UNIVERSITÀ POLITECNICA DELLE MARCHE

FACOLTÀ DI ECONOMIA "GIORGIO FUÀ"

Corso di laurea magistrale in economia e management

Curriculum Amministrazione, Finanza e controllo

AI RISK CONTROL FRAMEWORK: ASSESSMENT DI RISK MANAGEMENT SU SOFTWARE CHE UTILIZZANO L'INTELLIGENZA ARTIFICIALE

AI RISK CONTROL FRAMEWORK: ASSESSMENT RISK MANAGEMENT ON SOFTWARE THAT USES ARTIFICIAL INTELLIGENCE (IA SYSTEM)

Relatore:

chiar.ma prof.ssa Caterina Lucarelli

Tesi di laurea di:

Marialuisa Gallo

Anno accademico 2023-2024

Sommario

Introduzione Contesto attuale dell'era digitale

La diffusione della tecnologia ha imposto importanti sfide sia alle organizzazioni che alla giurisprudenza: le prime si sono domandate come potevano sfruttarla per ottimizzare i propri profitti, minimizzare i propri costi, ampliare il proprio portafoglio clienti, mentre la seconda si interroga su come tutelare le persone. La questione è diventata ancora più rilevante con l'avvento dell'Intelligenza artificiale (IA), e ci si chiede quali potranno essere le implicazioni e i rischi.

"*La nuova rivoluzione tecnologica, quella digitale, ha qualcosa di diverso rispetto alle precedenti: è arrivata molto velocemente e richiede un adeguamento rapido. Le innovazioni che in continuazione stanno nascendo richiedono una altrettanto veloce capacità di apprendimento e di adattamento. Anche perché, per funzionare, le nuove tecnologie hanno sempre bisogno di uomini e di donne che le sappiano non solo utilizzare ma anche inventare e gestire*[1]." In una delle ultime visite al Consiglio Nazionale della Ricerca (CNR), in occasione della presentazione del libro "*Intelligenza Artificiale. Cos'è davvero, come funziona, che effetti avrà,* Piero Angela, partendo da riflessioni su tematiche che riguardano il futuro, aveva rivolto un consiglio ai giovani: "Devono cercare l'eccellenza, senza mai accontentarsi. La cultura ti consente di porre le domande giuste, di essere intelligente e flessibile. E la flessibilità è una definizione dell'intelligenza.

L'elaborato avrà come obiettivo quello di affrontare un particolare rischio nato con la rivoluzione digitale, la nascita di Internet e la telecomunicazione: il rischio di sicurezza informatica o di cybersecurity. In particolare, per le istituzioni finanziarie, essa rappresenta una nuova frontiera dei rischi operativi. In un settore con un tasso di digitalizzazione estremamente alto, l'aumento delle cyber minacce ha raggiunto livelli inediti e gli attacchi informatici hanno

[1] Cfr Prefazione "*Intelligenza Artificiale. Cos'è davvero, come funziona, che effetti avrà*" a cura di Piero Angela

raggiunto un grado di imprevedibilità, di impatto potenziale e di capacità diffusiva senza precedenti. Il processo di gestione dei cyber rischi risulta, pertanto, una pratica fondamentale per la sicurezza di un'organizzazione, indipendentemente dalle sue dimensioni e dalla sua collocazione geografica. In un contesto globale segnato dall'incertezza e in assenza di uno standard normativo univoco sono ancora troppe le infrastrutture con scarsa sensibilità e preparazione alle minacce provenienti dal cyber spazio, esponendosi ogni giorno ad un attacco invisibile e potenzialmente disastroso.

La valutazione dei rischi si amplia con l'esplosione esponenziale dell'IA a servizio e a uso di tutti.

L'elaborato si sviluppa in modo crescente partendo dal generale al particolare: l'illustrazione tenterà di spiegare al lettore che cos'è un rischio nel contesto aziendale, quali sono gli strumenti e gli attori che intervengono nel processo di valutazione dei rischi.

Il secondo capitolo si apre con l'analizzare uno dei rischi più cruciali con l'avvento della tecnologia: il rischio di sicurezza informatica o rischio cyber e verranno presentati i modelli ICT legati alla sua gestione.

La conclusione è sviluppata presentando il brevetto della società Exprivia per l'analisi e valutazione dei rischi, denominato Risk Assessment. Dal prototipo già commercializzato, il progetto ha l'ambizione di aver sviluppato un framework valutativo dei risk per i sistemi dotati di intelligenza artificiale. L'elaborazione del prototipo è stata realizzate nel corso dell'ultimo anno nel contesto dell'esperienza lavorativa condotta dall'autrice presso la società Exprivia S.p.A., con l'obiettivo di sviluppare una ricerca e progettare un AI Framework Control.

Capitolo 1 Scenari e strumenti di rischi aziendali

1.1 L'importanza di analizzare e valutare i rischi aziendali

I soggetti, sia persone fisiche che giuridiche, corrono costantemente rischi, ma raramente sono in grado di valutarli. Essi provano ad analizzarli, sulla base della personale propensione, cercando di ridurne l'impatto. La percezione, soggettiva e oggettiva, positiva o negativa, di subire una perdita o un guadagno e di andare incontro ad un rischio è sicuramente influenzata da giudizi euristici, che esulano dalla ratio e dall'intelletto.

Il comportamento emotivo svolge nei processi decisionali in condizione di incertezza un ruolo fondamentale e la sua incidenza condiziona la scelta. In ambito economico, le conoscenze finanziarie non sono sufficienti a determinare un comportamento e gli operatori tendono a subire influenze dettate "dal cuore" anziché dalla mente, riponendo fiducia più negli altri (amici e parenti) che negli elementi oggettivi.

Le modalità di rappresentazione, framing effect[2], di un problema incidono sulla scelta ultima e uno stesso individuo, nonostante la sua personale indole, propensa o avversa, potrebbe manifestare preferenze diverse in una stessa situazione.

Ma cos'è il rischio? Quando e come corriamo rischi? I soggetti sono sempre consapevoli di andare incontro ad un rischio?

Il rischio può essere definito come l'eventualità di subire un danno connessa a circostanze, non sempre prevedibile e, di conseguenza, il pericolo può essere più o meno tenue. L'incertezza della situazione comporta la difficoltà ad essere consapevoli, perché spesso le potenzialità di

[2] Il pregiudizio cognitivo con cui le persone decidono sulle opzioni è suggestionato dalla modalità con cui le stesse opzioni, di guadagno e di perdita, sono presentate. La propensione a rischiare aumenta nel momento in cui le opzioni sono presentate e percepite positivamente.

un’azione sono sottovalutate o sopravvalutate o non affatto valutate. Esso può avere anche un riscontro positivo e dalla situazione è possibile trarre vantaggi.

Le persone fisiche corrono il rischio di salute, fisica o psichica, di perdere un bene di proprietà (un oggetto o un dato); i soggetti giuridici, quale l’attività aziendale esercitata professionalmente dall’imprenditore per la produzione e lo scambio di beni e servizi, non sono esenti dalle minacce e soventemente devono far fronte a situazioni non determinabili.

Possiamo definire il rischio aziendale come la possibilità che si verifichino eventi, che, inevitabilmente, si abbattano sull’azienda, pregiudicando il “normale” svolgimento dell’attività.

Indipendente dal settore in cui si opera, il rischio è connaturato ed intrinseco all’attività economica: deriva dalla concezione strutturale sistemica, dall’aleatorietà degli eventi, dall’ambiente circostante e dall’instabilità del mercato, rispetto ai quali l’azienda interagisce costantemente. È legato sia ai fenomeni che ricadono nell’azienda che ai mutevoli rapporti che essa instaura con l’esterno ed è parte integrante della strategia di ogni azienda.

Nel definire la strategia aziendale, il top management deve tener presente le fonti di aleatorietà “esterne”, cercare di anticipare e/o governare dinamicamente i rischi connessi e individuare i possibili scenari che si potranno realizzare e, per ciascuno di questi, definire delle linee di azione contingenti.

La relazione tra rischio e strategia non riguarda solo le aziende di grandi dimensioni e quelle già strutturate, ma è presente in tutte le organizzazioni che vogliono crescere nel lungo periodo, sia piccole e medie imprese, PMI che start up, sia organizzazione private che pubbliche.

È necessario conoscere bene quali sono i rischi e le conseguenze che le aziende devono fronteggiare, comprendere come si sono modificati i pericoli e come è cambiata la percezione

degli stessi, per prevenirli e ridurre il loro impatto, considerando che quelli più difficili restano gli eventi "cigni neri"[3], ovvero quelli senza precedenti. Questi ultimi sono talmente pericolosi per la loro imprevedibilità e risultano essere devastanti, perché minacciano la capacità di operare. Secondo alcuni studi[4] condotti da Boston Consulting Group[5] **(**BCG), è possibile prepararsi a tali rischi costruendo un'organizzazione che punti all'eccellenza nella gestione delle crisi al tal punto da essere pronta a contrastare tali avvenimenti. Di fatti, le aziende adattive sono quelle che riescono a superare periodi di turbolenza economica, perché hanno sfruttato vantaggi in ambienti dirompenti, quali:

- vantaggio del segnale, inteso come l'abilità di rilevare, acquisire e sfruttare modelli di informazioni e cercare di anticipare gli eventi;
- vantaggio della sperimentazione, inteso come la sperimentazione e l'utilizzo dei dati provenienti dal mercato per migliorare la propria offerta di mercato;
- vantaggio dell'organizzazione, inteso come l'elasticità e flessibilità di un'azienda ad adattarsi ai cambiamenti;
- vantaggio del sistema, inteso come l'abilità di modellare attivamente interi ecosistemi aziendali;
- vantaggio eco-sociale, riferendosi alla capacità di allineare il modello di business dell'azienda al contesto sociale e ambientale circostante.

