezioni, che intendono

procedere all'affidamento di forniture di beni, sistemi e servizi ICT correlati con l'elenco dei beni ICT di cui sopra, devono darne comunicazione al Centro di Valutazione e Certificazione Nazionale (CVCN, oggi parte dell'ACN) o ai centri di valutazione (CV). Esso, sulla base di una valutazione del rischio, anche in relazione all'ambito di impiego e in un'ottica di gradualità, può, entro trenta giorni, imporre condizioni e test di hardware e software.

6.4.4 Il regime sanzionatorio

L'impianto sanzionatorio disciplinato dal D.L. 105/2019, per la cui applicazione è competente l'ACN, prevede che siano irrogate sanzioni pecuniarie amministrative:

- da 200mila a 1 milione e 200mila euro per il mancato adempimento degli obblighi di predisposizione e di aggiornamento dell'elenco delle reti, dei sistemi informativi e dei servizi informatici;
- tra 250mila e 1 milione e 500mila euro per:
  - il mancato adempimento dell'obbligo di notifica;
  - l'inosservanza delle misure di sicurezza volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici;
  - nell'ambito dell'approvvigionamento di beni, sistemi e servizi ICT, destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici, per: la mancata collaborazione per l'effettuazione delle attività di test da parte dei soggetti individuati come fornitori; il mancato adempimento delle prescrizioni indicate dall'ACN in esito alle attività di ispezione e verifica svolte; il mancato rispetto delle prescrizioni di utilizzo dettate al committente da parte del CVCN.
- fra 300mila e 1 milione e 800mila euro per:
  - la mancata comunicazione al CVCN dell'affidamento nei termini prescritti (dove la comunicazione comprende la valutazione del rischio associato all'oggetto della fornitura, anche in relazione all'ambito di impiego);
  - l'impiego di prodotti e servizi sopra identificati in violazione delle condizioni imposte dal CVCN o in assenza del superamento dei test imposti dal CVCN ovvero dai centri di valutazione (CV) di cui si avvalgono Ministero della Difesa e Ministero dell'Interno.

In aggiunta, in talune fattispecie sono irrogate:

- la sanzione amministrativa accessoria dell'incapacità ad assumere incarichi di

direzione, amministrazione e controllo nelle persone giuridiche e nelle imprese, per un periodo di 3 anni a decorrere dalla data di accertamento della violazione;

- la pena della reclusione da 1 a 3 anni per coloro che, per ostacolare o condizionare l'espletamento dei procedimenti o delle attività ispettive e di vigilanza, forniscano informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi o ai fini delle comunicazioni o per lo svolgimento delle attività ispettive e di vigilanza oppure omettano di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto; sanzioni pecuniarie fino a 400 quote (calcolate secondo le regole della legge 231) all'organizzazione che ha violato norme e procedure del PSNC.

Intervista all'Amm. Sq. Ruggiero Di Biase, Comandante del Comando per le operazioni in rete della Difesa

D. Quali sono i trend dei rischi cyber che dovrebbero preoccupare di più le organizzazioni pubbliche e private italiane e in particolare quelle soggette al Perimetro di sicurezza nazionale cibernetica?

R. Al Comando per le operazioni in rete della Difesa, responsabile anche della postura di sicurezza e della protezione cyber dell'intera info-struttura del comparto, si osservano e si contrastano le molteplici attività cyber malevoli, siano esse connesse al cybercrime o tese allo spionaggio (State-sponsored), che hanno come obiettivo la violazione del complesso ICT della Difesa.

La cronaca dimostra che queste minacce sono in crescita esponenziale, sia in quantità che in qualità. L'ecosistema cyber "malevolo" sta raggiungendo livelli di globalizzazione e di business altamente lucrativi, chiara evidenza di attività ben orchestrate e finanziate da organizzazioni criminali o proxy di Stati anche ben connessi fra di loro: le cooperazioni tra detti attori diventano sempre più strette ed efficaci.

Le organizzazioni inserite nel Perimetro di sicurezza nazionale cibernetica, con i loro dati sensibili, sono particolarmente esposte. In tali scenari, fondamentale rimane l'educazione del personale, il livello di consapevolezza sulle vulnerabilità degli assetti cibernetici, costantemente sottoposti alla minaccia (gruppi criminali, advanced persistent threat (APT), ecc.), ed investire in capacità (uomini e mezzi) di prevenzione e di contrasto della minaccia.

D. Cosa serve oggi maggiormente per mitigare i rischi cyber?

R. Comprendere il livello di rischio delle proprie info-strutture rappresenta il primo fondamentale passo nel processo di costruzione della capacità di difesa delle proprie reti e servizi e di protezione dei relativi dati.

Per quanto riguarda i rischi legati ai malware, l'approccio proattivo è la migliore difesa.

Installare nella propria rete e mantenere aggiornato un programma anti-malware, oltre che sistemi di protezione in grado di interdire collegamenti, file o siti web sospetti, è sicuramente un eccellente ausilio per prevenire le infezioni.

Fondamentale oggi, nello sviluppo di nuove capacità, è l'approccio secure by design indubbiamente valido nella riduzione del rischio: un'adeguata architettura di sicurezza è parte integrante dell'architettura di sistema. Un altro punto di forza nel contrasto alla minaccia è la capacità di controllo dell'intera supply chain dei componenti, hardware e software, necessari allo sviluppo di un sistema.

Alla base di un'organizzazione di difesa cibernetica efficace vi è, senza dubbio, la capacità di condividere le informazioni, quella di analisi e di threat intelligence e, non da ultima, la capacità di identificare e valorizzare le lessons learned. A ciò va aggiunto l'adozione di standard di sicurezza conformi, modelli organizzativi e best practice validamente riconosciute, al fine di costituire una cornice di difesa consistente, possibilmente priva di anelli deboli che costituirebbero vulnerabilità nei confronti della minaccia.

Il personale specialista deve mantenersi costantemente aggiornato sull'evoluzione e livello di sofisticazione della minaccia. Altrettanto importante è una diffusa consapevolezza della minaccia tra gli utenti: le policy e le misure di sicurezza saranno efficaci solo se gli end user ne hanno conoscenza e le rispettano. L'esperienza insegna che la disattenzione può mettere a repentaglio la sicurezza dell'intero sistema.

D. Quanto è importante la cyber threat intelligence per la Difesa ai fini dell'analisi dei rischi e al loro trattamento?

R. Comprendere le minacce ad ogni livello, dallo strategico al tattico, è fondamentale per identificare, tracciare e contrastare efficacemente la minaccia. Altrettanto importante è la ricerca delle cosiddette tactics, techniques, procedures (TTP), ossia l'identificazione del comportamento di un attaccante durante la sua azione malevola; il riconoscimento di queste caratteristiche è fondamentale nella gestione di attacchi perpetrati da attori evoluti che fanno uso di advanced persistent threat (ATP).

I cyber actors, così come le relative capacità e attività, sono aumentati di numero ed in complessità e i possibili target hanno oggi bisogno di difese preventive e semi automatizzate, in grado di individuare le minacce emergenti e gestire rapidamente le enormi quantità di indicatori tecnici associati. In tale quadro, è importante anche lo scambio ed il supporto informativo che numerose società specializzate di cyber sicurezza forniscono attraverso piattaforme dedicate (Thread feed di IoC, Indicator of compromise).

D. Qual è il ruolo del COR della Difesa, nella risposta ai rischi cyber a livello nazionale, e quali sono i suoi rapporti con la neonata Agenzia per la cybersicurezza nazionale?

R. Un dominio nel quale la minaccia è molto specializzata e in continua evoluzione richiede lo sviluppo di strutture ordinative e organiche snelle e coese, che siano altamente specializzate e che lavorino in sinergia tra di loro seguendo una visione unica. Con la costituzione del Comando per le operazioni in rete (COR), la Difesa ha promosso una riorganizzazione dell'intero comparto C5, finalizzata a garantire, in area interforze, l'unicità di comando sul nuovo dominio del cyberspace, ossia un'unica autorità preposta alla gestione tecnico-operativa dell'intera Infrastruttura di rete e servizi ICT/C4 e a garantire la cornice di sicurezza e protezione dalla minaccia cibernetica, nonché a condurre l'intera gamma delle cyber operations. Questo garantisce al nuovo dominio la corretta connotazione operativa e, contestualmente, consente di stabilire rapporti più sinergici con le corrispondenti articolazioni delle Forze armate.

In linea con tali obiettivi, il COR ha già avviato lo sviluppo di una serie di capacità per operare con efficienza ed efficacia negli odierni scenari. Tali capacità, come previsto dall'Architettura cyber nazionale, se richiesto, sono messe a disposizione anche dell'autorità preposta ad assicurare la cyber resilienza del Paese. A parte l'esperienza operativa già acquisita, con riferimento al CERT Difesa, che potrebbe costituire un valido modello da coniare sul piano organizzativo e funzionale, il COR potrebbe porre a disposizione della costituenda Agenzia anche le proprie capacità operative, ponendosi quale force provider, e la Difesa tutta mettere in campo le proprie risorse nel settore della formazione, addestramento e delle esercitazioni (fra cui il Cyber range).

6.5 Il Digital Service Act

Il Digital Services Act (DSA) è una proposta di regolamento pubblicata dalla Commissione europea, la quale mira a definire un quadro comune legale europeo per bilanciare le responsabilità di utilizzatori, piattaforme e autorità pubbliche.
I cittadini dell'UE e di Paesi terzi sono esposti a rischi sempre maggiori nell'uso di servizi digitali. Il DSA introduce importanti garanzie per consentire ai cittadini di esprimersi liberamente, rafforzando il ruolo degli utenti nell'ambiente online nonché l'esercizio di altri diritti fondamentali come il diritto a un mezzo di ricorso efficace e alla non discriminazione, i diritti dei minori e la protezione dei dati personali.
Una corretta applicazione del DSA attenuerà il rischio che la libertà di espressione venga bloccata per errore o in modo ingiustificato, fronteggiando gli effetti dissuasivi su tale libertà e promuovendo la libertà di ricevere informazioni e manifestare opinioni, oltre a rafforzare le possibilità di ricorso a disposizione degli utenti.

6.5.1 A chi è rivolto il Digital Service Act

Le norme previste dal DSA si applicheranno all'interno dello SEE (Spazio economico europeo) senza alcuna limitazione, coinvolgendo anche i servizi di intermediari online stabiliti in Paesi extra-UE che offrono i propri servizi nell'Unione. Nel caso in cui il fornitore di servizi non abbia sede in UE, dovrà nominare un suo rappresentante, come previsto già in altre normative (ad esempio, GDPR).

6.5.2 La rilevanza giuridica dell'analisi del rischio

Il DSA stabilisce obblighi in termini di valutazione del rischio a carico delle piattaforme di grandi dimensioni. Sono considerate tali le piattaforme che prestano i propri servizi a un numero medio mensile di destinatari attivi del servizio nell'UE pari o superiore a 45 milioni.

6.5.3 Gli adempimenti per l'analisi del rischio

Le piattaforme online di grandi dimensioni avranno l'obbligo di individuare, analizzare e valutare i rischi derivanti dal funzionamento e dall'uso dei servizi che erogano nell'UE.

In particolare dovranno analizzare come i sistemi di moderazione dei contenuti, di raccomandazione e di selezione e visualizzazione della pubblicità influenzino i rischi sistemici succitati, compresa la diffusione potenzialmente rapida e ampia di contenuti illegali e di informazioni incompatibili con le condizioni generali dei prestatori di servizi intermediari.

Le piattaforme di grandi dimensioni dovranno valutare i rischi associati a:

- abuso dei propri servizi attraverso la diffusione di contenuti illegali, quale la diffusione di materiale pedopornografico o l'incitamento all'odio, e lo svolgimento di

attività illegali, quali la vendita di prodotti o servizi vietati dal diritto dell'Unione o nazionale, compresi i prodotti contraffatti;

- gli effetti del servizio sull'esercizio dei diritti fondamentali tutelati dalla Carta dei diritti fondamentali, compresi libertà di espressione e di informazione, il diritto alla vita privata, il diritto alla non discriminazione e i diritti del minore;
- la manipolazione intenzionale del servizio, con possibili impatti sulla salute pubblica, sul dibattito civico, sui processi elettorali, sulla sicurezza pubblica e sulla tutela dei minori, tenuto conto della necessità di garantire l'ordine pubblico, tutelare la vita privata e contrastare le pratiche commerciali fraudolente e ingannevoli.

Le misure di attenuazione dei rischi, che dovranno essere ragionevoli, proporzionate ed efficaci, adattate ai rischi individuati in fase prodromica di analisi, potranno comprendere, ove opportuno e senza pretesa di esaustività:

- l'adeguamento dei sistemi di moderazione dei contenuti o di raccomandazione, dei loro processi decisionali, delle caratteristiche o del funzionamento dei loro servizi, o delle loro condizioni generali;
- misure mirate volte a limitare la visualizzazione della pubblicità associata al servizio prestato;
- il rafforzamento dei processi interni o della vigilanza sulle loro attività, in particolare per quanto riguarda il rilevamento dei rischi sistemici;
- l'avvio o l'adeguamento della cooperazione con i segnalatori attendibili;
- l'avvio o l'adeguamento della cooperazione con altre piattaforme online attraverso i codici di condotta e i protocolli di crisi.

6.5.4 Il regime sanzionatorio

Gli Stati membri stabiliranno le norme relative alle sanzioni applicabili alle violazioni entro i limiti fissati dal DSA. In particolare, secondo la proposta attuale, l'importo massimo delle sanzioni non dovrà superare il 6% del reddito o del fatturato annuo del fornitore. In caso di comunicazione di informazioni inesatte, incomplete o fuorvianti, di mancata risposta o rettifica di informazioni inesatte, incomplete o fuorvianti e di inosservanza dell'obbligo di sottoporsi a un'ispezione in loco, la soglia sarà dell'1%.

6.6 La proposta di Regolamento IA

In data 21 aprile 2021, la Commissione europea ha presentato una proposta di Regolamento che stabilisce norme armonizzate in materia di intelligenza artificiale, con l'obiettivo di trovare, da un punto di vista normativo, un equilibrio tra l'innovazione e un'adeguata tutela dei diritti fondamentali degli individui. Le potenzialità garantite dall'IA, secondo il legislatore europeo, non possono essere sfruttate senza affrontare le implicazioni etiche e umane sottese all'utilizzo dell'intelligenza artificiale, con particolare riferimento alla vita delle persone e ai loro diritti fondamentali, tra cui rientrano il diritto alla riservatezza e alla protezione dei dati personali.
Il quadro normativo proposto sull'intelligenza artificiale si pone i seguenti obiettivi:

- assicurare che i sistemi di IA immessi sul mercato dell'Unione e utilizzati siano sicuri e rispettino la normativa vigente in materia di diritti fondamentali e i valori dell'Unione;
- assicurare la certezza del diritto per facilitare gli investimenti e l'innovazione nell'intelligenza artificiale;
- migliorare la governance e l'applicazione effettiva della normativa esistente in materia di diritti fondamentali e requisiti di sicurezza applicabili ai sistemi di IA;
- facilitare lo sviluppo di un mercato unico per applicazioni di IA lecite, sicure e affidabili nonché prevenire la frammentazione del mercato.

La Clusit Community for Security si è occupata di questo tema attraverso la pubblicazione del libro "Intelligenza Artificiale e Sicurezza: opportunità, rischi e raccomandazioni", disponibile gratuitamente alla consultazione[78].

6.6.1 A chi è rivolta la proposta

Secondo quanto previsto dall'articolo 2, la proposta di Regolamento troverebbe applicazione nei confronti di tutti i soggetti coinvolti nelle attività di immissione, messa in servizio o utilizzo di sistemi di IA, siano essi fornitori, distributori, utenti, importatori o rivenditori, che vengano effettuate nel territorio dell'Unione. La normativa si applicherà, inoltre, anche nel caso in cui il sistema di IA venga immesso nel mercato

78 https://iasecurity.clusit.it/

europeo da un fornitore non stabilito nell'Unione, o quando i risultati prodotti dal sistema saranno utilizzati all'interno dell'Unione e il fornitore e gli utenti si trovano in un Paese terzo.
L'articolo 2 precisa, inoltre, che il Regolamento non si applica:

- alle autorità pubbliche di un Paese terzo e alle organizzazioni internazionali qualora tali soggetti utilizzano sistemi di IA nell'ambito di accordi internazionali di cooperazione giudiziaria e di polizia con l'Unione o con uno o più Stati membri;
- ai sistemi IA sviluppati e usati unicamente in ambito militare.

6.6.2 La rilevanza giuridica dell' analisi del rischio

La Commissione ha ritenuto necessario adottare un approccio che non tentasse di regolare la tecnologia in quanto tale, ma che, sulla base dei livelli di rischio generati dall'utilizzo di sistemi di IA, distinguesse gli standard e i requisiti esigibili per la circolazione e l'utilizzo degli stessi, garantendo, al contempo, parità di condizioni per gli operatori UE e non UE e mantenendo valido il tradizionale approccio già applicato nell'ambito della sicurezza dei prodotti.
Partendo dal presupposto che non tutti i sistemi di IA presentano le stesse criticità, il legislatore europeo ha previsto adempimenti diversi a seconda dello specifico profilo di rischio.

Secondo tale impostazione, escludendo i sistemi il cui utilizzo è espressamente vietato (rischio inaccettabile), sono previsti, per i sistemi ad alto rischio, obblighi per i fornitori e obblighi proporzionati per gli utenti e per tutte le altre figure (importatori, distributori, rappresentanti autorizzati) che, a vario titolo, partecipano alla catena del valore dell'IA.
Inoltre, è richiesta l'adozione di procedure di valutazione preventiva di conformità dei sistemi di IA ad alto rischio che si accingono a essere immessi nel mercato dell'Unione. Questo adempimento sarà supportato da organismi notificati dagli Stati membri, che saranno coinvolti come terze parti indipendenti.

Per i sistemi considerati a basso o minimo rischio, è invece contemplata la possibilità di applicare volontariamente i requisiti obbligatori previsti per i sistemi di IA ad alto rischio o il ricorso a codici di condotta, creati e attuati autonomamente, da parte dei fornitori di tali sistemi.
È interessante notare come le peculiarità dei sistemi di IA, nonché dei possibili rischi

per la sicurezza e i diritti fondamentali associati al loro utilizzo, facciano sorgere delle responsabilità non solo in capo al fornitore per l'immissione sul mercato o della messa in servizio di un sistema di IA ad alto rischio (e ovviamente al fabbricante di tali sistemi), ma agli utenti (per l'uso fatto dell'IA), in genere considerati meri destinatari delle tutele previste dalle normative.

6.6.3 Gli adempimenti per l'analisi del rischio

La disciplina dei sistemi di IA è stata suddivisa in base a quattro categorie di rischio. A seconda dell'appartenenza a una fascia di rischio, il sistema di IA dovrà soddisfare determinati requisiti e sarà sottoposto al rispetto di specifici obblighi. Le fasce di rischio previste sono le seguenti:

- **Rischio inaccettabile**: fanno parte di questa fascia tutte quelle pratiche di IA considerate contrarie ai valori dell'Unione, in quanto lesive dei diritti fondamentali. L'utilizzo di tali sistemi è sostanzialmente vietato. Rientrano in questa categoria i sistemi di social scoring, i sistemi che possono manipolare il comportamento di soggetti vulnerabili come bambini o soggetti con disabilità o, ancora, i sistemi di identificazione biometrica (fra i quali spicca il riconoscimento facciale), effettuata a distanza e in tempo reale, a meno che l'uso non sia strettamente necessario al perseguimento di specifici obiettivi previsti nella normativa (per esempio per le forze dell'ordine).
- **Rischio alto**: sono ricompresi i sistemi IA, elencati neII'AIIegato III della proposta, che determinano un impatto potenzialmente negativo sulla salute e la sicurezza delle persone fisiche o sui loro diritti fondamentali (per esempio sistemi di IA per la valutazione del rischio di credito o per la selezione del personale). L'utilizzo di tali sistemi è subordinato al rispetto di precisi obblighi e limiti, tra i quali: l'obbligo a usare dataset di alta qualità (pertinenti, rappresentativi, ecc.); l'elaborazione di adeguata documentazione tecnica e la progettazione di funzionalità per la registrazione (log) che garantiscano la tracciabilità e verificabilità dei sistemi; la garanzia di un appropriato livello di trasparenza in grado di fornire chiare informazioni agli utilizzatori in merito alle capacità, ai limiti e alle modalità di utilizzo dei sistemi; la garanzia della supervisione umana (misure integrate nel sistema o che devono essere attuate dagli utilizzatori); l'adozione di robuste e accurate misure di sicurezza informatica.
- **Rischio basso e rischio minimo**: sono inclusi i sistemi di IA che, ad esempio, comportano un chiaro rischio di manipolazione dei contenuti (per esempio

deepfake) o che interagiscono con gli esseri umani (per esempio *chatbot*). La Commissione ha imposto, per questo tipo di sistemi, obblighi minimi di trasparenza, per consentire alle persone di essere informate di stare interagendo con una macchina al fine di compiere scelte consapevoli.

6.6.4 Il regime sanzionatorio

Il regime sanzionatorio, in caso di inosservanza del Regolamento, prevede sanzioni amministrative pecuniarie fino a 30 milioni di euro o fino al 6% del fatturato globale annuo dell'anno finanziario precedente.
È lasciata agli Stati membri la scelta delle sanzioni (effettive, proporzionate e dissuasive) da infliggere in caso di violazione al Regolamento, anche se è fortemente consigliato, per talune violazioni, tenere in considerazione i margini e i criteri stabiliti nel Regolamento. Gli Stati membri dovrebbero poi notificare alla Commissione la normativa relativa alle sanzioni adottata, comprese le sanzioni amministrative pecuniarie, e garantirne la corretta attuazione entro la data di applicazione del Regolamento.

6.7 La PSD2

La Direttiva UE n. 2366 del 2015 (Payment Services Directive 2; PSD2) abroga la precedente Direttiva 64 del 2007 (PSD1) e ribadisce e amplia gli obblighi e le responsabilità dei prestatori di servizi di pagamento dell'Unione e in particolare quelli:

- di trasparenza;
- informativi al consumatore sul servizio prestato (titolo III, capi 2 e 3);
- di sicurezza dei servizi prestati, adeguatezza delle misure a tutela degli utilizzatori dei servizi offerti e predisposizione di misure idonee alla gestione dei rischi connessi;
- di tutela dei dati personali trattati nell'espletamento dei servizi offerti (conformemente al GDPR);
- di notifica degli eventuali incidenti di sicurezza occorsi.

In Italia, la Circolare 285 di Banca d'Italia (vedere anche il paragrafo 6.9) è diventata, con i successivi aggiornamenti, lo strumento per attuare in Italia gli Orientamenti (*Guidelines*) operativi e le Regolamentazioni tecniche formulate da EBA a corollario

della PSD2.
Tali norme si pongono l'obiettivo di rafforzare la correttezza delle relazioni tra intermediari e consumatori e tutelare questi ultimi in tutte le fasi di relazione.
I processi bancari hanno fatto emergere, con anticipo rispetto ad altri settori, la necessità di far evolvere le abitudini medie degli utenti nell'uso degli strumenti digitali di fronte alla complessità e alla disomogeneità delle diverse esigenze, vuoi di adempimento normativo, vuoi di sicurezza, vuoi di *user experience*. A titolo di esempio, proprio queste norme hanno imposto, a metà settembre 2019, la *strong customer authentication*.

6.7.1 A chi è rivolta la PSD2

L'ambito di applicazione della Direttiva include i servizi di pagamento nel mercato interno dell'Unione, salvo le esplicite categorie di esclusione, disposte all'art. 3 della stessa.

6.7.2 La rilevanza giuridica dell' analisi del rischio

Gli argomenti trattati dalla PSD2 includono:

- la gestione degli incidenti gravi;
- le misure di sicurezza;
- i requisiti di governance;
- le procedure di controllo e di governo dei prodotti;
- la gestione dei rischi operativi e di sicurezza;
- i rapporti con la clientela;
- la gestione del sistema informativo;
- le soluzioni di esternalizzazione e il ricorso a servizi cloud;
- i meccanismi di autenticazione degli utenti e di comunicazione con le terze parti;
- la gestione delle frodi;
- i rapporti con le autorità di vigilanza.

L'elencazione sopra esposta ben può far comprendere come una corretta analisi del rischio sia fondamentale per tutti gli operatori che vogliano prestare servizi di pagamento e intermediazione finanziaria all'interno del mercato dell'Unione. Ciò non solo per garantire adeguata tutela a coloro che usufruiranno dei servizi offerti, ma anche per evitare di incorrere in sanzioni e richieste di risarcimento.

6.7.3 Gli adempimenti per l'analisi del rischio

I temi sopra esposti sono oggetto di attenzione per gli enti normatori e segnano un'evoluzione consistente del settore bancario nell'ambito organizzativo e tecnologico. Essi si poggiano su principi che fanno riferimento a:

- entità degli impatti previsti relativi ai problemi potenziali o ai fenomeni attesi;
- proporzionalità delle soluzioni in termini di complessità e di estensione;
- livello di criticità e importanza delle funzioni;
- registrazione dei fenomeni storici;
- livello di soddisfazione dei requisiti;
- identificazione, misura e gestione del rischio associato a specifiche scelte.

6.7.4 Il regime sanzionatorio

La PSD2, in quanto Direttiva, demanda ai singoli Stati membri la predisposizione di sanzioni, che siano "proporzionate, efficaci e dissuasive" (art. 103 PSD2). Sulla scorta di tali indicazioni, nel panorama italiano il regime sanzionatorio è stato predisposto mediante il D.lgs. n. 218 del 2017.
Sono previste sanzioni amministrative pecuniarie e la determinazione del quantum sanzionatorio segue i criteri previsti dall'art. 144-quater del TUB e, nello specifico:

- se il destinatario è persona fisica o giuridica;
- gravità e durata della violazione;
- responsabilità e capacità finanziaria di colui che ha commesso la violazione;
- vantaggio ottenuto o perdita evitata (se determinabile);
- livello di cooperazione per mitigare i danni prodotti dalla violazione;
- potenziali conseguenze e precedenti violazioni commesse.

È utile sottolineare due aspetti innovativi rispetto al passato, rinvenibili rispettivamente agli articoli 92 e 93 della direttiva:

- il diritto di regresso: un prestatore di servizi di pagamento, il quale sia stato sanzionato, ma la responsabilità sia attribuibile ad altri soggetti, può agire in regresso per il ristoro di quanto anticipato a titolo di sanzione e risarcimento del danno, rivalendosi sugli effettivi responsabili;
- l'esclusione di responsabilità, qualora la violazione derivi da circostanze anormali e imprevedibili o nei casi in cui il prestatore di servizi di pagamento sia vincolato da altri obblighi di legge previsti dal diritto dell'Unione o nazionale.

6.8 La proposta di Regolamento DORA

DORA (Digital operational resilience act) è una proposta di Regolamento del Parlamento e del Consiglio Europeo, relativo alla resilienza operativa digitale per il settore finanziario, che dovrebbe diventare effettivo negli Stati membri durante l'anno 2022. Alla stesura del presente libro, la versione definitiva non è stata ancora pubblicata e conseguentemente potrebbero sopraggiungere modifiche anche sostanziali.

DORA nasce per armonizzare a livello UE le norme già esistenti a livello dei singoli Stati membri e relative alla resilienza operativa digitale, i test di resilienza operativa digitale e gli approcci di vigilanza, ad esempio per quanto riguarda le dipendenze da terzi nel settore delle tecnologie dell'informazione e comunicazione (TIC).

La proposta approfondisce la dimensione della gestione dei rischi digitali e conferisce alle autorità di vigilanza finanziaria poteri di sorveglianza sui rischi dovuti alla dipendenza delle entità finanziarie da fornitori terzi di servizi di TIC. DORA istituisce un meccanismo coerente di segnalazione degli incidenti, che contribuirà a ridurre gli oneri amministrativi per le entità finanziarie e a rafforzare l'efficacia della vigilanza. Si noti che il Regolamento non imporrà una standardizzazione specifica, ma farà riferimento a standard settoriali e best practice riconosciute a livello internazionale.

6.8.1 A chi è rivolta la proposta

Per garantire la coerenza delle prescrizioni, il Regolamento DORA copre un ampio ventaglio di entità finanziarie regolamentate a livello di Unione Europea e, in particolare:

"enti creditizi, istituti di pagamento, istituti di moneta elettronica, imprese di investimento, fornitori di servizi per le cripto-attività, depositari centrali di titoli, controparti centrali, sedi di negoziazione, repertori di dati sulle negoziazioni, gestori di fondi di investimento alternativi e società di gestione, fornitori di servizi di comunicazione dati, imprese di assicurazione e di riassicurazione, intermediari assicurativi, intermediari riassicurativi e intermediari assicurativi a titolo accessorio, enti pensionistici aziendali o professionali, agenzie di rating del credito, revisori legali e società di revisione, amministratori di indici di riferimento critici e fornitori di servizi di crowdfunding".

In Figura 17 è riportata parte di una mappa che illustra la struttura - piuttosto articolata - della DORA.

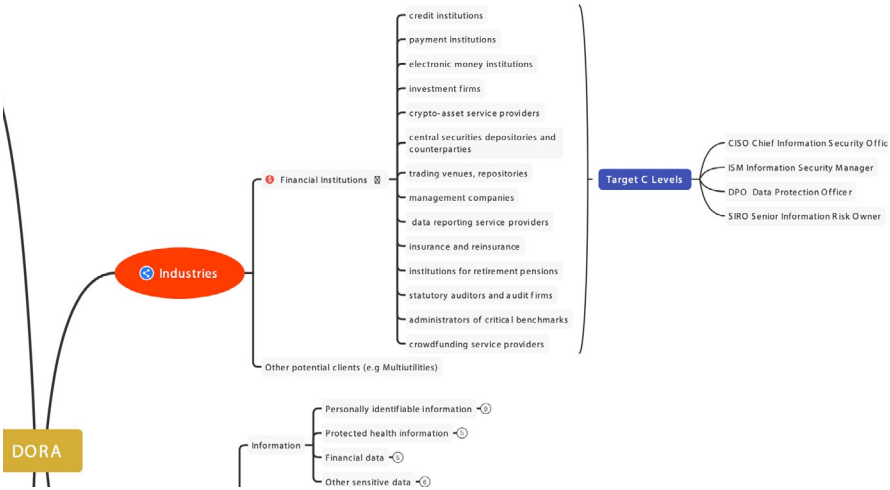

Figura 17 - Parte della struttura della DORA[79]

79 Figura degli autori (scaricabile in pdf da https://bit.ly/3fddzsZ).

6.8.2 Gli adempimenti per l'analisi del rischio

La proposta di Regolamento non impone un approccio specifico, ma "si affida a un utilizzo idoneo, da parte delle entità finanziarie, di norme tecniche riconosciute a livello europeo e internazionale (ad esempio ISO) o delle migliori pratiche del settore, nella misura in cui tale utilizzo sia pienamente conforme alle specifiche istruzioni delle autorità di vigilanza sull'utilizzo e l'integrazione delle norme internazionali"[80].
Le persone giuridiche operanti in ambito *finance e* coinvolte in incidenti hanno l'obbligo di segnalazione degli eventi considerati gravi e sono tenute a informare tempestivamente i propri utenti e clienti nei confronti dei quali l'incidente possa avere avuto un impatto, analogamente alle violazioni dei dati personali.

6.8.3 Il regime sanzionatorio

Pur trattandosi di un Regolamento, e come tale direttamente applicabile in ogni Stato dell'UE, il legislatore ha scelto di non indicare direttamente le sanzioni da imporre in caso di violazione della normativa, demandando ai singoli Stati la definizione di adeguate sanzioni amministrative, misure di riparazione, e sanzioni penali.
Tali misure potrebbero comprendere, ad esempio, la possibilità per le autorità competenti di:

- richiedere la cessazione, temporanea o permanente, di qualsiasi pratica o comportamento contrari alle disposizioni del regolamento;
- adottare qualsiasi tipo di misura, anche di natura pecuniaria, per assicurare che le entità finanziarie continuino a rispettare le prescrizioni di legge.
- Il livello della sanzione amministrativa o della misura di riparazione viene valutato secondo diversi parametri, quali ad esempio:
- la rilevanza, la gravità e la durata della violazione;
- il grado di responsabilità della persona fisica o giuridica responsabile della violazione;
- la solidità finanziaria della persona fisica o giuridica responsabile;
- l'importanza degli utili realizzati e delle perdite evitate da parte della persona fisica o giuridica responsabile, nella misura in cui possano essere determinati.

80 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0595.

6.9. La Circolare di Banca d'Italia numero 285

Dal 1° gennaio 2014 è applicabile la disciplina armonizzata per le banche e le imprese di investimento contenuta nel regolamento CRR (Regolamento UE 575/2013, Capital Requirements Regulation) e nella direttiva CRD IV (Direttiva 2013/36/UE, Capital Requirements Directive IV), che traspongono nell'Unione europea gli standard definiti dal Comitato di Basilea per la vigilanza bancaria.

La normativa regolamenta una serie di adempimenti in carico al mondo finanziario, volti a rafforzare i requisiti patrimoniali delle banche, attraverso l'accantonamento di quote di capitale proporzionali al rischio derivante dai crediti erogati.
Il quadro normativo si completa con l'emanazione delle misure di esecuzione, contenute in norme tecniche di regolamentazione o di attuazione adottate dalla Commissione europea su proposta dell'Autorità bancaria europea (ABE) e, in alcuni casi, delle altre Autorità europee di supervisione (ESA).

La Circolare n. 285 del 17 dicembre 2013 di Banca d'Italia si articola in tre parti, che raggruppano le disposizioni a seconda delle fonti normative da cui derivano (norme comunitarie oggetto di recepimento, norme comunitarie di diretta applicazione, materie non armonizzate):

- la parte prima detta le norme di attuazione della disciplina contenuta nella CRD IV, da recepire negli ordinamenti nazionali (ad esempio: disposizioni in materia di autorizzazione all'attività bancaria, operatività transfrontaliera, riserve di capitale e processo di controllo prudenziale);
- a parte seconda contiene, per ciascuna materia, l'indicazione, a titolo ricognitivo, delle norme europee immediatamente applicabili; definisce, se del caso, le linee guida utili alla piena e agevole applicazione del CRR; individua le discrezionalità nazionali esercitate dalla Banca d'Italia, le unità organizzative responsabili e i termini dei procedimenti amministrativi che hanno nel CRR la loro fonte diretta;
- la parte terza disciplina prevalentemente le materie o le tipologie di rischi che non hanno una derivazione normativa comunitaria, ma sono necessarie per rendere il sistema regolamentare italiano allineato agli standard di vigilanza definiti dagli organismi internazionali.

6.9.1 A chi è rivolta la Circolare 285

La normativa regolamenta una serie di adempimenti per il mondo finanziario, volti a rafforzare i requisiti patrimoniali delle banche accantonando quote di capitale proporzionali al rischio derivante dai crediti erogati.

6.9.2 La rilevanza giuridica dell'analisi del rischio

Nell'ambito della Circolare n. 285, la sezione III del capitolo 4 è dedicata all'analisi del rischio informatico.
Si tratta di un'attività che deve essere svolta nell'ambito delle iniziative di sviluppo di nuovi progetti e di modifica rilevante del sistema informativo.
Il processo va ripetuto con periodicità adeguata alla tipologia delle risorse ICT e dei rischi, nonché, tempestivamente, al verificarsi di situazioni che possono influenzare il complessivo livello di rischio informatico.

6.9.3 Gli adempimenti per l'analisi del rischio

La normativa è strutturata in tre "pilastri":

- Requisiti patrimoniali;
- Controllo delle autorità di vigilanza;
- Disciplina di mercato e trasparenza.