La gestione del rischio non deve costituire motivo di avversione al rischio e timore di subire costantemente perdite, anzi, la sua applicazione supporta le organizzazioni nell'identificazione

[3] Si fa cenno ad un concetto ben noto in economia. In particolare, si fa riferimento alla teoria del "cigno nero" che Nassim Nicholas Tales ha illustrato nel suo celebre saggio filosofico/letterario dell'epistemologo intitolato "Il cigno nero".
[4] Fonte degli studi: https://www.bcg.com/press/10january2024-imprese-e-gestione-del-rischio-non-e-il-momento-di-tagliare-i-fondi
[5] Multinazionale leader della consulenza strategica e fornisce servizi in diversi settori e aree geografiche le sue expertise ai clienti che vogliono identificare nuove opportunità, affrontare le sfide critiche e aiutarli nella trasformazione del business.

di nuove opportunità che possono essere sfruttate in modo sistematico e riuscire a trarre vantaggio anche da situazioni imprevedibili.

La pianificazione degli scenari, sia peggiori che migliori, risulta essere una strategia che consente all'azienda di pensare in anticipo a come può sfruttare al meglio gli ultimi sviluppi e tendenze del mercato, ottenendo un oggettivo vantaggio competitivo. Un prerequisito per effettuare frequenti analisi di scenario è la capacità di quantificare rapidamente l'impatto sulle metriche chiave. Per farlo, le aziende devono definire le premesse e i risultati richiesti, garantire la trasparenza sulla metodologia di calcolo e le ipotesi e stabilire un processo di pianificazione a risposta rapida. La recente esperienza ha insegnato che neanche la prevenzione può aiutare a sconfiggere eventi imprevedibili e fuori da ogni immaginazione[6]: l'azienda deve essere agile e adattarsi a nuovi scenari, deve essere poco burocratica[7] e rigida.

1.2. L'evoluzione della gestione del rischio aziendale: classificazione, variabili e strategie di mitigazione

A partire dagli anni '90, il rischio nell'attività imprenditoriale ha assunto particolare valenza, attraverso il supporto delle varie normative che hanno imposto l'obbligo per le imprese di dotarsi di procedure di contenimento del rischio e di controllo interno, portando all'attenzione di tutte le imprese la necessità di destinare adeguate risorse alla gestione dell'incertezza.

Diversi sono stati gli studi e gli autori, tra cui Finetti, Savage, Knight, Ferrero, che hanno tentato di fornire un'unica definizione di rischio, anche se risulta ancora difficile far confluire i diversi

[6] Il riferimento è alla situazione che si è verificata a febbraio 2020 con la pandemia mondiale. Molte aziende si sono trovate costrette a licenziare e a chiudere, mentre altre, sono state lungimiranti e hanno sfruttato il periodo, traendo vantaggio da una situazione non prevista.
[7] Le aziende burocratiche sono quelle che basano i loro processi su numerose normative. Solitamente sono molto burocratici gli enti pubblici.

aspetti e fornirne una completa ed esaustiva[8]. Si riporta in breve una classificazione dei rischi aziendali, che analizza dal generale al particolare, suddividendoli in elementi oggettivi e soggettivi

Partendo degli elementi soggettivi, questi dipendono principalmente dalle ipotesi formulate dal management sugli effetti derivanti da decisioni e comportamenti e derivano dall'esperienza, dal grado di conoscenza di chi la formula. In questo caso, il rischio aumenta quanto maggiore è il numero di elementi soggetti e, quindi, la possibilità di commettere errore nel costruire la previsione. L'esperienza del soggetto[9] diventa, quindi, parte integrante di tutto il processo della valutazione e, di conseguenza, il grado di incertezza e la probabilità di sbagliare possono differire in situazioni similari.

La restante parte della componente di rischio è l'oggettività correlata all'aleatorietà degli eventi che l'azienda è costretta a subire e alle modalità attraverso le quali gli eventi[10] si manifestano.

La valutazione del rischio è la risultante connessa al processo di formulazione delle ipotesi e ai processi di analisi valutative relativi a eventi incerti: e gli effetti sull'azienda con l'analisi di processi di valutazione, con la previsione e con la stima degli andamenti futuri.

Il potenziale rischio aziendale può essere, quindi, considerato come l'esito di un processo di analisi e di valutazione, originato dall'incertezza e dalla coesistenza di fatti dei quali non è possibile stabilire esattamente le manifestazioni future. La previsione e la valutazione della stima degli andamenti futuri, si basa sullo scostamento potenziale esistente tra l'ipotesi presunta

[8] Seppur la letteratura ha dato ampio contributo, non sarà oggetto di trattazione e, mi soffermerò a riportare solo una classificazione che analizza dal generale al particolare, suddividendo i rischi aziendale in elementi oggettivi e soggettivi. La scelta di non includere un approfondimento è dettata dalla scelta di soffermarsi si aspetti più pratici del tema.

[9] Il soggetto nella frase è il management o responsabili o chiunque abbia in azienda un ruolo decisionale/valutativo.

[10] Durante la trattazione dell'elaborato si fa uso della parola "evento" senza alcuna connotazione positiva o negativa. Si intende indicare solo un episodio non ordinario.

(elemento soggettivo) e quanto empiricamente osservato (elemento oggettivo). È strettamente correlato alla combinazione di variabili di sistema, quali istituzionali, economiche, patrimoniali, organizzative, che determinano sia l'esposizione al rischio, sia le potenzialità di creazione di valore dell'impresa. Le variabili che comportano fattori di rischio sono: istituzionali, economiche, patrimoniali, organizzative e produttive.

Innanzitutto, le variabili istituzionali comportano rischi prevalentemente inerenti al mancato soddisfacimento delle attese degli stakeholder, provocando una scarsa stabilità degli assetti proprietari, e delle relazioni che l'impresa intrattiene con altri portatori di interessi. È particolarmente importante l'insieme dei sistemi predisposti, per garantire all'impresa risultati coerenti con le aspettative dei vari stakeholder.

economiche sono relative alla gestione caratteristica, patrimoniale e finanziaria determinano le circostanze economiche che condizionano l'attività d'impresa e possono comportare l'insorgere di fenomeni rischiosi, derivanti da eventi aziendali, ovvero riconducibili al contesto competitivo.

Quando facciamo riferimento alle fonti di finanziamento e agli impieghi di tali risorse, le variabili che incidono sono quelle economiche, che rappresentano la criticità del reperimento di mezzi e dalle decisioni relative al loro investimento, nonché la possibilità di scelta di strutture finanziarie non ottimali.

Le variabili organizzative definiscono, invece, la struttura organizzativa dell'impresa, le sue procedure, il suo personale. I rischi sono riconducibili alla scarsa efficienza di tale assetto e all'eventualità che potrebbe essere pregiudicato il raggiungimento degli obiettivi prefissati.

Infine, le variabili produttive sono relative alla struttura tecnico-produttiva, quindi, scelta dei processi di realizzazione dell'output e della dimensione di quest'ultimo. L'incertezza è legata alla struttura dei costi e alla capacità del prodotto di soddisfare le esigenze della clientela.

Individuare le variabili consente di definire gli ambiti a cui fanno riferimento le varie tipologie di rischio che si configurano, cosicché l'azienda può definire le strategie e modalità di risk management da attuare. Oltre agli elementi soggettivi e oggettivi, il sistema dei rischi aziendali è caratterizzato anche da fattori interni ed esterni all'impresa. I principali fattori esterni o endogeni hanno origine da eventi esterni al complesso aziendale e sono in continuo mutamento, grazie alle continue complesse interazioni e possono essere ricondotti a quattro principali sistemi: economico, politico-giuridico, tecnologico ed ecologico. Hanno un impatto economico-patrimoniale sull'impresa, ma non risultano da essa influenzabili e gestibili e sui quali l'azienda non ha possibilità di modificarne la natura, la direzione e la dinamica. Risultano essere ingestibili e l'impresa può mettere in atto solo meccanismi di prevenzione e di trasferimento a terzi in modo da tutelarsi dall'eventuale manifestazione di questi pericoli. Rientrano in questa tipologia di rischi le variazioni del ciclo economico, la dinamica dei tassi di interesse e di cambio, le catastrofi naturali e tutte le variabili non governabili dall'impresa stessa.

I fattori interni riguardano sostanzialmente la struttura organizzativa dell'impresa stessa, il proprio management, le risorse, i processi, i meccanismi operativi, la propria cultura e i comportamenti e le dinamiche delle persone che in essa vi operano e sono la diretta conseguenza delle dinamiche poste in essere all'interno dell'impresa. Hanno origine dalle scelte dagli attori organizzativi dell'azienda (management, CEO, CdA, …), dall'organizzazione della produzione, dalla logistica, dal personale. L'azienda, quindi, è in grado di influenzare, almeno parzialmente, l'andamento e la portata di questi rischi, ma non ne è esente.

Oltre ai rischi endogeni ed esogeni, l'azienda è soggetta anche a rischi di natura prettamente economica, i cui effetti scaturiscono dal verificarsi dell'evento rischioso. Il rischio economico determina effetti positivi o negativi sull'attività d'impresa, generando impatti sulla produzione

di beni e/o servizi e sono in grado di produrre delle perdite monetarie. Il rischio non economico, o extra-aziendale, non genera effetti sull'attività aziendale, in quanto l'eventuale perdita generata, non è quantificabile a livello monetario, ma potrebbe provocare delle perdite che seppur non monetizzabili, che incidono sugli asset intangibili dell'impresa (impatto morale o sociale).

C'è da considerare che non tutti i rischi comportano impatto sfavorevole: i rischi speculativi possono produrre esiti anche positivi, nonostante siano connessi a situazioni incerte e future. Sono rischi imprenditoriali e non assicurabili per via della loro frequenza quotidiana di manifestazione, per la difficoltà di ridurre le conseguenze derivanti e dal ritardo di osservazione con cui vengono esaminati. Le principali aree di riferimento sono i rischi di business, collegati allo svolgimento dell'attività imprenditoriale (rischi finanziari, operativi e strategici), e i rischi derivati, derivanti dalle attività finanziarie diverse dal core business.

A differenza dei rischi speculativi, i rischi puri[11] sono eventi sempre sfavorevoli, caratterizzati da asimmetria negativa, imprevedibilità e da elevata probabilità di sostenere un onere elevato, senza poter mai ricavare un guadagno. Dato che non possono essere previsti ex-ante con la previsione, possono essere solo gestiti ex-post con il trasferimento del rischio e per tale ragione sono definiti anche rischi assicurabili, proprio in ragione del fatto che è possibile il loro trasferimento ad imprese assicurative, essendo connessi alla responsabilità civile, quelli che causano danni materiali alla proprietà di impresa o a quella altrui, a catastrofi naturali, morte, invalidità e malattia dei dipendenti. Hanno una manifestazione improvvisa e immediatamente osservabile, con effetti economici che si determinano in un brevissimo lasso di tempo, ma consentono di ridurre le conseguenze fisiche ed economiche dell'evento tramite l'adozione di tempestive misure di contenimento o riduzione del danno. Rientrano tra questa tipologia di

[11] Floreani, Introduzione al Risk Management, 2005

rischi quelli legati ai beni aziendali, quelli che possono determinare un impatto aziendale negativo in seguito al danneggiamento o alla perdita di disponibilità di beni aziendali, oppure quelli sulle persone, che possono determinare un impatto aziendale negativo in seguito a eventi che colpiscono le persone operanti nell'azienda, oppure, ancora, i rischi di responsabilità riguardanti gli impatti aziendali negativi che possono derivare da danni arrecati all'impresa a persone, animali o cose di terzi.

Nella realtà aziendale, è difficile individuare distintamente i rischi puri da quelli speculativi: di fatto tutti i rischi sono potenzialmente qualificabili come speculativi, se regolarmente formulati dalle aspettative e la differenza tra le due tipologie è una mera implicazione gestionale. Il processo logico di risk management può essere il medesimo; ciò che gli identifica è che nei rischi puri la modalità di gestione è la fase di identificazione e la prevenzione, invece per gli speculativi la fase fondamentale è quella di monitoraggio e la prevenzione non è efficace come modalità di gestione.

Altro elemento da tener presente nelle scelte strategiche sono indubbiamente le dinamiche dell'economia globale, il contesto competitivo e lo sviluppo atteso di un mercato. Attraverso le previsioni macroeconomiche, le analisi dei driver di domanda e offerta si possono definire gli scenari a supporto delle decisioni di medio-lungo periodo. Un processo che comporta rischi sistemici o non diversificabili, sintetizzabili nel concetto di rischio di mercato, essendo soggetto all'andamento del ciclo economico, alle oscillazioni del tasso di interesse e al tasso di cambio, alla propensione degli investitori e a qualsiasi evento la cui rischiosità non può essere eliminata mediante la diversificazione.

Altri rischi possono derivare dalle caratteristiche proprie dell'impresa stessa e al settore in cui essa opera. Per la loro natura possono essere mitigati attraverso il processo di diversificazione, mediante un processo costituito con numerose variabili aleatorie non perfettamente correlate

tra di loro, al fine di ridurre la variabilità complessiva attraverso la compensazione dei rischi, definiti specifici o diversificabili.

1.2.1 Evoluzione del rischio operativo[12]

Soprattutto nell'ultimo decennio, e in particolare nel 2020, si è verificato un aumento del numero e della portata dei rischi con i quali l'azienda deve confrontarsi. La facilità con cui un'azienda può essere attaccata ha consentito l'aumento della sensibilità e dell'interesse a prevenire i rischi.

Nella nona edizione dell'Allianz Risk Barometer[13] 2020, i rischi maggiormente percepiti a livello globale e visti come più pericolosi e costosi per le aziende sono diventati quelli informatici, con il 39% di risposte, contro il 15° posto e il 6% di risposte di sette anni fa, sorpassando l'interruzione dell'attività, che ha ottenuto il 37% di risposte. Da questo dato, emerge la consapevolezza della minaccia informatica e di come è cresciuta rapidamente negli ultimi anni, una spinta derivante anche dal commercio dei dati, al ricorso dei sistemi IT e da una serie di importanti incidenti.

La "scalata" verso la vetta della categoria "Cyber incidents" nella classifica è emersa già nel 2018, anno caratterizzato da numerosi attacchi informatici, alcuni dei quali con importanza mediatica e nell'anno successivo ha occupato il primo posto con Business interruption risk.

---

[12] Il rischio operativo è quello più importante a livello di gestione di un'impresa. Il rischio produttivo è tutto ciò che incide in via diretta sul patrimonio integrale dell'azienda. Riguarda aziende con molti costi fissi e piccoli margini di contribuzione
La Banca d'Italia, nelle Disposizioni di vigilanza per le banche Circolare n. 285 del 17 dicembre 2013, Titolo II - Capitolo 5, e nel recepire gli accordi di Basilea, ha definito il rischio operativo come la possibilità "*di subire perdite derivanti dall'inadeguatezza o dalla disfunzione di procedure, risorse umane e sistemi interni, oppure da eventi esogeni. Rientrano in tale tipologia, tra l'altro, le perdite derivanti da frodi, errori umani, interruzioni dell'operatività, indisponibilità dei sistemi, inadempienze contrattuali, catastrofi naturali."*
Sono ricompresi tra il rischio operativo anche quello legale (Tutte le tipologie di rischi sono presenti nell'allegato).

[13] Si tratta di un'indagine svolta annualmente a partire dal 2012 sui rischi aziendali. È condotta a livello mondiale da Allianz Global Corporate & Specialty e raccoglie circa 2.700 opinioni di esperti provenienti da oltre 100 Paesi, tra cui CEO, risk manager, broker ed esperti assicurativi.

Dall'interpretazione dei dati e dalla riconferma dell'indagine del 2020, gli incidenti cyber sono risultati le principali cause di interruzione dell'attività di cui le aziende temono per il maggiore impatto e per l'elevata perdita finanziaria.

È intuibile come i due rischi siano strettamente connessi tra di loro, dato che l'attacco informatico ha una valenza tale da poter compromettere la vita stessa dell'attività. Lo stesso CEO di Allianz Global Corporate & Specialty SE (AGCS), Joachim Müller, evidenziò "come il rischio informatico e il cambiamento climatico siano diventate le due sfide più impegnative che le aziende dovranno affrontare nel nuovo decennio", ma numerose sono le tipologie di danni e problematiche da fronteggiare. I Consigli di amministrazione e i risk manager, per ridurre i danni dalle performance operative, dai risultati finanziari e dalla brand reputation, devono obbligatoriamente affrontare i rischi informatici e quelli derivanti dal cambiamento climatico, perché "nell'era della digitalizzazione e del riscaldamento globale, la preparazione e la pianificazione di tali rischi è, quindi, sia una questione di vantaggio competitivo che di resilienza aziendale".

Un ulteriore incremento statisticamente significativo dei rischi aziendali è relativo allo scenario legislativo e regolamentare (+6%) e alle nuove tecnologie (+4%). La conseguenza che ne deriva è che le aziende si trovano ad affrontare rischi di violazioni di dati sempre più grandi e costose, un aumento del ransomware e degli incidenti di spoofing, con la sempre più alta possibilità di incorrere in sanzioni pecuniarie o controversie legali in materia di privacy. Una grande violazione dei dati, che può compromettere più di un milione di dati, costa in media 42 milioni di dollari, con un aumento dell'8% rispetto all'anno precedente. Il Deputy Global Head of Cyber di AGCS, Marek Stanislawski, ha affermato come "gli incidenti stanno diventando sempre più significativi e le grandi aziende sono colpite da attacchi sempre più sofisticati e da

ingenti richieste di estorsione. Cinque anni fa, una tipica richiesta di riscatto sarebbe stata di decine di migliaia di dollari, mentre ora può superare il milione di dollari".

Le piattaforme digitali e il ricorso alla supply chain se da un lato hanno consentito da un lato una maggiore sicurezza, una maggiore trasparenza e una tracciabilità delle attività più puntuale, dall'altro però risultano vulnerabili e un incendio in un data center o un guasto tecnico o l'attacco di un hacker, può provocare enormi perdite[14], tra cui l'interruzione dell'attività. È stata un'indagine realizzata da Deloitte che ha evidenziato come il timore degli incidenti informatici non frena la corsa delle imprese italiane verso l'uso e l'applicazione dell'Intelligent Automation, dato che i benefici derivanti sono rilevanti sia in termini di miglioramento di produttività, di efficienza e accuratezza, che in ambito di performance aziendali, di riduzione dei costi e aumento dei rischi.