Prende in considerazione numerose tipologie di rischi, compreso il rischio informatico.
I rischi del primo pilastro attengono a:

- rischio di credito (comprende il rischio di controparte, ossia il rischio che la controparte di un'operazione risulti inadempiente prima del regolamento definitivo dei flussi finanziari di un'operazione);
- rischio di mercato;
- rischio operativo.

Nel secondo pilastro sono dettagliati altri rischi, tra cui il rischio informatico (IT), ossia il rischio di perdite dovuto all'inadeguatezza o al guasto di hardware e software di infrastrutture tecniche suscettibile di compromettere la disponibilità, l'integrità, l'accessibilità e la sicurezza di tali infrastrutture e dei dati.
Relativamente alla gestione della sicurezza informatica vengono elencate alcune misure tecniche e organizzative che le banche devono necessariamente implementare e che comprendono:

- politiche di sicurezza;
- presidi fisici di difesa e procedure di autorizzazione e controllo per l'accesso fisico a sistemi e dati;
- regolamentazione dell'accesso logico a reti, sistemi, basi di dati;
- procedure di autenticazione per l'accesso alle applicazioni e ai sistemi;
- segmentazione delle reti di telecomunicazione;
- adozione di metodologie e tecniche per lo sviluppo sicuro del software;
- procedure per l'aggiornamento software e di meccanismi di controllo dell'integrità del software, del firmware e delle informazioni;
- separazione degli ambienti di sviluppo, collaudo e produzione;
- selezione e gestione del personale adibito al trattamento dei dati e allo svolgimento di operazioni critiche;
- procedure per lo svolgimento delle operazioni critiche;
- monitoraggio, anche attraverso l'analisi di log e tracce di audit;
- monitoraggio continuativo delle minacce e delle vulnerabilità di sicurezza;
- scansioni delle vulnerabilità (vulnerability scan) e prove di penetrazione (penetration test) adeguate al profilo di rischio informatico individuato dall'analisi del rischio;
- politiche di sicurezza per le applicazioni sviluppate dalle unità operative e di controllo;
- gestione dei cambiamenti;
- gestione degli incidenti di sicurezza informatica;
- disponibilità delle informazioni e delle risorse ICT.

6.9.4 Il regime sanzionatorio

Le sanzioni previste sono particolarmente onerose e anticipano quanto ripreso dal GDPR, prevedendo una sanzione amministrativa pecuniaria da euro 30.000 fino al 10% del fatturato, elevata fino al doppio dell'ammontare ottenuto, se determinabile.

6.10 Il Regolamento IVASS 38

Il Regolamento IVASS 38 del 3 luglio 2018 detta la disciplina del sistema di governo societario delle imprese assicurative e dei gruppi ai quali appartengono. L'implementazione normativa individua tre modelli di governance da adottare sulla base del principio di proporzionalità, perseguendo l'obiettivo di garantire una struttura organizzativa idonea (anche in termini di sistema di gestione dei dati e sistemi informatici):

- una chiara assegnazione e ripartizione dei compiti e delle responsabilità all'interno dell'organizzazione;
- l'adeguatezza dei flussi informativi tra i diversi attori del sistema;
- il rafforzamento della centralità dell'organo amministrativo.

Quest'ultimo viene riconosciuto come il responsabile finale del sistema di governo societario, in quanto ne definisce gli indirizzi strategici e ne garantisce la complessiva coerenza affinché tale sistema sia adeguato al modello di business nonché alla struttura societaria prescelta, alla natura, portata e complessità dei rischi. All'alta direzione, invece, è assegnata la responsabilità della promozione della cultura del controllo interno all'interno dell'organizzazione.

6.10.1 A chi è rivolto il Regolamento IVASS 38

Il Regolamento IVASS 38 detta la disciplina del sistema di governo societario delle imprese assicurative e dei gruppi ai quali appartengono.

6.10.2 La rilevanza giuridica dell'analisi del rischio

Nell'ambito dei presidi di governo, il Regolamento dettaglia la configurazione del sistema di gestione dei rischio, richiedendo la fissazione di un obiettivo di solvibilità che funga da perno attorno al quale definire la propensione al rischio dell'impresa. Naturalmente, il raggiungimento dell'obiettivo stesso rappresenta un indicatore della

qualità del sistema di governo dei rischi dell'impresa, come tale oggetto di sindacato da parte dell'Autorità di vigilanza.
Fra i rischi per i quali il regolatore ha ritenuto opportuno formulare esplicite prescrizioni, vanno annoverati, per quanto qui di interesse, il rischio di cyber security, di data quality e di continuità operativa.

6.10.3 Gli adempimenti per l'analisi del rischio

L'intervento regolamentare, muovendosi nel solco tracciato dal Regolamento IVASS 20/2008 e dal Provvedimento IVASS 17/2014, che, in linea con quanto stabilito dalla Direttiva Europea Solvency II, ha avuto il merito di traghettare le compagnie assicurative da un approccio per processi a uno guidato dai dati.
Decisioni strategiche e manageriali fondate su dati coerenti sono più facilmente analizzabili e condivisibili all'interno dell'azienda e di conseguenza più efficaci. È quindi necessario mitigare il rischio di governo e controllo dei dati: errori di rilevazione, malfunzionamento di sistemi, reportistica inadeguata a supportare le decisioni; rischi di pianificazione; disallineamento fra funzioni o processi.

6.10.4 Il regime sanzionatorio

La violazione delle prescrizioni del Regolamento ha come conseguenza l'applicazione del regime sanzionatorio previsto dall'art. 310 "Sanzioni amministrative pecuniarie" del Codice delle assicurazioni private che prevede l'irrogazione di sanzioni amministrative pecuniarie entro limiti edittali variabili da 30 mila euro al 10% del fatturato.

Le valutazioni dell'IVASS in merito alla misura delle pene da comminare tengono conto, tra l'altro: dell'irregolarità riscontrata (tipologia, durata, gravità, pregiudizio agli assicurati, agli aventi diritto alle prestazioni o all'esercizio delle funzioni di vigilanza), dei riflessi dell'irregolarità sulla situazione aziendale dell'impresa o gruppo di appartenenza e sul livello di esposizione ai rischi, della reiterazione delle violazioni della medesima natura, della natura del soggetto, dei vantaggi eventualmente ottenuti in conseguenza della condotta irregolare, della collaborazione attiva ed autonoma del soggetto interessato.

6.11 Il Regolamento sui dispositivi medici

Il progresso tecnologico derivante dalle più recenti ricerche universitarie e industriali sta consentendo di realizzare dispositivi medici digitali che permettono di fornire direttamente terapie al paziente, introducendo logiche e algoritmi sempre più complessi, grazie allo sviluppo dell'intelligenza artificiale, sempre più biocompatibili e meno invasivi, grazie ai recenti sviluppi della nanotecnologie e dell'ingegneria tessutale.
Il recente sviluppo di questi dispositivi offre nuove opportunità ai privati e alla sanità pubblica, che riescono a migliorare la loro efficienza e fornire cure di qualità più alta a un maggior numero di persone.
Nessuna tecnologia, seppur evoluta, può considerarsi a "rischio zero". Conseguentemente l'intero corpus regolamentare internazionale si basa su un approccio basato sul rischio.
Più esattamente l'intera materia è disciplinata dal Regolamento Ue 2017/745, pubblicato in Guce a maggio 2017, ma pienamente efficace solo da maggio 2021.
Il Regolamento 2017/745 per i dispositivi medici stabilisce una struttura legislativa di riferimento con i seguenti obiettivi:

- assicurare che i dispositivi immessi sul mercato dell'Unione e utilizzati siano sicuri e presentino un adeguato beneficio;
- fornire un quadro normativo di riferimento che consenta lo sviluppo di nuove tecnologie.

6.11.1 A chi è rivolto il Regolamento

Il Regolamento UE 2017/745 stabilisce che il soggetto che si qualifica come "fabbricante" del dispositivo medico è tenuto a garantire il rispetto dei "requisiti essenziali di sicurezza e prestazione del dispositivo" riportati nell'allegato I del Regolamento.
Il fabbricante deve sviluppare processi e soluzioni tecniche in grado di minimizzare il rischio durante tutto il ciclo vita del prodotto e strategica in tal senso è la creazione di sistemi di gestione per la qualità dedicati, come quello basato sulla ISO 13485. Infatti un approccio basato sul rischio impatta su tutta l'organizzazione e il ciclo di vita del prodotto, dalla progettazione allo smaltimento, passando per l'immissione in commercio, il mantenimento e fino all'eventuale al ritiro dal mercato.

6.11.2 La rilevanza giuridica dell' analisi del rischio

Per garantire efficacia e sicurezza dei dispositivi medici, il Regolamento si basa su due pilastri fondamentali: la massima mitigazione del rischio e un rapporto accettabile tra beneficio e rischio residuo (art. 10 e Allegato I del Regolamento).
Il primo pilastro, la mitigazione massima del rischio, prevede che qualsiasi rischio debba essere ridotto con tutte le strategie tecnicamente possibili, fino a raggiungere una massimizzazione della riduzione dei rischi, cioè il punto in cui ogni nuovo intervento non potrebbe abbattere ulteriormente i rischi a diminuire, contemporaneamente, i benefici ai pazienti.
Il secondo pilastro, la superiorità del beneficio rispetto al rischio, prevede che il beneficio fornito dal dispositivo sia accettabile rispetto al rischio residuo a cui il paziente è esposto.

6.11.3 Gli adempimenti per l'analisi del rischio

L'immissione in commercio dei dispositivi medici ha vincoli normativi e di buone prassi (standard spesso resi obbligatori dalle norme armonizzate) peculiari che tengono conto del fatto che i dispositivi medici interagiscono per definizione con la salute delle persone.
La gestione del rischio (Allegato I) prevede un'identificazione del contesto, un'analisi dei rischi e un trattamento del rischio: in questo caso si procede essenzialmente a ridurre la probabilità degli accadimenti, dato che l'impatto ultimo potrebbe essere la morte o gravi danni alla salute del paziente.
Per le specificità del mondo della sanità digitale, la gestione dei rischi richiede un approccio multi-disciplinare, in cui il rischio clinico, il rischio tecnologico e il rischio legato ai dati debbano essere tenuti in considerazione in modo sinergico.
La mitigazione dei rischi, come presentata nel Regolamento 2017/745, deve seguire preferibilmente un approccio *safe-by-design*; solo nel caso in cui non vi siano soluzioni tecnologiche disponibili, è possibile intervenire prevedere allarmi o istruzioni per l'uso sicuro.

Tale approccio, coerente tra le diverse norme specificatamente medicali, quali la ISO 14971 (con l'edizione del 2019 suggerisce di valutare gli aspetti di integrità, riservatezza

e disponibilità dei dati) e la IEC 62304, può essere facilmente esteso anche alla gestione dei rischi cyber.
Su tale tipologia di rischi poi il Medical Device Coordination Group (organo tecnico della Commissione in ambito di dispositivi medici) nel 2019 ha emanato specifiche linee guida denominate "MDCG 2019 -16 Guidance on Cybersecurity for medical devices". Il processo di gestione e mitigazione del rischio clinico, inoltre, agisce per evitare che soluzioni tecniche per la mitigazione dei rischi relativi alla sicurezza dei dati impattino negativamente sulla sicurezza del paziente.
Un esempio classico è quello della necessità di bilanciare l'accesso al dato regolato via password con l'immediata disponibilità di dati e funzioni in caso di emergenza o urgenza clinica: un defibrillatore non deve certo richiedere una password per essere attivato!

6.11.4 Il regime sanzionatorio

Il Regolamento 2016/745 non stabilisce un regime sanzionatorio, ma richiede agli Stati membri di emanare specifiche sanzioni in materia (art. 113).
Lo Stato italiano, con la Legge 53/2021, ha previsto che il governo emani, entro maggio 2022, decreti legislativi di adeguamento, tra cui anche un decreto specifico sulle sanzioni.

6.12 UNECE 1959 e Automotive

Le auto sono sempre più connesse e lo diverranno ancor di più in futuro. Oltre alle tecnologie GPS, WiFi e Bluetooth, le nostre auto si arricchiscono di nuove funzionalità, quali connettività V2V (*vehicle to vehicle*) e V2X (*vehicle to everything*), *keyless entry*, aggiornamenti OTA (over the air), controlli da remoto, fino ad arrivare nel breve futuro alle auto a guida autonoma.
La facilità con cui i cybercriminali hanno dimostrato di poter violare le centraline e i sistemi delle auto più recenti rivela che la sicurezza informatica dei nuovi veicoli è molto vulnerabile.
Il mercato degli autoveicoli è regolato da accordi internazionali per assicurare determinati livelli di sicurezza delle persone, protezione ambientale, efficienza energetica e protezione dal furto. Gli accordi di riferimento sono il 1958 Agreement, noto anche

come UNECE 1958, e il 1998 Parallel agreement. Essi sono gestiti dal WP.29 del Forum Mondiale per l'armonizzazione delle normative sui veicoli (World forum for harmonisation of vehicle regulations).
Recentemente il WP.29 ha regolamentato il mercato degli autoveicoli anche con normative in materia di cybersecurity.
La ISO/SAE 21434 è uno standard internazionale creato congiuntamente dalla ISO (Organizzazione internazionale per la normazione) e SAE (Society Automotive Engineers, ente di normazione nel campo dell'industria aerospaziale, automobilistica e veicolistica) con l'intento di fornire requisiti di cybersecurity per i componenti automotive, l'organizzazione dei processi e lo sviluppo dei prodotti.

6.12.1 A chi è rivolta l'ISO/SAI 21434

Lo standard ISO/SAE 21434 è rivolto agli OEM (*original equipment manufacturer*) e ai fornitori automobilistici di componentistica (TIERs).
La ISO/SAE 21434 entrerà in vigore nell'Unione Europea da luglio 2022 e gli OEM e TIER dovranno adeguarsi in breve, con partenze diversificate per i vari Paesi in base all'accordo UN-ECE 1958. Altri Paesi invece, tra i quali ad esempio Giappone (JASPAR), Cina (ICV-Program) e Corea del sud, ne hanno stabilito l'efficacia già dal 2021.

6.12.2 La rilevanza giuridica dell'analisi del rischio

Lo standard ISO/SAE 21434 e il WP29 richiedono agli OEM (*original equipment manufacturer*) e ai fornitori automobilistici di componentistica (TIERs) di analizzare le minacce e i rischi durante il ciclo di vita di un veicolo per determinare gli impatti per un utente della strada (conducenti, motociclisti, ciclisti, pedoni, ecc.).

6.12.3 Gli adempimenti per l'analisi del rischio

Il processo di valutazione del rischio è chiamato "TARA" (*threats analysis and risk assessment*).

Lo standard si compone delle seguenti aree:

- gestione della cybersecurity;
- metodi di risk assessment;
- fase iniziale di concepimento di un prodotto;
- sviluppo del prodotto;
- produzione, esercizio e manutenzione;
- processi di supporto.

L'adozione della ISO/ISAE 21434 può essere affiancata dal TISAX, sviluppato dal VDA (Verband del Autobilindustrie[81]) per valutare la maturità del sistema di gestione per la sicurezza delle informazioni (simile a quello richiesto dalla ISO/IEC 27001) dalle società che operano nell'ambito automotive[82].

6.13 Il D. Lgs. 231 del 2001

Il D. Lgs. 231/2001 ha introdotto nell'ordinamento italiano un regime di responsabilità amministrativa in capo alle persone giuridiche in caso di commissione di reato da parte delle persone fisiche che rivestono posizioni di vertice (cosiddetti "apicali") e ove da tale reato derivi un interesse o vantaggio per l'organizzazione stessa.
Più precisamente, la responsabilità dell'organizzazione può sorgere quando un soggetto cosiddetto "apicale" (persona che riveste funzioni di rappresentanza, amministrazione, direzione dell'ente o di una sua unità organizzativa oppure che esercita, anche di fatto, la gestione e il controllo dello stesso) oppure una persona, sottoposta alla direzione o alla vigilanza di un soggetto apicale, pone in essere uno dei reati richiamati dalla legge stessa (i cosiddetti "reati presupposto") per un interesse o vantaggio dell'ente stesso.
L'ipotesi classica è quella di un dirigente che corrompe un funzionario pubblico per ottenere l'aggiudicazione di un appalto: in tale ipotesi, oltre alla responsabilità penale in capo al soggetto che ha posto in essere l'atto corruttivo, potrà essere applicata una sanzione amministrativa in capo all'ente che ha tratto vantaggio dall'atto del suo apicale.
La disciplina prevede poi la possibilità per la persona giuridica di evitare l'applicazio

81 www.vda.de.

82 https://www.ictsecuritymagazine.com/articoli/tisax-la-valutazione-del-livello-di-maturita-della-sicurezza-delle-informazioni-nellambito-automotive/.

ne della sanzione amministrativa qualora abbia posto in essere, in via preventiva, un modello di organizzazione e gestione (detto MOG) volto ad evitare la commissione del reato.
Il D.Lgs. 231/2001 prevede tra i reati presupposto anche i delitti informatici, richiamando varie fattispecie tra cui:

- Accesso abusivo ad un sistema informatico e telematico;
- Detenzione e diffusione abusiva di codici di accesso ai sistemi informatici o telematici;
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico;
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche;
- Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche;
- Danneggiamento di informazioni, dati e programmi informatici;
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità;
- Danneggiamento di sistemi informatici o telematici;
- Danneggiamento di sistemi informatici o telematici di pubblica utilità;
- Documenti informatici (falsità);
- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica.

6.13.1 A chi è rivolto il D.Lgs 231/2001

La norma venne introdotta in Italia con l'intento di reprimere la corruzione e diffondere la cultura della trasparenza e del rispetto delle regole all'interno delle organizzazioni.

I soggetti chiamati quindi all'applicazione della disciplina sono, in generale, gli enti forniti di personalità giuridica, le società e le associazioni anche prive di personalità giuridica. Sono esclusi dall'ambito di applicazione lo Stato, gli enti pubblici territoriali, gli altri enti pubblici non economici nonché gli enti che svolgono funzioni di rilievo costituzionale.

6.13.2 La rilevanza giuridica dell' analisi del rischio

La responsabilità amministrativa dell'ente si basa sulla cosiddetta "colpa da organizzazione": si puniscono infatti gli enti che non sono riusciti ad impedire, attraverso il MOG, la commissione di reati all'interno della propria organizzazione.
In sostanza il D. Lgs. 231/2001 chiede agli enti di effettuare un'analisi del rischio circa la possibilità che vengano posti in essere i reati presupposto e, a valle di tale analisi, di attuare un MOG che, ove abbia correttamente identificato i rischi reato e ove sia stato implementato in maniera efficace, può evitare l'applicazione della sanzione stessa.

6.13.3 Gli adempimenti per l'analisi del rischio

L'art. 6 comma 2, relativo alla creazione ed implementazione del MOG, stabilisce che gli obiettivi da soddisfare sono:

- individuare le attività nel cui ambito possono essere commessi reati;
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione dei reati;
- prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Stante tali indicazioni, l'organizzazione deve, come primo passo, mappare tutti i processi, individuare le potenziali fattispecie tra i reati presupposto applicabili e associare a ciascun processo i reati presupposto applicabili.
È necessario dunque, attraverso il coinvolgimento dei responsabili di ogni processo, identificare le attività a rischio e il corrispondente livello di rischio in base alla frequenza e alla rilevanza dell'attività, nonché alla gravità del reato.
Nella valutazione del rischio e, in particolare, in quella relativa al sistema informatico, gli enti devono tenere in considerazione il rischio di commissione di uno dei reati presupposto previsti dall'art. 24bis e adottare le misure tecniche ed organizzative neces-

sarie per contrastarlo. Si pensi, ad esempio, alla rilevanza dei delitti di accesso abusivo ad un sistema informatico o di detenzione e diffusione abusiva di codici di accesso ai sistemi informatici o telematici per qualsiasi organizzazione, che utilizzi sistemi digitali di trattamento delle informazioni.

Definite responsabilità e livelli di rischio, si deve poi identificare uno o più controlli a presidio dei rischi rilevati e verificare l'esistenza di presidi già posti in essere. Ciascun controllo ha una capacità intrinseca (predefinita) di abbattere le probabilità di commettere il reato. Il livello di rischio mitigato dai controlli esistenti si definisce come «rischio residuo». Si procede quindi a identificare gli scostamenti tra il modello esistente e il modello a tendere.

Tutti gli standard di controllo individuati dovrebbero essere recepiti dalle procedure interne in modo da diventare attività prescrittive, cogenti, tracciate e verificabili.
Il D. Lgs 231/2001 richiede il monitoraggio costante dei rischi, delle attività e dei controlli, in maniera da poter modificare il MOG quando vengono scoperte significative violazioni delle prescrizioni o quando intervengono mutamenti nell'organizzazione o nell'attività (articolo 7 comma 4).
Il monitoraggio passa anche attraverso la nomina di un Organismo di vigilanza, con il compito di verificare l'efficacia del MOG e di proporre le misure correttive ritenute necessarie.

6.13.4 Il regime sanzionatorio

Nell'ipotesi in cui venga posto in essere un reato presupposto e l'ente non abbia realizzato o applicato un MOG efficace, all'ente può essere applicata una sanzione amministrativa di natura interdittiva o pecuniaria, nonché la confisca e la pubblicazione della sentenza.

Relativamente alla sanzione pecuniaria, il quantum è misurato in quote, in un numero compreso tra 100 e 1000; l'importo delle quote varia da un minimo di € 258,23 a un massimo di € 1.549,37. La quantificazione delle quote viene decisa dal giudice tenendo conto della gravità del fatto, del grado di responsabilità dell'ente, dell'attività svolta dall'ente per tentare di eliminare o attenuare le conseguenze del fatto o per prevenire la commissione di ulteriori illeciti.

6.14 Il Codice della crisi d'impresa

Le crisi economiche che hanno caratterizzato gli ultimi anni hanno imposto una rivisitazione del concetto di "fare impresa", soprattutto in chiave di assunzione di rischi e di prevenzione della crisi e dell'insolvenza. Il Codice della crisi d'impresa e di insolvenza (CCII), D. Lgs. 14/2019, risultava un intervento indispensabile dato il continuo evolversi della realtà economico-sociale.

Il DL 118 del 2021 ha posticipato l'entrata in vigore della gran parte delle disposizioni del CCII, riservando al legislatore l'opportunità di apportare in corso d'opera le rettifiche che si rendono necessarie per il recepimento della Direttiva europea 2019/1023/UE (cosiddetta Direttiva Insolvency).

6.14.1 A chi è rivolto il CCII

Il CCII esplicita l'obbligo, posto in capo all'imprenditore, di istituire adeguati assetti organizzativi, amministrativi e contabili adeguati alla natura e dimensione dell'impresa. Il dettato della norma prevede che tale profilo di adeguatezza vada valutato anche soppesando la capacità di "rilevazione tempestiva della crisi dell'impresa e della perdita della continuità". Il Consiglio nazionale dei dottori commercialisti ed esperti contabili ha così riassunto i più importanti indici di adeguatezza:

- l'adozione di organigramma e funzionigramma;
- la precisa attribuzione dei poteri decisionali e delle deleghe;
- l'esistenza di procedure di gestione del rischio;
- l'attendibilità dei flussi informativi;
- la presenza di procedure che assicurino che il personale sia competente e adeguato a svolgere la propria funzione;
- la presenza, la diffusione e l'aggiornamento delle procedure.

6.14.2 La rilevanza giuridica dell'analisi del rischio

L'analisi del rischio è soggettiva per ogni persona giuridica e deve rispettare una scala di criticità (con valori differenti per ogni tipologia di rischio rilevata) da assegnare ai processi più importanti (ossia quelli che, se non monitorati e governati costantemente, possono portare alla crisi di impresa). Tra i rischi va annoverato il rischio informatico.

6.14.3 Gli adempimenti per l'analisi del rischio

Il modello organizzativo costituisce la vera architrave del sistema di responsabilità dell'ente. Si ritiene che si potranno applicare le interpretazioni già studiate per il Modello organizzativo richiesto dal D. Lgs. 231/2001. L'impresa non dovrà, dunque, duplicare i documenti organizzativi ma, al più, potrà provvedere ad aggiornare e implementare i modelli organizzativi di cui già dispone,se già presenti.

Intervista a Daniela Marucci, Dirigente responsabile della linea Corporate e trasporti di UnipolSai.

D. L'analisi del rischio informatico implica l'analisi dei rischi correlati, quali quello di continuità operativa e di catena di fornitura. La vostra attività di analisi sui clienti prevede l'adozione di soluzioni per ottenere una visione di insieme di questi rischi e dei relativi impatti economici?

R. L'impostazione che abbiamo dato all'attività di valutazione del profilo di rischio di un cliente corporate va proprio nella direzione indicata di visione di insieme con il fine di comprendere il livello di esposizione per i principali rischi operativi e il corrispondente impatto finanziario.

Il tool elaborato da UnipolSai si pone l'obiettivo di sensibilizzare le aziende in merito al processo di identificazione, valutazione e gestione dei rischi senza volersi in alcun modo sostituire a un processo di enterprise risk management, ma fornendo all'azienda spunti di riflessione sui rischi cui può essere esposta. Lo strumento, che, per quanto sopra esposto, deve essere considerato come un "esercizio" cui i manager si sottopongono al fine di cominciare ad avvicinarsi alle tematiche di risk management, considera un insieme predefinito di rischi identificati grazie all'esperienza maturata da UnipolSai e, sulla base delle risposte a un que-

stionario sottoposto ai manager dell'azienda, produce in output una prima mappatura dei rischi, valutati in termini di «probabilità di accadimento» e «magnitudo» secondo una scala di valutazione costruita da UnipolSai.

Questa valutazione può essere approfondita con analisi ad hoc condotte dal team di Analisi rischi e loss prevention. Attraverso sopralluoghi mirati vengono fornite indicazioni di loss prevention volte all'identificazione di azioni di mitigazione del rischio.

Il rischio cyber è uno dei rischi analizzati attraverso il tool R.O.

D. Nel substrato economico italiano, dominato da piccole e medie imprese, qual è la struttura dei controlli interni più diffusa e quali i presidi di mitigazione del rischio adottati dalle aziende nel vostro portafoglio clienti?

R. UnipolSai è leader nel settore assicurativo danni e quindi riteniamo che l'approccio alla gestione del rischio della nostra clientela sia rappresentativo di quello del mondo delle PMI italiane. Purtroppo riscontriamo una carenza di attenzione al tema di gestione dei rischi che si amplia al diminuire delle dimensioni aziendali.

A titolo esemplificativo citiamo un'indagine sulle medie aziende, svolta da Mediobanca per Cineas, che evidenzia che il numero delle società che dichiarano di elaborare una mappatura dei rischi ha raggiunto il 67% del totale. Tuttavia il numero delle aziende che discute delle tematiche connesse ai rischi nel CdA è ancora molto contenuto (circa 14%), a dimostrazione di una scarsa diffusione della cultura del rischio rispetto alle aziende di dimensioni maggiori e con una presenza internazionale.

Il passaggio per le aziende dal risk assessment alla risk governance è fondamentale per una gestione consapevole ed in grado di affrontare in modo tempestivo ed efficace le situazioni di crisi. Da non dimenticare che è obbligo, per l'imprenditore, dotare l'azienda di un assetto organizzativo in linea con la sua natura e dimensioni, ciò al fine di garantire la continuità aziendale a fronte di situazioni di crisi (Codice della crisi dell'impresa e dell'insolvenza).

D. Con riferimento all'assicurazione del rischio cyber, quali sono le garanzie a cui sono più interessati i clienti?

R. Le garanzie di maggior interesse per i clienti sono diverse a seconda della dimensione dell'azienda. Sulle realtà più piccole c'è un maggiore esigenza legata al ripristino e al supporto nella gestione della crisi: soluzioni di "pronta ripresa" che mettano a disposizione del cliente un incident response manager sono tra le più richieste.

Sulle aziende più strutturate c'è una attenzione particolare al ristoro dei danni per interruzione di attività.

E' trasversale la richiesta di garanzie per il pagamento del prezzo del riscatto in caso di ransomware. I nostri contratti non prevedono questa voce di indennizzo, poiché non troviamo eticamente sostenibile una simile garanzia, che finirebbe per fomentare e foraggiare tale fenomeno criminale.

6.15 Il regolamento eIDAS

Il Regolamento eIDAS del 2014, che ha abrogato la Direttiva del 1999 in materia di identificazione elettronica e servizi fiduciari per le comunicazioni elettroniche, è stato emanato per garantire all'interno dell'Unione il "buon funzionamento del mercato interno e l'adeguata sicurezza dei mezzi di identificazione elettronica e dei servizi fiduciari".
In tal senso, tale normativa:

- istituisce un quadro giuridico per firme, sigilli e sistemi identificazione (servizi fiduciari o trust service);
- fissa le condizioni che uno Stato membro deve seguire per il riconoscimento di mezzi identificazione elettronica di persone (fisiche e giuridiche) provenienti da altro Stato membro;
- stabilisce norme relative ai servizi fiduciari in particolare nelle transazioni elettroniche.

Il bene giuridico tutelato è la certezza giuridica degli ambienti online, mediante la corretta identificazione dei soggetti e, più in generale, la sicurezza delle interazioni elettroniche del consumatore, delle imprese e delle istituzioni all'interno del mercato comune dell'Unione Europea.

6.15.1 A chi è rivolto il Regolamento eIDAS

Il regolamento eIDAS si rivolge ai soggetti che prestano servizi fiduciari stabiliti all'interno dell'UE e ai soggetti titolari di uno dei regimi di identificazione elettronica notificati dallo Stato membro in cui è stabilito. Il Regolamento non si applica ai cosiddetti "sistemi chiusi", ossia quei sistemi che sono vincolati al solo diritto interno di un singolo Stato membro (e solo da questo riconosciuti) e ai sistemi derivanti da accordi conclusi da un numero definito di partecipanti.
Il Regolamento, in ordine a determinazione di danni e procedure applicabili, non si sostituisce alla normativa nazionale prevista in materia: ogni Stato membro, inoltre, può rilasciare mezzi di identificazione elettronica, purché sia rispettato almeno uno dei livelli di adeguatezza stabiliti nell'atto di esecuzione di cui all'art. 8 paragrafo 3 del Regolamento.

I prestatori di servizi fiduciari extra UE, prima di poter operare con l'UE devono essere

qualificati mediante la verifica del rispetto dei livelli di adeguatezza richiesti dal Regolamento.

6.15.2 La rilevanza giuridica dell'analisi del rischio

I soggetti di cui al punto che precede, al fine di offrire i propri servizi nel rispetto di quanto previsto dal Regolamento, devono necessariamente effettuare un'analisi del rischio volta, in particolar modo, al rispetto dei requisiti di sicurezza, adeguatezza e affidabilità richiesti dalla norma. In ragione di ciò, all'interno di ogni Stato membro è istituito un organo di vigilanza con compiti di controllo e verifica dell'adeguatezza di tali soggetti. L'analisi del rischio è importante anche al fine di attuare un sistema di monitoraggio e notifica delle violazioni di sicurezza e perdita di integrità, visti gli obblighi di segnalazione alle autorità dettati dalla norma.

6.15.3 Gli adempimenti per l'analisi del rischio

Gli operatori che intendano offrire servizi fiduciari devono:

- attuare misure tecniche, organizzative, di sicurezza (al fine di garantire adeguato livello di sicurezza nella prestazione dei servizi) e informative verso le persone fisiche e giuridiche, soprattutto per ciò che concerne gli effetti negativi relativi alle violazioni di sicurezza;
- entro 24 ore dalla scoperta di una violazione, effettuare le notifiche all'organismo di vigilanza e a tutti gli altri enti interessati; se la violazione può avere impatti negativi sugli interessati, questi vanno informati tempestivamente; se la violazione è di interesse pubblico, allora deve essere data informazione al pubblico;
- ogni 24 mesi (per gli operatori di servizi fiduciari qualificati) trasmettere una relazione all'organismo di valutazione della conformità ed essere sottoposti ad audit; ciò nonostante, ogni qualvolta lo volesse, l'organismo può richiedere una verifica su un prestatore di servizi fiduciari;
- informare l'organismo di vigilanza per ogni variazione e cessazione delle attività svolte;
- applicare misure conformi a garantire sicurezza, formare il proprio personale e

qualificare i propri fornitori correttamente;
- possedere un'assicurazione adeguata per eventuali danni che possono provocare i propri servizi;
- informare i propri clienti sui servizi offerti e le eventuali limitazioni.

Il prestatore di servizi fiduciari qualificati che rilascia certificati ha l'obbligo di riconoscere e identificare i soggetti cui tale certificato è rilasciato mediante i seguenti criteri:
- presenza concreta della persona fisica o suo legale rappresentante;
- a distanza, solo se sono rispettati i requisiti di cui all'art. 8 del regolamento con livello di adeguatezza significativo o elevato;
- mediante firma elettronica qualificata o sigillo elettronico qualificato;
- altre modalità riconosciute a livello nazionale tali da garantire alto livello di affidabilità della presenza della persona cui viene rilasciato il certificato.

6.15.4 Il regime sanzionatorio

Il Regolamento chiarisce alcuni profili di responsabilità, determinando, in primo luogo, una responsabilità per lo Stato membro che non adotta una adeguata e sistematica azione di verifica e vigilanza sui propri operatori.
Oltre a ciò, il regolamento sanziona gli operatori che rilasciano strumenti di identificazione elettronica (se per dolo o negligenza ha comportato danni alla persona fisica o giuridica) e coloro i quali gestiscono le procedure di autenticazione. Nella determinazione del danno e delle responsabilità si applicano le norme nazionali e va posto più l'accento sulle conseguenze correlate all'inadeguatezza dell'analisi del rischio che alla sola mancanza.
Inoltre, per i servizi fiduciari, ovviamente, sono responsabili coloro che prestano tali servizi per ogni danno cagionato, per dolo o negligenza, a persone fisiche o giuridiche nella mancata applicazione della normativa prevista dal Regolamento. In tal caso, l'onere della prova (qualora si tratti di servizi fiduciari resi da un soggetto non qualificato) spetta alla persona fisica o giuridica che afferma di aver subito un danno. Nel caso di un prestatore qualificato, invece, vi è presunzione di dolo o negligenza, salvo prova contraria che deve essere prodotta dal prestatore di servizi.
Se i prestatori di servizi informano gli utenti dei disservizi non sono responsabili dei danni che derivano dall'utilizzo di servizi oltre i limiti indicati (fatte salve le norme nazionali in tema di responsabilità).
Le sanzioni sono disposte da ogni singolo stato membro e devono essere effettive, proporzionate e dissuasive.

7. Approcci per la valutazione del rischio

In questo capitolo sono elencati gli approcci più noti per la valutazione del rischio e applicabili a quello digitale.

7.1 ISO 31000 e ISO 31010

La norma ISO 31000[83] "Risk Management – Guidelines" è uno standard internazionale che fornisce principi e linee guida generali per la gestione del rischio. Redatto dall'ISO (International Organization for Standardization), è stato pubblicato per la prima volta nel 2009 e successivamente aggiornato nel 2018.
L'impianto si contraddistingue per:

- i principi di gestione del rischio (otto), incardinati sul concetto di creazione e protezione del valore;
- enfatizzazione del coinvolgimento e dell'impegno dei vertici, affinché garantiscano l'integrazione della gestione del rischio nell'organizzazione;
- un modello aperto, adattabile a ogni tipologia di organizzazione e rischio, a diversi livelli (strategico, operativo, di programma o di progetto);
- accentuazione della natura iterativa del processo di gestione del rischio.

La ISO 31000 è accompagnata dalla IEC 31010[84] "Risk management — Risk assessment techniques", la cui ultima edizione è del 2019. È un elenco di approcci per l'analisi dei rischi. Ogni metodo viene incasellato in base alla fase di gestione del rischio più utile per il suo utilizzo.

7.1.1 Ambito di applicazione

La ISO 31000:2018 non ha l'obiettivo di prescrivere adempimenti o enumerare requisiti a cui ottemperare per ottenere una certificazione.