Figura 1.1 Principali rischi aziendali

Cosa rischia il mondo

La classifica dei rischi più sentiti a livello mondiale nel 2020.
Il ranking varia in base alla posizione raggiunta ogni anno da ciascuno dei rischi indicati dagli intervistati

Rischio percepito rispetto al 2019

↑ Superiore ↓ Inferiore ↔ Nessun cambiamento

		Percentuale	Classifica 2019		Tendenza
1	Rischi informatici (crimine informatico, violazione dei dati, guasti IT)	39%	2	37%	↑
2	Interruzione di attività (anche della supply chain)	37%	1	37%	↓
3	Cambiamenti nello scenario legislativo e regolamentare (sanzioni economiche, protezionismo, Brexit, disgregazione dell'Eurozona)	27%	4	27%	↑
4	Catastrofi naturali (tempeste, inondazioni, terremoti)	21%	3	28%	↓
5	Cambiamenti nei mercati (volatilità, aumento della competizione/arrivo di nuovi operatori, fusioni e acquisizioni, stagnazione e fluttuazione del mercato)	21%	5	23%	↔
6	Incendio, esplosioni	20%	6	19%	↔
7	Cambiamento climatico/aumentata instabilità metereologica	17%	8	13%	↑
8	Danno reputazionale o d'immagine	15%	9	13%	↑
9	Nuove tecnologie (impatto dell'aumento della maggiore interconnettività, delle nanotecnologie, dell'intelligenza artificiale, della stampa 3D, dei droni)	13%	7	19%	↓
10	Cambiamenti nello scenario macro economico (programmi di « austerity », aumento del prezzo dei beni di consumo primari, inflazione/deflazione)	11%	13	8%	↑
11	Rischi politici (guerra, terrorismo, sommosse)	9%	11	9%	↔
12	Carenza di manodopera qualificata	9%	10	9%	↓
13	Blackout energetici	8%	17	2%	↑
14	Mancanza di qualità, difetti seriali, richiamo di prodotti	8%	12	9%	↓
15	Furto, frode e corruzione	7%	15	7%	↔
16	Rischi ambientali (inquinamento)	7%	14	7%	↓
17	Rischi sanitari (es. pandemie)	3%	16	3%	↓
	Altro	3%			

Fonte: Allianz Global Corporate & Specialty

Tabella 1.1 L'immagine mostra il confronto tra la classifica 2019 e 2020 elaborata da Allianz Global Corporate & Specialist, nel Allianz Risk Barometer. La grafica è a cura del Corriere della Sera.

[14] Affermazione effettuata da Raymond Hogendoorn, Global Head of Property and Engineering Claims di AGCS.

Dalla classifica emerge, inoltre, che anche le vicende geopolitiche e gli attentati terroristici incidono sempre di più le aziende con danni alle proprietà, interruzioni d'attività e perdita di reddito, dovuti alla prolungata chiusura dei negozi, al mancato afflusso di clienti e turisti e all'impossibilità per i dipendenti di raggiungere il loro posto di lavoro per problemi di sicurezza.

Rispetto agli ultimi 6 anni, è stato verificato un aumento del +37,5% di attacchi informatici nel 2019, rispetto ai precedenti 6 anni, una crescita del +12% crescita di malware e attacchi DDOS dal 2018 al 2019, il 48% in più degli attacchi gravi nel triennio 2017 – 2019 e un aumento del fatturato mondiale del cybercrime di 1.000 miliardi nel 2020, giro d'affari criminali, che sta superando per rilevanza il traffico di droga.

Bisogna evidenziare inoltre, come l'emergenza sanitaria causata dal virus SARS-CoV-2 ha innalzato gli attacchi informatici. I dati in Italia sono stati rilevati dall'Osservatorio Cybersecurity di Exprivia[15] che ha registrato nel secondo trimestre dell'anno un aumento del 250% rispetto al periodo precedente, un aumento nel trimestre luglio-agosto-settembre con 148 tra attacchi, incidenti e violazioni della privacy, la metà dei quali solo a settembre. Il mese che ha registrato il numero più alto di violazioni è stato giugno con 86 attacchi, seguito da settembre che ne ha registrati 70. La maggior parte di questi episodi di attacchi, incidenti e violazioni della privacy a danno di aziende, privati e pubblica amministrazione, sono correlati al Coronavirus, che ha imposto lo smart working, una maggiore connessione ai social network, alla riapertura delle industrie subito dopo il lockdown e alla mole di dispositivi IoT connessi in rete senza protezione, facendo emergere l'inadeguatezza con cui aziende ed enti pubblici, ma anche soggetti privati, proteggono dati sensibili e sistemi informatici.

[15] La società si occupa di progettazione e sviluppo di tecnologie software innovative e di prestazione di servizi IT per il mercato bancario, medicale, industriale, telecomunicazioni e Pubblica Amministrazione.

Il 60% di tali episodi ha provocato il furto dei dati, superando sia le violazioni della privacy (11% dei casi) che le perdite di denaro (7%), con 18 milioni di euro di sanzioni che sono state irrogate dal Garante per la protezione dei dati personali.

Gli episodi di cybercrime hanno colpito in particolare sistemi di videosorveglianza, la PA, di cui i Comuni, sono stati gli enti che hanno mostrato una maggiore vulnerabilità e il settore Finance, settore molto redditizio e di interesse dei cyber-criminali.

Anche il settore Industry, in particolare aziende energetiche e manifatturiere, la sanità e il settore retail sono state vittime di attacchi rilevanti.

L'evoluzione delle minacce di cyber crime verificatasi nell'ultimo decennio, con l'incremento vissuto nell'ultimo anno, hanno imposto sempre di più l'uso di modelli "intelligenti" di analisi dei rischi. La gestione della sicurezza delle informazioni deve rappresentare uno dei fattori principali per raggiungere gli obiettivi aziendali e un punto strategico per consentire la crescita della digitalizzazione nelle organizzazioni. I modelli intelligenti sono capaci di adattarsi al contesto aziendale e ai processi interni all'organizzazione, oltre ai fattori esogeni in grado di influenzare il profilo di rischio aziendale. I processi tradizionali di tutela non sono più in grado di garantire la protezione.

Il rischio operativo, insito nell'attività di impresa può essere contenuto riorganizzando i processi di controllo interni dell'impresa in modo da rispondere in maniera puntuale ed efficace ai mutamenti di mercato. Riconoscere i segnali di un'anomalia permette all'organizzazione di pianificare un potenziale scenario e di calcolare le potenziali perdite. L'utilizzo di key Risk Indicatoris supporta il calcolo e il monitoraggio dei fattori che più frequentemente incidono sull'andamento dell'azienda. Gli indicatori sono dinamici e differenti nelle differenti realtà e sfruttano algoritmi sofisticati ed evoluti, rilasciando un cruscotto informatico e cronologico su cui il management può lavorare.

1.1.2. Gestione del rischio nel sistema d'azienda: Il Risk Management

Conoscere un rischio, consente di diminuire la probabilità di subire una perdita, di poterla contenere e gestire, ma non in modo assoluto dato che le sfide strategiche che oggi attraversano il sistema economico e imprenditoriale risultano di non facile risoluzione. Si inizia a strutturare un piano di risk management all'interno delle organizzazioni statunitensi tra la fine degli anni '40 e l'inizio degli anni '50, mentre in Europa viene inserito tra i processi aziendali a partire dagli anni '70. La disciplina ha avuto un'evoluzione molto rilevante con una rapida accelerazione, grazie alle sfide odierne: si è passati da una visione puramente assicurativa del rischio a una visione più gestionale, che comporta la necessità di trattare il rischio in maniera proattiva, cogliendo i vantaggi di certe scelte. Non nasce, quindi, come funzione di controllo, ma nasce come funzione di supporto, evoluzione che è stata influenzata da numerosi eventi, imposizioni normative, fenomeni tecnologici, sfidanti e innovativi, e i macro-trend che caratterizzano il mercato dei consumatori e degli investitori, che hanno consentito il rafforzamento e la sensibilizzazione verso il ruolo ricoperto da tale area.

Il risk management rappresenta una dimensione di governo e gestione dell'impresa volta al presidio della stabilità strategica e reddituale dell'impresa[16] . Consente al CdA[17] e il top management[18] di prendere decisioni strategiche e d'investimento di medio – lungo periodo consapevoli degli eventi rischiosi. Può considerarsi, in questa accezione, l'espressione di una cultura d'impresa costituita sulla capacità di individuare le fonti di ogni tipologia di rischio d'impresa, saperle valutare e trattare correttamente.

L'importanza della gestione del rischio d'impresa non sempre è sufficientemente percepita e compresa da tutte le organizzazioni: spesso è considerato ulteriore costo da affrontare, senza

[16] Tratto dall'articolo "Outsourcing risk management" Popoli, 2008
[17] O al board aziendale
[18] Il cd C-Suite

tener conto dei vantaggi competitivi che si possono acquisire e ai benefici valoriali e culturali potenzialmente ottenibili.