83 https://www.iso.org/standard/65694.html.

84 https://www.iso.org/standard/72140.html.

Scopo dello standard è fornire principi e linee guida per la gestione dei rischi e che siano applicabili flessibilmente a:

- ogni tipologia di impresa, indipendentemente dal settore merceologico di appartenenza e dalla forma giuridica adottata (privata, pubblica, associazione, individui);
- ogni tipologia di rischio, di qualunque natura o conseguenza (positiva o negativa);
- l'intero ciclo di vita dell'organizzazione, a livello strategico, operativo, di programma o di progetto.

7.1.2 Architettura del framework

La struttura dello standard ISO/IEC 31000 nell'attuale versione 2018 risulta essere semplice e sequenziale. Il corpo della norma presenta le parti introduttive presenti all'interno dei capitoli 1 (Campo di applicazione dello standard), capitolo 2 (Riferimenti normativi) e capitolo 3 (Termini e definizioni). Nei capitoli successivi vengono descritti i componenti di una gestione dei rischi efficiente, efficace e coerente. Tali componenti riguardano i principi, il framework e il processo di gestione del rischio, come illustrato nella figura 1.

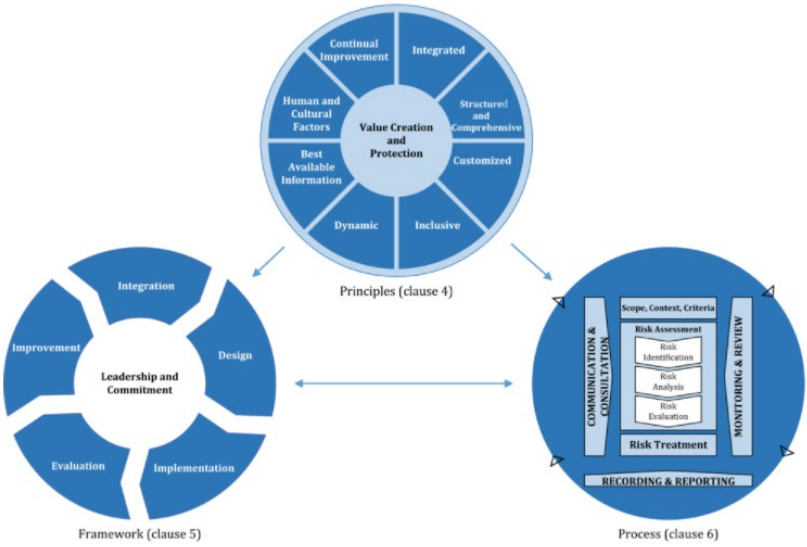

Figura 18 - Componenti della ISO 31000:2018[85]

85 ISO 31000:2018. Risk management — Guidelines. Svizzera: ISO, 2018.

Nel capitolo 4 vengono descritti i principi alla base della gestione del rischio che dovrebbero essere presi in considerazione in fase di implementazione del framework e dei processi di gestione del rischio dell'organizzazione. Per far sì che la gestione del rischio sia efficace, un'organizzazione dovrebbe implementare un processo che:

- sia parte integrante di tutti i processi organizzativi;
- sia sistematico, strutturato e tempestivo;
- sia su misura;
- sia trasparente e inclusivo;
- sia dinamico, iterativo e permetta di reagire al cambiamento;
- sia basato sulle migliori informazioni disponibili;
- tenga in considerazione fattori umani e culturali;
- favorisca il miglioramento continuo dell'organizzazione.

Il capitolo 5 descrive il framework di gestione del rischio. L'adozione di un adeguato framework, ossia di un approccio strutturato, dovrebbe permettere all'organizzazione di includere la gestione del rischio all'interno dei processi organizzativi, decisionali e di governo. Il framework dovrà essere adattato al contesto esterno e interno in cui viene applicato. Il capitolo 6 descrive il processo di gestione dei rischi che prevede l'applicazione sistematica di politiche, procedure e pratiche per stabilire il contesto e valutare, trattare, monitorare, riesaminare, registrare e segnalare i rischi.

7.1.3 Eventuali evoluzioni

Una modifica o evoluzione della ISO 31000 al momento non è prevista. ISO sta però sviluppando, prendendo spunto dalla ISO 31000, la ISO/IEC 23894 "Tecnologia dell'informazione – Intelligenza artificiale – Gestione del rischio", con linee guida per gestire i rischi tipici dei sistemi di intelligenza artificiale.

7.2 ISO/IEC 27005

La ISO/IEC 27005[86] "Information security risk management" definisce un modello formale di analisi e gestione dei rischi allineato alla ISO 31000, ma all'interno della famiglia

86 https://www.iso.org/standard/75281.html.

27000. Essa, soprattutto negli allegati, fornisce informazioni utili a creare una metodologia ad-hoc.
La ISO/IEC 27005 fu pubblicata in una prima edizione nel 2008 e una seconda nel 2011.
L'attuale terza edizione della ISO/IEC 27005 è stata pubblicata nel 2018.
Una quarta edizione è in fase di stesura e dovrebbe essere pubblicata alla fine del 2022.

7.2.1 Ambito di applicazione

La ISO/IEC 27005 è applicabile a tutti i tipi di organizzazione (p.e. imprese commerciali, agenzie governative, organizzazioni no-profit) che intendono gestire i rischi che possono compromettere la sicurezza delle informazioni.

7.2.2 Architettura del framework

La struttura della ISO/IEC 27005 è semplice e sequenziale. Può essere vista come composta da due parti tra loro complementari:

- il testo della norma, che non deve essere considerata di per sé una metodologia di analisi dei rischi, ma un modello di gestione dei rischi relativi alla sicurezza delle informazioni;
- elementi pratici negli allegati.

Entrando nello corpo della norma, si nota che i primi capitoli sono introduttivi.
Dal capitolo 7 al capitolo 12 sono presentati i passi sequenziali, che riprendono quanto già previsto all'interno dello standard ISO 31000, per applicarlo alla sicurezza delle informazioni. Nelle appendice sono forniti esempi pratici.
Vediamo nel seguito il contenuto dei singoli capitoli del corpo della norma.

Stabilire il contesto
Il contesto e l'ambito della gestione del rischio per la sicurezza delle informazioni devono essere definiti per garantire che tutte le attività pertinenti siano prese in considerazione nella valutazione del rischio.

Valutare il rischio
L'obiettivo è quello di determinare un elenco completo e ordinato dei rischi che possono creare, incrementare, prevenire, degradare, accelerare o ritardare il raggiungimento degli obiettivi (impattando quindi l'integrità, riservatezza e disponibilità) relativi alla sicurezza delle informazioni.

La valutazione dei rischi è suddivisa in tre fasi e sotto attività:

- Identificazione dei rischi (§ 8.2) per determinare cosa può accadere e causare una potenziale perdita, attraverso le seguenti attività:
  - ► identificazione degli asset (§ 8.2.2);
  - ► Identificazione delle minacce (§ 8.2.3);
  - ► Identificazione dei controlli esistenti (§ 8.2.4);
  - ► Identificazione delle vulnerabilità (§ 8.2.5);
  - ► Identificazione delle conseguenze (§ 8.2.6).
- Analisi dei rischi (§ 8.3), che può essere effettuata in vari gradi di dettaglio a seconda della criticità delle risorse, dell'entità delle vulnerabilità conosciute e degli incidenti precedenti che coinvolgono l'organizzazione. L'analisi può essere qualitativa o quantitativa o una combinazione di queste. La norma prevede di valutare, per le minacce individuate, le conseguenze e la probabilità di accadimento. Tramite l'utilizzo di questi parametri è possibile determinare il livello di rischio (§ 8.3.4).
- Ponderazione dei rischi (§ 8.4), ossia il loro confronto con i criteri di accettabilità, determinati dalla predisposizione al rischio dell'organizzazione

Trattare il rischio

A seconda di come sono stati valutati, la ISO/IEC 27005 indica quattro opzioni di trattamento dei rischi:

- Risk retention – non sono previste ulteriori azioni di trattamento;
- Risk modification – vanno introdotti, rimossi o cambiati controlli di sicurezza in modo che il rischio residuo possa essere rivalutato come accettabile;
- Risk avoidance - l'attività o la condizione che determina il rischio deve essere evitata;
- Risk sharing - il rischio deve essere condiviso con un'altra parte (fornitore, assicurazione).

Accettazione, comunicazione e monitoraggio

La norma prevede che venga preparato un elenco di rischi accettati (§ 10) con una giustificazione se non soddisfano i normali criteri di accettazione del rischio.

La comunicazione del rischio (§ 11) è un'attività per raggiungere un accordo tra le parti interessate su come trattare i rischi. Essa richiede di scambiare e condividere informazioni sul rischio tra le parti interessate.

I rischi non sono statici: minacce, vulnerabilità, probabilità o conseguenze possono cambiare anche improvvisamente. Per questo motivo la norma richiede un monitorag-

gio costante per rilevare questi cambiamenti.

7.2.3 Eventuali evoluzioni

L'approccio proposto dalla ISO/IEC 27005 si basa sul metodo di identificazione di asset, minacce e vulnerabilità, che è una delle possibili modalità richieste dalla ISO/IEC 27001 per un sistema di gestione della sicurezza delle informazioni. Nella futura versione della norma, prevista per fine 2022, sarà dato più spazio ad altri approcci.

7.2.4 Esperienza nell'uso di ISO 31000 e ISO/IEC 27005

Di seguito un caso pratico di applicazione di un modello di analisi del rischio, implementato dall'Università degli Studi di Camerino e in linea con quanto richiesto dagli standard ISO/IEC 27005 e ISO 31000. Il modello nasce nell'ambito dell'implementazione di un sistema di gestione della sicurezza delle informazioni (SGSI) predisposto secondo lo standard ISO/IEC 27001[87].
A livello pratico è stata adottata la metodologia Magerit, implementata avvalendosi dello strumento software PILAR. L'approccio utilizzato è articolato in cinque distinti passaggi:

- Identificazione degli asset di rilievo per l'ateneo, avendo modo di prestare particolare attenzione alle dipendenze tra di essi, e avendo cura di procedere a partire dai dati e dai processi che li elaborano. Gli asset sono stati valorizzati utilizzando una scala qualitativa.
- Identificazione delle minacce che possono interessare le varie tipologie di asset e successivo abbinamento tra i gruppi di asset e le minacce.
- Misurazione dell'esposizione di un asset ai rischi, ipotizzando teoricamente il caso peggiore. Nel calcolo del rischio sono state considerate anche le contromisure, sia riducendo la frequenza della minaccia (caso delle contromisure preventive) sia limitando l'impatto causato (caso delle contromisure contenitive).
- Determinazione dell'impatto che le minacce possono avere sul sistema, sia considerando il valore degli asset, sia considerando il livello di compromissione teorica

87 F. Ciclosi, M. Mauri, A. Polzonetti. University ICT security certification, European Journal of Higher Education IT. 2016, 1, pagg. 101-110. https://www.eunis.org/erai/2016-1/.

causabile da tali minacce. Sono state utilizzate due tipologie di calcolo: l'impatto cumulativo e l'impatto riflesso.

- Calcolo del valore di rischio, considerando sia l'impatto, sia le frequenze di accadimento delle minacce. In tale fase i singoli rischi sono stati combinati o raggruppati con riferimento a ogni asset e si è ottenuto un valore globale del rischio relativo al singolo asset, espresso secondo una scala a otto valori. Successivamente, nella scala sono stati definiti due valori di soglia denominati: allerta e intervento. Il valore di allerta rappresenta la soglia sotto la quale non si ritiene necessario applicare ulteriori contromisure, mentre il valore di intervento, corrisponde alla soglia sopra la quale devono essere individuate immediatamente delle opportune contromisure atte a riportare il valore del rischio al di sotto della soglia stessa. In tale ottica, l'ateneo ha ritenuto opportuno accettare il valore di rischio residuo, nel caso in cui lo stesso sia minore di quello della soglia di intervento fissata.

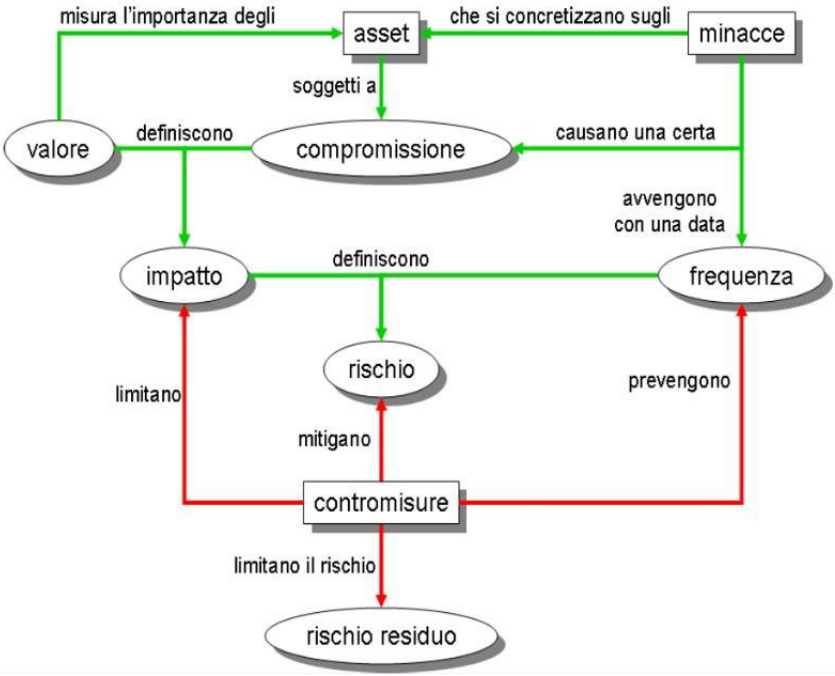

Figura 19 - La metodologia di trattamento del rischio adottata dall'Università degli Studi di Camerino [88]

88 Fonte: https://security.polito.it/~lioy/01jem/lab03.pdf.

Infine, i rischi individuati sono stati trattati per diminuirne il valore. Le azioni sono registrate e monitorate in un registro di miglioramento e collegate alle debolezze riscontrate.

#	Fonte	Rif. Doc.	Punto ISO27001	Debolezza	Azione
1	AR	DS-03, § 6.3.1, contromisure [AUX6]	9.2.3	I cablaggi non sono tutti protetti e identificabili	Errori di configurazione, interferenze ed operazioni di intercettazione dei dati possono accadere facilmente senza un controllo dei cablaggi

Conseguenze	Priorità	Respons.	Risorse	Entro il	Stato al 25/06/2015 evidenze	% Comp
Etichettare tutti i cavi rilevanti per i sistemi, separare i cablaggi di alimentazione da quelli per i dati, controllare che non sia possibile intercettare in maniera non autorizzata del traffico di dati accedendo ai cablaggi	Media	Rossi	Interne	31/12/14	PT-45 - Sicurezza e schema dei cablaggi.doc - V.3 del 22/1/2014	100

Figura 20 - Un estratto del registro delle azioni di miglioramento di Unicam

La valutazione del rischio viene svolta su base almeno annuale, divenendo parte di un processo ciclico di miglioramento continuo.
A completamento del processo di miglioramento continuo, sono stati definiti indicatori finalizzati al monitoraggio dell'efficacia dei controlli (vedere Figura 21).

cod	*descrizione*	*frequenza*	*rif. Annex A*	*2012*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*2014*	*minimo*	*ideale*
I27	Qualità delle password	6m	A.11.3.1	2			3			4			5			5	**5**	**2**	**4**

Figura 21 - Un estratto della tabella degli indicatori di Unicam

Anche per la gestione di questi indicatori sono stati definiti due valori soglia: uno di accettabilità e uno di desiderabilità.

7.3 COSO ERM Framework

La Committee of Sponsoring Organization of the Treadway Commission (COSO) è una commissione statunitense indipendente costituita nel 1985 su iniziativa congiunta di cinque organizzazioni del settore privato e sponsorizzata dalle maggiori associazioni professionali e industriali. La sua missione è quella di fornire "leadership di pensiero attraverso lo sviluppo di framework e linee guida complete rispetto all'*enterprise risk management (ERM)*, il controllo interno e la deterrenza contro le frodi ". Il principio fondamentale che guida le attività di COSO è quello per cui una buona gestione del rischio e un efficace controllo interno sono necessari per il successo a lungo termine di tutte le organizzazioni.

Il primo standard pubblicato, "Internal Control - Integrated Framework", è stato rilasciato nel 1992 e ha fornito un framework completo per aiutare le organizzazioni a valutare e migliorare i propri sistemi di controllo interno. Sebbene tale framework fosse utile per ridurre i rischi rispetto a comportamenti fraudolenti e conformità normativa, non conteneva indicazioni su come identificare e valutare i rischi per i quali attuare i controlli interni.

Nel 2004 COSO ha pubblicato il documento '"Enterprise Risk Management – Integrated Framework". Tale pubblicazione ha ottenuto un'ampia accettazione da parte delle organizzazioni nei loro sforzi per gestire il rischio. L'approccio tenuto nella versione del 2004 era molto legato a ciò che può essere verificato in fase di audit piuttosto che sul rischio all'interno della definizione della strategia.

COSO, in collaborazione con PwC, ha quindi rilasciato nel 2017 il "Enterprise Risk Management – Integrating with Strategy and Performance" per evidenziare l'importanza di considerare il rischio nella definizione della strategia e nel guidare le prestazioni al fine di creare valore. Questo documento non sostituisce il "Internal Control – Integrated Framework", sebbene siano presenti alcune aree di sovrapposizione, la cui ultima versione risale al 2013 e che continua ad essere aggiornato da COSO. I due documenti sono distinti e complementari.

Secondo la visione di COSO, l'ERM non è un processo o un'attività realizzata da una funzione dedicata, ma è diffuso all'interno dell'organizzazione nel suo complesso, in ogni funzione e in ogni processo. In questo modo è possibile gestire efficacemente i rischi che potrebbero compromettere la capacità di raggiungere gli obiettivi in ottica di miglioramento continuo, nella consapevolezza che ogni rischio può essere visto anche come un'opportunità.

7.3.1 Ambito di applicazione

Il framework è rivolto ad organizzazioni di ogni tipologia e dimensione.
Al fine di facilitare l'adozione del framework da parte delle organizzazioni, COSO ha predisposto il documento "ERM - Integrating with Strategy and Performance – Compendium of Examples", che contiene esempi di pratiche adottate da organizzazioni di diverse dimensioni e operanti in diversi settori. COSO continua inoltre a rilasciare guide per l'applicazione dell'ERM ad ambiti e settori specifici. Si prendano come esempi:

- COSO Issues Guidance for Healthcare Providers (2019);
- Enterprise Risk Management for Cloud Computing (2021).

7.3.2 Architettura del framework

Il COSO analizza la strategia da tre diverse prospettive:

- la possibilità che strategie e obiettivi di business siano non allineati con missione, visione e valori;
- le implicazioni della strategia scelta;
- il rischio nell'esecuzione della strategia.

Figura 22 - Schema del COSO[89]

Il framework è organizzato in cinque componenti:

- **Governance & Culture**: questo componente rappresenta la base della definizione degli obiettivi e della gestione dei rischi. La governance definisce il cosiddetto

89 COSO. Enterprise Risk Management: Integrating with Strategy and Performance - Executive Summary. S.l.: COSO, 2017. https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf.

"tono" dell'organizzazione, ovvero l'impostazione dell'organizzazione, e si attua rinforzando l'importanza dell'ERM, definendone gli obiettivi e le modalità di raggiungimento, stabilendo le responsabilità e i sistemi di supervisione. La cultura riguarda i valori etici dell'organizzazione, i comportamenti attesi e la comprensione dei rischi.

- **Strategy and Objective-Setting**: questo componente si concentra sulla definizione della strategia per realizzare la missione dell'organizzazione e generare valore. Viene stabilita la propensione al rischio dell'organizzazione e allineata con la strategia; gli obiettivi mettono in pratica la strategia fungendo da base per identificare, valutare e rispondere al rischio.
- **Performance**: questo componente si concentra sull'identificazione e la valutazione dei rischi che possono avere impatto sul raggiungimento degli obiettivi strategici e di business. Ai rischi viene assegnata una priorità basata sulla gravità nel contesto della propensione al rischio, vengono stabilite le risposte più opportune e ne viene misurata l'efficacia. I risultati di questo processo vengono riportati agli stakeholder.
- **Review and Revision**: i principi di questo componente contemplano il riesame, la valutazione dei cambiamenti in atto e degli eventuali rischi correlati, la verifica delle iniziative avviate nel caso di scostamenti rispetto alle prestazioni attese e le strategie intraprese. L'intero ERM deve essere monitorato, al fine di perseguirne il miglioramento.
- **Information, Communication & Reporting**: deve essere definito un processo di raccolta e condivisione delle informazioni provenienti da fonti interne ed esterne, in modo da permettere all'organizzazione di gestire, per tempo, situazioni che potrebbero ostacolare il raggiungimento degli obiettivi.

I componenti sono a loro volta supportati da 20 principi di base.

Figura 23 - Componenti del COSO e i 20 principi base[90]

90 COSO. Enterprise Risk Management: Integrating with Strategy and Performance - Executive Summary. S.l.: COSO, 2017. https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf.

I cinque componenti, come da grafica, avvolgono e concatenano i passi dello sviluppo e dell'esecuzione della strategia. Tali componenti sono:

- missione, visione e valori fondamentali;
- sviluppo della strategia;
- formulazione di obiettivi;
- implementazione e performance;
- aumento del valore.

Figura 24 - COSO: sviluppo ed esecuzione di una strategia[91]

7.4 NIST Cyber Security Framework

Il Cybersecurity Framework (o CSF) nasce nel 2013 in seguito a un ordine esecutivo del Presidente degli Stati Uniti, nel quale veniva richiesto lo sviluppo di un'architettura per la cybersecurity da adottare su base volontaria, basato sulla gestione del rischio e che fosse "flessibile, ripetibile nell'applicazione, efficiente ed efficace a livello di costo di utilizzo e implementazione". Il CSF fu sviluppato attraverso una cooperazione di piccole e grandi organizzazioni, compresi gli erogatori di servizi per le infrastrutture critiche nazionali statunitensi, con il coordinamento del National Institute of Standards and

91 COSO. Enterprise Risk Management: Integrating with Strategy and Performance - Executive Summary. S.l.: COSO, 2017. https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf.

Technology (NIST).
Il framework offre un approccio flessibile alla gestione della cybersecurity, considerando gli asset fisici, informatici e le persone.

7.4.1 Ambito di applicazione

Pensato inizialmente per le sole infrastrutture critiche, è in realtà applicabile a ogni organizzazione che voglia meglio gestire il rischio di cybersicurezza.

7.4.2 Architettura del framework

La versione attuale è la 1.1 dell'aprile 2018, composta da cinque domini (core functions):

- **Identify** (ID) – Conoscenza relativa ai sistemi, tecnologie, informazioni e le altre risorse e capacità che devono essere protette; definizione delle priorità di intervento in relazione alla strategia e missione dell'organizzazione; definizione dei processi atti a perseguire gli obiettivi definiti per mezzo dell'analisi dei rischi.
- **Protect** (PR) – Sviluppo e attuazione di appropriati presidi al fine di garantire l'erogazione dei servizi.
- **Detect** (DE) – Sviluppo e attuazione di appropriate attività deputate alla rilevazione e identificazione di eventi di sicurezza informatica.
- **Respond** (RS) – Pianificazione, sviluppo e attuazione di appropriate attività di reazione a un evento di sicurezza informatica identificato e rilevato.
- **Recover** (RC) - Sviluppo e attuazione di appropriate attività atte a ripristinare le risorse e capacità che sono state compromesse da un evento di sicurezza informatica.

Fondamentale è il concetto di miglioramento continuo, che il CSF considera come necessario per l'eccellenza e la competitività.

Ogni dominio è suddiviso in categorie (categories), ossia gruppi di attività deputate a specifici e definiti obiettivi di sicurezza informatica, e sotto-categorie, specifiche e dettagliate attività aventi natura tecnica o manageriale.
Ogni sottocategoria a sua volta prevede micro-attività a livello di obiettivo da raggiungere.

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

Figura 25 - NIST CSF: Domini e categorie[92]

7.4.3 Trattamento del rischio nel CSF

La valutazione del rischio nell'ambito del framework è esplicitamente prevista da tre requisiti appartenenti alla categoria "Identify":

92 https://doi.org/10.6028/NIST.CSWP.04162018.

- ID.RA Risk Assessment;
- ID.RM Risk Management;
- ID.SC Supply Chain Risk Management.

In particolare, il requisito ID.RA prevede una procedura di identificazione di

- minacce e vulnerabilità;
- probabilità (likelihood);
- impatto sul business.

Questi elementi permettono di determinare il rischio e stabilire su tale base le azioni di mitigazione.
Il framework lascia ampio spazio di scelta per realizzare l'analisi.
I requisiti nella categoria ID.RM richiedono una chiara definizione dei processi che si occupano della gestione del rischio e delle procedure per determinare la tolleranza al rischio da parte dell'organizzazione, con una chiara condivisione dei risultati dell'analisi e delle decisioni all'interno della stessa.
Il requisito ID.SC richiede la gestione dei rischi derivanti dai legami coi fornitori di prodotti e servizi informatici. Tale requisito è quanto mai appropriato nello scenario attuale, in cui tali legami sono sempre più critici e alla base di eclatanti violazioni come quelle di SolarWinds, Microsoft Exchange e Colonial Pipeline.

7.5 Il Framework nazionale per la cyber security (FNCS)

Il Framework nazionale per la cyber security (FNCS) è stato pubblicato nel 2015 dal Centro di ricerca di cyber intelligence and information security (CIS) dell'Università Sapienza di Roma, e dal Laboratorio nazionale di cybersecurity del Consorzio interuniversitario nazionale per l'informatica (CINI).
Il FNCS, pur riprendendo i concetti fondamentali di minacce cyber e la struttura del CSF del NIST, da cui è stato derivato, si differenzia da esso introducendo strumenti per facilitare la contestualizzazione allo specifico settore di business.

7.5.1 Ambito di applicazione

Il FNCS ha l'obiettivo di fornire a tutte le organizzazioni, andando oltre l'iniziale target delle PMI,un ausilio operativo di gestione del rischio cyber, adattabile alla realtà nazionale e a ogni business.

7.5.2 Architettura del framework

L'architettura del FNCS permette di costruire un modello personalizzato, attraverso le seguenti modalità:

- selezione delle sottocategorie utili per lo specifico tipo di organizzazione (settore, dimensioni, ecc.);
- assegnazione di livelli di priorità, basati su una valutazione del rischio in termini di esposizione alla minaccia, probabilità di accadimento e impatto:
  - **Alta**: interventi che permettono di mitigare in modo sensibile uno dei tre fattori di rischio e sono da attuare a prescindere dalla complessità realizzativa;
  - **Media**: interventi che permettono di mitigare almeno uno dei tre fattori di rischio e che risultano di semplice attuazione;
  - **Bassa**: interventi che permettono di mitigare almeno uno dei tre fattori di rischio e che risultano complessi da realizzare;
- definizione di linee guida di implementazione, almeno per le sottocategorie a priorità alta;
- almeno per le sottocategorie a priorità alta, assegnazione di livelli di maturità che rappresentino uno strumento per identificare gli obiettivi di miglioramento; sulla base della differenza fra livello di maturità corrente e quello desiderato va definito un piano di azione.

Con il rilascio del FNCS 2.0 nel febbraio 2019, oltre all'aggiunta della categoria "Data Protection" che allarga l'ambito di controllo anche alla normativa privacy e al GDPR, viene introdotto il "Prototipo di contestualizzazione".
Si tratta di un'ulteriore modalità di implementazione che permette di definire un modello, da utilizzare nel processo generale di contestualizzazione, in grado di concentrarsi su una specifica normativa o regolamento tecnico. Un prototipo di contestualizzazione si basa sui seguenti elementi:

- per ogni sottocategoria viene definita una classe di implementazione (obbligato-

ria, consigliata, libera);

- per ogni sottocategoria viene definita una priorità di attuazione;
- una guida che descrive il contesto di applicazione del prototipo, i vincoli nella selezione delle sottocategorie e un elenco di controlli relativi alle sottocategorie considerate.

Relativamente alle classi di implementazione (vedere Figura 26):

- le sottocategorie indicate come obbligatorie nel prototipo vengono selezionate nella contestualizzazione;
- le sottocategorie indicate come consigliate nel prototipo vengono valutate in considerazione delle specifiche caratteristiche dell'ambito applicativo previsto per la contestualizzazione;
- gli eventuali ulteriori vincoli sulla selezione delle sottocategorie, documentati nella guida di applicazione del prototipo, devono essere applicati;
- viene indicato, per ogni sottocategoria selezionata a seguito dei precedenti passi, un livello di priorità (preferibilmente pari o superiore a quello indicato nel prototipo, tenendo conto di eventuali vincoli documentati nella guida di applicazione del prototipo);
- gli eventuali controlli di sicurezza documentati nella guida di applicazione del prototipo possono essere integrati nelle linee guida all'applicazione della contestualizzazione.

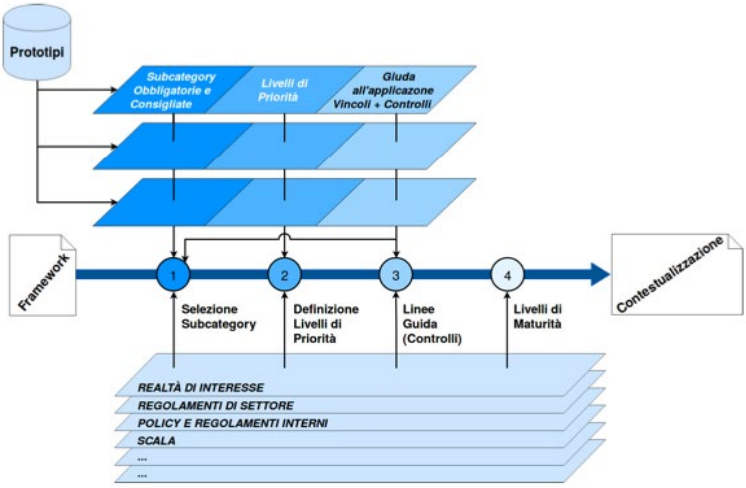

Figura 26 - Contestualizzazione del Framework attraverso l'implementazione di prototipi[93]

93 Framework Nazionale per la Cybersecurity e la Data Protection. S.l.: CIS-Sapienza CINI Cybersecurity National Lab, 2019.

Esempi di prototipi specifici riguardano:

- GDPR e MMS Agid[94];
- Circolare Banca d'Italia N.285 del 17.12.2013;
- FFIEC IT Examination Handbook;
- CPMI IOSCO Guidance;
- PCI DSS;
- PSD2;
- NIS, Reg. di Esecuzione UE 2018/151;
- CAD, DPCM e Regolamenti Collegati.

7.5.3 Esperienza nell'uso del FNCS

I processi di governo della cybersecurity in InfoCert includono il sotto-processo "Security Strategy & Program" (Figura 27), dedicato alla redazione del piano strategico e alla pianificazione del relativo programma di attuazione. Il FNCS è stato selezionato come strumento principale per la sua impostazione.

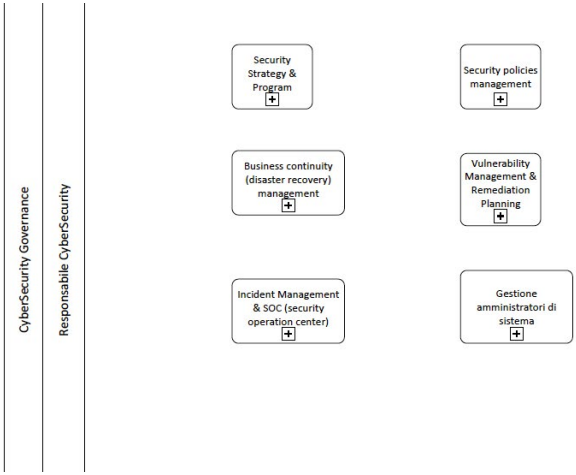

Figura 27 - Processi di governo della cybersecurity in InfoCert[95]

94 Prototipi messi a disposizione direttamente nel sito www.cybersecurityframework.it.

95 Fonte: InfoCert.

Modalità di implementazione del FNCS in InfoCert

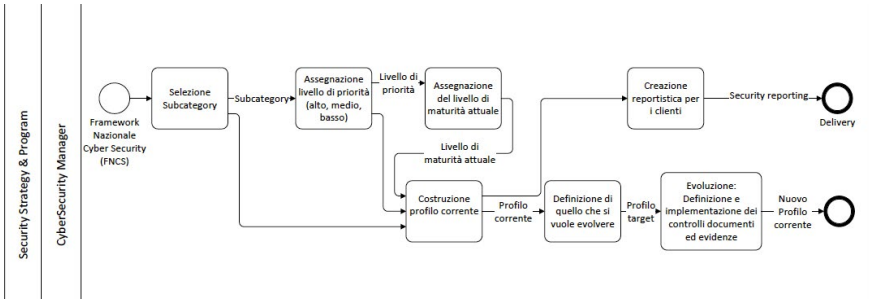

Figura 28 - Sotto-processo Security Strategy & Program[96]

Sfruttando la possibilità di costruire un modello personalizzato, in InfoCert si è definito un modello ad hoc basato sui passi attuativi standard (Figura 28):

- Selezione delle sottocategorie: sono state selezionate le sottocategorie rilevanti per InfoCert; i rischi derivanti dall'erogazione di servizi fiduciari hanno portato all'inclusione della quasi totalità delle sottocategorie.
- Assegnazione dei livelli di priorità alle sottocategorie: per ogni sottocategoria è stato valutato il rischio; da tale valutazione si è potuto assegnare le priorità di implementazione (alta, media e bassa).
- Assegnazione dei livelli di maturità usando una scala a tre valori (M1: bassa, M2: media, M3: alta).

A valle del processo di contestualizzazione, gli ambiti di utilizzo dello strumento sono stati:

- Programma di sicurezza: dall'identificazione dello scostamento fra maturità corrente e maturità attese delle sottocategorie ad alta priorità è stato possibile costruire un programma dei lavori allineato con i principali rischi emersi; a titolo esemplificativo, nel corso della pianificazione 2021, l'analisi in oggetto ha rilevato una maturità non adeguata su tematiche afferenti allo sviluppo sicuro, alla capacità di rilevamento degli incidenti e alla consapevolezza del personale; sono stati pertanto attivate iniziative finalizzate all'introduzione di strumenti di analisi statica di codice nel processo di sviluppo, all'integrazione nell'ambito del SOC di nuove fonti informative e all'attivazione di una campagna di prevenzione dal social engineering, in particolare dal phishing.

96 Figura degli autori.

- Reportistica della sicurezza per i clienti: InfoCert offre servizi critici per i quali deve essere assicurato un livello di sicurezza adeguato a ogni cliente; la completezza dei controlli del FNCS e la possibilità di metterli in relazione con le principali normative e framework, ha permesso di costruire un reporting in grado di fornire evidenze oggettive sul livello di adeguatezza; in termini pratici, per ogni cliente enterprise è stato redatto un insieme documentale costituito dalla lista dei controlli, dal giudizio sintetico di copertura e dal dettaglio delle evidenze a garanzia del giudizio espresso; tale strumento costituisce uno degli elementi fondamentali di qualificazione come "low risk provider".

Intervista ad Antonella Caproni, Coordinatore Team Governance Cybersecurity, Banca Monte dei Paschi di Siena.

D. Perché MPS ha deciso di applicare il Framework Nazionale per la CyberSecurity e la Data Protection, a che bisogno rispondeva e tra quali altri framework è stato scelto e perché?

R. Il Gruppo Montepaschi ha, tra gli obiettivi del proprio Piano Strategico per la Sicurezza Logica, l'adozione di un cybersecurity framework quale strumento di governo e miglioramento continuo. Si tratta di un modello interno di misurazione del grado di maturità della sicurezza, utile ad individuare gli ambiti di miglioramento e orientare, di conseguenza, gli investimenti in maniera coerente alle reali esigenze.

A tal proposito, ci siamo interessati subito al Framework Nazionale per la Cybersecurity e la Data Protection, presentato nel 2015. Dal 2019 BMPS collabora con il CIS – La Sapienza ed altri attori del contesto economico e finanziario con il risultato di aver adattato il Framework Nazionale per la Cybersecurity alle esigenze del comparto bancario creando un Modello customizzato alla realtà BMPS. Le recenti linee guida nazionali per gli Operatori Essenziali sottoposti alla Direttiva NIS fanno riferimento proprio a tale Framework confermando, quindi, la coerenza del percorso di BMPS.

D. E' stata un'esperienza positiva e quali sono le lezioni apprese? Come bisogna organizzarsi per avere successo nell'implementazione e quanto lavoro deve essere svolto per farlo? Ci sono dei consigli che vi sentite di dare alle organizzazioni che iniziano adesso ad utilizzarlo?

R. L'applicazione del Framework in BMPS è stata un'esperienza positiva e onerosa in termini di risorse. Per questo stiamo lavorando a un miglioramento del processo. Oggi siamo all'automazione delle fasi di gestione delle evoluzioni del Framework, per sua natura oggetto di evoluzioni gestite dall'organizzazione che lo adotta. Inoltre, stiamo ottimizzando il processo di assessment attraverso la realizzazione di una piattaforma unica per la gestione dei questionari di valutazione, della raccolta delle informazioni e delle evidenze a supporto. In questo

modo è possibile ottenere rapidamente anche report di rendicontazione.

Il Framework ha successo se ha un forte commitment aziendale, ed è necessaria anche una forte condivisione interna e unitarietà di intenti con le Funzioni di Controllo Aziendali.

D. Quali sono i vantaggi derivanti dall'adozione del Framework e quali sono gli sviluppi futuri previsti?

R. Per gestire la cybersecurity è utile dotarsi di uno strumento interno certificato che consegna autonomia alle strutture interne anche per la valutazione dei risultati e la gestione dei razionali sottostanti. Occorre occuparsi di uno svariato numero di aspetti e, contemporaneamente, mantenere un quadro d'insieme per un corretto governo della sicurezza, mentre fuori e dentro tutto cambia. Il Framework è una bussola che orienta strategie di gestione del rischio cyber. Assomma uno strumento strategico-operativo a uno di controllo e di compliance normativo.

Ci auguriamo che il modello adottato da noi venga utilizzato anche da altri, siamo convinti che mettere a fattor comune il lavoro svolto sia un'opportunità per il rafforzamento della cyber-capability del "sistema Paese". Infatti, all'interno del sistema bancario-assicurativo domestico esistono disomogeneità nell'approccio strategico-operativo, di gestione e controllo della cyber-security superabili attraverso l'adozione di questo strumento comune che definisce profili di sicurezza "target", condivisi con gli altri operatori della realtà finanziaria e delinea una metrica di valutazione rispetto agli obiettivi, fornendo così un benchmark comune di riferimento.

7.6 I CIS controls (CCSC)

I "CIS Critical Security Controls for Effective Cyber Defense" (CCSC), oggi alla versione 8, furono sviluppati per la prima volta all'inizio del 2008. Attualmente sono pubblicati dal Center for Internet Security (CIS)[97].

Inizialmente pubblicati dal SANS Institute nel 2009, i controlli CIS sono stati razionalizzati all'interno di un consorzio formato da organizzazioni del settore pubblico e privato.

Dalla loro pubblicazione iniziale, la proprietà dei controlli è stata trasferita prima al Consiglio per la sicurezza informatica (CCS) nel 2013, e infine al CIS nel 2015.

97 https://www.cisecurity.org/controls/.

7.6.1 Ambito di applicazione

I controlli di sicurezza proposti sono prioritari per proteggere aziende e entità governative in primo luogo contro gli attacchi comuni e più frequenti.

7.6.2 Architettura del framework

La versione 7 aveva introdotto una prioritizzazione dei controlli attraverso il concetto di Implementation Group (IG), pensato primariamente per fornire supporto alle realtà più piccole che, per la limitatezza delle risorse, avrebbero difficoltà a implementare tutti i controlli.

Le priorità sono state derivate dall'identificazione dei controlli maggiormente efficaci nel contrastare i pattern di attacco più frequenti riportati dal Verizon Data Breach Investigation Report e dal Multi-State Information Sharing and Analysis Center® (MS-ISAC®).

I tre Implementation Group sono insiemi di controlli via via più estesi, fino a comprendere tutti i controlli nell'IG3. L'IG1, quello più semplice, è l'insieme di controlli essenziali e utile a garantire un livello minimo di sicurezza da garantire in ogni organizzazione.

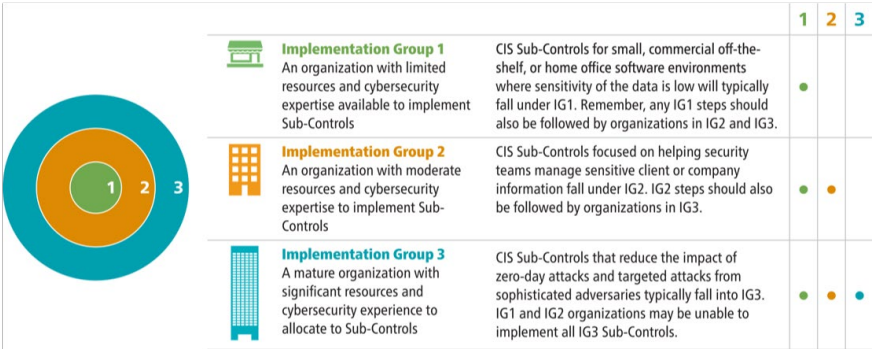

Figura 29 - Gli Implementation Group dei CIS controls[98]

98 https://www.cisecurity.org/case-study/school-district-enhances-cyber-hygiene-with-cis-controls/.

Nella corrente versione 8 i controlli totali sono organizzati in 18 categorie tematiche (un'azione di consolidamento ha ridotto le categorie rispetto alle 20 della versione precedente e i controlli da 171 a 153). Esse coprono sia le operazioni più basilari (per esempio, "Inventory and Control of Enterprise Assets", "Inventory and Control of Software Assets", "Account Management") sia quelle più avanzate relative alla sicurezza applicativa o alla risposta agli incidenti ("Application Software Security", "Incident Response Management") tipicamente applicate dalle organizzazioni più grandi e strutturate.

Vengono introdotte raccomandazioni relative a "Cloud-based computing", "Mobile environments" e "Changing attacker tactics". La versione 8 combina e consolida i controlli in termini di "activities", piuttosto che in relazione a chi gestisce i dispositivi.

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
9.1	**Ensure Use of Only Fully Supported Browsers and Email Clients** Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	Applications	Protect	●	●	●
9.2	**Use DNS Filtering Services** Use DNS filtering services on all enterprise assets to block access to known malicious domains.	Network	Protect	●	●	●
9.3	**Maintain and Enforce Network-Based URL Filters** Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.	Network	Protect		●	●
9.4	**Restrict Unnecessary or Unauthorized Browser and Email Client Extensions** Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.	Applications	Protect		●	●

Figura 30 - Esempio di controlli del CIS[99]

L'integrazione con il NIST CSF è evidente per l'indicazione, in corrispondenza di ciascun controllo, della pertinente *core function* del CSF.

99 https://www.cisecurity.org/controls/v8/#learn-about-v8

7.7 ENISA - Guideline on security measures under the EECC

Nel 2009 la riforma del quadro legislativo per le comunicazioni elettroniche dell'Unione europea ha introdotto gli articoli 13a e 13b nella Direttiva 2009/140/EC (Framework Directive). L'articolo 13a impone agli Stati membri di assicurarsi che i fornitori di comunicazioni elettroniche siano in grado di gestire opportunamente i rischi per la cyber security e adottino misure di sicurezza adeguate a garantire la sicurezza e l'integrità di reti e servizi. Stabilisce inoltre per i fornitori l'obbligatorietà di notifica di tutti gli incidenti di sicurezza significativi alle autorità nazionali competenti, le quali, a loro volta, devono riferire annualmente in merito a tali incidenti all'ENISA e alla Commissione europea (CE). L'articolo 13b descrive il modo in cui le autorità possono vigilare e far rispettare tali requisiti di sicurezza.

Nel 2010, l'ENISA, la Commissione europea e gli esperti dei ministeri e delle autorità di regolamentazione delle telecomunicazioni degli Stati membri dell'UE hanno costituito l'"Article 13a Expert Group". L'Expert Group ha raggiunto un consenso su due orientamenti tecnici non vincolanti per l'attuazione dell'articolo 13a e cioè la "Technical Guideline on Incident Reporting" e la "Technical Guideline on Security Measures".

Nel dicembre 2018 è stata adottata una nuova serie di regole per le telecomunicazioni denominata "European Electronic Communications Code", abbreviata in EECC. Esse aprono la strada all'introduzione di reti in fibra ottica ad altissima capacità e a reti mobili di prossima generazione (5G) che favoriscono l'Internet of Things (Iot) e nuovi modelli di business. L'articolo 40 dell'EECC, che sostituisce l'articolo 13a, contiene requisiti di sicurezza dettagliati per i fornitori di comunicazioni elettroniche. L'articolo 41 dell'EECC, che sostituisce l'articolo 13b, illustra come l'autorità competente può far rispettare tali requisiti di sicurezza.

Sebbene i requisiti di sicurezza previsti dall'EECC siano simili a quelli previsti dalla Framework Directive, esistono importanti differenze.

L'Article 13a Expert Group ha cambiato nome in ECASEC (European competent authorities for secure electronic communications). Il documento "Guideline on security

measures under the EECC" dell'ENISA[100], ora alla quarta edizione, fornisce alle autorità competenti gli orientamenti e i dettagli tecnici relativi all'attuazione degli articoli 40 e 41 dell'EECC. In particolare il documento si concentra sulle modalità con cui i fornitori devono valutare i rischi di sicurezza e adottare adeguate contromisure utili a ridimensionare i livelli di rischio rilevati.

7.7.1 Ambito di applicazione

L'EECC si applica ai fornitori di comunicazioni elettroniche.

7.7.2 Architettura del framework

La linea guida è strutturata in 29 obiettivi di sicurezza di alto livello, raggruppati in 8 domini. Per ogni obiettivo sono elencate specifiche misure di sicurezza dettagliate che potrebbero essere adottate dai fornitori per raggiungere l'obiettivo di sicurezza. Queste misure di sicurezza sono raggruppate in 3 livelli di crescente sofisticazione.
Le misure di sicurezza contenute nella linea guida sono neutre sotto il profilo tecnologico. ENISA sta sviluppando linee guida supplementari più dettagliate per reti e tecnologie specifiche come, ad esempio, la linea guida già pubblicata sul 5G[101].
L'allegato 6 "Mapping to International Standards" contiene un riferimento a standard ISO di sicurezza e in particolare a ISO/IEC 27001 e ISO/IEC 27002.

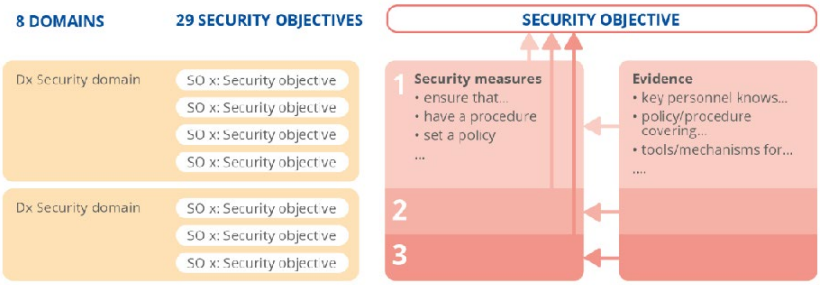

Figura 31 - Struttura generale della Guideline on security measure[102]

100 https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc.

101 https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc.

102 https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc

L'ambito di applicazione delle misure di sicurezza definite è costituito da tutti gli asset del provider (compresi gli asset di terze parti) che, se compromessi o in errore, possono avere un impatto negativo sulla sicurezza delle reti e dei servizi. Né gli obiettivi di sicurezza di alto livello né le misure di sicurezza dettagliate sono raccomandazioni vincolanti; per definizione i rischi sono diversi e molto legati ai vari contesti di riferimento.
È compito dei singoli fornitori l'esecuzione di analisi per determinare quali risorse rientrano nell'ambito di applicazione, così come quello di valutare il rischio per determinare quali sono le misure di sicurezza appropriate. Siccome i rischi evolvono nel tempo, la loro valutazione deve essere sempre aggiornata per affrontare i cambiamenti e gli incidenti gestiti.
La guida non indica una metodologia di valutazione del rischio da utilizzare, che quindi può essere scelta a discrezione del fornitore, ma indica che il focus, in accordo con l'articolo 40 dell'EECC, debba essere sui rischi per gli utenti che si affidano alle reti e ai servizi di comunicazione forniti dal fornitore, e non sui rischi per il fornitore.

7.8 Misure minime di sicurezza di AgID

Nel 2015, AgID pubblicò il documento "Misure minime di sicurezza ICT per le pubbliche amministrazioni". Esso contiene controlli, indicati come AgID Basic Security Control(s) (ABSC), e reputati indispensabili per assicurare il minimo livello di protezione nella maggior parte delle situazioni.
Per identificare gli ABSC si è partiti dalla versione 6 dei CCSC (paragrafo 7.6), anche se l'insieme dei controlli definiti è più simile alla versione 5.1.
Le misure minime:

- forniscono un riferimento operativo direttamente utilizzabile (checklist);
- stabiliscono una base comune di misure tecniche;
- forniscono uno strumento per verificare lo stato di protezione e poter tracciare un percorso di miglioramento;
- responsabilizzano le Amministrazioni sulla necessità di migliorare e mantenere adeguato il proprio livello di sicurezza.

7.8.1 Ambito di applicazione

Le Misure minime di sicurezza ICT (MMS) rappresentano le misure di sicurezza che le PA centrali e periferiche devono adottare al fine di dimostrare, in caso di incidenti, di avere adottato misure atte a fornire almeno un minimo livello di sicurezza. Consistono in controlli tecnologici, organizzativi e procedurali.
Le MMS, pur essendo il punto di riferimento per tutte le PA, offrono un supporto metodologico soprattutto per le PA più piccole, che hanno meno possibilità di avvalersi di professionalità specifiche.

7.8.2 Architettura del framework

Le prime 5 classi di controlli seguono l'ordine dei CCSC e sono i seguenti:

Primi 5 controlli di ABSC (CCSC) per una protezione di base	
ABSC 1 (CSC 1)	Inventario dei dispositivi HW autorizzati e non autorizzati
ABSC 2 (CSC 2)	Inventario dei SW autorizzati e non autorizzati
ABSC 3 (CSC 3)	Proteggere le configurazioni di HW e SW sui dispositivi mobili, laptop, workstation e server
ABSC 4 (CSC 4)	Valutazione e correzione continua della vulnerabilità
ABSC 5 (CSC 5)	Uso appropriato dei privilegi di amministratore

Fra le misure minime è previsto che le PA accedano a servizi di allarme (*early warning*) per rimanere aggiornate sulle nuove vulnerabilità di sicurezza. A tal proposito lo CSIRT[103] fornisce servizi informativi a tutte le amministrazioni accreditate.

103 https://csirt.gov.it/.

Oltre ai citati 5 controlli ve ne sono di ulteriori aggiunti da AgID:

Ulteriori 3 controlli aggiunti da AgID	
ABSC 8 (CSC 8)	Difese contro i malware
ABSC 10 (CSC 10)	Copie di sicurezza
ABSC 13 (CSC 13)	Protezione dei dati

Ogni controllo dei CSC prevede un livello più granulare costituito da famiglie di misure di dettaglio più fine. AgID ha previsto un terzo livello, le sottocategorie, similmente al FNSC (paragrafo 7.5).
Ogni ABSC è quindi contraddistinto da tre numeri che rappresentano, nell'ordine, la classe, la famiglia e la sottocategoria. Nella tabella seguente è fornito un esempio di controllo.

ABSC_ID#			Descrizione	FNSC	Liv. Attuazione		
Classe	Famiglia	Subcat.		Subcat FNSC	Min.	Std.	Alto
1	1	2	Implementare ABSC 1.1.1 attraverso uno strumento automatico	ID.AM-1		x	x

È opportuno notare che, a seconda della complessità del sistema informativo a cui si riferiscono e della realtà organizzativa dell'Amministrazione, le misure minime possono essere attuate in modo graduale seguendo tre livelli crescenti:

- **Minimo**: è il livello sotto il quale nessuna PA, indipendentemente dalla sua natura e dimensione, può scendere e i controlli in essa indicati sono obbligatori:
- **Standard**: è il livello che ogni amministrazione della PA dovrebbe assumere come base di riferimento nella maggior parte dei casi;
- **Avanzato**: può essere considerato come l'obiettivo al quale devono tendere tutte le PA a cominciare da quelle maggiormente esposte ai rischi.

Sembrerebbe che l'attuazione pratica delle MMS sia avulsa da un'analisi del rischio. In realtà non è così e infatti numerose sottocategorie dell'ABSC 4 richiamano esplicitamente l'analisi del rischio. Sul sito istituzionale[104] viene fatta esplicito riferimento agli standard ISO 31000 e ISO/IEC 27005.

7.8.3 Eventuali evoluzioni

L'Agenzia per la Cybersicurezza Nazionale è stata istituita a giugno 2021, assumendo le funzioni in materia di cybersicurezza precedentemente attribuite ad AgID. È ipotizzabile che possa procedere all'aggiornamento delle MMS.

7.8.4 Esperienza nell'uso delle MMS AgID

Gli atenei, pur caratterizzati da ambienti fortemente complessi ed eterogenei, da un lato non gestiscono direttamente tutte le risorse attivabili in rete, dall'altro adottano un paradigma di accesso alla rete incentrato sull'approvazione dell'utente e non del dispositivo. Pertanto, nella prima metà del 2017 il Gruppo di lavoro del CODAU "Misure minime ICT per le PA" interpellò l'AgID, ottenendo alcuni chiarimenti in merito al perimetro da considerare per l'applicazione delle MMS e alle responsabilità connesse all'applicazione delle misure stesse.

Relativamente al perimetro, AgID chiarì che "non è definito in termini assoluti; è infatti necessaria un'analisi della specifica realtà in esame che consideri le sue peculiarità e il contesto di riferimento nel quale è inserita per individuare una partizione [...] dei sistemi e della rete", specificando inoltre che "in tale stratificazione la parte centrale («core») costituisce la zona di massima criticità, per la quale va assolutamente garantito il rispetto di tutte le misure di sicurezza necessarie per impedirne la compromissione".

Relativamente alla complessità dell'articolazione organizzativa degli atenei, AgID chiarì che "in essi sono tipicamente presenti strutture dotate di ampia autonomia, che si estende anche alla definizione, implementazione ed erogazione di servizi", quindi "la responsabilità di applicazione delle misure minime va, per tali strutture, ascritta al responsabile della struttura stessa". Inoltre, sempre secondo l'Agenzia, nel caso in cui l'utilizzo di dispositivi e postazioni sia sotto il completo controllo e responsabilità dei

104 https://www.sicurezzait.gov.it/cyber/gestioneRischio.html.

singoli utenti (situazione molto diffusa nell'ambito dei gruppi di ricerca) la responsabilità dell'attuazione delle misure minime potrebbe essere direttamente dei singoli utenti.

"Dunque, in ambito accademico il modello proposto è quello di una piramide di responsabilità in cui le misure minime ICT per la PA sono sì applicate globalmente dall'Amministrazione, ma in modo da lasciare la possibilità che per suoi specifici sottodomini si utilizzino differenti insiemi di controlli, a cura del responsabile dello specifico sottodominio".

Per quanto concerne l'applicazione delle MMS presso l'Università di Camerino[105], l'ateneo optò per la loro integrazione all'interno del sistema di gestione della sicurezza delle informazioni (SGSI), certificato ISO/IEC 27001 dal 2012. Il 29 settembre 2017 l'ateneo costituì un gruppo di lavoro per l'applicazione delle MMS, coordinato dal referente per il SGSI, conferendogli l'incarico di svolgere le attività tecniche necessarie, per poi proporre alla Direzione generale gli interventi adeguativi, nonché per attuarli appena approvati dalla Governance di ateneo. Ulteriore compito del gruppo era quello di produrre tutta la documentazione di supporto.

Considerando la scadenza del 31 dicembre 2017 e quindi le tempistiche fortemente ristrette, il gruppo si riunì più volte, dapprima per individuare in via preliminare gli interventi, e poi per definire le tempistiche di massima delle singole attività e assegnarle al personale coinvolto in ciascuna di esse.

Entro il termine del 31/12/2017 il gruppo completò l'implementazione di tutte le soluzioni tecnico-organizzative individuate e compilò il documento "Modulo di implementazione delle misure minime ICT" in modo da avere una sorta di indice con rimandi ai differenti documenti del SGSI. Proprio nella compilazione di questo documento si è materialmente realizzata l'integrazione tra SGSI e MMS.

ABSC_ID#			Descrizione	Modalità di implementazione	Livello
13	8	1	Bloccare il traffico da e verso url presenti in una blacklist.	L'Ateneo blocca tutto il traffico diretto verso URL incluse in un'apposita blacklist. Il dettaglio di tale implementazione è descritto nel documento del SGSI denominato "PT - 68 - URL Filtering".	M

Figura 32 - Esempio di compilazione del modulo di implementazione delle misure minime ICT per la PA

105 F. Ciclosi, G.P. Gentili, G. Rappi, e A. Belfiore, The risk analysis as a unified approach to satisfy GDPR, NIS Directive and ISO 27001 requirements. EUNIS 2018 Congress - Book of Proceedings. 2018, pagg. 49-60.

Per quanto concerne l'implementazione pratica dei controlli, l'ateneo scelse di non limitarsi all'implementazione dei soli controlli minimi, attuando tutti quelli di tipo standard (tranne uno) e tre di tipo alto.
La richiamata integrazione con il SGSI ha fatto sì che venissero modificate 11 procedure tecniche esistenti e aggiunte altre 7 procedure tecniche.

7.9 COBIT® 2019 e RiskIT di ISACA

L'acronimo COBIT significava originariamente "Control Objectives for Information and Related Technologies", ponendo l'attenzione dei lettori sul termine "Control", che letteralmente significa "governo", "verifica".
ISACA rilasciò per la prima volta COBIT nel 1996, originariamente come insieme di obiettivi di controllo per aiutare gli auditor finanziari a muoversi meglio negli ambienti legati all'IT.
Rendendosi immediatamente conto del valore del framework oltre il solo ambito dell'auditing, ISACA rilasciò una versione più ampia (la 2) nel 1998 e lo ampliò ulteriormente, aggiungendo le linee guida, nella versione 3 del 2000.
Con le versioni 4 e 4.1, rispettivamente nel 2005 e 2007, ISACA aggiunse framework correlati:

- Val IT per i processi e le responsabilità relativi all'IT nella creazione di valore;
- Risk IT per la gestione del rischio, la cui prima versione è del 2009 e che fornisce una visione dei rischi relativi all'IT e dei controlli di sicurezza, dal vertice alle attività operative.

COBIT 5 del 2012 si basa sui framework COBIT 4.1, Val IT 2.0, Risk IT, sull'IT Assurance Framework (ITAF) di ISACA e sul Business Model for Information Security (BMIS).
L'ultima versione, COBIT® 2019, è stata rilasciata nel 2018 e include nuovi approfondimenti.
COBIT® 2019 costituisce anche la base per gli audit dell'IT, come le precedenti versioni. Per questo utilizzo, ISACA fornisce una serie di Assurance Guides per ambiti specifici dell'ICT, evidenziando i rischi specifici per ciascun ambito e i riferimenti ai processi di COBIT® 2019.

7.9.1 Ambito di applicazione

L'ambito di applicazione del COBIT® 2019 è l'*enterprise governance of information and technology* (EGIT).

7.9.2 Architettura del framework

Il framework RiskIT si basa sui principi degli altri standard e framework riconosciuti a livello internazionale quali COSO ERM, AS/NZS 43603 e ISO 31000; tuttavia, la terminologia utilizzata in Risk IT può talvolta differire da quella utilizzata in altri standard.
Il rischio IT è quello associato all'uso, alla proprietà, al funzionamento, al coinvolgimento, all'influenza e all'adozione dell'IT. Il rischio IT può essere classificato in diverse categorie:

- IT benefit/value enablement risk: associato all'opportunità di utilizzare la tecnologia per migliorare l'efficacia e l'efficienza dei processi o per abilitare nuove iniziative;
- IT programme and project delivery risk: associato al contributo dell'IT a nuove o migliori soluzioni, normalmente nella forma di progetti e programmi e al portafoglio di investimenti;
- IT operations and services delivery risk: associato alle prestazioni dei sistemi e dei servizi IT che possono portare a un'interruzione o a un degrado del valore dell'organizzazione.

RiskIT si basa su principi guida per una gestione efficace del rischio IT. I principi si basano su concetti di ERM comunemente accettati, applicati al settore dell'IT. Tali principi sono:

- stretta connessione agli obiettivi di business;
- allineamento della gestione dei rischi IT con l'ERM complessiva (se applicabile);
- bilanciamento di costi e benefici della gestione del rischio;
- promozione di una comunicazione equa e aperta del rischio IT;
- approccio che parte dai vertici con l'attribuzione delle responsabilità personali;
- processo continuo e integrato nelle attività quotidiane.

7.9.3 Eventuali evoluzioni

Cobit è un framework in continua evoluzione ed è già al lavoro un nuovo gruppo di lavoro per adeguarlo al mondo IT in continua evoluzione.

7.10 IEC 62443-3-2

La IEC 62443-3-2[106] "Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design" è una norma che specifica la modalità di analisi e gestione dei rischi per il mondo OT industriale. La sua ultima edizione è del 2020 ed è una parte della IEC 62443, inizialmente sviluppata come ISA99.

Agli inizi degli anni Duemila si costituì, con il nome di ISA99, il comitato per la sicurezza dei sistemi di automazione e controllo industriale di ISA che riunisce esperti di sicurezza informatica industriale di tutto il mondo. La serie di standard ISA99 si sviluppò quindi per la sicurezza dei sistemi di automazione e controllo industriale (IACS), anche a causa dei primi incidenti e attacchi di un certo rilievo.

I documenti, originariamente indicati come standard ANSI/ISA-99 o ISA99, sono stati successivamente rinumerati come serie ANSI/ISA-62443 nel 2010. Il contenuto di questa serie è stato poi recepito come standard internazionale.
Lo standard IEC 62443 fa riferimento, oltre che alla sicurezza delle informazioni, anche agli aspetti di salute e sicurezza delle persone e ambientali, inoltre viene data molta importanza alla disponibilità e all'integrità dei sistemi.

7.10.1 Ambito di applicazione

Anche se IEC 62443 è stato inizialmente sviluppato per il settore dei processi industriali, i campi di applicazione sono in continua espansione (grazie anche alla pervasività dei sistemi IACS) in sempre nuovi settori come la generazione e la distribuzione dell'energia, i trasporti e, più in generale, in tutte le infrastrutture critiche.
Gli IACS includono:

106 https://webstore.iec.ch/publication/30727.

- sistemi hardware e software come DCS, PLC, SCADA, rilevamento elettronico in rete e sistemi di monitoraggio e diagnostica;
- interfacce usate per fornire controllo, sicurezza fisica e operazioni di produzione con connessione interna, verso gli operatori, il network o le macchine, operazioni di produzione e assemblaggio con funzionalità continue, a batch, discrete o altre tipologie di processo.

Gran parte del successo dello standard è dovuto al fatto che i tradizionali standard IT non sono appropriati per gli IACS. Gli IACS, infatti, hanno requisiti prestazionali e di disponibilità diversi dagli abituali sistemi informatici (con richiesta di maggiore affidabilità, spesso senza possibilità di fermi manutentivi) nonché un ciclo di vita estremamente più lungo. Inoltre, gli attacchi a certi IACS possono avere ricadute ambientali o minacciare la salute pubblica e la vita delle persone.

La norma IEC 62443 riguarda non solo la tecnologia dei sistemi di controllo, ma anche i processi di lavoro, le contromisure e la gestione delle risorse umane.

7.10.2 Architettura del framework

La serie di norme IEC 62443 è organizzata in quattro parti:

- Generale, che tratta argomenti comuni a tutta la serie:
  - 1-1 (TS): terminologia, concetti e modelli;
- Politiche e procedure, si concentra su metodi e processi associati alla sicurezza IACS:
  - 2-1: definizione di un programma di sicurezza per IACS;
  - 2-3 (TR): gestione delle patch in ambiente IACS;
  - 2-4: requisiti del programma di sicurezza per i fornitori di servizi IACS;
- Sistema, che riguarda i requisiti a livello di sistema:
  - 3-1 (del 2009): Tecnologie di sicurezza per IACS;
  - 3-2: valutazione del rischio di sicurezza per la progettazione del sistema;
  - 3-3: requisiti di sicurezza per i sistemi e livelli di sicurezza;
- Componenti e requisiti, che fornisce requisiti dettagliati per i prodotti IACS:
  - 4-1: requisiti del ciclo di vita dello sviluppo prodotto sicuro;
  - 4-2: requisiti tecnici di sicurezza per i componenti IACS.

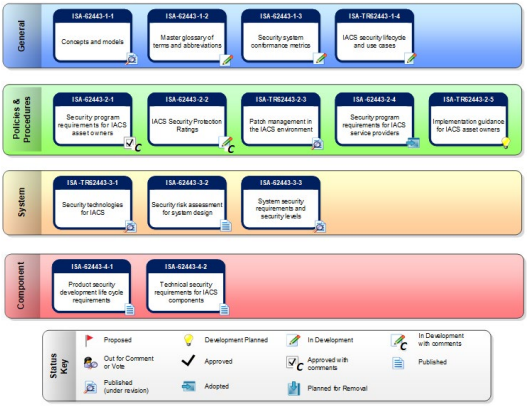

Figura 33 - Architettura del Framework e configurazione attuale[107]

Esse prevedono la realizzazione di un sistema di gestione della cybersecurity denominato CSMS (*cyber security management system*), similmente alla ISO/IEC 27001, come mostrato nella figura sottostante.

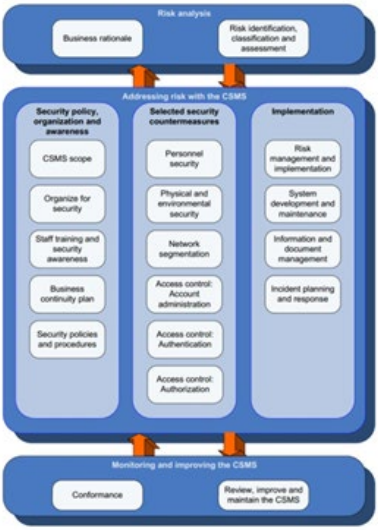

Figura 34 - Cyber security management system (CSMS)[108]

107 ISO/IEC JTC 1/SC 27/WG 4 N 4874 "Liaison Officer's Report on IEC TC65 WG10 and ISA99 Activities 2021-04".

108 IEC 62443-2-1:2010 Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program. Svizzera: IEC, 2010

La IEC 62443 adotta un approccio alla sicurezza informatica basato sul rischio. Questo si evidenzia in tutte le parti dello standard (generale, per i sistemi e per le componenti). Lo standard sottolinea l'importanza di mitigare il rischio della propagazione di un incidente o un attacco informatico attraverso la segmentazione e la segregazione degli impianti e delle reti in zone e conduit con difese specifiche.

7.10.3 Eventuali evoluzioni

Lo standard non ha ancora raggiunto una configurazione stabile. Per esempio alcune sue parti (come la 2-2) non sono ancora state pubblicate, mentre altre sono in discussione per aggiornamento.

7.11 GAMP 5 e la validazione dei sistemi informatici GxP

GAMP5 ("A Risk-Based Approach to Compliant GxP Computerized Systems") è una linea guida rilasciata dall'ISPE (International Society for Pharmaceutical Engineering, associazione no-profit che realizza le linee guida per implementare le Regulation dell'FDA americana) a febbraio 2018. Rappresenta lo strumento più recente e aggiornato nell'approccio alla convalida dei sistemi informatici GxP nell'ambito farmaceutico[109].
GxP è un'abbreviazione per "buona pratica" e la "x" identifica un particolare settore, per esempio clinico (GCP), fabbricazione (GMP) e laboratorio (GLP).
Il primo prodotto dell'organizzazione fu una Guida per i fornitori rilasciata ai membri il 1° marzo 1994 e pubblicata un anno dopo. Man mano che le aspettative continuavano ad evolversi, anche la guida veniva sviluppata, con le pubblicazioni di GAMP 2 nel 1996, GAMP 3 nel 1998, GAMP 4 nel 2001 e GAMP 5 nel 2008.
Negli anni, ulteriori guide (GPG, Good practice guidelines) hanno accompagnato le GAMP, estendendole a un'ampia varietà di sistemi informatici.
GAMP 5 ha dimostrato come la gestione del rischio di qualità può essere completamente integrata nel ciclo di vita del sistema informatico.

109 Pier Luigi Agazzi. GAMP 5 - Come assicurare la conformità delle soluzioni industry 4.0 ai requisiti delle GMP. Novembre 2018. https://www.adeodata.eu/GAMP-5-Medical-Devices-0d14df00.

7.11.1 Ambito di applicazione

GAMP5 fornisce una guida pratica specifica per il settore farmaceutico per ottenere sistemi informatici conformi GxP.
Oggi le buone pratiche GAMP sono utilizzate a livello globale dalle società regolamentate e dai loro fornitori e sono ampiamente supportate dalle agenzie di regolamentazione (evidenziate da alcune norme e in diversi documenti di orientamento normativo).

7.11.2 Architettura del framework

Le linee guida GAMP sono utili per allineare le attività di convalida dei sistemi informatici tra i produttori, gli enti regolatori e i fornitori di sistemi. Il documento è strutturato in due parti principali, la prima fornisce una presentazione dei concetti fondamentali per la convalida: il ciclo di vita del software, le categorie del software (e dell'hardware) e l'analisi del rischio.Nella seconda parte (Appendici) vengono riportate numerose indicazioni per la redazione dei documenti e costituiscono un prezioso ausilio nella convalida di questi sistemi. L'assunzione di base di GAMP 5 è che il rigore delle attività di convalida è commisurato alla criticità delle funzioni di un sistema, mediante l'approccio all'analisi dei rischi in 5 passi come illustrato in Figura 35.

Figura 35 - I cinque passi per la gestione del rischio[110]

110 GAMP® 5 Guide: A Risk-Based Approach to Compliant GxP Computerized Systems. USA: ISPE, 2008.

- **Passo 1** - Valutazione iniziale per comprendere a fondo il tipo di processo da valutare.
- **Passo 2** – Identificazione delle funzioni con impatto sulla salute del paziente, la qualità del prodotto e l'integrità dei dati. La scomposizione del processo ha il vantaggio di ridurre la complessità delle analisi.
- **Passo 3** – Valutare il rischio e identificare i controlli. Partendo da ogni funzione si procede a un'analisi di potenziali danni derivanti da eventi avversi e quali controlli devono essere introdotti per mitigare i rischi. Si parte sfruttando lo schema mostrato in Figura 35, derivato da FMEA (Failure mode and effect analysis). Le formule sono usate su fogli di calcolo. ISO 14971 e ICH Q9 sono gli approcci raccomandati per la gestione del rischio relativo alla qualità.