Il risk management è un processo dinamico e continuo che ha il compito di identificare i rischi intrinseci nell'attività aziendale. L'output del processo è sviluppare strategie per mitigare e controllare i rischi e preservare l'organizzazione, evitando o limitando interruzioni di servizio e/o disfunzioni.

Il processo, fondamentale per qualsiasi tipo di azienda, coinvolge gli altri elementi del sistema di controllo aziendali[19] e per essere efficace deve essere integrato nella cultura dell'organizzazione, diventando quindi parte integrante dei processi e realizzare una strategia aziendale efficace.

La gestione del rischio è iterativa e aiuta le organizzazioni a definire la strategia, raggiungere gli obiettivi e prendere decisioni informate. La gestione del rischio fa parte della governance e della leadership ed è fondamentale per il modo in cui l'organizzazione viene gestita a tutti i livelli. Contribuisce al miglioramento dei sistemi di gestione e si basa su principi, quadro e processi delineati dalla normativa indetta dall' Organizzazione internazionale per la normazione, ISO 31000:2018[20]. L'Organismo Internazionale per la standardizzazione, ISO, ha delineato a partire dal 2009, in conformità con IEC, le linee guida per un processo di risk management ottimale e supportare le organizzazioni ad adottare condotte che consentono di gestire in modo efficiente, efficace e coerente il rischio. La direttiva fornisce una ragionevole

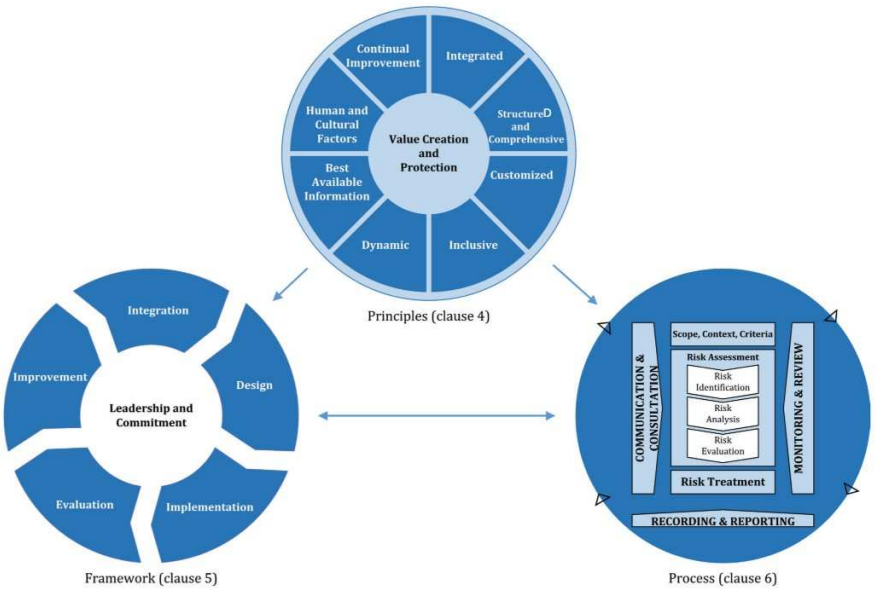
[19] Il risk management è il risultato dell'analisi di informazioni derivati diverse aree aziendali, come dal controllo interno e valutazione delle performance, e fornisce utili linee guida per la delineazione della strategia e dei processi gestionali

[20] L'ISO è l'Organizzazione Internazionale per la Standardizzazione (*International Organization for Standardization)* è una federazione mondiale di organismi di normazione nazionali (organismi membri dell'ISO). Il lavoro di preparazione degli standard internazionali viene normalmente svolto attraverso i comitati tecnici ISO. È la principale organizzazione a livello mondiale per la definizione di norme tecniche.

Fonte: https://shahrdevelopment.ir/wp-content/uploads/2020/03/ISO-31000.pdf
Fonte: https://www.iso.org/directives-and-policies.html

sicurezza che gli obiettivi definiti in fase di pianificazione siano raggiunti garantendo che il rischio residuale si collochi al di sotto di una soglia di accettabilità.

Figura 1.2: Principi, quadro e processo



Fonte: https://www.myr.it/norma-iso-31000-cose-e-come-la-utilizziamo/

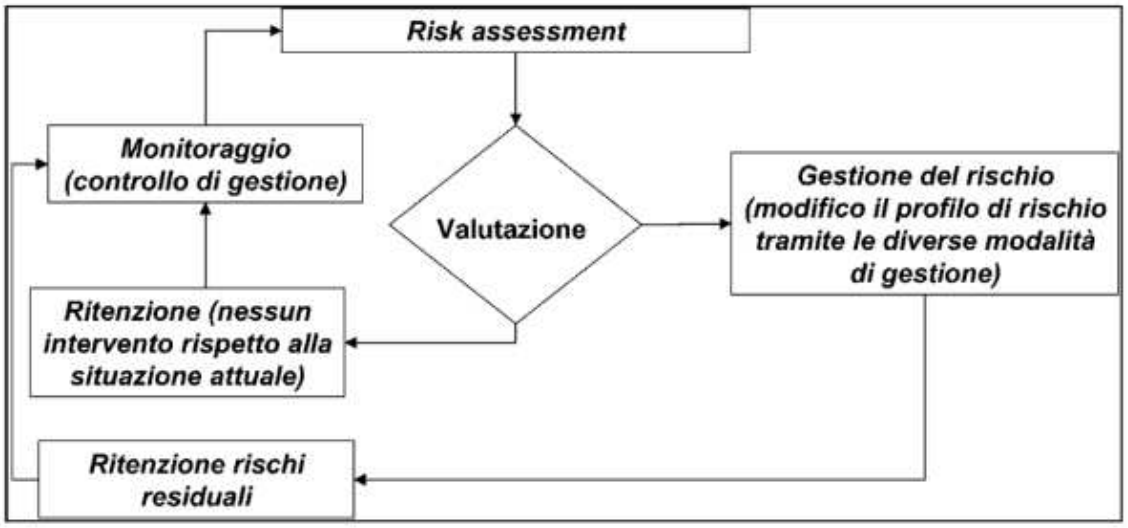
La pratica, fondamentale per migliorare la resilienza e la capacità dell'organizzazione, è costituita da otto principi, evidenziati nello schema in alto nel grafico a torta con il titolo "Value Creation and Protection", rappresentano la base per la gestione del rischio. I principi devono essere presi in considerazione per costruire la struttura e i processi di gestione di rischio, che si compongono di cinque fasi principali: definizione del rischio, mappatura, risk management, reporting di comunicazione del rischio residuo e monitoraggio.

La prima fase di definizione del rischio: si identificano i rischi e si allineano con gli obbiettivi strategici. È una fase estremamente delicata, in cui le variabili che analizzate sono differenti in ogni organizzazione. Sarà importante interrogarsi sulla probabilità che un rischio si realizzi e che impatto avrà sull'organizzazione

La seconda fase è la mappatura del rischio o Risk Assessment**:** Caratterizzata da quattro principali tipologie di rischio (operativo, strategico, di compliance e di natura economico-

finanziaria), ha l'obbiettivo di identificare i rischi che limitano o interferiscono con il conseguimento degli obiettivi predisposti dal management. Per ogni singolo rischio identificato, si deve valutare la natura, l'impatto, positivo o negativo, e la probabilità di accadimento. Il valore di rischio è l'indice risultante dal prodotto fra probabilità e impatto di un determinato evento. Nella fase di risk assessment è ricompresa anche la fase di risk appetite, la propensione di rischio dell'organizzazione che il vertice ha identificato. Si definisce una soglia massima di rischio alla quale l'organizzazione è in grado di esporsi, senza compromettere il proprio business. Se il rischio calcolato come probabilità per l'impatto supera la soglia di risk appetite è necessario avviare la fase successiva di risk management. Il Risk assessment è una valutazione continua e constante, per intervenire in caso di modifiche. Tramite le diverse modalità di gestione e applicazione della/e strategia/e più inerenti, è possibile diminuire il livello di rischio.

Figura 1.3: La valutazione dei rischi di un'azienda/attività/funzione



Fonte immagine tratta da "Enterprise Risk Management. I rischi aziendali e il processo di risk management" di Alberto Floreani

La terza fase è il Risk Management**:** Lo scopo della seguente attività è quella di mitigare il rischio quando si supera il risk appetite e, quindi, necessario riportare il rischio alla soglia di

tolleranza, eliminando il rischio in eccesso, attraverso la cessione del rischio o il cambiamento di prassi e procedure aziendali, con diverse modalità di trattamento del rischio che consentono di abbassare il livello di rischio e di renderlo tollerante. Si compone di due momenti:

a. formulazione, fase in cui si definiscono le alternative strategiche che derivano dall'analisi dell'ambiente interno ed esterno in cui opera l'azienda. Il sistema di controllo interno di un'azienda deve essere designato in base alla tipologia di esposizione ai rischi presenti nelle operazioni aziendali.
b. realizzazione, fase in cui si pianifica un piano strategico, volto a circoscrivere le perdite che potrebbero verificarsi a causa di eventi.

Il risk management si attua anche ai rischi ineliminabili[21] .

La quarta fase Reporting di comunicazione del rischio residuo. Una volta individuato nella fase di risk management la soglio di rischio, è necessario redigere un report per comunicare al management i risultati conseguiti, attraverso informazioni tempestive e chiare. Dal rischio residuo, calcolato al netto delle misure di sicurezza e mitigazione, si evidenzia il rischio residuo, insito anche dopo l'applicazione delle misure di contenimento. È compito del vertice aziendale prendere la decisione finale sul bilanciamento fra minacce e opportunità.

La gestione del rischio non giunge mai ad una vera chiusura: infatti la quinta fase è costituita dal monitoraggio continuo, che permette di migliorare ed intervenire, in caso di lacune e/o modifiche normative.

Il processo fin qui descritto, non è una tantum, ma deve essere ripetuto nel tempo, in quanto il rischio è mutevole nel tempo. Il processo di risk management varia al variare delle condizioni aziendali, del settore e geo-politiche. Inoltre, attraverso le continue osservazioni consentono di

[21] Si parla di rischi che sono ineliminabili, nel momento in cui è eliminato non è più un rischio, il rischio per definizione compromette l'obiettivo e quando non lo compromette più non è un rischio.

aggiornare gli output di processo, in quanto deriva da informazioni storiche, attuali e aspettative future.

Il processo di gestione del rischio deve prendere in considerazione eventuali limitazioni incertezze delle informazioni, dell'operatività e degli errori umani.

Awims System di Zucchetti è una società che ha sviluppato una piattaforma SaaS per la gestione efficiente e sicura della forza lavoro e ha delineato lo schema che viene presentato di seguito per presentare il loop delle fasi che compongono il risk management.

Il modello circolare, rappresentato in Fig 1.3, illustra le cinque fasi del processo di gestione del rischio. Attorno al "Risk Management Process" (Processo di Gestione del Rischio) ruotano cinque segmenti di colori diversi, ognuno dedicato a una specifica fase del processo.

Figura 1.4: Illustrazione del processo di Risk Management

Fonte: https://www.awms-system.com/blog/prodotto/risk-management-significato-fasi-e-strategie/.

Il sistema è costituito da tre componenti fondamentali:

I. la componente soggettiva formata dagli attori del processo,
II. l'insieme di attività volte all'identificazione, valutazione e trattamento del rischio
III. la componente oggettiva che sono le tecniche e gli strumenti utilizzati per fare risk management.

Nel processo è importante definire non solo l'obiettivo sul quale il rischio va ad agire, ma anche il responsabile della gestione di quel rischio, il risk manager, figura alla quale sono richieste competenze gestionali a 360°, dalla conoscenza approfondita del business e dei mercati finanziari, al settore assicurativo e alla gestione d'impresa. La figura di risk manager è obbligatoria per società quotate in borsa, mentre per le PMI è ricoperta dall'imprenditore che definisce il rischio, la soglia di accettabilità (risk appetite), decide come correggere i rischi rilevati e quali azioni implementare.

1.1.3. Obiettivi del risk management e normativa di riferimento

Il processo di valutazione dei rischi è incentrato sugli obiettivi: la definizione del rischio pone l'attenzione sull'incertezza degli obiettivi, e, quindi, è indispensabile averli ben chiari.

Per affrontare il tema del risk management in ottica innovativa e più resiliente rispetto ai metodi tradizionali, è essenziale considerare diverse dimensioni, attori coinvolti e normativa in vigore. La fase di monitoraggio evidenzia la necessità di controllare costantemente i rischi che cambiano nel tempo, condizionati sia dal contesto esterno che interno. La gestione del rischio deve anticipare, rilevare, riconoscere e risponde a tali cambiamenti ed eventi in modo appropriato e tempestivo, ed essere continuamente migliorata attraverso l'apprendimento e l'esperienza.

L'obiettivo principale che il risk management o "gestione del rischio" persegue è quello di minimizzare le perdite e massimizzare l'efficacia e l'efficienza dei processi produttivi, ricorrendo a processi complessi che consentono alle aziende di valutare, in primis, la probabilità che un dato evento si verifichi e, successivamente, calcolare il modo di evitarlo o come ridurne gli effetti, trasferirla a terzi o come accettarne, in parte o totalmente, le conseguenze minimizzando gli impatti sull'attività di impresa.

Nel 2004, CoSO of the Tradeway Commission[22], costruisce un approccio al risk management, allo scopo di guidare i manager nella valutazione e nel miglioramento della gestione del rischio aziendale complessivamente inteso. Lo scopo della sua creazione è fornire delle linee guida per il management sui seguenti temi: aspetti organizzativi, audit interno, enterprise risk management e financial reporting.

Il modello integrato di l'Enterprise Risk management (ERM)[23] Framework intende comprendere tutti i rischi aziendali ed deve essere realizzato dal consiglio di amministrazione, dal management e da altri operatori della struttura aziendale, per formulare la strategia nell'organizzazione, progettato per individuare eventi potenziali che possono influire sull'attività aziendale, per gestire il rischio entro i limiti di rischio accettabile e per fornire la ragionevole sicurezza sul conseguimento degli obiettivi aziendali. Per il settore bancario[24], sono stati delineati framework più specifici, che tengono conto delle sue specificità e peculiarità.

Un altro organismo, già citato, che ha delineato standard normativi in materia di Risk management, con l'obiettivo di proteggere le informazioni aziendali da minacce di varia natura, è l'ISO:

- ISO 31000: risk management Principles and Guidelines[25]

[22] Il "Committee of Sponsoring Organization of the Treadway Commission" è una Commissione indipendente USA. Ha prodotto nel 1992 il "CoSO Report 1" (Internal Control over Finacial Reporting) e nel 2004 il "CoSO Report 2" (ERM, integrated framework), il cui modello include il CoSO 1 e offre una ricca sezione di tecniche applicative, talvolta alternative fra loro, a supporto dell'applicazione del modello. È uno standard internazionale di fatto fra i modelli ERM.

[23] Enterprise Risk Management - Integrated Framework (2004) sarà dedicato il paragrafo 1.2

[24] Gli istituti finanziari sono soggetti a maggiori vincoli rispetto ad altri settori, proprio per l'importanza del servizio che svolgono.
La gestione del rischio è stata introdotta in questi sistemi in modo radicato, un esempio possono essere gli accordi di Basilea.

[25] La ISO 31000, al contrario degli altri standard prodotti dal medesimo organismo, si pone come una guida da seguire, e non come una certificazione internazionale per le imprese che utilizzano determinati standard.

- ISO/IEC 31010:2009: Risk Management- Risk Assessment Techniques
- ISO GUIDE 73: 2009 che va a definire una serie di termini
- ISO 27001: strumento internazionale che definisce i requisiti per un sistema di gestione della sicurezza delle informazioni (SGSI)

L'implementazione di questi standard aiutano le organizzazioni a valutare i rischi e implementare le opportune salvaguardie, garantendo la privacy e la protezione dei dati sensibili.

Un'altra agenzia non regolatoria che promuove l'innovazione con il progresso della scienza, degli standard e delle tecnologie delle misurazioni è il National Institute of Standards and Technology, NIST[26], in cui, all'interno è stata costituito un framework che consiste in standard, linee guida e best practice per aiutare le organizzazioni a migliorare la loro gestione dei rischi per la sicurezza informatica, denominato NIST Cybersecurity Framework, NIST CSF. L'istituto promuove

la comprensione migliora la gestione dei rischi per la privacy, alcuni dei quali riguardano direttamente la sicurezza informatica e contribuisce a fornire indicazioni su alcune aree prioritarie, quali crittografia, istruzione e forza lavoro, tecnologie emergenti, gestione del rischio, gestione dell'identità e degli accessi, misurazioni, privacy, reti affidabili e piattaforme affidabili. Nello specifico, il NIST CSF fornisce una base di partenza per implementare la gestione della sicurezza delle informazioni e dei rischi per la sicurezza informatica, per le organizzazioni USA, ma è preso in considerazioni anche da realtà. Il framework è elastico per

[26] Gli incarichi di sicurezza informatica del NIST sono definiti da statuti federali, ordini esecutivi e politiche USA.

adattarsi al meglio ai processi di sicurezza di qualsiasi tipo di organizzazione, indipendentemente dal settore, fatturato, numero dipendenti.

Per ottenere una visione strategica e tattica dettagliata e realizzare una difesa a più livelli, estremamente resiliente nelle varie forme di attacco, l'ISO 27001 e il NIST CSF sono strumenti che devono essere utilizzare in modo complementari: infatti, il primo fornisce un framework rigoroso per la gestione della sicurezza a livello organizzativo, il secondo tratta di scenari di rischio cyber.

Le differenze che intercorrono tra i vari standard riflettono le differenti motivazioni e le specifiche tecniche ritenute più importanti dai loro ideatori e risultano adattabili alle varie organizzazioni e situazioni.

Gli standard cercano di stabilire una visione comune per quanto riguarda la struttura, i processi e le azioni da porre in atto e sono costantemente aggiornati per i continui mutamenti a cui è soggetta la disciplina.

1.1.4. Enterprise Risk Management

Il Framework "Enterprise Risk Management[27] – Aligning Risk with Strategy and Performance" ("Framework CoSo ERM") rappresenta un modello di riferimento per determinare processi robusti di gestione dei rischi in grado di orientare al meglio le strategie in base alle performance, considerando discontinuità che potrebbero derivare da scenari avversi, ma plausibili.