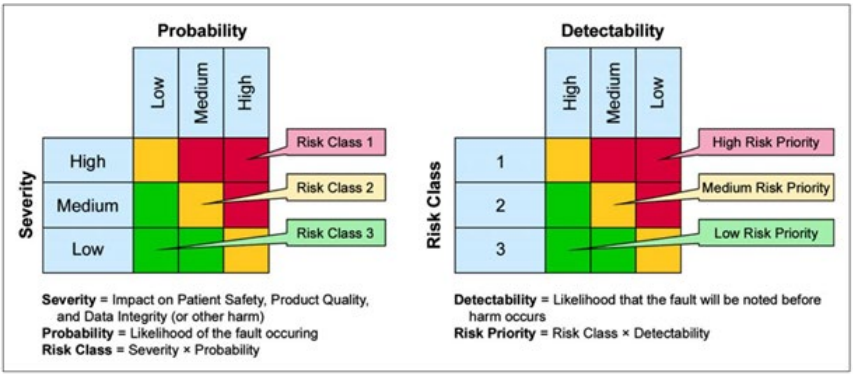

Figura 36 - Metodo per la valutazione del rischio[111]

- **Passo 4** – Identificare, realizzare e verificare i controlli sulla base del livello di rischio. Successivamente si procede a una valutazione del rischio residuo. Questa valutazione deve accertare se, a seguito dell'applicazione dei controlli selezionati, i rischi sono realmente mitigati.
- **Passo 5** – Monitorare i controlli. Il rischio residuo deve essere nuovamente valutato per accertare se i controlli sono adeguati, se sono presenti rischi precedentemente non riconosciuti e se il nuovo livello di rischio è accettabile. Se i controlli sono troppo rigorosi, potrebbe essere suggerito un approccio più efficiente. La valutazione periodica porterà a un miglioramento dei processi, dei controlli e della strategia di rischio complessiva.

111 GAMP® 5 Guide: A Risk-Based Approach to Compliant GxP Computerized Systems. USA: ISPE, 2008.

7.11.3 Eventuali evoluzioni

L'evoluzione di GAMP è orientata ad affrontare le sfide del settore della convalida dei sistemi informatici, compresi i concetti di "Case for Quality" (per l'identificazione, da parte di FDA, dei produttori di dispositivi), il "CSA" e i nuovi requisiti Pharma 4.0 (guida di ISPE per introdurre i concetti di industria 4.0.

7.12 Altri approcci

Oltre a quelli illustrati nei paragrafi precedenti, segnaliamo i seguenti:

#	Riferimento	Breve descrizione
1	ENISA Cloud Computing Risk Assessment[112] (2009)	E' il technical report di un gruppo di lavoro ENISA che illustra alcuni dei rischi presenti nel cloud computing.
2	ENISA RM/RA[113]	È una panoramica dei contenuti rilevanti trovati nella letteratura corrispondente sulla gestione del rischio.
3	NIST SP800-30r1[114]	La "Guide for Conducting Risk Assessments" definisce un modello formale di analisi e gestione dei rischi per la sicurezza delle informazioni.
4	NIST SP800-37r2[115]	Il "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy" definisce il modello che devono adottare le strutture federali USA per la gestione del rischio.
5	"Linea Guida per lo sviluppo del software sicuro" di AgID (Allegato 4)[116]	Le "Linee guida per la modellizzazione delle minacce ed individuazione delle azioni di mitigazione conformi ai principi del Secure/Privacy by Design" definiscono un modello di analisi dei rischi utile nel processo di sviluppo software.

112 https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

113 È una panoramica dei contenuti rilevanti trovati nella letteratura corrispondente sulla gestione del rischio.

114 https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

115 https://www.nist.gov/privacy-framework/nist-sp-800-37.

116 https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro.

6	MAGERIT V3[117] (2012)	Metodologia di analisi dei rischi relativi alla sicurezza delle informazioni sviluppata per l'amministrazione pubblica spagnola ma diffusa in Europa grazie al software PILAR. Già illustrata nel paragrafo 5.3.1.
7	MEHARI[118] (Rev.2017)	Metodologia di gestione del rischio relativo alla sicurezza delle informazioni nel 1996 e più volte aggiornata. L'ultimo aggiornamento a seguito della pubblicazione della ISO/IEC 27001:2013 e della ISO/IEC 27005:2011.
8	EBIOS RM	Metodo per valutare e gestire i rischi secondo tecniche di raccolta dati tramite workshop con un approccio top-down
9	Privacy Impact Assessment – CNIL Methodology (2018)	Metodologia di Information Risk Management focalizzata sui rischi ai dati personali. La metodologia può essere utilizzata per creare tool o modelli di analisi dei rischi diversi dal tool offerto dal CNIL stesso.
10	Standard-200-3	"Risk Analysis based on IT-Grundschutz". IT-Grundschutz è un framework della tedesca BSI.
11	BS 6079-3:2000	"Project management—Guide to the management of business related project risk" del British Standards Institute.
12	King IV report	"King IV report on governance" dell'Institute of Directors in Southern Africa.
13	CSA Cloud Controls Matrix (CCM)	Insieme di controlli che coprono tutti gli aspetti del cloud, inclusa la valutazione del rischio. Può essere usato per valutare un servizio cloud.

117 https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro.

118 http://meharipedia.x10host.com/wp/home/

119 https://www.ssi.gouv.fr/en/guide/ebios-risk-manager-the-method/.

120 https://www.cnil.fr/en/PIA-privacy-impact-assessment-en.

121 https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.html?nn=409850.

122 https://cloudsecurityalliance.org/research/cloud-controls-matrix/. 8. I rischi in ambienti e contesti specifici

8. I rischi in ambienti e contesti specifici

Con i prossimi capitoli si intende illustrare il tema dell'analisi dei rischi in riferimento a specifiche tecnologie o ambienti di utilizzo.

Naturalmente, dato lo spazio limitato a disposizione, gli argomenti non potranno essere trattati in modo esaustivo. D'altra parte, come già richiamato, ad alcuni di essi sono stati dedicati precedenti lavori della Community negli anni passati (cloud, IoT, mobile, intelligenza artificiale, social), a cui si rimanda per ulteriori approfondimenti.

8.1 Infrastruttura informatica

Nonostante l'inarrestabile crescita nell'adozione delle nuove tecnologie IT, l'infrastruttura informatica classica è fondamentale e molteplici sono le situazioni di rischio che si devono affrontare anche in questo caso, facilmente offuscate dalla confidenza che trasmettono "i server nella stanza accanto, sotto controllo diretto".

Un'analisi completa degli elementi che rappresentano una minaccia per l'erogazione dei servizi IT richiede un'analisi dei componenti (o strati) di cui essi sono costituiti e dei momenti che ne caratterizzano il ciclo di vita. Gli elementi classici (e non necessariamente esaustivi) dell'infrastruttura informatica da considerare sono:

- la rete e gli apparati di rete;
- i server;
- gli end-point, (pc, tablet, smartphone, ecc.), che costituiscono un bersaglio privilegiato per qualsiasi attaccante, in quanto la maggior parte degli utenti svolge su di essi le attività più esposte a rischi di sicurezza (installazione di software, navigazione web, lettura della posta elettronica, ecc.);
- il middleware e le componenti di integrazione e interoperabilità applicativa;
- data containers e database.

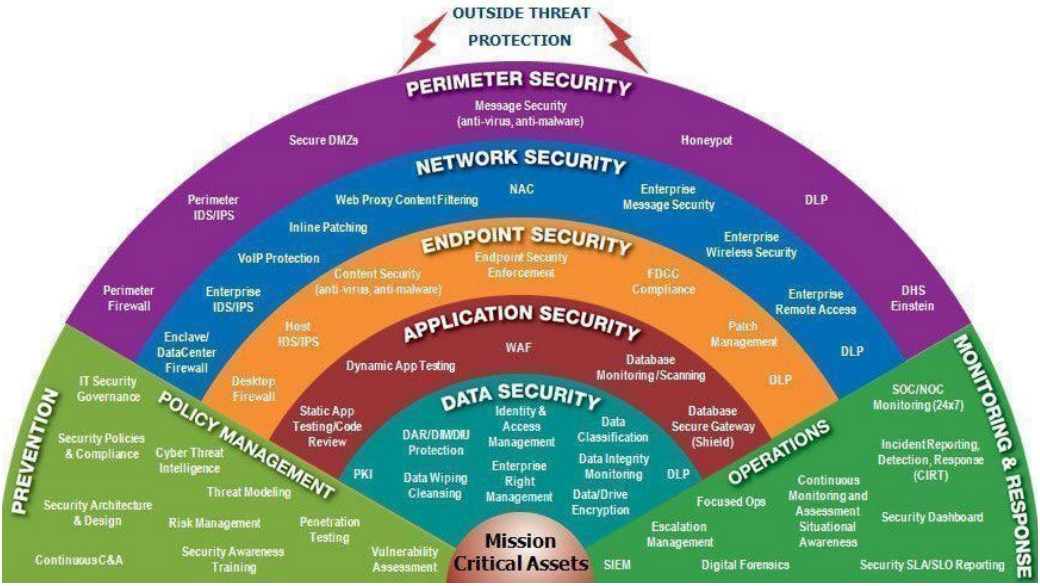

Figura 37 - Modello della data-centric security[123]

Nell'infrastruttura IT classica, si è sempre dato particolare rilievo al rischio di compromissione della sicurezza dei dati (e delle applicazioni che li trattano) e quindi alla necessità di garantire per essi la riservatezza, integrità e disponibilità. Alcuni esempi di eventi dannosi a riguardo sono:

- il fermo dei sistemi critici, dovuto a un guasto di un componente hardware, anche a causa della sua obsolescenza, o a un problema applicativo;
- un disastro che coinvolga il data center dove sono ospitati (causato da incendio, inondazione, terremoto);
- la corruzione dei dati, causato da errore umano, da problemi applicativi o da un attacco da parte di malintenzionati (ad esempio con un ransomware);
- l'accesso non autorizzato ai dati da parte di malintenzionati e la conseguente violazione di dati personali o critici.

123 Fonte: 2010, 2012 Northrop Grumman Corporation.

8.2 Cloud computing

Il cloud computing rappresenta una scelta tecnologica basata sul consumo "a servizio" dell'infrastruttura e di una svariata gamma di risorse informatiche, e si caratterizza per la forte flessibilità ed elevata velocità di adozione, con approvvigionamento su richiesta (on-demand) commisurato al fabbisogno dell'utente.
L'apparente facilità di fruizione è spesso causa di scelte troppo affrettate o compiute senza la necessaria consapevolezza dei rischi connessi.
Alcune tra le più comuni vulnerabilità specifiche con cui un utilizzatore di servizi cloud potrebbe trovarsi a fare i conti riguardano:

- il minore controllo sull'infrastruttura e sui servizi adottati, con anche il rischio per cui alcuni servizi utilizzati vengano dismessi;
- la mancanza di competenze interne e fornitori adeguati per operare sul cloud, con il rischio di adottare soluzioni troppo complesse da governare e conseguente aumento dell'esposizione ad attacchi;
- l'attivazione di risorse, la proliferazione di dati e la forte distribuzione dei servizi potenzialmente incontrollate e con l'ulteriore rischio di attivare servizi e poi non attivare i processi di dismissione nel momento in cui questi non sono più necessari;
- la criticità delle credenziali degli amministratori di sistema sul cloud che, se compromesse, permetterebbero a un attaccante di eliminare servizi, server o applicazioni;
- il lock-in nei confronti del cloud provider, ossia l'impossibilità di rivolgersi ad altri fornitori magari più competitivi e innovativi a causa delle tecnologie peculiari del primo fornitore e alle incompatibilità con versioni, linguaggi e sistemi operativi diversi;
- l'aumento della spesa per l'infrastruttura, perché le risorse in cloud vengono proposte on line a costi molto contenuti, con poca evidenza della proiezione del costo totale e si possono attivare più risorse di quelle necessarie senza riuscire a correlare i costi con i servizi effettivamente fruiti.

C'è da considerare il fatto che il contratto di cloud computing, almeno per quanto attiene ai più famosi provider statunitensi (es. Google, AWS, Microsoft) non è quasi mai negoziabile e l'oggetto dell'accordo (il servizio) viene accettato "as it is", ovvero così com'è stato predisposto dal fornitore: diverse clausole celano significative criticità di questo modello architetturale, che facilmente si traducono in veri e propri rischi, sempre a carico degli utilizzatori.

Per una trattazione completa sul cloud computing si suggerisce la lettura della pubblicazione Clusit "Consapevolmente Cloud".

Intervista a Cesare Burei, Socio Clusit, Formatore CINEAS e AIBA Cyber Risk, Co-Amministratore Margas - Broker e Consulente di Assicurazioni

L'avvento del cloud computing sta posizionando la tecnologia as a service, di cui è in grado di potenziare le principali caratteristiche di scalabilità, flessibilità e misurabilità, in vetta agli strumenti irrinunciabili per il business.
Secondo uno degli ultimi report dell'Osservatorio per la Trasformazione Digitale del Polimi, l'84% delle imprese medio-grandi utilizza almeno un servizio sul cloud pubblico, mentre nell'ultimo anno, con la pandemia, la migrazione sulla nuvola ha registrato un'impennata al 42% anche nelle piccole e medie imprese, da anni ferme a una crescita del 30%.
A fronte di questa crescita, l'impatto della standardizzazione tecnologica sull'economia sta determinando profili di asimmetria contrattuale e preoccupanti squilibri nelle responsabilità tra fornitori di servizi cloud (CSP, *cloud service provider*) e clienti.
L'esternalizzazione di infrastrutture e applicativi, di norma posti sotto l'esclusivo controllo dell'utilizzatore, produce una reale condivisione del rischio a cui il mercato reagisce comunemente con l'utilizzo di clausole di manleva che tentano di esonerare il CSP, tipicamente in caso di violazione, dispersione, irraggiungibilità e cancellazione del dato. È proprio così? E se sì, come può tutelarsi l'azienda utente? Lo chiediamo a Cesare Burei di Margas, broker assicurativo specializzato, stakeholder nell'individuazione e gestione del rischio e delle responsabilità.

D. Nella sua qualità di broker, direttamente in ascolto del mercato, lei ritiene che vi sia sufficiente consapevolezza rispetto ai rischi (tecnici, giuridici, reali, virtuali) che le imprese italiane si assumono con la migrazione sul cloud?

R. Direi di no e il caso del CSP lussemburghese OVH ne è la dimostrazione. Un'attenta lettura dei contratti, per quanto emessi da un soggetto considerato di dimensioni tali da non consentire trattativa, avrebbe dovuto mettere in luce la necessità di acquistare separatamente i servizi di backup. La mitigazione del rischio nell'ambito delle nostre possibilità, con una attenta valutazione costi e benefici, è imprescindibile responsabilità di chi va sulla nuvola e lo aiuta ad assicurarsi al meglio. In questo caso c'è stato un chiaro errore o più probabilmente una errata considerazione della propria sicurezza da parte dei clienti o anche dei system integrator che hanno rivenduto il servizio.

D. Quindi, secondo esperienza, che tipo di protezione assicurativa potrebbe essere maggiormente efficace per gli operatori che vogliono cavalcare la trasformazione digitale e usare soluzioni in cloud per crescere?

R. La conoscenza delle soluzioni proposte dal mercato, ma soprattutto aver seguito o gestito alcuni particolari sinistri, mi ha aiutato a farmi un'idea più precisa di quali siano e sarebbero gli strumenti assicurativi di cui le organizzazioni hanno bisogno.

La polizza chiave per l'organizzazione che si preoccupa di danni e costi conseguenti a un incidente o attacco informatico ai sistemi ICT, è senz'altro la cosiddetta "Polizza cyber". Si tratta di un contratto assicurativo solitamente costituito da una sezione "costi e danni propri" e una di "responsabilità verso terzi in ambito privacy" per problematiche connesse al trattamento di dati di terze parti.

Le garanzie chiave rifondono: 1. i costi per consulenti o servizi per l'analisi del caso e la ripartenza; 2. i costi fissi non cessanti in caso di fermo aziendale; 3. le attività necessarie verso clienti o il garante privacy. Spesso sono inclusi anche una serie di servizi di assistenza in emergenza e l'assistenza legale. È chiaro che, se il perimetro digitale dell'azienda si estende al cloud, anche la polizza deve seguire e devo preoccuparmi di capire se e a quali condizioni questo sia possibile, fondamentalmente verificando se il contratto risponde in tutto o in parte ai confini di responsabilità concordati con il provider.

Un altro passo importante è sapere se e come il provider sia assicurato, dato che non basta la "semplice" polizza di Responsabilità civile generale. Se è impraticabile negoziare questi aspetti con le big tech come Microsoft o Google, è invece altamente consigliato valutarli prima della migrazione quando si tratta con i provider nazionali e europei, peraltro vincolati al rispetto del GDPR.

La copertura assicurativa a tutela del CSP e indirettamente del suo cliente è nota come "ICT professional indemnity" o "RC professionale ICT". Sarà sufficiente richiedergli copia di un certificato di vigenza e sottoporlo per ogni evenienza all'attenzione del proprio broker assicurativo. Se fornitore e cliente sono assicurati e bene, in caso di sinistro che li veda coinvolti entrambi, il supporto dato dalle polizze sarà fondamentale per fornire risorse di emergenza supplementari a quelle organizzative preventivamente introdotte e risolvere la crisi nel più breve tempo possibile, evitando lunghe controversie.

D. Mentre in Usa il mondo assicurativo ha da tempo intercettato la profilazione di questi nuovi rischi connessi al progresso tecnologico, cosa propongono le compagnie europee ed italiane ai clienti dei CSP e ai CSP?

R. Le soluzioni rispettose dell'aspetto cloud esistono già sul mercato assicurativo. Anche italiano**.** Le più valide sono indirizzate soprattutto ai clienti enterprise, mentre per le PMI i prodotti disponibili sono meno aderenti alle loro realtà e spesso di difficile comprensione. Da broker assicurativo vedo un problema serio: il fatto che non esista univocità nelle definizioni chiave di queste polizze. Il modo molto difforme di definire un "sistema informativo", un "incidente informatico", un "furto IT", "un attacco hacker", rende veramente difficile fornire alle organizzazioni un serio lavoro comparativo. Va anche messo in luce che per le conseguenze di un malfunzionamento infrastrutturale (interruzione di energia elettrica o connettività), non interverrà

quasi nessun contratto assicurativo. Per questo è importante eseguire preventivamente un risk assessment, formalizzare delle procedure di risk management e poi pensare alla stipula della polizza cyber. Procedere al contrario si rivelerà poco efficace, se non controproducente, nel momento della crisi.

In ogni caso, a fronte della quantità di incidenti segnalati in Italia, siamo ancora poco e sotto assicurati. L'anno scorso abbiamo intercettato l'esigenza di un CSP che, conscio di questa realtà e intendendo interpretare al meglio il suo ruolo di innovation driver, ha voluto costruire con noi un modo semplice ed economico di portare il concetto di risk management alla clientela: usa la mia tecnologia sicura, scegli servizi di cyber security come il backup e il DR per mitigare il tuo rischio e potrai accedere a una piccola polizza cyber integrata. La soluzione era ovviamente standardizzata, ma pensata ad hoc per i clienti del cloud.

Il bundle non è stato compreso dal mercato, fondamentalmente perché non sono chiari ai più i confini di responsabilità o perché il cliente del cloud ritiene che tutte le responsabilità – e relativi costi – ricadano sul CSP.

Su questo fronte c'è molto da fare, a partire dalla contrattualistica che il CSP propone: spesso altamente criptica per l'imprenditore medio italiano, poco esperto di cosiddetti wall-contracts predisposti sul modello anglosassone, e frammentati in più accordi separati redatti rigorosamente in lingua inglese. Si potrebbe immaginare di impiegare in questo settore una buona dose di "design thinking" per sintetizzare e chiarire in una grafica semplificatrice cosa è a carico delle parti rispetto alle responsabilità che derivano dal contratto di servizio e renderla parte integrante dell'accordo.

Forse faciliterebbe la comprensione dei confini di responsabilità e quindi di chi deve proteggere cosa. Per il come, basta affidarsi a un partner assicurativo competente, sia in ambito ICT che assicurativo.

8.3 IoT

Come già evidenziato nella pubblicazione Clusit intitolata "IoT Security e Compliance: Gestire la complessità e i rischi", la valutazione dei rischi relativi ai dispositivi IoT deve includere quelli relativi alle entità e ai processi coinvolti nella loro progettazione e gestione.
Una classificazione dettagliata dei rischi derivanti da tutti i possibili sistemi IoT esistenti non sarebbe pratica, e forse nemmeno possibile. Le tecnologie IoT esistenti sono infatti numerose, e in continua e rapida evoluzione. Nel seguito presentiamo solo alcuni di questi rischi.

Gli scenari di rischio possono essere raggruppati in diverse famiglie:

- uso scorretto e non deliberato di un componente della soluzione IoT: questo può essere determinato anche dalla mancanza di consapevolezza delle singole persone che ne fanno uso o, nel caso delle organizzazioni, che ne permettono l'uso;
- attacco deliberato a un componente IoT, al fine di usarlo in maniera scorretta e non prevista;
- malfunzionamenti dei dispositivi hardware o del software;
- configurazione non corretta dei sistemi di accesso - interfacce per gli utenti e machine-to-machine - o delle connessioni (ad esempio con sistemi di cifratura inadeguati).

Tra le vulnerabilità di interesse per i **progettisti** di soluzioni IoT possiamo identificare le seguenti:

- carenze nella individuazione delle potenziali criticità di sicurezza ICT relative al sistema IoT considerato;
- mancato rispetto del principio di security-by-design;
- carenze nelle competenze del personale tecnico;
- mancato rispetto di leggi e regolamenti generali e settoriali.

Per quanto riguarda le **organizzazioni utilizzatrici di soluzioni IoT**, invece, possiamo individuare le seguenti vulnerabilità :

- carenze nell'assegnazione di responsabilità relative all'adozione e manutenzione di prodotti IoT;
- carenze nei meccanismi di gestione dei progetti in ambito IoT, con particolare riferimento alla realizzabilità delle soluzioni, alle fasi di collaudo e al passaggio in esercizio;
- carenze nei processi di ricerca di soluzioni sul mercato e nei criteri tecnico-economici di scelta;
- carenze nelle competenze del personale tecnico interno o del fornitore dedicato al progetto;
- carenze nella scelta delle componenti del sistema IoT (hardware, firmware, software) sicure;
- carenze di integrazione "sicura" delle componenti tra di loro e con il resto del sistema informatico, dovuta a carenze nella progettazione e nei test di integrazione;
- configurazione non corretta degli applicativi software e dei singoli dispositivi (ad esempio, installazione su segmenti di rete inappropriati o impostazione non

corretta della password o dei parametri di connessione), e conseguente accesso non autorizzato o intercettazioni;
- indisponibilità della connessione alla rete o a Internet, o di alimentazione elettrica;
- mancato rispetto di leggi e regolamenti generali e settoriali.

Alcuni scenari sono tipici e specifici della componente IoT della soluzione. Ad esempio, per i **dispositivi** vanno considerate:

- minacce relative alla compromissione dei dispositivi da parte di malintenzionati;
- minacce relative all'obsolescenza dei dispositivi;
- minacce ambientali, considerando che possono essere installati all'esterno e quindi soggetti a fenomeni atmosferici, in luoghi pubblici e quindi soggetti ad atti di vandalismo, in ambienti frequentati da molte persone o bambini che li possono danneggiare inavvertitamente;
- inadeguato monitoraggio e manutenzione;
- minacce relative alla perdita fisica del dispositivo, che possono comportare il suo uso da parte di persone non autorizzate o l'impossibilità, per l'utilizzatore autorizzato, di continuare ad usare la soluzione IoT;
- difficoltà di aggiornamento, considerando che potrebbero manifestarsi vulnerabilità non solo del software o del firmware, ma anche dell'hardware;
- mancanza di disponibilità a causa di limiti della banda di rete o di installazione su segmenti di rete inappropriati.

Per quanto riguarda i rischi relativi agli **applicativi software** (§ 8.13), alla componente **cloud** (§ 8.2) e alla **componente edge** (§ 8.4) di una soluzione IoT, si rimanda il lettore ai paragrafi corrispondenti di questo libro.

Per quanto riguarda gli **impatt**i, è necessario considerare l'uso previsto della soluzione IoT. Qui di seguito vengono forniti alcuni esempi:

- i dispositivi medici impiantabili, come pacemaker e defibrillatori, possono avere conseguenze letali in caso di uso scorretto o malfunzionamento;
- i dispositivi medici di elaborazione dati (ad esempio, apparecchiature di imaging) potrebbero avere importanti impatti sulla privacy, se violati;
- nell'ambito dei trasporti, la compromissione o il malfunzionamento del sistema di frenatura o di altri sistemi di assistenza alla guida possono avere impatti letali;
- i sistemi di domotica, inclusi quelli di rilevazione dei fumi e spegnimento degli incendi, se violati, possono avere impatti sulla privacy e sulla sicurezza degli abitanti, tanto più dannosi se si considera che alcuni di essi sono progettati proprio per proteggere le dimore e i loro abitanti;

- i video monitor, collocati nella camera da letto dei bambini per il controllo remoto degli stessi, possono trasmettere a TV, ricevitori portatili, PC e smartphone; se configurati non correttamente o violati da malintenzionati, permettono la ripresa e la diffusione di diversi aspetti privati di persone inconsapevoli;
- i sistemi di tracciamento (come ad esempio i sistemi GPS delle vetture aziendali, o i telefoni aziendali utilizzati per la reperibilità) potrebbero essere usati in modo scorretto in ambito lavorativo e violare la privacy dei lavoratori;
- i sistemi indossabili (wearable) potrebbero consentire a malintenzionati di raccogliere informazioni sugli spostamenti di una persona o sui luoghi che visita (è noto il caso di un dispositivo indossabile dotato di GPS, utilizzato da un militare durante il suo tempo libero, che ha portato ad individuare una base militare la cui localizzazione doveva rimanere segreta);
- i sistemi di controllo industriale potrebbero consentire dei sabotaggi da parte di malintenzionati a scopo di ricatto, o di terroristi a scopo dimostrativo.

In generale, quindi, gli **impatti** possono essere i seguenti:

- compromissione della salute e della vita di persone fisiche;
- perdita o danneggiamento di proprietà;
- indisponibilità di sistemi di interesse pubblico e di infrastrutture critiche;
- violazione del diritto alla privacy per le singole persone fisiche, e sanzioni per l'organizzazione che usa o vende prodotti o servizi che non garantiscono un adeguato livello di privacy;
- violazione di norme e regolamenti che comportano altre multe delle autorità o contestazioni dei clienti, e il conseguente impatto reputazionale;
- costi di ripristino o adeguamento per l'utilizzatore o per l'organizzazione che usa o vende prodotti o servizi che non rispondono ai contratti, alle leggi e a altre norme.

Concludiamo segnalando che anche il rapporto NISTIR 8228 del 2019[124] identifica i principali rischi dell'IoT ed i relativi obiettivi di mitigazione del rischio.

124 https://csrc.nist.gov/publications/detail/nistir/8228/final.

8.4 Edge computing

Molto spesso, quando si parla di edge computing si pensa alla cosiddetta *Internet of Things* (IoT), ma le due realtà sono leggermente diverse. L'IoT si riferisce infatti a qualsiasi sistema di dispositivi che ricevono e trasferiscono dati. Il termine e*dge computing* si riferisce, più in generale, all'informatica distribuita, che porta l'archiviazione dei dati e la potenza di calcolo più vicino all'origine dei dati o ai dispositivi che li raccolgono. Le informazioni vengono così elaborate vicino all'origine dei dati, anziché svolgerle in un cloud centralizzato o in un data center tradizionale.

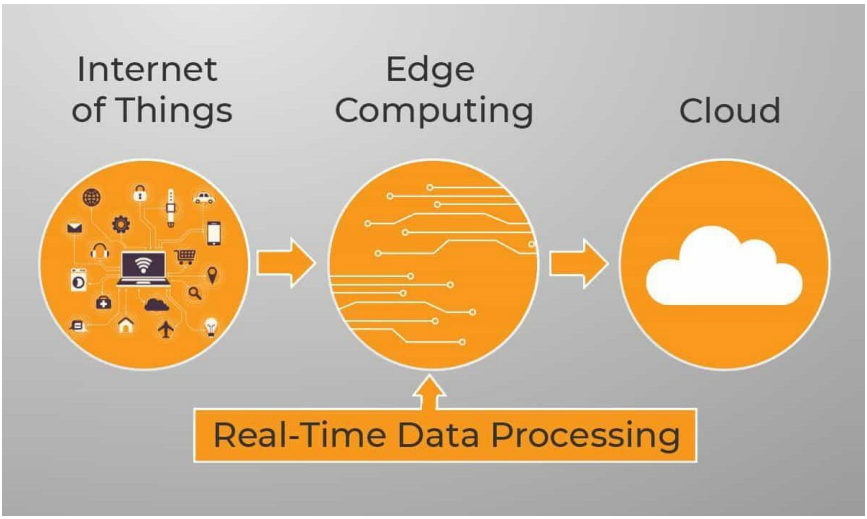

Figura 38- Relazione tra Internet of Things, edge computing, e cloud[125]

Con la maggiore diffusione di sensori e dispositivi che raccolgono informazioni per quasi tutti gli scopi immaginabili (dagli edifici intelligenti e le reti elettriche alle fabbriche, aeroplani, automobili e punti vendita) l'espansione "verso l'*edge*" è così pronunciata che Forrester[126] già nel 2021 prevedeva che il 2022 si sarebbe rivelato il vero punto di svolta per questo tema e Gartner[127] prevede che entro il 2025 il 75% dei dati aziendali sarà generato ed elaborato al di fuori dei tradizionali data center o del cloud.

125 Fonte: https://phoenixnap.com/blog/edge-computing-vs-cloud-computing

126 https://www.forrester.com/blogs/predictions-2021-edge-computing-hits-an-inflection-point/.

127 https://www.gartner.com/smarterwithgartner/gartner-top-strategic-technology-trends-for-2021.

L'*edge computing* favorisce anche molti casi d'uso per l'intelligenza artificiale: basti pensare a tutte quelle situazioni dove è necessaria una latenza ridottissima, come ad esempio il movimento autonomo (per evitare le collisioni è necessario che sia il dispositivo ottico a riconoscere gli oggetti in avvicinamento, senza attendere l'elaborazione dell'unità centrale) e dove è obbligatorio mantenere un certo livello di privacy (come avviene negli assistenti virtuali, che devono riconoscere gli ordini ed elaborare il parlato mantenendo tutti i dati sul dispositivo, senza condivisione con server esterni).
Il settore si è mosso approntando versioni ridotte dei normali framework di sviluppo ed elaborazione, come ad esempio tinyML, per consentire l'addestramento e il funzionamento di reti neurali su dispositivi dalla potenza e dalla disponibilità energetica limitata.
Il cambio di paradigma dettato dall'*edge computing* introduce nuove minacce alla sicurezza informatica. Tra questi vanno considerati:

- Conservazione e protezione dei dati: i dati raccolti ed elaborati mancano della sicurezza fisica di un data center. Rimuovendo semplicemente un'unità disco da una risorsa edge o copiando i dati da una semplice scheda di memoria, le informazioni possono essere compromesse e anche perse, visto che le risorse locali sono limitate ed è più difficile garantire un backup.
- Password e autenticazione: i dispositivi perimetrali, in particolare IoT, spesso non effettuano controlli robusti e quindi possono essere sfruttati da malintenzionati (p.e. un'università negli USA ha subito un attacco dDOS che ha sfruttato le password deboli dei dispositivi IoT[128]).
- Proliferazione incontrollata delle operazioni: man mano che le organizzazioni usano sempre più dispositivi periferici per gestire una gamma più ampia di operazioni, diventa più difficile tracciarli e monitorarli.
- Aumento della latenza: man mano che cresce il traffico di rete IoT aumenta anche la latenza, e quindi i tempi di risposta della rete.
- Analisi dei dati: la sicurezza può essere compromessa quando i dati vengono inviati senza che siano stati analizzati precedentemente in maniera appropriata.
- Difficoltà del monitoraggio di sicurezza digitale e fisica, dato che i dispositivi sono spesso lontani da un'infrastruttura dati centralizzata o da un data center.

128 https://campustechnology.com/articles/2017/02/13/university-hackers-attacked-5000-iot-devices-on-campus.aspx.

8.5 Intelligenza artificiale

L'intelligenza artificiale (IA) è una disciplina che da circa settant'anni studia l'emulazione dell'intelligenza umana da parte di "macchine", intese sia come software sia - in certi casi - come hardware. Come indicato nella pubblicazione Clusit del 2020 dal titolo "Intelligenza Artificiale e Sicurezza – Opportunità, rischi e raccomandazioni"[129], porta con sé rischi che si sviluppano su diverse dimensioni:

- rischi di natura etica: alcune decisioni assunte autonomamente dall'IA potrebbero infatti essere valutate - secondo criteri umani - in modo profondamente negativo, e per alcuni potrebbero giungere a rappresentare un pericolo per la stessa sopravvivenza del genere umano;
- rischi di natura tecnica: la complessità tecnica degli algoritmi utilizzati in ambito IA potrebbe comportare disfunzioni, anche difficilmente analizzabili, quali:
  - i pregiudizi di cui l'algoritmo potrebbe risentire;
  - l'emersione di risultati discriminatori;
  - la mancanza di trasparenza del sistema decisionale;
- rischi inerenti la privacy dei soggetti interessati, in particolare:
  - l'IA fa ricorso ad un impiego massivo di dati personali, elaborati in maniera da estrarne ulteriori informazioni, ad esempio comportamentali;
  - l'IA potrebbe non adempiere adeguatamente alla normative vigenti in termini di consensi al trattamento, corretto trasferimento di dati all'estero, ecc.;
- rischi inerenti i temi della cybersicurezza: oltre ai rischi di carattere più generale inerenti l'infrastruttura - come ad esempio l'indisponibilità dei servizi in cloud, la corruzione dei dati, anche dovuta ad azioni malevole, la presenza di vulnerabilità o di configurazioni scorrette del software, ecc. - vanno menzionati i rischi di cyber attacchi specifici del mondo IA, in particolare quelli relativi alla possibilità di minare l'IA a livello logico tramite i cosiddetti adversarial attacks.

Non va poi dimenticato che anche gli attaccanti possono avvalersi di strumenti basati sull'IA per ottenere informazioni sui sistemi o sulle persone oggetto di attacco, in particolare per identificare la modalità migliore per effettuare un attacco efficace, i punti più vulnerabili, ecc. L'IA può anche essere usata per proporre contenuti politici o commerciali costruiti ad arte e ritenuti interessanti per la vittima, per indurla a comportarsi o a votare in un certo modo, a fare certi tipi di dichiarazioni, o ad acquistare certi tipi di prodotti.

129 https://iasecurity.clusit.it/.

In ambito assicurativo e bancario possiamo assistere ad un ulteriore tipo di utilizzo degli strumenti di IA, per la predizione del rischio di insolvenza del cliente, nel momento in cui chiede un prestito, una carta di credito, o vuole stipulare una polizza assicurativa. Benché in questo caso gli strumenti di IA siano utilizzati come strumenti per la valutazione del rischio, naturalmente non sono esenti essi stessi dai rischi che abbiamo specificato sopra, come l'essere soggetti a pregiudizi e a comportamenti discriminatori.