Ha una struttura concettuale secondo la quale un'organizzazione dovrebbe integrare i processi di risk management nella gestione del proprio business con l'obiettivo di realizzare la strategia, migliorare la misurazione dei risultati (performance) e creare valore nel lungo termine,

[27] ERM è stato già in parte trattate nei precedenti capito. Di seguito si riserva una trattazione più completa ed esaustiva

migliorando la capacità di risposta a eventi imprevisti e di adattamento alle mutevoli condizioni di mercato.

Nella fig.3 è rappresentato attraverso la forma elicoidale del DNA umano, per dimostrare che le sue cinque componenti sono l'identità delle aziende: governance e culture, strategy e objective-setting, performance, review e revision, information, communication e reporting.

Per riuscire in un'efficace gestione dei rischi si deve partire dall'individuazione specifica e accurata delle strategie chiave e degli obiettivi di business dell'organizzazione.
Secondo il Framework, le organizzazioni devono identificare i potenziali eventi di rischio che potrebbero mettere a rischio la propria business continuity, la propria capacità di implementare le strategie e conseguentemente, difficoltà a raggiungere l'obbiettivo prefissato.

Figura 1.5: DNA del processo di ERM

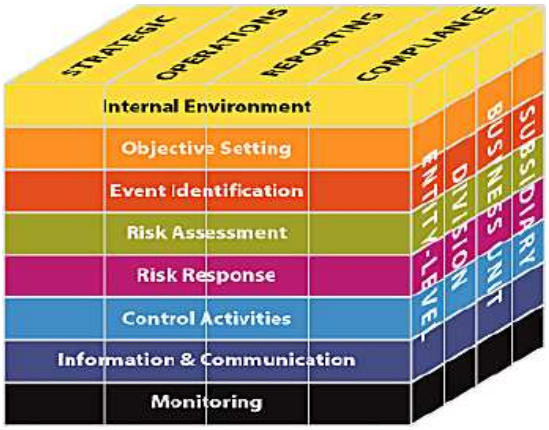
Figura 1.5: Enterprise Risk Management: Apply ERP to environmental, social and governance- related risks

Le strategie e gli obiettivi aziendali sono la chiave per costruire il processo di ERM che ha un approccio "strategy-driven" piuttosto che "riskdriven".

Il Framework COSO ERM[28] posiziona la gestione dei rischi al centro della catena del valore tra la missione, la visione e le performance, racchiudendo in un cubo, riportato di seguito le sei componenti sei principali aziendali più due trasversali[29], che possono essere ricondotte a quattro sezioni aziendali (subsidiary, business unit, divisione entity level) e quattro tipi di obiettivo, strategico, operazioni, reportistica e compliance.

Si evince una rappresentazione che integra la gestione dei rischi "a silos" con la cultura dell'organizzazione e dei processi di definizione, sviluppo della strategia e delle performance aziendali, promuovendo la condivisione delle informazioni all'interno dell'organizzazione.

Figura 1.6. Raffigurazione grafica con cubo delle aree del ERM



Fonte https://leganerd.com/2013/03/27/laudit-dei-sistemi-informativi/

L'ERM deve fornire una visione dinamica per la gestione del rischio organizzativo interno ed esterno attraverso misure strategiche o operative, garanzia della sicurezza dei dipendenti, gestione di programmi e progetti, protezione dei dati sensibili, forza lavoro, gestione dei talenti, rispetto delle normative statutarie e identificazione delle minacce finanziarie.

Un quadro pratico e completo consente al vertice aziendale di prendere decisioni efficaci per

[28] Il Framework ERM ha suscitato l'attenzione da parte di autorità di regolamentazione e agenzie di rating, portando a considerare il processo di gestione dei rischi come un'attività guidata da esigenze di compliance.
[29] Il modello ERM proposto da CoSO è rappresentato da un cubo le cui dimensioni sono costituite da 8 componenti che corrispondono alle "righe" del cubo; 4 tipi di obiettivi, le "colonne"; 4 livelli organizzativi dell'impresa, le "sezioni".

proteggere l’impresa dai danni e creare opportunità per consentire la continuità migliorando al tempo stesso le prestazioni. Compito del Risk manager è predisporre dall’analisi dei rischi, un piano degli imprevisti, applicando l’ERM agile, flessibile e basato sui dati ed esperienza empirica, applicando un approccio “Tone from the Top”, in azioni concrete con cui l'organizzazione possa raggiungere la mission e gli obiettivi di business.

Capitolo 2 Il processo di gestione del rischio informatico

2 La CyberSecurity

“Mentre un bene aziendale tangibile può essere protetto fisicamente in maniera più o meno agevole, la protezione dei dati rappresenta un’importante sfida per l’azienda. Esse, infatti, possono esistere in più posti contemporaneamente, possono essere trasferite ovunque in un battito di ciglia ed essere sottratte senza che ci si possa accorgere del furto.” Bruce Schneier, di Security Guru ha spiegato che cos’è la cybersecurity (cyber sicurezza o sicurezza informatica). Una disciplina che indica l’attività di analisi e il rilevamento delle minacce informatiche, e l’adozione di misure adeguate di prevenzione e contrasto per garantire la sicurezza di sistemi informatici. si intende quel ramo dell'informatica che si occupa dell'analisi delle vulnerabilità, del rischio, delle minacce o attacchi e della protezione dell'integrità fisica (hardware) e logico-funzionale (software) di un sistema informatico e dei dati in esso contenuti o scambiati.

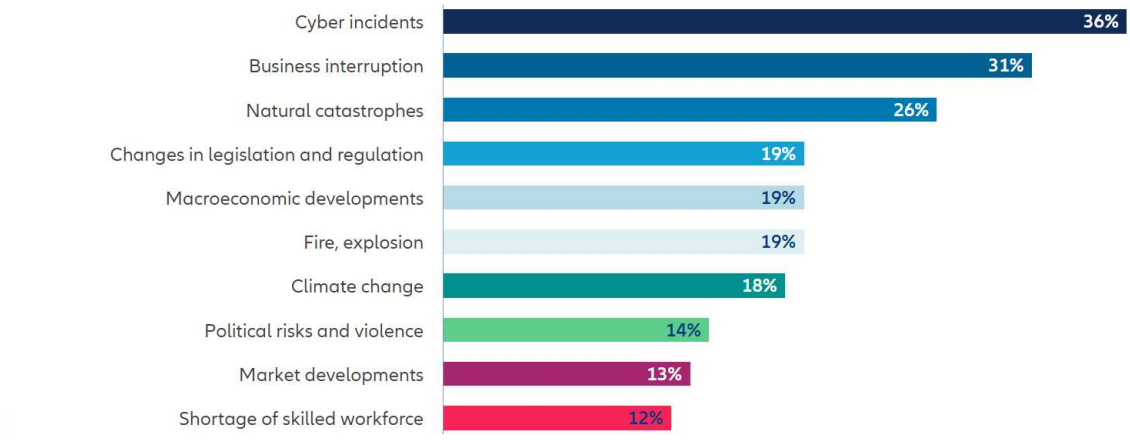
La CyberSecurity si distingue da molte altre scienze in quanto i reali competitor non sono coloro che forniscono soluzioni migliori, ma gli attaccanti che ogni giorno sviluppano tecniche e metodologie per compromettere i servizi utilizzati da coloro che si difendono per averne un beneficio. L’ “invasione” della digital trasformation supportata da tecnologie dell’informazione e dalla comunicazione (ICT), diventano

il motore trainante dello sviluppo economico e sociale delle società moderne, che è stata accompagnata negli ultimi anni da una crescente esposizione dei sistemi e delle infrastrutture ad attacchi informatici sempre più sofisticati e letali.

Per essere efficace, la CyberSecurity richiede delle misure di sicurezza che si fondano su tre elementi: le persone, i processi e la tecnologia. Questo approccio su tre fronti aiuta le organizzazioni a difendersi dagli attacchi specializzati come dalle minacce interne più comuni, per esempio le violazioni accidentali di dati o errori umani.

Per comprendere l'importanza della disciplina, dobbiamo paragonarla a una porta blindata, un mezzo che ha lo scopo di prevenire il problema del ladro, esattamente come la CyberSecurity si pone lo scopo di proteggere nel cyberspazio. Adottando un approccio di prudenza e consapevolezza, le misure di protezione si estendono nel momento in cui la sola porta blindata non è sufficiente per proteggere dall'intrusione e dal furto.

Figura 2.1: I primi 10 principali rischi globali aziendali nel 2024



Fonte: Allianz Risk Barometer | Allianz Commercial

Gli attacchi informatici sono, quindi, sempre più diffusi, coordinati e sofisticati. Nell'ultimo anno, il numero di attacchi alle password rilevati da Microsoft è salito alle stelle: da 579 a oltre 4.000 al secondo, di cui:

- 4.000: attacchi alle password al secondo
- 72 minuti: tempo medio impiegato da un utente malintenzionato per accedere ai tuoi dati privati se apri un'e-mail di phishing
- 3,5 milioni: carenza globale di professionisti della cybersecurity qualificati. Ecco perché è più importante che mai fornire ai team addetti alla sicurezza soluzioni innovative che li aiutino a rilevare, analizzare e rispondere rapidamente alle crescenti minacce informatiche.

Inoltre, gli ultimi anni sono stati caratterizzati da scenari di guerra cyber, che provocano un rischio di impatti, perché gli ambiti digitali sono estesi e pervasivi molto più di quanto non appaia superficialmente.