8.5.1 Rischi di natura tecnica

Considerate le diverse tipologie di rischio elencate sopra, possiamo classificare le minacce legate all'uso di sistemi di IA come segue. Le **minacce verso i sistemi di IA** si dividono in minacce **accidentali** (come ad esempio malfunzionamenti, indisponibilità dell'infrastruttura di calcolo, eccezioni non gestite nell'implementazione) e minacce **deliberate**, quali gli attacchi informatici al sistema implementato, reverse engineering, reconnaissance, information gathering, poisoning, evasion.
Per quanto riguarda le minacce causate dai sistemi di IA, le possiamo dividere in:

- Errori di addestramento (o classificazione): a seconda del campo di applicazione, questi errori possono sfociare in problemi etici, discriminatori (come nel caso, ad esempio, di una decisione presa da un giudice con il supporto di algoritmi di IA addestrati su dati "falsati" o prevenuti nei confronti di certe etnie o generi[130]) o fisici, come nei casi della guida autonoma, della domotica, dell'utilizzo di sistemi IoT, o di sistemi usati in ambito sanitario[131].
- Utilizzo della tecnologia per scopi malevoli o illeciti, come ad esempio lo sviluppo di armi biochimiche, la realizzazione di attacchi informatici "adattivi", la violazione deliberata della privacy delle persone.
- Rischi intrinseci nell'utilizzo dei sistemi di IA, ossia nell'interazione uomo-macchina. Fanno parte di questa tipologia le seguenti minacce:
  - mancanza di trasparenza: il sistema arriva a un risultato, ma non si riesce a capire come lo ha prodotto;
  - dequalificazione (deskilling) dei lavoratori: si teme che un sistema IA con un'elevata accuratezza possa portare, nel tempo, i lavoratori umani a dare sempre ascolto all'IA e a non essere più sufficientemente preparati;
  - creazione di informazioni personali da dati anonimizzati o non particolari:

130 MIT Media Lab - Gender Shades. https://www.media.mit.edu/projects/gender-shades/overview/.

131 Malicious Uses and Abuses of Artificial Intelligence. S.l.: EUROPOL, 2021. https://www.europol.europa.eu/publications-documents/malicious-uses-and-abuses-of-artificial-intelligence.

vi sono casi dove incrociando database di dati di per sé non particolari, oltre che anonimizzati, i sistemi possono ricreare o individuare dati particolari (gli esempi sono sempre più numerosi[132]).

Un aspetto fondamentale, ma spesso trascurato, è che la valutazione del rischio in una qualsiasi applicazione dovrebbe sempre tener conto del rischio legato al NON utilizzo di una certa soluzione basata su IA. Esistono infatti già molte applicazioni in cui l'utilizzo dell'IA consente di ridurre sensibilmente il rischio, pur tenendo in conto i rischi che l'IA stessa può introdurre. Un caso è quello legato alla (pur acerba) tecnologia per la guida autonoma[133].

8.5.2 Rischi di natura giuridica

Passiamo ora a considerare i rischi legati all'IA, dal punto di vista giuridico. Come già indicato nel paragrafo 6.6, la proposta di regolamento europeo sull'intelligenza artificiale prevede una valutazione della potenziale rischiosità dei sistemi automatizzati, con la loro suddivisione in tre principali categorie, in ordine di criticità:

- le **applicazioni vietate** perché pregiudizievoli per la dignità umana (ad esempio social scoring, riconoscimento biometrico, manipolazione);
- gli impieghi dell'IA **altamente pericolosi** (ad esempio credit scoring, i sistemi di IA relativi a infrastrutture pubbliche essenziali, come giustizia e sicurezza sociale, dispositivi medici o regolamentati, e sistemi di trasporto);
- le applicazioni che **non presentano alcun potenziale lesivo a priori**.

Uno dei temi ancora molto dibattuti sotto il profilo giuridico è proprio quello dei criteri di imputazione della responsabilità rispetto ai diversi attori della filiera. In diritto, rischio e responsabilità (civile) sono due concetti molto prossimi che interessano dal punto di vista soggettivo diversi attori: l'ideatore e programmatore dell'algoritmo, lo sviluppatore che addestra il sistema, il rivenditore che lo mette sul mercato, l'operatore che lo sceglie per implementare un prodotto o servizio, fino ad arrivare all'utilizzatore che è tenuto a farne un uso adeguato.
La peculiarità del settore, che impone di trovare soluzioni innovative anche dal punto di vista giuridico, sta nel fatto che la componente algoritmica di un prodotto o servizio è per sua natura "in costante evoluzione", ovvero in progressivo sviluppo applicativo (IA come componente dinamica). Gli obblighi di conformità, trasparenza, robustezza

132 https://venturebeat.com/2020/10/21/researchers-find-evidence-of-racial-gender-and-socioecono- mic-bias-in-chest-x-ray-classifiers/.

133 Tesla Vehicle Safety Report. https://www.tesla.com/VehicleSafetyReport.

e sicurezza dunque non possono cessare con la messa in commercio del bene, ma dovranno essere costantemente garantiti durante l'intero ciclo di vita del sistema di IA: il rischio diventa dunque concetto permanente perché intrinseco a quello di "apprendimento" e di "inafferrabilità computazionale" (black box).
L'importanza della **qualità del dato** nella valutazione del rischio in ambito IA è fattore di massimo significato: il dato, oltre ad essere compromesso da pregiudizi ab origine, potrebbe anche essere stato estrapolato in difetto delle garanzie poste in difesa della privacy dell'interessato (ad esempio, assenza di consenso).

8.6 Smart working

Lo *smart working* è definito dalla Legge n. 81 del 22 maggio 2017 come "(...) modalità flessibile di esecuzione del rapporto di lavoro subordinato allo scopo di incrementare la produttività e agevolare la conciliazione dei tempi di vita e di lavoro (...)".Questa forma organizzativa si è spesso diffusa senza la consapevolezza e, soprattutto, senza la preparazione necessaria per affrontarne i rischi. Alcune criticità riguardano i **dispositivi** utilizzati per lo *smart working*, come ad esempio:

- Mancanza di formazione, sensibilizzazione e addestramento degli utenti sull'uso dei dispositivi usati al di fuori della sede dell'organizzazione.
- Promiscuità nell'utilizzo di dispositivi (pc, smartphone, ecc.), che include l'utilizzo - per scopi lavorativi - di dispositivi dell'organizzazione e di dispositivi personali. Mentre i primi sono più facilmente gestibili in modo centralizzato da parte dell'organizzazione (p.e. applicando configurazioni predefinite e impostando specifiche regole di sicurezza anche con soluzioni di mobile device management), i secondi in genere sfuggono al controllo dell'organizzazione (shadow IT). L'uso contemporaneo di dispositivi personali e di lavoro (p.e. con la sincronizzazione dell'email di lavoro anche sul proprio pc personale) ha come conseguenza la proliferazione di copie delle informazioni che sfuggono al controllo dell'organizzazione.
- Connessione alle reti aziendali di dispositivi non autorizzati e potenzialmente vulnerabili o compromessi.
- Protezione inadeguata dei dispositivi (p.e. assenza di cifratura del disco fisso a partire da BIOS e mancanza di automatismi per il blocco automatico dello schermo del dispositivo in caso di inutilizzo).
- Mancanza di regole per il corretto utilizzo dei dispositivi anche al di fuori delle

sedi dell'organizzazione (p.e. obbligo dell'utente di disattivare i servizi di rete e bloccare il proprio PC nel momento in cui si allontana dalla postazione di lavoro, divieto di concedere l'utilizzo del proprio PC a terzi non autorizzati in particolar modo quando l'utente è connesso alla rete dell'organizzazione).

- Compromissione delle credenziali di accesso ai sistemi, dovuta a un approccio più rilassato alla sicurezza (oltre che all'assenza di sistemi di autenticazione a più fattori).
- Mancanza di soluzioni e procedure per la gestione degli episodi di furto o di smarrimento del dispositivo, anche con soluzioni di blocco o cancellazione remoti e geolocalizzazione.
- Difficoltà nell'esecuzione dei backup anche per i limiti della banda di rete disponibile all'utente.
- Criticità nella gestione degli aggiornamenti (sistema operativo, software di sicurezza, ecc.), così come nell'identificazione e nella risposta a eventuali vulnerabilità.
- Complicazione della gestione degli incidenti di sicurezza e delle violazioni di dati personali in assenza di adeguati strumenti di end-point detection & response.
- Insicurezza delle connessioni, se non usano protocolli di crittografia adeguati. Le VPN sono canali di comunicazione sicuri ma, se violati, possono fornire anche all'attaccante un canale di comunicazione verso i sistemi dell'organizzazione.
- Vulnerabilità delle reti domestiche usate dagli utenti per connettersi.
- Il lavoro remoto può prevedere la messa a disposizione di un terminale nella sede dell'organizzazione e un PC presso l'abitazione del lavoratore. Quando i dipendenti sono assenti dall'ufficio - in certi casi, interi locali sono lasciati totalmente non presidiati per ore o giorni - i terminali possono essere oggetto di attacchi con componente fisica. In passato, situazioni simili si verificavano durante i periodi di ferie, ma erano comunque rese più difficili dal fatto che in sede era sempre presente qualche dipendente per monitorare attività sospette o rilevare la presenza di persone non autorizzate ad aggirarsi per le stanze e ad accedere ai terminali.

Ci sono poi i rischi connessi agli **strumenti** di collaborazione e comunicazione, che, oltre a dover essere configurati, gestiti e utilizzati correttamente, devono essere supportati da specifiche strategie per assicurarne la continuità operativa visto che, in caso di blocco, potrebbero compromettere l'operatività del personale che li utilizza per il lavoro da remoto.
Lo smart working fa anche uso di servizi cloud, dei quali si è trattato al § 8.2.
Misure di sicurezza specifiche sono descritte nella NIST SP 800-46[134].

134 https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final.

8.7 La catena di fornitura

Figura 39 - La catena di fornitura[135]

Oggi qualsiasi organizzazione - dalla più piccola alla più grande e dalla pubblica alla privata - si avvale di numerosi fornitori per servizi e prodotti di varia natura, condividendo anche informazioni confidenziali.
La mancanza di disponibilità, un malfunzionamento o un attacco cyber subito dal fornitore potrebbero causare un effetto a catena con conseguenze devastanti sui clienti. Esemplificativo, in tal senso, è il caso SolarWinds[136].
Una corretta valutazione del rischio in tutta la catena di fornitura è dunque un elemento fondamentale per migliorare la sicurezza. E' doveroso ricordare che numerosi sono i rischi associati alla catena di fornitura, ad esempio: rischi finanziari e creditizi, dipendenza produttiva da altre terze parti, situazione geopolitica e geografica, normative locali, continuità, operativi e cyber[137].

Alcuni rischi specifici da considerare e relativi alla filiera di fornitura:

- chiusura o indisponibilità dei fornitori, che, nel caso di prodotti, non possono più offrire assistenza o aggiornamenti e, nel caso di servizi, ne interrompono l'erogazione, anche improvvisamente e senza avvisare;

135 www.cosonline.com.

136 https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know.

137 ENISA Threat Landscape for Supply Chain Attacks – July 2021. S.l.: European Union Agency for Cybersecurity (ENISA), 2021.

- prodotti e servizi non più mantenuti e aggiornati e quindi con vulnerabilità non più trattate; questo può succedere anche se il fornitore continua a operare, ma decide di non seguire più lo sviluppo o la manutenzione di un determinato prodotto o servizio; in alcuni casi avvisa per tempo i clienti, in altri no; in tutti e due i casi, la migrazione a nuovi prodotti o servizi può essere complicata dall'uso di formati proprietari o comunque non sufficientemente diffusi;
- compromissione dei prodotti e servizi dei fornitori; tali prodotti e servizi possono poi essere usati per attaccare i suoi clienti (come nel caso Solarwinds); in alcuni casi, per attaccare un'organizzazione, gli attaccanti sfruttano ambienti meno sicuri dei suoi fornitori; questo può avvenire attaccando i sistemi di gestione del software (repository di configurazione e gestione delle versioni del software), accedendovi senza autorizzazione e quindi modificando il software per farlo distribuire con incluse backdoor o vulnerabilità;
- nel caso di fornitori di sviluppo, inaffidabilità degli sviluppatori esterni che non seguono regole di sviluppo sicuro e, quindi, consegnano software con vulnerabilità;
- attacchi ai fornitori di servizi di monitoraggio e controllo della rete e dei sistemi (p.e. NOC); questi potrebbero essere vittima di un ransomware che poi viene diffuso anche nelle infrastrutture informatiche dei clienti gestiti.

I fornitori dovrebbero essere classificati in base alla tipologia di servizio fornito e ai dati da gestire o a cui hanno accesso e sulla base di questo variano i rischi a cui potrebbero essere sottoposti.
I rischi dei fornitori dovrebbero essere analizzati durante tutto l'iter contrattuale, ossia prima della stipula del contratto, nel corso della durata e anche, per un tempo ragionevole, dopo la chiusura del contratto.
Strumenti per supportare l'analisi dei rischi sono:

- **Intelligence sui fornitori** attraverso analisi e correlazione delle informazioni disponibili sui fornitori provenienti da fonti interne (anagrafica fornitori, utenze presenti, incidenti pregressi, tecnologie fornite dalle terze parti, ecc.) e fonti esterne quali report di Intelligence e OSINT (data breach o altri eventi di sicurezza subiti dai fornitori, modifiche organizzative quali acquisizioni e fusioni, vulnerabilità che interessano sistemi forniti da terze parti, ecc.). Esistono diversi software (p.e. Bitsight) che forniscono report di dettaglio tali da consentire un'azione immediata di analisi e remediation.
- **Quick assessment,** con questionari di autovalutazione in materia di cybersecurity che possono essere a risposta chiusa (SI/NO) o risposta multipla.
- **Monitoraggio fornitori tramite sistemi di sicurezza interni,** attraverso strumenti quali CASB (cloud access security broker), l'analisi del traffico di rete, i log

dei sistemi IAM (identity access management), DLP (data loss prevention) e DRM (digital right management).

- **Audit sui fornitori,** considerando che nei contratti dovrebbe essere sempre prevista una clausola dedicata al "diritto di audit" e le modalità per poterlo esercitare.

8.8 La continuità operativa

La continuità operativa richiede la *business impact analysis* (BIA) e il *risk management* (RM) per progettare le strategie di continuità. Tali strategie saranno documentate nel *Business continuity plan* (BCP), che conterrà altresì: *Disaster recovery plan* (DR), *Crisis management & communication plan* (CM&CP), *Emergency plan*, *Incident response plan* (IRP).

Per i sistemi informatici si fa riferimento ai seguenti parametri:

- **RTO (recovery time objective)** - periodo di tempo dopo un incidente, entro cui deve essere ripristinato un prodotto, un servizio o un'attività o entro cui le risorse devono essere recuperate, ossia qual è il tempo desiderato di ripristino;
- **RPO (recovery point objective**) - il punto in cui i dati utilizzati da un'attività devono essere ripristinati per consentire all'attività di operare sul recupero, ossia qual è l'intervallo di tempo massimo dall'ultima copia dei dati valida (back up).

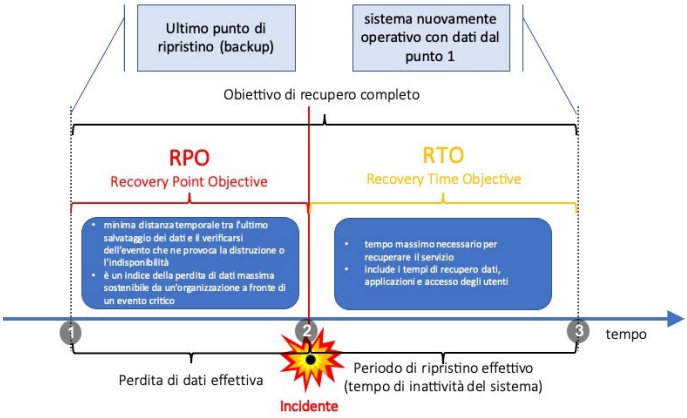

Figura 40 - RTO e RPO[138]

138 Figura degli autori.

Tali parametri vanno definiti per ogni processo ritenuto critico: più questo è importante per un'organizzazione, minore deve essere il tempo di RTO e RPO.
Tuttavia questa astrazione trova scarso riscontro nella realtà in quanto l'importanza di un processo e le conseguenze negative sull'organizzazione derivanti da una sua interruzione non sono costanti nel tempo, ma possono variare in funzione de: il giorno dell'anno e l'ora del giorno; l'avvicinarsi di una scadenza (fiscale, legale, contrattuale...); periodi di punta o chiusure stagionali o di manutenzione. Alcuni processi hanno scadenze imprescindibili anche nel corso di una singola giornata lavorativa e quindi anche RTO molto stringenti (ad esempio di 2 ore) non garantiscono un ripristino sufficientemente rapido se, per esempio, il fermo è avvenuto a un'ora da una scadenza fondamentale. Anche nel caso dell'RPO questo non dovrebbe essere definito genericamente, ma dovrebbe essere legato allo scenario di indisponibilità.
Per quanto riguarda gli RPO, essi potrebbero essere differenti per ciascun processo, ma questo potrebbe portare ad avere copie di dati non allineate.
Nella continuità operativa sono analizzati i rischi di continuità per prevenirli e mitigarne gli impatti. Pertanto i professionisti della continuità e quelli della gestione del rischio dovrebbero lavorare in modo sinergico, visto che si tratta di discipline che condividono un obiettivo comune: quello di preservare la salute e l'integrità fisica di dipendenti, clienti e terzi, salvaguardare i beni e la redditività, proteggere l'immagine dell'azienda e dei suoi prodotti.
È anche dimostrato che, quando le diverse funzioni partecipano sinergicamente alla creazione del BCP, sono in grado di evitare che si creino distorsioni nella progettazione dei piani di DR, Crisis management e Crisis communication.

8.9 Social network

Sono sempre di più le aziende che utilizzano i social network come canale di comunicazione (con i clienti in primis, ma anche fornitori, azionisti e investitori). I social network rappresentano infatti oggi i media più seguiti da parte di tutto il pubblico. A differenza dei media tradizionali, che prevedono un unico punto di controllo di tutto ciò che viene trasmesso, sui social network i messaggi giungono, spesso incontrollati, da molteplici fonti: la stessa organizzazione nel momento in cui vengono pubblicate comunicazioni o articoli, i collaboratori che si presentano in nome dell'organizzazione per cui lavorano o il pubblico che utilizza lo strumento dei commenti per trasmettere e rendere pubblici messaggi all'organizzazione stessa.

Le organizzazioni utilizzano diverse modalità, tutte valide, per usare questo mezzo di

comunicazione. Chi non ha una struttura interna dedicata si appoggia ad agenzie che si occupano di curare la comunicazione. Le più grandi utilizzano anche la voce dei dipendenti, chiamati *ambassador*, come strumento per aumentare le comunicazioni e come espediente per mostrare fedeltà da parte dei collaboratori.

Il primo rischio legato ai social network riguarda quindi la reputazione che l'azienda si costruisce, l'immagine cioè che l'azienda fornisce di se stessa attraverso tutto quello che è presente sui social network.
Non ci riferiamo solo all'attenzione di non pubblicare contenuti scandalosi, lesivi per la propria immagine perché palesemente negativi (violenza, incitamento all'odio, linguaggio volgare, ecc.). Il punto è costruire e mantenere una reputazione che sia in linea con il tono che l'organizzazione ha deciso di adottare nella sua comunicazione, che ci sia coerenza tra quello che viene comunicato e il codice etico, in modo da costruire e comunicare un'immagine integrata e coerente anche attraverso i social network.

È quindi bene che vengano definiti lo stile ed il tono comunicativo che l'azienda vuole mostrare. Va definito anche l'approccio che l'azienda vuole mantenere quando risponde a commenti o recensioni negative, per evitare di doverlo improvvisare durante un'emergenza.
Le agenzie, se usate per lavorare sui social in nome e per conto dell'organizzazione, potrebbero non essere strutturate per adottare queste indicazioni sullo stile comunicativo o coinvolgere correttamente gli ambassador.
La divulgazione di informazioni riservate è un altro rischio a cui si deve far fronte quando i collaboratori di un'organizzazione utilizzano i social network. Spesso una leggerezza o una disattenzione portano alla condivisione di informazioni riservate o piani strategici con il mondo intero.

Un possibile rischio tecnico è rappresentato dalla condivisione delle credenziali con cui si può accedere al profilo dell'organizzazione e che va ridotto al minimo. Questo avviene soprattutto se sono usate credenziali uniche per tutti i responsabili della comunicazione sui social network.

Da un punto di vista psicologico, si segnala il rischio di permettere al personale di usare le proprie credenziali personali per accedere ai social per conto dell'organizzazione. In questo caso, il rischio è che la persona non distingua più, seppur inconsapevolmente, le diverse modalità con cui comunicare (come persona singola o in nome dell'organizzazione) o proteggere le informazioni.

8.10 I rischi OT

Il sistema di controllo industriale (ICS, *industrial control system*, o IACS, *industrial automation and control systems*) comprende diversi tipi di sistemi di controllo utilizzati nella produzione industriale.
Si parla anche di sistemi OT (*operational technologies*), per distinguerli dai sistemi informatici o IT (*information technology*), dedicati alla gestione delle informazioni.
All'interno di questi termini generali sono racchiuse diverse sigle che rappresentano tecnologie dedicate con funzioni specifiche, di seguito le principali:

- sistemi di controllo distribuito (DCS) che monitorano e controllano grandi impianti come centrali elettriche e raffinerie;
- sistemi SCADA (supervisory control and data acquisition) che monitorano e controllano asset dispersi come reti elettriche, acquedotti o anche impianti industriali;
- controllori logici programmabili (PLC) che controllano i singoli processi e macchinari;
- unità terminali remote (RTU) che fungono da concentratori di dati;
- dispositivi da campo "intelligenti" (ICS IIOT), come sensori che misurano il processo (pressione, temperatura, livello, flusso, ecc.), analizzatori che monitorano i componenti chimici, azionamenti che aprono e chiudono le valvole o fanno partire e fermano motori.

In sostanza, un sistema di controllo industriale è un sistema composto da diversi sistemi, progettato per monitorare e controllare i processi fisici e garantire operazioni e produzioni sicure e automatizzate.
Per i sistemi IT, si valutano i rischi alla riservatezza, integrità e disponibilità (RID) delle informazioni. Nel mondo OT invece, gli aspetti più importanti sono quelli dell'affidabilità e della sicurezza delle persone.

Negli ultimi anni assistiamo all'evoluzione di molte organizzazioni che stanno facendo leva sulle conoscenze, sulle tecnologie e metodologie del mondo IT nei loro ambiente OT, al fine di trarre dei vantaggi competitivi. Sfruttano sistemi IT di analisi dei dati per elaborare le informazioni estratte dai sistemi SCADA e ICS IIOT. Questo sicuramente porta vantaggi e aumenta l'efficienza, ma aggiunge rischi.
Secondo l'"Electricity Grid Cybersecurity Report" del GAO[139], si possono individuare 4

139 Electricity Grid Cybersecurity. USA: GAO, Marzo 2021.

categorie di rischi informatici più importanti in ambito OT:

- Perdita di controllo e azioni indesiderate dei sistemi, guidati da persone non autorizzate.
- Blocco o distruzione di componenti fisiche operative. Attraverso un'operatività da remoto, gli attaccanti possono danneggiare fisicamente gli impianti, come è successo nel dicembre 2014, quando un attacco informatico ha portato all'arresto di un altoforno e quindi a danni fisici alle strutture di un'acciaieria tedesca[140].
- Mancanza di informazioni e visibilità sui processi industriali. Un attaccante, entrando nei sistemi di controllo, potrebbe potenzialmente nascondere lo stato dei processi. Questa condizione di Denial of Service (subita nel 2019 da un operatore del settore energetico americano[141]), pur impedendo al personale tecnico di monitorare la situazione, può avvenire senza effetti distruttivi e senza un blocco effettivo dei processi.
- Perdita di produttività e danni economici. Un blocco, dovuto ad esempio a un ransomware, può comportare per molti giorni il fermo della produzione, con danni economici rilevanti.

Altre caratteristiche esclusive degli ICS dal punto di vista della cybersecurity sono:

- Molti di questi sistemi hanno un'aspettativa di vita prevista tra i 10 ed i 25 anni. Le architetture e la stretta connessione con il processo controllato comportano che non possono essere aggiornati facilmente e non si possono installare patch in modo rapido ed automatico.
- Il personale deputato alla gestione dell'OT manca spesso delle competenze di cybersecurity considerate dominio di conoscenza dell'IT.
- Mancanza di attenzione da parte dei vertici dell'organizzazione e difficoltà a ottenere fondi per affrontare la cyber security in modo sistematico.
- Poca storia e casistica ufficialmente documentata sugli incidenti ai sistemi OT, soprattutto per la reticenza, da parte dei responsabili, a rendere pubbliche queste informazioni.

140 https://st.ilsole24ore.com/art/impresa-e-territori/2014-12-21/germania-cyberattacco-danneggia-l-altoforno-una-acciaie- ria-143554.shtml.

141 https://www.securityinfo.it/2019/05/03/attacco-dos-al-sistema-energetico-usa/.

8.11 I rischi degli edifici intelligenti

Figura 41 - Componenti di uno smart building[142]

E' doveroso domandarsi perché facciamo gli edifici intelligenti visto che questi implicano dei rischi di varia natura. I motivi sono principalmente due:

- **comfort sostenibile**: non siamo disposti a rinunciare al livello di comfort che abbiamo acquisito ma, allo stesso tempo, lo spreco è un "lusso" che non ci possiamo più permettere ;
- **miglioramento della qualità della vita**: l'automazione può aiutare le persone diversamente abili a sentirsi più autonome,

Più in dettaglio si possono elencare alcuni dei principali benefici dello *smart building*:

- ottimizzazione dell'efficienza energetica così da ridurre i costi e soprattutto l'impatto ambientale;
- miglioramento della cosiddetta user-experience: sia che si tratti di abitazioni, uffici o servizi pubblici, si può aumentare il livello di comfort e di vivibilità con l'uso della tecnologia, ad esempio con smart-devices con capacità di realtà aumentata

142 Fonte immagine: https://www.worktechacademy.com/smart-ecosystem-secrets-successful-smart-building/

o intelligenza artificiale;
- avere costantemente la corretta illuminazione, la temperatura ottimale, ecc.;
- mobilità intelligente negli edifici;
- monitoraggio continuo per rilevare incendi, allagamenti, eventuali cedimenti, ecc.
- sicurezza degli accessi fisici.

La valutazione dei rischi deve considerare:
- il sistema di automazione;
- la tipologia di edificio;
- la tipologia di utenza/servizio;
- il grado di connessione dell'automazione a reti esterne (IoT).

Cominciamo con un esempio banale, ovvero, la luce delle scale di un condominio. L'automazione, in questo caso, viene installata in un'ottica di "ritardo all'off". Ovvero, il sistema automatizzato eroga il servizio quando vi è una richiesta da parte dell'utenza e, automaticamente, dopo un certo lasso di tempo, se l'illuminazione non viene spenta manualmente, il servizio di erogazione viene interrotto fino alla prossima richiesta di attivazione (p.e. tramite la pressione di un pulsante). Se non ci fosse questa semplice automazione la luce probabilmente rimarrebbe sempre accesa 24 ore su 24. Tuttavia, l'automazione, implementata per ottimizzare il consumo energetico, può generare dei rischi connessi a un suo malfunzionamento in grado di generare dei disservizi, quali ad esempio la mancanza di illuminazione delle scale per più di una notte o un impianto di illuminazione "sempre acceso": in entrambi i casi si tratta di un rischio "accettabile". La situazione sarebbe ben diversa se il malfunzionamento si verificasse in un sistema automatizzato di evacuazione dei fumi di scarico di un parcheggio sotterraneo, dal momento che tale sistema gestisce il ricambio di aria in base alla presenza di gas tossici generati dalle auto in movimento, regolando ventilatori che sono molto energivori. In caso di malfunzionamento, i conducenti sono esposti al rischio di avvelenamento da monossido di carbonio, assolutamente da evitare. Pertanto, viene predisposto un sistema di emergenza meccanico indipendente per evitare la presenza di un SPF (*single point of failure*).

Di seguito alcuni esempi di rischi relativi agli smart building:
- **Rilevazione dei fumi** – l'automatizzazione di questa funzionalità è particolarmente critica e implica un monitoraggio continuo del funzionamento attraverso controlli funzionali periodici.
- **Illuminazione automatizzata** in caso di persone diversamente abili, RSA (residenze sanitarie per anziani) e social housing – L'accensione delle luci, in presenza di persone diversamente abili, menomate o paralizzate, deve essere garantita anche tramite comandi vocali (tipologia di automazione alternativa – fail over).

- **Connessioni con reti esterne**, per cui si devono considerare i rischi relativi al cloud e all'IoT. E' necessario verificare se la connettività non è necessaria al buon funzionamento dell'automazione o, invece, è fondamentale. In questo ultimo caso è necessario valutare i rischi di affidabilità dell'impianto e di sicurezza dei dati presenti in rete e l'adozione di soluzione di continuità operativa.

E' doveroso sottolineare come l'analisi dei rischi connessi agli smart building sarà sempre più necessaria a fronte dell'introduzione dell'Indice di prontezza all'intelligenza degli edifici (SRI - smart readiness indicator), introdotto dalla direttiva EU 2018/844/UE (EPBD III, Energy performance of buildings Directive III) e attuata dal Dlgs.48/2020. Esso molto probabilmente in futuro affiancherà l'APE (Attestato Prestazione Energetica). L'SRI valorizza un edificio a seconda del suo livello di intelligenza e connettività.

Figura 42 - Le 3 principali funzionalità dell'SRI

8.12 Mobile

I rischi in ambito mobile sono particolarmente rilevanti, a causa del crescente numero di dispositivi venduti (principalmente smartphone, come riportato in Figura 43) e di utenti di tali dispositivi (Figura 44).

Figura 43 - Numero di smartphone venduti nel mondo, dal 2007 al 2021[143]

143 https://www.statista.com/statistics/263437/global-smartphone-sales-to-end-users-since-2007/.

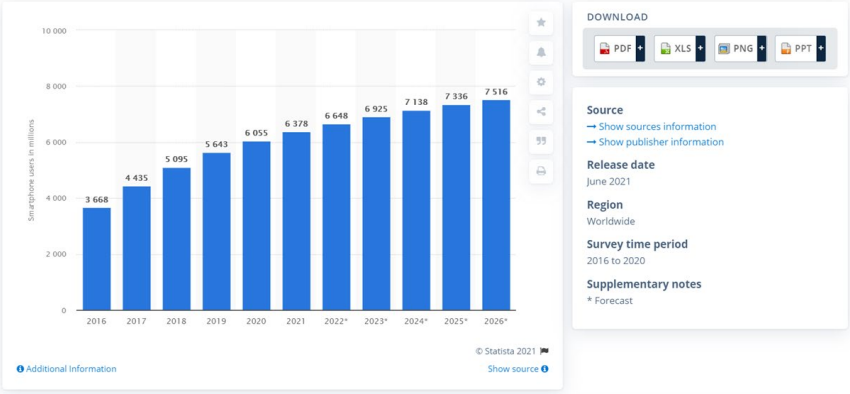

Figura 44 - Crescita del numero di utenti di smartphone, dal 2016 al 2021[144]

Tenuto conto del fatto che, di solito, un dispositivo mobile contiene i dati personali del proprietario, oltre ad alcuni dati relativi ai suoi contatti, si capisce come sia cresciuto nel tempo il numero di tentativi di prendere il controllo di tali dispositivi, ad esempio proponendo all'utente di installare una applicazione malevola (Figura 44).

Figura 45 - Numero di pacchetti di installazione malevoli individuati, dal 2Q 2019 al 2Q 2020[145]

D'altra parte, fortunatamente, nel corso degli anni si sono evoluti anche gli strumenti di analisi delle minacce e delle vulnerabilità. Come si può vedere in Figura 45, questo miglioramento nell'efficacia degli strumenti di analisi si traduce nel fatto che il numero di attacchi sembra essersi assestato su un trend costante, anziché crescere.

144 https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/.

145 https://securelist.com/it-threat-evolution-q2-2020-mobile-statistics/98337/.

Figura 46 - Numero di attacchi a dispositivi mobili, dal 1Q 2019 al 2Q 2020[146]

Analizzando lo scenario attuale, possiamo affermare che, oggi, ogni essere umano ha sempre con sé un dispositivo mobile, di giorno e di notte, ovunque si trovi. A questa osservazione possiamo aggiungere le seguenti considerazioni:

- i dispositivi mobili utilizzano diversi meccanismi di comunicazione (tramite SIM, Bluetooth, NFC, Wi-Fi, GPS, ecc.), sono ricchi di funzionalità (autenticazione biometrica, sensori, e molto altro) e hanno alcune caratteristiche - come ad esempio i dati presenti nelle memorie di massa, o la possibilità di sincronizzare i contenuti con il PC via cavo - che li rendono un bersaglio estremamente appetibile per un potenziale attaccante;
- eventuali attacchi possono portare alla compromissione di messaggi e comunicazioni, registrazioni audio, immagini e video, informazioni di localizzazione, dati personali e documenti memorizzati, backup e piattaforme cloud, history e cronologia, e sistemi di autenticazione.

Relativamente agli impatti, è da ricordare che oggi i dispositivi mobili sono diventati essenziali per lo smart working.

Owasp Top 10 Mobile Risks indica i seguenti dieci rischi per il Mobile[147]:

- **M1** - Utilizzo improprio di una funzionalità del dispositivo, o mancato utilizzo dei controlli di sicurezza;
- **M2** - Archiviazione non sicura dei dati, come l'accesso a un dispositivo smarrito o rubato, l'accesso alla memoria da parte di applicazioni non sicure, ecc.;
- **M3** - Intercettazione delle comunicazioni e degli scambi di dati, ad esempio nelle applicazioni client-server;

146 https://securelist.com/it-threat-evolution-q2-2020-mobile-statistics/98337/.

147 https://owasp.org/www-project-mobile-top-10/.

- **M4/6** – Autenticazione o autorizzazione non sicura: sfruttamento delle vulnerabilità di autenticazione o autorizzazione attraverso attacchi automatizzati;
- **M5** - Crittografia non adeguata (ad esempio, utilizzo di protocolli crittografici obsoleti o non robusti), non applicata o applicata in maniera parziale;
- **M7/8/9/10** - Vulnerabilità legate alle applicazioni: ad esempio, scarsa qualità del codice, presenza di codice malevolo, gestione non sicura dell'autenticazione e delle sessioni.

La guida NIST SP 800-124 per la gestione della sicurezza dei dispositivi mobili nelle imprese[148] individua i seguenti rischi:

- sfruttamento delle vulnerabilità dei dispositivi, spesso tramite applicazioni scaricate e installate dagli utenti;
- perdita e furto del dispositivo, facilitata dalle caratteristiche intrinseche dei dispositivi mobile, quali il fatto che sono portatili e di dimensioni ridotte;
- accesso alle risorse aziendali con dispositivi configurati in modo non sicuro, sia a livello di sistema operativo che a livello di applicazioni utilizzate;
- furto di informazioni tramite phishing, ancora più grave ora che i dispositivi sono spesso utilizzati per l'autenticazione multifattoriale, usando token, SMS, o altro;
- installazione di certificati non sicuri, che possono in cascata generare ulteriori problemi di sicurezza, come ad esempio l'installazione di applicazioni non sicure;
- utilizzo di dispositivi non autorizzati, nel caso in cui l'organizzazione non utilizzi sistemi di network access control, oppure nel caso in cui vengano utilizzati dispositivi rooted o jailbroken;
- intercettazione delle comunicazioni, facilitata dai servizi di connettività presenti su tutti i dispositivi, ad esempio tramite Wi-Fi o Bluetooth;
- presenza di malware, facilitata dalla semplicità di installazione di applicazioni anche provenienti da terze parti non certificate;
- errata configurazione delle funzionalità di sicurezza del dispositivo, come avviene nel caso della scelta di PIN troppo semplici, oppure di notifiche a schermo visibili anche quando il dispositivo è bloccato;
- violazioni della privacy a causa di un uso errato dei sistemi, delle app o dei social network;
- perdita di dati a causa di problemi di sincronizzazione, causati anche dalla connessione di dispositivi dell'organizzazione (sicuri) con dispositivi personali (non sicuri);
- Shadow IT, ovvero utilizzo contemporaneo di dispositivi dell'organizzazione e personali: ad esempio, e-mail di lavoro configurata e letta sul telefono dell'orga

148 https://csrc.nist.gov/publications/detail/sp/800-124/rev-2/draft.

nizzazione e su quello personale;
- sfruttamento di vulnerabilità derivanti da errori di configurazione;
- errori nella gestione delle utenze e dei privilegi di amministrazione.

Per quanto riguarda MITRE[149], è bene precisare che si tratta di un framework molto ampio, che tratta tecniche di attacco anche molto diverse tra loro, molte delle quali coincidono con quelle elencate sopra. Senza approfondire ulteriormente è bene sottolineare che alcuni attacchi possono essere portati a termine anche senza avere un accesso diretto al dispositivo, ad esempio operando attraverso le reti di comunicazione e i servizi. Fanno parte di questa categoria, ad esempio, le intercettazioni delle comunicazioni non crittografate tra server e dispositivi mobili e il reindirizzamento di chiamate e di SMS, tecniche di jamming o di DoS.
Negli attacchi verso i servizi, anziché violare un dispositivo si prova a violare i servizi da esso utilizzati, come ad esempio il sistema di Mobile Device Management che lo gestisce o il servizio in cloud dove sono memorizzate le informazioni di backup. La morale che ne possiamo trarre è che la protezione dei dispositivi mobili passa necessariamente per la messa in sicurezza delle reti e dei servizi ad essi collegati.
Un ulteriore rischio è legato al fatto che i meccanismi di multi factor authentication (MFA) sono sempre più spesso implementati nel dispositivo e permettono l'accesso a servizi critici come l'home banking e VPN aziendali.

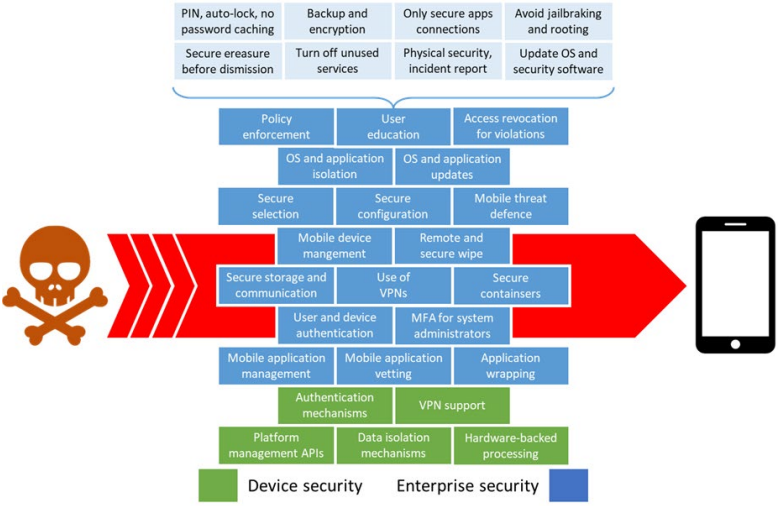

Figura 47 - Ambiti relativi all'analisi dei rischi legati al mobile[150]

149 https://attack.mitre.org/tactics/mobile/.

150 Fonte e copyright: SERNET S.p.A.

8.13 I rischi nelle applicazioni

La sicurezza applicativa (application security) è un concetto ampio, che include diversi aspetti che vanno oltre la qualità e la sicurezza del codice applicativo: in particolare, comprende temi quali l'organizzazione dei processi di sviluppo, le soluzioni e le tecnologie adottate, e la sicurezza delle architetture e degli ambienti applicativi (considerando quindi reti, sistemi, dispositivi, apparati, servizi, ambienti, ecc.).
L'adozione di un processo di sviluppo adeguato riduce il rischio di dover correggere vulnerabilità o difetti, i cui costi aumentano quanto più tardi queste criticità vengono identificate, come illustrato in Figura 47.

Figura 48 - Aumento dei costi di risoluzione delle vulnerabilità, in funzione dell'avanzamento nelle fasi di sviluppo dell'applicativo[151]

I rischi legati agli applicativi sono numerosi e si possono identificare in vari contesti, che vengono riportati di seguito.
Partendo dai rischi legati alla **qualità dell'applicativo**, abbiamo rischi quali:

- incapacità di confermare (commit) o rifiutare in toto (rollback) una transazione;
- incapacità di prevedere tutti gli effetti di una transazione sui dati;
- assenza di conferme intermedie;
- indisponibilità (timeout) di componenti applicative o tecnologiche.
- In sede di sviluppo del software i rischi più rilevanti sono quelli legati a:
- mancata identificazione dei rischi e delle contromisure;
- competenze carenti degli sviluppatori sulle buone pratiche di sviluppo interne e stabilite sulla base di specifici standard (come OWASP, MITRE, CWE, ecc.);
- utilizzo di software di terze parti o di librerie non sicure perché obsolete o vulnerabili;
- mancato controllo dello sviluppo software affidato a terzi (non comunicazione dei requisiti di sicurezza, dei criteri di accettazione del software e della attribuzione di licenze e diritti di proprietà del codice);

151 Fonte e copyright: SERNET S.p.A.

- insicurezza degli ambienti di sviluppo, test e produzione (perché non separati o senza adeguate autorizzazioni, backup, log, controllo delle versioni del codice).

I principali rischi legati al **test del software** riguardano invece:

- inefficacia delle attività di test perché non adeguatamente pianificate o documentate, senza la verifica dei requisiti di sicurezza, eseguiti in un ambiente non realistico,non accompagnati da vulnerability assessment, penetration test o code review;
- gestione inadeguata dei dati di test, specie quando si tratta di dati personali o copie reali delle informazioni di produzione (in ambienti di test, sviluppo e produzione non separati, senza adeguate procedure di controllo degli accessi all'ambiente di test, di raccolta dei log; di anonimizzazione, di cancellazione dopo il completamento dei test).

In sede di **rilascio del software**, i rischi possono derivare da:

- passaggio in ambienti di produzione senza il superamento dei test di sicurezza;
- mancata adozione di un processo controllato di rilascio del software in ambiente di produzione.

Vi sono poi i rischi legati al **software sviluppato**, che possono essere tratti da pubblicazioni come "OWASP Top 10 Web Application Risk"[152] e "OWASP API Security Project"[153] e da librerie di vulnerabilità come MITRE, CWE, CVE, CAPEC, ecc.

8.14 Big data e analytics

Tutte le organizzazioni raccolgono e archiviano enormi quantità di dati grezzi, siano essi dati strutturati o non strutturati. Considerandone l'enorme quantità, si parla di Big data.

I rischi legati alla gestione dei big data sono indicati nel seguito:

- **Mancato controllo degli accessi**. L'estrema eterogeneità delle fonti dati e dei meccanismi di analisi può portare a ribaltare facilmente il principio del "need to know" (si punta a consentire l'accesso alle sole informazioni necessarie all'utente per lo svolgimento delle proprie mansioni) generando il rischio di un eccesso di disponibilità di dati agli utenti.

152 https://owasp.org/www-project-top-ten/.

153 https://owasp.org/www-project-api-security/.

- **Dark data**. Per una gran parte di dati non strutturati - immagini, video, conversazioni – si può perdere visibilità e controllo. Questi sono detti dark data e alcune statistiche parlano già di una loro sovra-presenza[154].
- **Errata interpretazione dei dati**. La stratificazione delle elaborazioni dei dati e l'interpretazione possono portare ad aggregazioni e sintesi informative che espongono al rischio di errata interpretazione.
- **Errori negli analytics**. I big data da soli non rappresentano un valore. Serve aver sviluppato algoritmi che trasformano i dati in informazioni rilevanti (analytics). Errori nello sviluppo degli analytics possono portare a una cattiva interpretazione dei dati e quindi a decisioni sbagliate.
- **Rischio economico**. I costi legati alla manutenzione dei dati possono crescere rapidamente. Sono infatti richiesti storage, procedure di data retention conformi alle norme, processi di sicurezza e backup, accesso sicuro ai dati, personale competente e dedicato. Il tema è verificare che questo costo sia superato dai vantaggi economici.
- **Cattiva qualità dei dati**. La cattiva qualità dei dati può pregiudicare fin dall'origine il loro successivo utilizzo (ad esempio si pregiudica l'efficacia dei successivi modelli predittivi e delle analisi). In questi casi si usa il termine GIGO (garbage-in, garbage-out) per descrivere il concetto di risultati di cattiva qualità derivanti dall'analisi di dati di cattiva qualità.
- **Rischio di violazioni dei dati personali.** L'enorme quantità dei dati espone gli stessi a possibili accessi indesiderati, distruzione, esfiltrazione. Questo può avere impatti negativi, dalla perdita economica, al danno reputazionale, alla possibilità di incorrere in sanzioni per il mancato rispetto delle principali norme, soprattutto a quella relativa ai dati personali (GDPR). Anche dati anonimizzati possono essere usati per risalire all'identità degli utenti (così come ad altre informazioni teoricamente cancellate dal database) attraverso attività di correlazione fra dati apparentemente spuria.
- **Rischi legati a procedure automatizzate o all'IA**. Una persona o un gruppo di persone possono non essere in grado di gestire uno o più enormi database attraverso procedure automatizzate. Questo potrebbe introdurre errori nella lettura e interpretazione dei dati.

154 https://siliconangle.com/2015/10/30/ibm-is-at-the-forefront-of-insight-economy-ibminsight/.

8.15 Settore sanitario

Il PDTA (percorso diagnostico-terapeutico-assistenziale) è ad oggi fortemente digitalizzato sia nel percorso di medicina generale che ospedaliero. Il processo di cura del paziente parte dall'ipotesi di diagnosi, passa attraverso la gestione della terapia e prosegue nelle fasi di assistenza (anche domiciliare) e di follow-up. I software che regolano questo percorso sono cruciali non solo per l'ottimizzazione delle tempistiche, ma anche per la corretta diagnosi e l'erogazione della terapia più adeguata, nelle tempistiche più opportune.

Il Regolamento 2017/745 (MDR), già presentato al paragrafo 6.11, sui dispositivi medici è stato corredato da una specifica linea guida "MDCG 2019-16" che richiama principi di tutela dei dati in ottica privacy e cyber security, e che fornisce indicazioni su come integrare la gestione del rischio relativo alla sicurezza dei dati nella gestione del rischio relativo al dispositivo medico. Questo richiede, a cura dei progettisti della tecnologia sanitaria, l'individuazione dei rischi clinici collegati ai rischi relativi alla sicurezza dei dati; il processo di gestione e mitigazione del rischio clinico, inoltre, agisce per evitare che soluzioni tecniche per la mitigazione dei rischi relativi alla sicurezza dei dati impattino negativamente sulla sicurezza del paziente. Un esempio classico è quello della necessità di bilanciare l'accesso al dato regolato via password con l'immediata disponibilità di dati e funzioni in caso di emergenza o urgenza clinica. Un defibrillatore non deve certo richiedere una password per essere attivato!

Dal punto di vista della gestione dei rischi, la norma di riferimento ISO 14971:2019 e la guida per la sua applicazione, ISO/TR 24971:2020, presentano una sezione specifica sulla sicurezza dei dati, vista in ottica di sicurezza clinica.
All'interno del mondo dei dispositivi medici i rischi sono molteplici e possono dipendere principalmente dalla natura tecnologica del dispositivo, nonché dagli impatti del dispositivo sul percorso di salute del paziente.

Esempi di conseguenze associabili a un'applicazione per dispositivi mobili sono:

- Terapia errata, causata per esempio da:
  - Progettazione del dispositivo non basata su prove cliniche robuste: il dispositivo potrebbe essere stato progettato facendo riferimento solamente all'esperienza di uno o più esperti clinici.
  - Problemi di cybersecurity: la compromissione dei dati può portare a situazioni pericolose, modificando il percorso terapeutico del paziente e potenzialmente arrecandogli un danno di salute.

  - ► Errori del paziente: una cattiva usabilità dell'interfaccia potrebbe portare all'introduzione di errori utente che possono portare ad ulteriori situazioni pericolose quali ad esempio perdita dei dati o messa a disposizione dei medici di dati inaffidabili o corrotti.
- Mancato beneficio a causa dell'interruzione della terapia perché percepita come troppo complessa o troppo invadente.
- Rischio di epilessia: questo rischio ricade nei rischi intrinseci relativi alla tecnologia, in quanto basato sulla trasmissione di informazioni visive su schermo.

Oltre a questi rischi, va considerato quello di non conformità e il fatto che il settore sanitario è oggi particolarmente preso di mira dai cyber criminali, per lo più a scopo di lucro, con l'uso di ransomware o la raccolta di dati dei pazienti.
I rischi possono essere categorizzati come nella tabella seguente, considerandone la macro categoria di perdita di integrità, disponibilità e riservatezza e gli impatti:

- sui pazienti e sul percorso diagnostico-terapeutico-assistenziale;
- sul sistema sanitario pubblico.

	Impatti sul PDTA	Impatti sulla sanità
Perdita di integrità	• Dati incompleti per giungere a diagnosi; • Errori di terapia; • perdita di storico di terapia; • perdita di informazioni sull'aderenza terapeutica; • patient mixup; • utilizzo di dati da diversi fonti non compatibili e conseguenti errate trasformazioni del dato; • errata configurazione orario con conseguente perdita della consequenzialità delle decisioni; • interruzione PDTA per impossibilità di identificare il paziente oppure irrintracciabilità dei dati; • errori nei macchinari e conseguenti ritardi.	• Comportamenti inaspettati del sistema, incluso il blocco; • dati incompleti per manutenzione o usura della macchina; • dati errati per le prestazioni e lo stato operativo; • perdita della rintracciabilità delle prestazioni; • errata assegnazione di esami ai pazienti; • perdita della sincronizzazione dello storico dati.

Perdita di disponibilità	• Incapacità di diagnosi (in situazioni di urgenza); • dati non integrati per giungere a diagnosi; • prescrizione di farmaci a cui il paziente è allergico oppure prescrizione incoerente tra terapia domiciliare e terapia ospedaliera; • rischi di assistenza non coordinata tra ospedale-territorio-medico di base; • mancato coinvolgimento del professionista per mancanza del servizio e interruzione del percorso.	• Impossibilità di pianificare le attività e l'occupazione delle macchine e necessità di manutenzione straordinaria; • impossibilità di pianificare la manutenzione ordinaria e straordinaria delle macchine; • incapacità di proseguire con le attività cliniche.
Perdita di riservatezza	• Violazione dei dati e condivisione di dati personali sanitari; • condivisione con figura professionale errata del percorso terapeutico.	• In caso di diffusione di dati, danno di immagine e economico e calo della fiducia nel servizio.

L'approccio afap (as far as possible) alla mitigazione del rischio, previsto nel Regolamento europeo, costringe il progettista alla analisi di impatto di tutte le mitigazioni tecnicamente disponibili. In particolare il processo richiede l'implementazione in ordine di priorità di:

- utilizzo di soluzioni progettuali intrinsecamente sicure;
- utilizzo di allarmi e protezioni;
- informazioni di sicurezza (avvertenze, precauzioni, controindicazioni) e formazione degli operatori e degli utenti.

Bisogna fare anche attenzione che le soluzioni di sicurezza (controllo degli accessi, cifratura e anonimizzazione) non introducano ulteriori rischi clinici legati alla non disponibilità del dato.
Si segnala la mancanza di una standardizzazione delle piattaforme software a livello nazionale o internazionale. Essa ha come conseguenza la frammentazione delle soluzioni e problemi di progettazione e di qualità delle soluzioni software utilizzate. Si segnalano, come standard oggi disponibili:

- **IEC 62304** per il software incluso nei dispositivi medici;
- **IEC 82304** per il software per la salute;
- **MDCG 2019-16** per l'inclusione delle soluzioni di cybersecurity nei dispositivi medici.

8.16 I rischi del 5G

Il 5G si pone diversi obiettivi ad alto impatto economico-sociale (sono i cosiddetti "obiettivi cardine"), i quali saranno auspicabilmente raggiunti mediante il rispetto dei requisiti tecnici determinati da ITU, 3GPP e 5GPPP: esemplificativamente si pensi alle smart cities, alla medicina di precisione, alle evoluzioni dell'Internet of Things, all'abbattimento delle distanze e alla possibilità di ridurre l'impatto energetico attraverso l'integrazione delle differenti tipologie di energie rinnovabili.
Tuttavia, oltre ai molteplici fattori positivi, è importante porre attenzione sulle criticità e i rischi di cyber security e protezione dei dati personali connessi a tale evoluzione tecnologica. La nuova architettura e infrastruttura di rete decentralizzata, lo smart computing ai margini della rete e una sempre più stretta dipendenza dai software incrementano le superfici di attacco e i punti di accesso sfruttabili dal cybercrime.
È necessario, pertanto, analizzare compiutamente i rischi del contesto sopra delineato, soprattutto per garantire un adeguato livello di sicurezza delle reti di quinta generazione, senza vanificare i molteplici aspetti positivi che ne potranno derivare.
A tal fine, l'UE nel dicembre 2019 ha istituito il NIS Cooperation Group, gruppo di lavoro dedicato all'analisi dei rischi impattanti sulle reti 5G all'interno dell'Unione. Questi, anche mediante il supporto dell'ENISA, nel gennaio 2020 ha pubblicato il "5G toolbox"[155], documento contenente le prime linee guida per ogni Stato membro e preliminari valutazioni in merito agli scenari di rischio al fine di costruire un comune framework di analisi e misure di mitigazione volte alla prevenzione e gestione delle minacce cyber correlate alle reti 5G.
Oltre a tali preliminari valutazioni e seguendo l'evoluzione delle implementazioni tecniche, nel corso degli ultimi 2 anni ENISA ha elaborato ulteriori documenti relativi all'analisi dei rischi e delle minacce connesse al 5G.

All'interno degli stessi, l'Agenzia individua dapprima i maggiori scenari di rischio, ripartendoli in cinque categorie; nello specifico:

- insufficienti misure di sicurezza (configurazione errata delle reti e mancanza di controlli degli accessi);
- catena di approvvigionamento del 5G (scarsa qualità dei prodotti e dipendenza da singoli fornitori all'interno di singole reti o mancanza di diversificazione su base nazionale);
- modus operandi dei principali attori delle minacce (interferenza statale attraverso la catena di approvvigionamento del 5G e sfruttamento delle reti 5G da parte della criminalità organizzata o di gruppi criminali che mirano a colpire gli utenti

155 https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

finali);
- interdipendenze tra le reti 5G e altri sistemi critici (perturbazione significativa di infrastrutture o servizi critici e guasti di rete gravi e generalizzati causati dall'interruzione della fornitura di energia elettrica o di altri sistemi di supporto);
- dispositivi degli utenti finali (sfruttamento dell'IoT e di dispositivi mobili o intelligenti).
- Successivamente, adottando una metodologia di analisi fondata sugli asset, vengono determinate le potenziali superfici di attacco; queste, attraverso una categorizzazione di alto livello, sono distinte in tecniche e non tecniche (quali, esemplificativamente, risorse umane, processi e policy).

Le superfici di attacco "tecniche" sono in particolare minacce a:
- **elementi generici**: minacce che in genere colpiscono qualsiasi sistema o rete ICT, importanti poiché aiutano a definire e inquadrare quelle specifiche del 5G (denial of service, data breach, data leak, distruzione o manipolazione di dati, software o hardware exploitation, codici malevoli, abuso delle credenziali di accesso, furto di identità o spoofing);
- **infrastrutture fisiche**: minacce all'infrastruttura IT che supporta la rete 5G (attacchi fisici, danni o perdita di apparecchiature, guasti o malfunzionamenti delle apparecchiature, interruzioni dei servizi, disastri naturali o sabotaggi dolosi);
- **core e software defined network**: minacce agli elementi della rete centrale 5G (abuso degli accessi e delle credenziali di autenticazione, API's exploitation, sfruttamento di vulnerabilità per erronea configurazione di rete, memory scraping, manipolazioni del traffico di rete, dei dati e information gathering, sniffing e side-channel attack);
- **access network**: minacce verso la tecnologia radio e wireless di accesso al 5G (abuso dei protocolli e dello spettro di rete, poisoning e flooding attack, jamming, spoofing, hijacking, manipolazione ed interferenze nella comunicazione radio e wireless);
- **multi-edge computing**: minacce verso i componenti "ai margini" della rete, quali gateway e dispositivi degli utenti (man-in-the-middle, edge node overload e API's exploitation);
- **virtualization**: minacce connesse alla virtualizzazione dell'infrastruttura di rete e delle funzioni IT sottostanti (abuso dei protocolli di rete, denial of service, abuso delle risorse cloud e sfruttamento delle vulnerabilità di rete).

Quanto sinora esposto rappresenta solo un sunto dell'attuale panorama in materia, stante anche la non completa realizzazione delle reti 5G (e delle sue applicazioni) su scala globale e la costante evoluzione dei requisiti tecnici che andranno a comporre successivamente il quadro definitivo.

9. Prodotti per l'analisi dei rischi

Ogni azienda può strutturarsi in vari modi per gestire l'analisi dei rischi, purché il processo risulti documentato e ripetibile. Ciò significa che non è importante quale strumento venga utilizzato (carta e penna, un documento di testo, un foglio elettronico o uno strumento specializzato), quanto il fatto che venga seguito un processo rigoroso.
Nel momento in cui il processo di analisi diviene particolarmente approfondito e tratta una grande quantità di informazioni, l'utilizzo di strumenti non automatizzati comporta un crescente (e tendente all'insostenibile) costo di gestione.
Esiste una vasta gamma di prodotti, alcuni più evoluti e strutturati, altri simili a fogli elettronici, con l'obiettivo di raccogliere dati per realizzare un'analisi del rischio fondata su dati oggettivi. Uno degli aspetti più rilevanti degli strumenti più evoluti riguarda la possibilità di creare scenari ed effettuare simulazioni, in modo da poter valutare l'impatto delle possibili misure di mitigazione e riduzione dei rischi.
A puro titolo indicativo, e senza volontà alcuna di promuovere o privilegiare alcuno strumento, sono brevemente descritti di seguito alcuni strumenti, in modo da potersi fare un'idea di quali siano le funzionalità più utili per le proprie esigenze e per valutare il prodotto più adatto alle proprie esigenze.

9.1 Funzionalità

Vi possono essere diversi approcci e quindi funzionalità di uno strumento per l'analisi del rischio, che dipendono essenzialmente dagli obiettivi definiti dall'organizzazione e dalla sua strutturazione.
Nella descrizione seguente cercheremo di elencare le funzionalità in un modo strutturato che tenga conto dell'approccio all'analisi del rischio e che quindi aiuti un'organizzazione a identificare le funzionalità necessarie.

- Stabilire il contesto:
  - definizione del perimetro di analisi;
  - dimensioni dell'ambito (numero di dipendenti, sedi, fatturato, ecc...);
  - identificazione delle localizzazioni geografiche e delle attività;
  - identificazione dei processi;

- ► identificazione degli asset e le loro relazioni, anche con i processi;
- ► identificazione delle implementazioni a livello infrastrutturale dell'azienda (es. autenticazione, disaster recovery, SIEM);
- ► identificazione dell'infrastruttura di sicurezza implementata (firewall, antivirus, disaster recovery, ecc...);
- ► identificazione delle politiche di sicurezza.

• Identificazione, analisi e ponderazione dei rischi:
- ► identificazione delle minacce e vulnerabilità;
- ► esempi di rischi per i processi basilari per i principali segmenti di mercato;
- ► assegnazione di pesi ai vari aspetti analizzati (probabilità e conseguenze);
- ► possibilità di aggiungere o personalizzare i rischi già presenti nello strumento;
- ► possibilità di analizzare i dati a livello di asset e di processo;
- ► acquisizione delle configurazioni dei sistemi di sicurezza (es. firewall, strumenti di sicurezza, autenticazione, policy).

• Classificazione dei rischi:
- ► classificazione dei rischi in base alla tipologia di rischio e al livello di rischio;
- ► possibilità di classificare il rischio in base al framework utilizzato;
- ► possibilità di personalizzare l'analisi effettuata.

• Definizione delle priorità:
- ► identificazione delle priorità di intervento;
- ► possibilità di eseguire analisi di simulazione "what if" in modo da definire in modo più ragionato le priorità di intervento.

• Trattamento del rischio:
- ► definizione di un piano di trattamento del rischio (accettazione, mitigazione, aumento, condivisione, ecc.);
- ► identificazione del rischio atteso dopo le azioni volte a modificare il rischio;
- ► definizione di un piano di controllo delle azioni (individuazione di responsabili e scadenze).

• Monitoraggio del rischio:
- ► possibilità di eseguire in modo semplice (possibilmente automatico o eventualmente manuale) analisi del rischio successive e periodiche in modo da evidenziare sia l'evoluzione dei rischi individuati che l'occorrere di nuovi rischi;
- ► possibilità di integrazione con sistemi come i SIEM ed i tool di vulnerability assessment.

9.2 Prodotti

Di seguito sono descritti alcuni prodotti per l'analisi del rischio presenti sul mercato. L'elenco non è esaustivo e ulteriori soluzioni sono state censite da ENISA[156].

9.2.1 AgID Cyber risk management

AgID ha predisposto un tool di cyber risk management che consente a ogni PA di effettuare le operazioni di self assessment, predisporre gli opportuni piani di trattamento e mantenere il monitoraggio delle iniziative intraprese ai fini di ridurre il livello di rischio.
Il tool è accessibile in modalità web[157].
Le fasi sono le seguenti:

- definizione delle caratteristiche, primarie e secondarie, del servizio e assegnazione del profilo di criticità allo stesso;
- valutazione dei possibili impatti derivanti dalla perdita di RID (riservatezza; integrità; disponibilità) legata ad aspetti di carattere economico, reputazionale, legale e operativo;
- identificazione delle minacce, dei controlli di sicurezza e calcolo dei livelli di rischio;
- predisposizione del piano di trattamento;
- monitoraggio del rischio nel tempo.

Il processo di self assessment può avvenire secondo due modalità distinte, a scelta dell'utente in fase di avvio della procedura:

- per servizio: ogni fase del processo, dall'assegnazione del profilo di criticità all'analisi del rischio, viene effettuata su tutti i servizi; la PA risponde ai controlli di sicurezza previsti dal tool e declinati su ciascun servizio;
- per PA (procedura semplificata): l'amministrazione risponde ai controlli di sicurezza previsti senza fornire le indicazioni specifiche per servizio.

Le due modalità, che devono essere considerate come possibili successivi livelli di

156 https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools.

157 https://www.sicurezzait.gov.it/cyber/.

avvicinamento alla gestione del rischio, offrono gradi di attendibilità differenti:

- l'esecuzione dell'assessment per servizio porta a risultati di alto profilo di attendibilità;
- la modalità di assessment per PA, più agevole e veloce, offre risultati con un grado di attendibilità minore, in quanto opera sui dati aggregati e a un livello di approssimazione maggiore.

9.2.2 AI4 REDFLAGS by ARISK®

È una piattaforma software sviluppata da ARISK S.r.l, spin off universitario del Politecnico di Torino per il settore pubblico e privato.
Il software si basa su un algoritmo di calcolo proprietario, basato sul machine learning, per l'analisi predittiva dei rischi.
Obiettivo del software è fornire un cruscotto con le criticità determinate dai rischi di cybersecurity, ambientali, sociali, di governo, di continuità, di sicurezza fisica.

9.2.3 Galvanize

Galvanize è una soluzione per l'ERM.

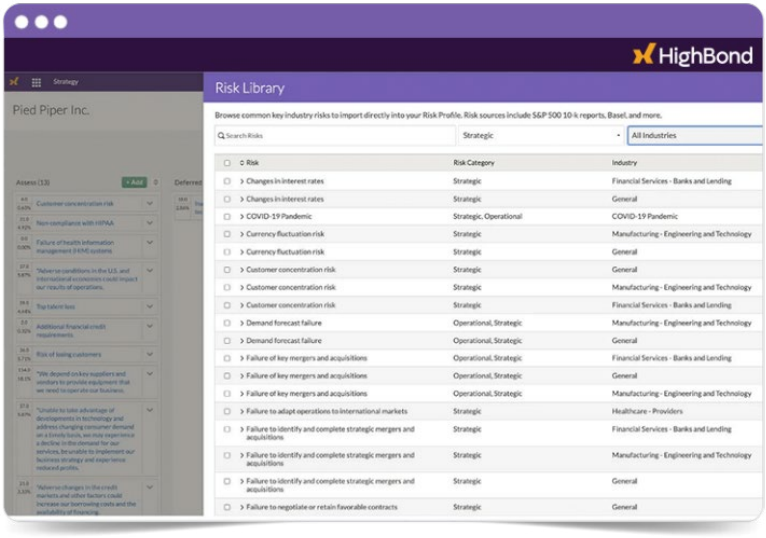

Figura 49 - Un'interfaccia di Galvanize

Essa permette di configurare best practice, framework e standard normativi di riferimento e specifici del settore e utilizza librerie di controlli e rischi per facilitare il lavoro. Il tool permette di indicare le opzioni di trattamento del rischio e dimostrare la conformità ai più noti standard.

9.2.4 IBM OpenPages with Watson

IBM OpenPages with Watson è una soluzione di Governance, Rischio e Conformità (GRC) altamente scalabile e con funzionalità di intelligenza artificiale. Centralizza le funzioni di gestione del rischio all'interno di un ambiente progettato per identificare, gestire, monitorare e creare report sui rischi e sulla conformità normativa.

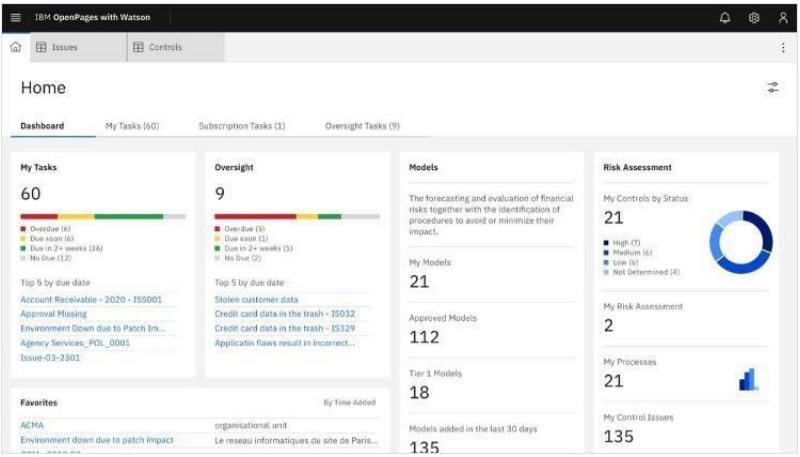

Figura 50 – Un'interfaccia di IBM OpenPages with Watson

Permette quindi di seguire il processo tipico di valutazione dei rischi (RCSA), la valutazione delle perdite, l'identificazione delle azioni di mitigazione, il monitoraggio degli indicatori di rischio (KRI), il monitoraggio dei problemi e i casi di insuccesso e propone cruscotti, sistemi di gestione della documentazione e dei dati condivisi, dei ruoli e delle responsabilità sulle azioni di gestione e controllo e i relativi workflow.

Ha un modulo specifico per la gestione del rischio relativo alle terze parti e ne supporta la categorizzazione in base a rischio, criticità e altri fattori.

9.2.5 MasterCard Cyber Quant

Cyber Quant, sviluppato in Israele e acquisito da MasterCard, è una piattaforma che misura i rischi per la sicurezza informatica di un'organizzazione, segnala le lacune e stima l'impatto dei nuovi controlli considerando le minacce, creando risultati e raccomandazioni personalizzati.

Cyber Quant calcola diverse misure da cui emerge un insieme quantitativo di metriche. La metodologia alla base del sistema si basa sul modello TARA (*Threat agent risk assessment*) di Intel e sul modello FAIR (*Factor analysis of information risk*), derivato dal framework Value at Risk (VaR) per la cybersecurity e il rischio operativo.

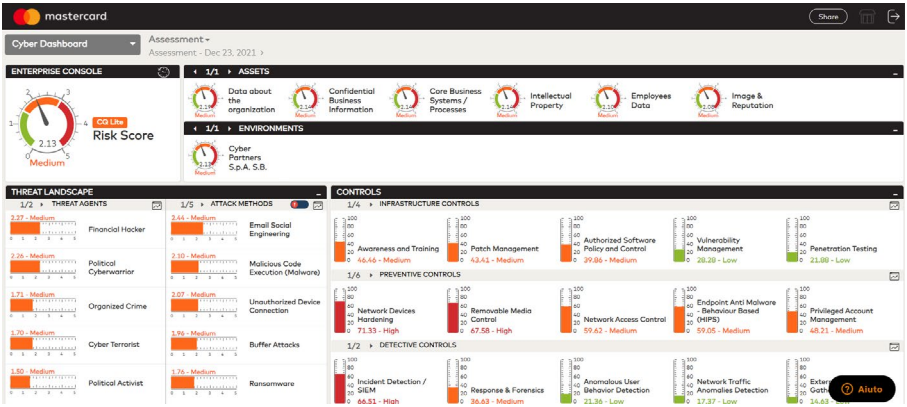

Figura 51 – Un'interfaccia di Cyber Quant

Cyber Quant permette di correlare i risultati con i requisiti di ISO/IEC 27001, NIST CSF, NIST 800-53, GDPR, PCI-DSS, HIPAA e altro.

9.2.6 MetricStream

MetricStream Enterprise GRC, sviluppato negli Stati Uniti, raccoglie i dati su rischio e conformità da tutta l'organizzazione e da terze parti.

Figura 52 - Un'interfaccia MetricStream

Funzionalità chiave includono quelle di gestione del rischio, incluso quello di continuità, di gestione della conformità normativa grazie all'integrazione di molti requisiti, inclusi regolamenti intersettoriali, impegni normativi, casi e sondaggi, gestione degli audit interni SOX, analisi delle prestazioni dell'organizzazione.

9.2.7 OneTrust

Il software privacy OneTrust è stato progettato per la conformità al GDPR, al CCPA, allo standard ISO/IEC 27001 (tramite il prodotto specifico OneTrust GRC) e ad altre normative di sicurezza e privacy a livello mondiale.

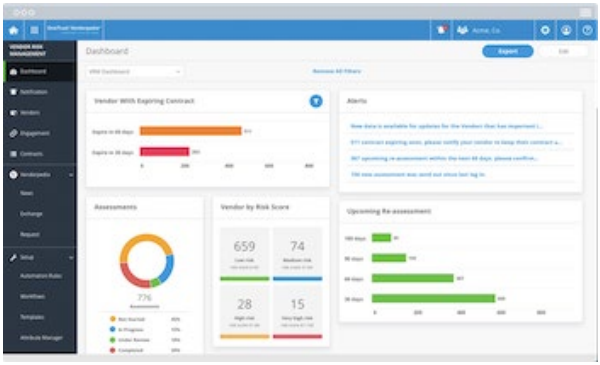

Figura 53 - Un'interfaccia OneTrust

Inoltre, esso permette di valutare la sicurezza e la privacy delle terze parti, redigere il registro dei trattamenti, monitorare gli SLA e le prestazioni.

9.2.8 Oracle

L'offerta Oracle per la valutazione del rischio dei Database è composta da 2 soluzioni:

- Database Security Assessment Tool – (DBSAT);
- Data Safe (DS).

DBSAT

DBSAT è una soluzione semplice e gratuita basata su script che supporta:

- l'analisi del rischio, raccogliendo le informazioni di configurazione dal database e significative per la sicurezza, valutando lo stato di sicurezza corrente e fornendo consigli sulle possibili azioni atte alla mitigazione dei rischi identificati;
- data discovery, analizzando i nomi dei campi del database e gli eventuali commenti e le tabelle contenenti potenziali dati critici.

Section	Pass	Evaluate	Advisory	Low Risk	Medium Risk	High Risk	Total Findings
Basic Information	0	0	0	0	0	1	1
User Accounts	5	0	0	4	2	1	12
Privileges and Roles	5	16	0	0	0	0	21
Authorization Control	0	1	1	0	0	0	2
Fine-Grained Access Control	0	1	4	0	0	0	5
Auditing	0	4	2	0	6	0	12
Encryption	0	1	1	0	0	0	2
Database Configuration	5	3	0	3	2	1	14
Network Configuration	1	1	0	0	3	0	5
Operating System	1	0	0	2	1	1	5
Total	**17**	**27**	**8**	**9**	**14**	**4**	**79**

Figura 54 - Un'interfaccia di Oracle DBSAT

DBSAT fa riferimento a best practice e normative internazionali per la sicurezza dei dati:

- Oracle Database STIG (Security Technical Implementation Guide);
- CIS (Center for Internet Security - Oracle Database Benchmarks);
- GDPR (Regolamento generale sulla protezione dei dati).

Data Safe (DS)

Figura 55 – Un cruscotto di Oracle Data Safe

Data Safe è un servizio cloud che fornisce una valutazione dello stato di sicurezza del database, sia esso in esecuzione sul cloud o in locale. L'analisi avviene sia dalla prospettiva delle configurazioni del sistema, come per DBSAT, sia dalla prospettiva del rischio associato agli utenti del database.
Per la parte di analisi della configurazione, DS realizza una valutazione con gli stessi controlli del DBSAT, ma con due funzionalità in più: programmazione della periodicità delle analisi e evidenziazione delle differenze rispetto alle analisi precedenti.

Data Safe fornisce inoltre un'analisi del rischio relativa agli utenti dei database (user assessment), identificando quelli ad alto rischio per eventualmente rimuovere i ruoli e i privilegi non strettamente necessari.
La funzionalità di *data discovery* presente in Data Safe fornisce una ricerca dei dati sensibili più ricca rispetto a quella presente in DBSAT perché è in grado di analizzare anche il contenuto delle tabelle e non soltanto i metadati (nome dei campi e commenti).
Data Safe completa le funzionalità di analisi del rischio del database con una gestione integrata di DB Audit Management/Analysis e Data Masking

9.2.9 Prevalent

Prevalent permette di valutare i rischi relativi alla sicurezza informatica e alla privacy originati dai fornitori. La piattaforma Prevalent TPRM è una soluzione basata su cloud

per la valutazione e il monitoraggio del rischio dei fornitori e che permette di automatizzare il processo di valutazione e la gestione delle azioni correttive durante l'intero ciclo di vita del fornitore.
La piattaforma è completata da reti di vendor intelligence che offrono accesso su richiesta a report di rischio completi e standardizzati su migliaia di aziende.

9.2.10 Riesko

Riesko è una piattaforma software che supporta l'ERM ed è fruibile via web. Riesko è una piattaforma che permette di strutturare, organizzare e uniformare il processo di gestione dei rischi, favorendo la partecipazione e il contributo alla valutazione e trattamento dei rischi dei responsabili dei processi aziendali.

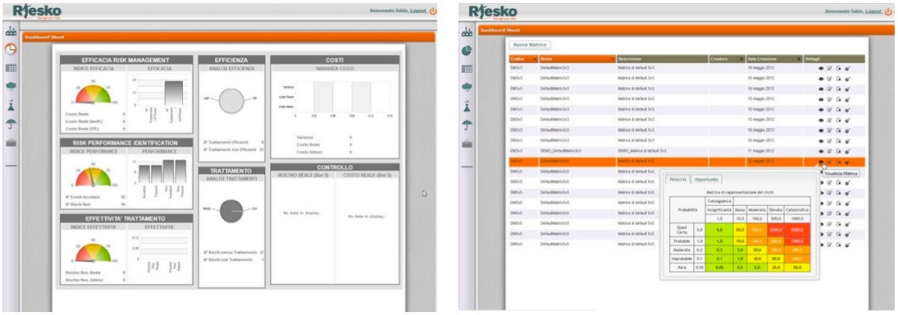

Figura 56 - Interfacce di Riesko

9.2.11 RSA Archer

RSA Archer Suite è una piattaforma a supporto delle seguenti attività: analisi della resilienza del sistema, gestione del rischio operativo, gestione del rischio IT, gestione degli audit, controllo di terze parti, gestione della conformità normativa.
Le caratteristiche principali di RSA Archer Suite includono:

- tassonomia del rischio integrata,
- standard di settore integrati,
- database di informazioni economiche,
- modelli di flusso di lavoro,

- analisi dei rischi su richiesta,
- simulazioni matematiche,
- tabelle delle perdite

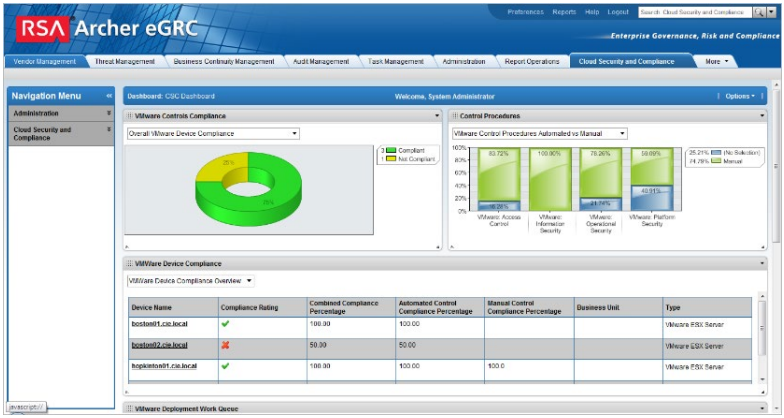

Figura 57 - Interfaccia di RSA Archer Suite

9.2.12 ProcessUnity

Il software ProcessUnity permette di valutare e monitorare i fornitori di un'organizzazione, anche per la selezione, la *due diligence* e il monitoraggio continuo.

Figura 58 - Un'interfaccia di ProcessUnity

9.2.13 SAI360

Figura 59 - Schema di SAI 360[158]

SAI360 è un software cloud con contenuti didattici su etica e conformità progettati per aiutare le organizzazioni a gestire efficacemente il rischio e la conformità relativamente a sicurezza informatica e protezione dei dati personali.
Presenta requisiti mappati su framework e controlli di: ITIL, COBIT, NIST CSF, ISO/IEC 27001, ISO 31000, PCI, GDPR e HIPAA.

9.2.14 ServiceNow

ServiceNow Governance, Risk and Compliance (GRC) offre le seguenti funzionalità:

- gestione del rischio;
- gestione delle policy e della conformità:
- gestione degli audit, assegnando le priorità;
- gestione del rischio dei fornitori, inclusa la due diligence.

158 https://www.sai360.com/.

10. Associazioni di riferimento

Le principali associazioni in Italia:

- **ANRA** - Associazione nazionale dei risk manager e responsabili assicurazioni aziendali - https://www.anra.it/
- **Aused** - Associazione tra utenti di sistemi e tecnologie dell'informazione - https://www.aused.org/
- **BCI Italy Chapter** - The Business continuity institute - https://www.thebci.org/group/italy.html
- **Clusit** - Associazione Italiana per la sicurezza informatica - https://clusit.it/
- **CSA Italy** - Cloud security alliance Italy - https://cloudsecurityalliance.it/

Le principali associazioni in Europa e nel mondo:

- **BCI** - The Business continuity institute - https://www.thebci.org/
- **CSA** – Cloud security alliance - https://cloudsecurityalliance.org/
- **Ferma** - Federation of european risk management associations - https://www.ferma.eu/
- **IFRIMA** - International federation of risk and insurance management associations - https://www.ifrima.org/
- **RIMS** - The Risk management society® - https://www.rims.org/
- **RMA** – The Risk management association - https://www.rmahq.org

Altre associazioni che si occupano di audit e tematiche relative ai rischi, in ambito italiano e internazionale:

- **AIEA** - Associazione italiana information systems auditors (ISACA - capitolo di Milano) - http://aiea.it/
- **ECIIA** - European confederation of institutes of internal auditing - https://www.eciia.eu/
- **ISACA Rome Chapter** - Information systems audit and control association (ISACA - capitolo di Roma) - https://www.isacaroma.it/
- **ISACA Venice Chapter** - Information systems audit and control association (ISACA - capitolo di Venezia) - https://engage.isaca.org/venicechapter/home
- **ISACA** - Information systems audit and control association - https://www.isaca.org/

11. Le certificazioni professionali

Di seguito le certificazioni, o meglio, gli attestati di qualifica riconosciuti a livello internazionale in gestione dei rischi.
Al riguardo vanno distinte le certificazioni di carattere generale rispetto a quelle specificatamente dedicate ai rischi ICT.
Per quanto riguarda queste ultime, la valutazione dei rischi è una parte dell'attività che viene svolta da parte dei soggetti che possiedono certificazioni in ambito sicurezza.

Al riguardo vanno quindi prese in considerazione le certificazioni di:

- **(ISC)²: CISSP, SSCP**
- **ISACA: CISM, CRISC**

Vanno inoltre prese in considerazione le certificazioni in ambito ISO, tra cui quelle di **auditor e lead auditor dei sistemi di gestione per la sicurezza delle informazioni basati sulla ISO/IEC 27001.**

Specificatamente dedicata alla metodologia FAIR, The Open Group rilascia la certificazione **Open FAIR™ Certification.**

Per quanto attiene certificazioni di carattere generale:

- **ANRA** (Associazione nazionale risk manager & insurance manager – Sito: www.anra.it) offre il percorso per la formazione della figura professionale del risk manager, accreditato da FERMA, iter formativo il cui superamento conferisce per equipollenza la certificazione europea professionale Rimap® (acronimo di "Risk management professional"). La certificazione è valida in ventidue stati europei ed è anche riconosciuta in America Latina, Asia e USA.

  Vi è inoltre la possibilità di accedere alla Certificazione RIFT - RIMAP® (RIFT, acronimo di Rimap fast track), corso di 24 ore che fornisce una panoramica completa sulla disciplina del risk e insurance management.
- **Institute of risk management** (Sito: https://www.theirm.org/), permette di conseguire certificazioni in ambito di risk management (in lingua inglese) della durata di 5-9 mesi e, precisamente:
  - International certificate in enterprise risk management (Certificato internazionale in gestione del rischio aziendale);
  - International certificate in financial services risk management (Certificato internazionale in gestione del rischio dei servizi finanziari);
  - Digital risk management certificate (Certificato di gestione del rischio digitale);

- Supply chain risk management certificate (Certificato di gestione del rischio della catena di approvvigionamento);
- Certificate in operational risk management (Certificato di gestione del rischio operativo);
- International diploma in risk management (durata di 3 anni).

Vi sono associazioni che forniscono corsi di certificazione sul rischio, quali:

- RMA (Sito: https://www.rmahq.org/);
- ISACA (Sito: https://www.isaca.org/);
- RIMS-the Risk Management Society (Sito: https://www.rims.org/).

Inoltre, ci sono corsi di perfezionamento e Master a livello italiano erogati dai principali atenei italiani e consorzi universitari, quali:

- Università degli Studi di Verona (Sito: https://www.univr.it/it/);
- Politecnico di Milano (Sito: https://www.polimi.it/);
- CINEAS - Consorzio universitario per l'ingegneria nelle assicurazioni (Sito: https://www.cineas.it/);
- Cuoa (Sito: https://www.cuoa.it/.it/);
- Mib Trieste School of management (Sito: https://mib.edu/).

12. Una vita risk based

In questo libro ci siamo focalizzati sul rischio digitale, che sicuramente è uno dei principali temi su cui occorre che le organizzazioni piccole, medie o grandi pongano sempre più attenzione. E non solo le organizzazioni, ma anche i singoli con i loro comportamenti.

Tuttavia, esistono anche altri tipi di rischio, oltre a quello digitale, con cui dobbiamo fare i conti nel quotidiano. Potremmo dividerli in due categorie principali.
Ci sono innanzitutto quelli che fanno parte della nostra vita, che rappresentano l'altra medaglia nei cambiamenti importanti, nelle decisioni da prendere. A ogni alternativa, a ogni bivio nella nostra vita, a ogni opportunità è sempre associato un rischio. La decisione può essere stimolante o fonte di stress, possiamo scegliere bene o sbagliare, ma tutto ciò fa parte della vita.

Esiste una seconda categoria di rischi per così dire non voluti, non cercati, che non dipendono da noi ma dal mondo in cui viviamo. Rischi che dobbiamo tenere in considerazione nelle nostre scelte come individui e come comunità. Siamo sicuramente aiutati da analisti che li valutano e ci mettono in guardia, da strumenti che ci indicano come ridurli e compensarli, per quanto possibile. Però purtroppo la realtà non è sempre così lineare.

Non tutti i rischi sono ugualmente prevedibili, in alcuni casi un rischio può presentarsi inaspettato. Si tratta dei cosiddetti *cigni neri*: si pensi ad esempio alla crisi del 1929 che è arrivata trovando un mondo completamente impreparato ad affrontarla, o all'attentato alle torri gemelle; o anche alla crisi finanziaria del 2008. Anche la pandemia che stiamo vivendo fa parte di questo secondo tipo di rischi. Col senno di poi alcuni di questi avvenimenti potevano essere previsti. Ma di fatto sono stati dei fulmini a ciel sereno.

Occorre salire di livello, abbandonare il dettaglio, alzarci di qualche chilometro; e avremo una percezione molto più chiara. Così è anche per un cigno nero come questa pandemia. Se osserviamo secondo la nostra esperienza risulta un cigno nero, perché la nostra vita è temporalmente limitata, ci soffermiamo su dettagli che abbiamo già vissuto, e un evento simile non lo abbiamo mai vissuto. Ma se allarghiamo la visuale prendendo in considerazione un arco temporale di qualche secolo, allora il quadro risulterà sicuramente molto più chiaro.

Un cigno nero ha un risvolto psicologico ed emotivo (sia dal punto di vista individuale e personale, sia sulla psicologia di massa) molto diverso rispetto ai rischi che possono essere previsti in base alla nostra diretta aspettativa ed esperienza.

Se proviamo a leggere ad esempio “1918. L’influenza spagnola. La pandemia che cambiò il mondo” di Laura Spinnei (ed. Marsilio) ci accorgiamo come alcuni meccanismi che caratterizzarono la reazione sociale di allora, non sono così diversi rispetto a quelli che stiamo vivendo attualmente. Anche l’evolversi delle reazioni risulta simile: inizialmente, adesso come allora, nella prima fase le persone si sono sentite unite di fronte al pericolo comune, ritrovandosi tutti disposti anche a sacrificarsi per gli altri. Mano a mano che la pandemia è proseguita senza segni di cedimento, col passare dei mesi, con le restrizioni, allora come adesso hanno cominciato a venire fuori meccanismi simili di protesta e di insofferenza.

13. Raccomandazioni finali

13.1 Raccomandazioni alle organizzazioni

La crisi la pandemica, i principali attacchi informatici e altri eventi recenti, hanno tutti messo in luce la fragilità dei sistemi globali e le gravi carenze nella preparazione delle organizzazioni a gestire grandi crisi.

DI fatto, il contesto in cui si trovano a operare le organizzazioni è estremamente erratico, il cosiddetto VUCA World, ossia un mondo caratterizzato da volatilità (*volatility*), incertezza (*uncertainty*), complessità (*complexity*) e ambiguità (*ambiguity*). Ne consegue che le organizzazioni devono - quanto prima - prendere in considerazione una riprogettazione del proprio modello organizzativo, riconfigurando strategie, strutture e processi, oltre a sostituire le tradizionali strutture gerarchiche per silos, le logiche di potere decisionale nelle mani del vertice e dei flussi top-down, con strutture tra loro interrelate e flussi bottom-up.

Il processo di digitalizzazione in atto comporta, inoltre, una inevitabile ed urgente riqualificazione della forza lavoro, sia in termini di aumento o cambiamento delle competenze (*upskilling* e *reskilling*), sia in termini di adozione di nuovi modelli organizzativi che facilitino la diffusione di una cultura digitale unitamente alle competenze adeguate all'interno dell'organizzazione.

Ne consegue che diventa sempre più urgente e necessario attuare un efficace ed efficiente sistema di gestione dei rischi per garantire la resilienza dell'organizzazione, considerando che la resilienza è una priorità di tutte le organizzazioni. Essa implica:

- anticipare il rischio;
- collegare la gestione del rischio alla strategia aziendale;
- evitare lacune nella percezione del rischio;
- misurare e monitorare costantemente i dati rilevanti.

Il supporto di professionisti di gestione del rischio e di continuità operativa diventa, in questo momento, strategico e fondamentale in quanto è necessario condividere i piani di trattamento del rischio, i piani di continuità e di gestione dell'emergenza e della crisi e comunicare ciò che ogni piano comporta e come si evolverà, cercando allo stesso tempo il coinvolgimento e il contributo di tutti gli attori (interni ed esterni all'organizzazione).

L'organizzazione, concepita come una rete, fatta di connessioni, vasi comunicanti ed estremamente fluida, è in grado di avviare processi di innovazione inter-funzionali e che coinvolgono altre organizzazioni. Le idee "fluiscono" all'interno della cosiddetta "bionic organization" che fa leva su tecnologia e persone per potenziare la crescita, l'innovazione, l'efficienza, la resilienza e la competitività.

Un'organizzazione "agile" e "adaptive" che presuppone la capacità di "fluttuare" come una farfalla ma, al tempo stesso, dotata delle "forze" necessarie per risultare vincente e competitiva.

Concludendo, è tempo per una transizione o, meglio, una metamorfosi. Siamo di fronte a una trasformazione necessaria e profonda che investe tutta la società a livello globale. Nuovi paradigmi sono necessari. La gestione del rischio e la pianificazione della continuità aziendale sono destinate a confrontarsi con il nuovo approccio "agile & adaptive" che scaturirà in una calibrata sintesi di *lessons learned* dalla pandemia e di predisposizione o revisione di piani flessibili in modo da aiutare le organizzazioni a prepararsi per il prossimo evento "disruptive", indipendentemente dalla tipologia di interruzione.

Non ci resta che metterci all'O.P.E.R.A. (schema ideato dalla società di consulenza strategica Roland Berger GMBH): O-pen up operations, P-erfect your value chain, E-mbrace digital, R-eorchestrate value generation, A-ccelerate the learning game.

13.2 Raccomandazioni alla società in generale

13.2.1 Connessione e comunicazione

La sicurezza delle reti è solo la base per una solida difesa IT. A fronte della disponibilità di evoluti strumenti tecnici di protezione dei sistemi informativi, è d'obbligo la crescita della consapevolezza delle minacce e dei rischi e quindi la contaminazione del saper vivere in un'era digitale, tanto da parte del sistema pubblico che da quello privato.

In questa chiave una comunicazione chiara può fare la differenza come chiave di volta. È importante, dunque, che la comunicazione riponga nella formazione sulla sicurezza il suo braccio armato come parte integrante della transizione digitale.

Le persone e le comunità hanno il diritto di partecipare all'evoluzione tecnologica per poter assumere consapevolmente decisioni che riguardano i loro interessi economici, la propria privacy e tutto ciò che risiede nel macrocosmo digitale ed è ha valore per loro.

Lo scopo della comunicazione non è quello di diffondere la preoccupazione dell'opinione pubblica, ma creare un pubblico informato che sia coinvolto, interessato, ragionevole, riflessivo, orientato alla soluzione e collaborativo.

L'obiettivo di un programma efficace di comunicazione sui rischi informatici non può essere manipolatorio, ma deve mirare a una consapevole e obiettiva decisione da parte dei soggetti coinvolti. Quindi una comunicazione che sia definita come scambio di informazioni e di valutazioni sui rischi tra gli esperti, le pubbliche amministrazioni, i mass media, i gruppi di interesse e i cittadini, finalizzata ad aiutare a prendere decisioni circa l'accettare, ridurre o evitare il rischio.

La specificità dei rischi in questione produce un tipo di comunicazione tecnica, scientifica e quindi necessariamente da tradurre in un metalinguaggio comprensibile che abbia lo scopo di informare, educare o persuadere i riceventi, perché ha in sé l'incertezza associata a un possibile esito negativo e mira a raggiungere uno specifico cambiamento.

Obiettivo è, dunque, motivare le persone ad adottare determinate precauzioni, stimolare la popolazione a raggiungere un determinato consenso rispetto a decisioni da prendere, tranquillizzare rispetto a un rischio, allertare i destinatari, sollecitando un adeguato grado di preoccupazione e di azione.

Esperimenti scientifici hanno dimostrato che la partecipazione del pubblico durante il processo decisionale sui rischi può portare a una maggiore accettazione delle politiche di trattamento del rischio. I soggetti sono spesso più preoccupati per questioni come la fiducia, la credibilità, il controllo, i benefici, la competenza, la volontarietà, l'equità, l'empatia, la cura, la cortesia che per quel che riguarda le statistiche e i dettagli di valutazione quantitativa del rischio. Quindi un'efficace comunicazione a due vie per verificare il livello di conoscenza attraverso interviste, focus group e sondaggi.

È la fiducia in chi gestisce il rischio, non la statistica a ridurre la preoccupazione nelle persone.

Bisogna essere, ancora prima che un portavoce, un essere umano e parlare al cuore e non solo al cervello della gente. Una fonte molto esperta può essere giudicata meno credibile se ne percepiscono intenti manipolativi, mentre se la fonte sembra agire per tutelare gli interessi altrui è giudicata sicuramente più credibile.

Fondamentale è, tra l'altro, il coordinamento e la collaborazione con fonti credibili: scienziati universitari e consulenti sono tra le fonti credibili e disponibili per stabilire alleanze con terze parti, arruolando e preparando dei portavoce ed evitare contrasti con le altre fonti che accrescono le preoccupazioni e consentono una migliore gestione

delle informazioni sui rischi.

Importante è soddisfare le esigenze dei media quali trasmettitori principali di informazioni sui rischi e determinanti per un ruolo fondamentale nella creazione di agende, evoluzione di status e diffusione dei risultati. Quindi favorire un linguaggio chiaro ed empatico per evitare che il gergo tecnico diventi una barriera alla comunicazione di successo con il pubblico. In condizioni di scarsa fiducia, l'empatia e la cura hanno spesso più peso di numeri e fatti tecnici.

13.2.2 Uso degli standard

Attraverso l'utilizzo di *good practice* efficaci e la realizzazione di un ISMS (sistema di gestione della sicurezza delle informazioni), è possibile migliorare sensibilmente la postura in relazione al rischio informatico. L'utilizzo di standard di riferimento permette alle organizzazioni di gestire le proprie procedure di sicurezza in modo centralizzato e coerente e secondo priorità condivise, oltreché orientato alla propria missione.

- Alcune aree particolarmente sensibili sono:
- l'integrazione e cooperazione tra il management e lo staff tecnico per identificare le corrette strategie e gli adeguati investimenti;
- la regolare formazione e aggiornamento di tutto il personale perché la gestione del rischio si realizza attraverso la collaborazione di tutti;
- l'attribuzione delle giuste priorità alla valutazione del rischio in modo da affrontare le minacce reali e non sprecare tempo e risorse per affrontare minacce poco probabili o poco significative;
- il riesame periodico e regolare delle policy e delle procedure perché ogni sistema di sicurezza trae giovamento dal miglioramento continuo, anche se si tratta di un compito oneroso.

14. Glossario

Asset: Tutto ciò che ha valore per l'organizzazione.

Conseguenza: esito di un evento che influenza gli obiettivi. Una conseguenza può essere certa o incerta e può avere effetti positivi o negativi sugli obiettivi. Le conseguenze possono essere espresse qualitativamente o quantitativamente. Qualunque conseguenza può amplificarsi attraverso effetti in cascata. [Fonte: Guida ISO/IEC 73:2009]

Controllo: misura che mantiene e/o modifica il rischio. [Fonte: ISO 31000:2018]

Disponibilità (availability): Garanzia di un accesso e un utilizzo tempestivi e affidabili delle informazioni. [Fonte: FIPS 200 NIST]

Evento: il verificarsi o modificarsi di un particolare insieme di circostanze. Un evento può consistere in uno o più episodi e può avere una pluralità di cause e di conseguenze. Un evento può essere anche qualcosa che non accade. [Fonte: Guida ISO/IEC 73:2009]

Gestione del rischio: attività coordinate per guidare e tenere sotto controllo un'organizzazione con riferimento al rischio. [Fonte: Guida ISO/IEC 73:2009]

Incidente: uno o più eventi che hanno una significativa probabilità di compromettere le attività di un'organizzazione e minacciare la sicurezza o le prestazioni di un sistema.

Information security: conservazione della riservatezza, integrità e disponibilità delle informazioni. [Fonte: ISO/IEC 27000:2018]

Integrità (Integrity): La protezione contro la modifica o la distruzione impropria delle informazioni e include la garanzia del non ripudio e dell'autenticità delle informazioni. [Fonte: FIPS 200 NIST]

Likelihood: possibilità che qualcosa si verifichi. Nella terminologia della gestione del rischio, il termine "verosimiglianza" (o "possibilità") è utilizzato per riferirsi alla eventualità che qualcosa accada, sia esso definito, misurato, determinato oggettivamente o soggettivamente, qualitativamente o quantitativamente, e descritto utilizzando termini generici o in modo matematico (come probabilità o frequenza con riferimento ad un dato intervallo di tempo). [Fonte: Guida ISO/IEC 73:2009]

Livello di rischio: grandezza di un rischio o di una combinazione di rischi, espressa in termini di combinazione delle conseguenze e loro verosimiglianza (likelihood). [Fonte: Guida ISO/IEC 73:2009]

Minaccia (threat): causa potenziale di un incidente non desiderato, che può risultare in un danneggiamento a un sistema o a una organizzazione. [Fonte: ISO/IEC 27000:2018]

Mitigazione del rischio: opzione di trattamento del rischio che prevede di ridurlo mediante l'applicazione di uno o più controlli di sicurezza.

Procedura: modo specificato per svolgere un'attività o un processo [Fonte: ISO 9000:2015]

Processo: insieme di attività correlate o interagenti che utilizzano input per fornire un risultato previsto [Fonte: ISO 9000:2015]

Processo di gestione del rischio (risk management process): l'applicazione sistematica di politiche, procedure e pratiche di gestione alle attività di comunicazione, consulenza, definizione del contesto e identificazione, analisi, valutazione, trattamento, monitoraggio e revisione del rischio. [Fonte: ISO Guide 73:2009]

Propensione al rischio (risk appetite): quantità e tipo di rischio che un'organizzazione vuole perseguire o accettare. [Fonte: ISO Guide 73:2009]

Progetto: sforzo temporaneo per raggiungere uno o più obiettivi definiti [Fonte: ISO 21502:2020]

Rischio accettabile: il livello di rischio residuo che è stato valutato essere un livello ragionevole di potenziale perdita o interruzione per un sistema specifico. [Fonte: Critical Infrastructure Assurance Office USA]

Rischio digitale: tipologia di rischio a cui sono esposti dati e servizi digitalizzati e che generalmente si esprimono come conseguenza o attraverso l'utilizzo di tecnologie di carattere digitale.

Rischio residuo: rischio rimanente dopo il trattamento del rischio. [Fonte: ISO Guide 73:2009]

Riservatezza (confidentiality): Preservazione delle restrizioni autorizzate all'accesso e alla divulgazione delle informazioni, compresi i mezzi per proteggere la privacy delle persone e le informazioni proprietarie. [Fonte: FIPS 200 NIST]

Sistema di gestione (management system): insieme di elementi interconnessi o interagenti di un'organizzazione per stabilire politiche, obiettivi e processi per raggiungere tali obiettivi. [Fonte: ISO/IEC 27000:2018]

Stakeholder: qualsiasi individuo, gruppo di persone o organizzazione che può

influenzare, essere influenzato da, o percepire di essere interessato da un rischio. [Fonte: Guida ISO/IEC 73:2009]

Titolare del rischio (risk owner): persona o entità con la responsabilità e l'autorità per gestire un rischio. [Fonte: ISO Guide 73:2009]

Vulnerabilità: proprietà intrinseca di qualcosa che risulta nella predisposizione a una minaccia che può portare a un evento con conseguenze. [Fonte: ISO Guide 73:2009]

15. Autori, contributori e ringraziamenti


GeriCO
Gestione Rischi
e Continuità Operativa


GRC team
Governance, Risk & Compliance


InfoCert
TINEXTA GROUP


OFFICIAL
(ISC)²
CHAPTER
ITALY


IUSINTECH®
DIRITTO • INNOVAZIONE • TECNOLOGIA


Liguria
Digitale


LUTECH


mead
YOUR DIGITAL INTEGRATOR


Ecosistema.AI


ORACLE


Pluribus One
seeing one in many


Posteitaliane


PQE GROUP
GLOBAL QUALITY SOLUTIONS


protiviti
Global Business Consulting


REXILIENCE
#BEYOND_CYBERSECURITY


Riesko
Manage your risks


PKF


S2E
business & technology consultants


sernet


ServiTecno


LA&P
legal and tax counsel


STEFANELLI&
STEFANELLI
STUDIO
LEGALE


The Innovation Group
Innovating business and organizations through ICT


UnipolSai
ASSICURAZIONI

15.1 Editor e team leader

- Orlando Arena, Consulente
- Fabrizio Bulgarelli - PKF GODOLI RAS, Partner
- Andrea Cabras - Vodafone, Secure by Design & Prevent
- Cesare Gallotti, Consulente di sicurezza delle informazioni, qualità e privacy
- Francesca Gatti - Clusit
- Valeria Lazzaroli - Arisk, Chief Risk Officer
- Alberto Leporati - Università degli Studi di Milano-Bicocca, Professore Associato; Comitato Scientifico Clusit
- Federica Maria Rita Livelli - Business Continuity & Risk Management Consultant; BCI Italy Chapter Board Member (Deputy Leader), ANRA (Board Member); CLUSIT - Comitato Scientifico (Member)
- Roberto Obialero - CLUSIT, S2E, Cybersecurity & Data Protection Advisor; CD Clusit, CISO S2E
- Stefano Ramacciotti - (ISC)² Italy Chapter, Presidente Italy Chapter
- Manuel Angelo Salvi - GRC Team, ISO 27001 e GDPR Consultant, DPO
- Silvia Stefanelli - Studio Legale Stefanelli & Stefanelli, Avvocato
- Mario Testino - ServiTecno, COO e Consigliere
- Alessandro Vallega - Consiglio Direttivo Clusit, Founder and Chairman Clusit Community for Security

15.2 Autori

- Elena Agresti - Poste Italiane, Information Security Manager
- Leonardo Antonelli - Oracle, Master Principal Sales Consultant
- Davide Ariu - Pluribus One, CEO
- Stefano Barboni - Riesko, Senior Partner
- Giovanni Belluzzo - InfoCert, Head of Cybersecurity - Chief Information Security Officer
- Gianluca Bocci - Poste Italiane, Security Professional Master - Corporate Affairs, Tutela Aziendale
- Angelo Bosis - Oracle, Technology Architect Director

- Fabio Bucciarelli - Lutech Group, Senior Security Advisor
- Giancarlo Butti - Internal Auditor
- Andrea Caccia - ANORC, Consulente
- Dario Carnelli - Codd&Date Suisse, IT Strategy & GRC Advisor
- Davide Carnelli - Consulente Architetture e Data Management
- Andrea Castello - CSQA Certificazioni, Digital Improvement and Development Executive Manager
- Marco Ceccon - Deloitte Risk Advisory, Director
- Francesco Ciclosi, Università degli Studi di Trento - Ministero dello Sviluppo Economico
- Luciano Colombo - IT Architect freelance
- Igino Corona - Pluribus One, Chief Technology Officer
- Rita Eva Cresci - IUSINTECH, Innovation Lawyer
- Marco Crociani - Security Governance Consultant
- Giuseppe Cusello - Cyber Partners S.p.A. (Gruppo RINA), GRC Director
- Nicla Ivana Diomede - Università degli Studi di Milano, Responsabile Cybersecurity, Protezione Dati e Conformità
- Elenio Dursi - Clusit, IT project manager and Scientific Committee Board Member at Clusit
- Ambrogio Ferretti - A2A, Senior IT Auditor
- Enrico Ferretti - Protiviti, Managing Director
- Giustino Fumagalli - Gerico Security Srl, Socio (attività consulenze)
- Cristina Gaia - Cybereason, Regional Marketing Manager
- Chiara Gatti - UnipolSai Assicurazioni s.p.a., Responsabile Sottoscrizione Rischi Cyber (head of cyber risk underwriting)
- Carlo Guastone - Sernet spa, Vicepresidente Business Development
- Marco Locatelli - Rexilience, CEO
- Massimiliano Magri - COSTERGROUP , Smart Readiness Indicator evangelist
- Lorena Manco - UnipolSai Assicurazioni s.p.a., Sottoscrittore Rischi Cyber (Cyber risk underwriter)
- Davide Manconi - Plenitude, Cyber Security Manager
- Andrea Mariotti - EY, Associate Partner Cybersecurity & Digital Protection
- Carlo Mauceli - Microsoft, Chief Technology Officer e Chief Security Officer per Microsoft Italia

- Luigi Mauro - Protiviti, Manager
- Savino Menna - Studio LA&P, Avvocato Senior Partner - Head of Tech Law, Cybersecurity & Data Protection Department
- Paola Meroni - Whirlpool Corporation - Global Privacy Manager
- Riccardo Modena - Sernet spa, Manager LoB Business “ICT Governance”; Senior Consultant (Information Security, Privacy, Business Continuity, Service Management ed Execution Improvement)
- Enzo Mudu - IBM Italy, Associate Partner - IBM Security Services
- Paolo Panza - ICT Quality Manager
- Ignazio Parrinello - Mead Informatica, Responsabile Compliance
- Maurizio Pastore - Liguria Digitale, Responsabile servizi Privacy
- Maria Roberta Perugini - IUSINTECH, Avvocato
- Riccardo Ranza - Consulente IT e Security
- Alice Ravizza - USE-ME-D srl, Founder
- Andrea Rui - Consulente IT e Security, e Comitato Scientifico Clusit
- Luca Sambucci - Notizie.ai, Blogger ed esperto di security e IA
- Fabio Saulli - Cyber Partners S.p.A. (Gruppo RINA), Director
- Paolo Sferlazza - Gerico Security Srl , Information Security Advisor Trainer and Auditor
- Nicola Sotira - Poste Italiane, Responsabile CERT di Poste Italiane
- Giulio Spreafico - AIEA, Auditor di Sistemi Informativi e Consulente Rischi ICT, Sicurezza e Privacy
- Roberto Tordi - CERTFin, Research Analyst
- Guglielmo Troiano - Grant Thornton, Manager Data Protection Services
- Elena Vaciago - THE INNOVATION GROUP, Associate Research Manager
- Luca Zammarchi - PQE Group, Digital Governance International Delivery Director
- Luigi Zampetti - Studio Legale Stefanelli & Stefanelli, Partner

15.3 Contributori

Ringraziamo le persone intervistate per averci dato il loro punto di vista su questo tema:

- Cesare Burei - Socio Clusit, Formatore CINEAS e AIBA Cyber Risk, Co-

Amministratore Margas - Broker e Consulente di Assicurazioni

- Antonella Caproni - Coordinatore Team Governance Cybersecurity, Banca Monte dei Paschi di Siena
- Carlo Cosimi - Presidente ANRA, Head of Corporate Insurance and Risk Financing, Saipem Spa
- Ruggiero Di Biase - Comandante del Comando per le Operazioni in Rete della Difesa
- Valentina Frediani - Avv. Valentina Frediani, CEO Colin & Partners
- Daniela Marucci - UnipolSai, Dirigente Responsabile della Linea Corporate e Trasporti
- Valentina Paduano - Chief Risk & Sustainability Officer Sogefi Group, FERMA Board Member
- Sofia Scozzari - CEO & Founder Hackmanac, Direttivo Women For Security e Comitato Scientifico Clusit.

15.4 Ringraziamenti

Hanno aiutato nella realizzazione di questo libro anche Valentina Falcioni di Oracle, Sara Obialero (grafica impaginatrice/ logo design) e Alessia Pilato di Rexilience (per la raccolta dati).

Rischio digitale Innovazione e Resilienza

Conoscere, affrontare e mitigare il rischio digitale