Per proteggersi, bisogna adottare dei concetti legati alla cyberigiene per riportare i concetti digitali alla stregua di un livello quotidiano e di base. Tutto deve diventare parte integrante dei comportamenti giornalieri. Iniziando a ragionare in questo modo si acquisirà la consapevolezza dei rischi giornalieri e delle misure di protezione necessarie per proteggere i propri dati e device e successivamente si diventa capaci di rivalutare il tema a livello della propria organizzazione e comprenderlo anche a livello nazionale o internazionale.

È necessaria una modifica culturale e una presa di coscienza rapida su quelli che sono i rischi di un incidente in ambito sicurezza: mancanza di cultura e consapevolezza sono le vulnerabilità più spesso sfruttate dagli attaccanti, prima ancora che vulnerabilità sul software o sull'hardware.

La distanza tra risorse di tempo, denaro e professionalità tra chi è specializzato negli attacchi e chi si difende, rende fondamentale ottimizzare gli investimenti per ridurre i rischi e i danni di un attacco. Gli investimenti, pertanto, non possono essere solo in funzione del ritorno economico, ma effettuati con la consapevolezza che la non-sicurezza del singolo dispositivo intelligente può trasformarsi nella non-sicurezza dell'intero pianeta digitale. Gli attaccanti non sono solo interessati a compromettere

un servizio, ma anche a catturare i dispositivi che verranno utilizzati come sorgente per successivi attacchi, senza creare alcun danno apparente al legittimo proprietario, che spesso è inconsapevole. Lo scopo è raccogliere una grande quantità di dati per rivenderli sul Dark Web. Il dato è oggi l'oro digitale, attorno al quale le organizzazioni possono acquisire dettagli sui propri potenziali clienti.

La sicurezza informatica è necessaria per sostenere il processo di digitalizzazione, che ha permesso una rapida e dinamica condivisione e l'archiviazione dei dati, esponendo, allo stesso tempo, le organizzazioni a rischi di divulgazione, compromissione, distruzione e perdita.

Tale rischio cresce con l'aumento del numero di informazioni processate, delle tipologie di dispositivi utilizzati (smartphone, laptop, server, etc.) e con l'impiego dei diversi strumenti di condivisione e di collaborazione (sistemi di cloud sharing, e-mail, etc). I principali fattori che incidono nei cyber risk sono i comportamenti umani, fallimenti tecnologici, processi non conformi ed eventi esterni.

I comportamenti umani sono quelli che maggiormente incidono: la rapidità nelle azioni, la poca consapevolezza e la distrazione hanno indotto numerosi utenti a cadere vittima di incidenti, truffe e sbagli, causando ingenti danni a se stessi e all'organizzazione.

Un approccio di cybersecurity di successo ha diversi livelli di protezione distribuiti su computer, reti, programmi o dati che si intende mantenere al sicuro. In

un'azienda, le persone, i processi e la tecnologia devono integrarsi a vicenda per creare una difesa efficace dagli attacchi informatici.

Gli utenti devono comprendere e rispettare i principi di sicurezza dei dati di base, come scegliere password complesse, diffidare degli allegati nelle e-mail e eseguire il backup dei dati. Scopri di più sui principi di base della cybersecurity.

2.2. Evoluzione del quadro normativo in materia di sicurezza cibernetica[30]

Come illustrato nel precedente capitolo e in particolare dalla Fig.2.1, gli ultimi anni sono stati caratterizzati da un incremento dei rischi legati alla sicurezza informatica. L'analisi dei rischi cyber nel contesto aziendale è oggi essenziale nella gestione del rischio operativo e componente chiave dell'ERM.

La sicurezza delle informazioni è un metodo volto a salvaguardare le Informazioni e gli strumenti informatici, rispetto a tre parametri fondamentali, indicati dal NIST, quali: riservatezza, integrità e disponibilità (RID). Essi rappresentano le misure idonee di sicurezza che il legislatore europeo ha evidenziato all'interno della Regolamento Generale sulla Protezione dei Dati personali n679/2016 GDPR, nell'art 32 par 1 lett. L'art 32 delinea "la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento", associando la triade RID alla resilienza, ovvero alla capacità di

[30] Si informa il lettore che la trattazione della normativa non rispetterà alcun ordine cronologico

reazione che un’organizzazione ha implementato per garantire la continuità aziendale, nonostante eventi informatici impegnativi (attacchi informatici, disastri naturali o crisi economiche). La resilienza ha un forte impatto sulla capacità di un'organizzazione di continuare le operazioni aziendali con tempi di inattività minimi o nulli.

La riservatezza di un dato è garantita se l’accesso alle informazioni è riservato esclusivamente ai soggetti che hanno diritto ad accedervi per l’intero durante del ciclo di vita dell’informazione, ossia da quando viene generata e/o raccolta a quando viene distrutta, passando ovviamente per ogni tipo di conservazione. Ad esempio, si configura una violazione della riservatezza allorché un dato classificato come segreto, venga accidentalmente visto da soggetti non autorizzati alla lettura di questa tipologia di dati.

L’integrità di un dato è la caratteristica dell’informazione di non essere in alcun modo alterata o corrotta. In questo caso stiamo parlando di ogni evento che può alterare e corrompere le informazioni, e quindi ad esempio una modifica accidentale di un’informazione, o la corruzione della stessa, che può avvenire per ipotesi con il guasto ad un supporto di memorizzazione (anche parziale).

Infine, il concetto di disponibilità dell’informazione impone che una necessaria informazione deve essere accessibile in un determinato momento. Se tuttavia ciò non accade, il danno che ne può derivare è enorme. Pensiamo ad una sala operatoria

e ad un chirurgo che deve accedere ai dati di un paziente per eseguire l'operazione e gli stessi non siano accessibili.

L'acuirsi dei temi legati alla sicurezza della rete e infrastruttura informatica è evidenziata dalla corposa normativa emanata da diversi enti e organismi. La CyberSecurity si è trasformata da tema "della singola rete locale" circoscritta all'organizzazione a mezzo/strumento di contrapposizione fra Stati.
L'esigenza di prevenire e contrastare in maniera coordinata le minacce informatiche è una priorità dell'agenda legislativa europea e tra i temi del G7 2024, con il risultato che dal 201631 a oggi si è riscontrato un esponenziale ampliamento del quadro normativo sulla cybersicurezza, sia a livello mondiale che europeo.

La lista di decreti attuativi nazionali e proposte legislative, l'articolano un quadro di norme che intendono disciplinare il tema la sicurezza dei sistemi informatici, genericamente per tutti i settori e in maniera verticale, soprattutto per quelli ritenuti critici come aeroporti, acquedotti, banche e intermediari finanziari.

La complessità e la continua l'evoluzione del quadro normativo in materia di sicurezza cibernetica è molto complesso. La Fig. 2.2. offre una sintetica panoramica del quadro complessivo di disposizioni in vigore.

[31] A livello EU, l'anno 2016, con l'approvazione del Reg. GDPR, rappresenta l'inizio di un importante processo di regolamentazione della tematica sulla sicurezza informatica e tutela dei dati.

Figura 2.2: Timeline l'evoluzione del quadro normativo in materia di sicurezza cibernetica

Fonte: di propria creazione ed utilizzata all'interno della presentazione aziendale di Exprivia

Le organizzazioni devono far riferimento alla normativa, agli standard, framework e documenti che sono stati emessi e redatti da enti di normazione internazionali quali la ISO e la NIST. Da enti europei specializzati quali Agenzia dell'Unione europea per la cibersicurezza (ENISA) o organizzazioni private, quali Systems Audit and Control Association, ISACA[32]. Ulteriori Enti istituzionali come la Banca d'Italia sono intervenuti e per emettere una normativa per armonizzare e fornire specifiche su discipline particolari nei settori critici(come per intermediari finanziari, settore trasporti, energia, acquedotti) per dare indicazioni su buoni

[32] Si tratta di un'associazione professionale internazionale focalizzata sulla governance IT, nata negli USA, ma fornisce una guida in ambito di cybersicurezza per tutte le organizzazioni e gli enti istituzionali.

comportamenti da adottare per rimuovere, o almeno in parte abbattere il rischio cyber.

A livello operativo è necessario tener presente tutte queste raccomandazioni, per sviluppare una metodologia peculiare che tenga conto dell'elevata variabilità della materia, affiancando quindi alla tradizionale analisi dei rischi attività di team intelligence o forensic analysis, oltre che di aggiornamento, elaborazione e condivisione delle informazioni con partner e istituzioni.

La finalità degli apparati normativi e quella di tutelare le organizzazioni, pubbliche e private, e gli stakeholders coinvolti da incidenti cyber più o meno gravi, in grado di avere impatti sugli asset materiali ed immateriali.

L'emergenza pandemica e la conseguente accelerazione della digitalizzazione dei servizi e dell'uso del lavoro da remoto[33].

Si vuole ripercorrere brevemente la cronologia normativa della disciplina cyber.

Oltre agli enti di normazione di settore, anche il Parlamento europeo si è preoccupato di regolamentare Gli aspetti di Security e diligenza, come il Cyber Security Act. La direttiva NIS2 è una guida importante ruolo di indirizzo sulla sicurezza delle reti e dei sistemi informativi e rappresenta un'evoluzione significativa del quadro normativo europeo per la sicurezza delle reti e dei sistemi informativi, ampliando il campo d'applicazione rispetto alla precedente direttiva

[33] Erroneamente, nell'uso comune si parla di smartworking riferendosi alla modalità di lavoro da casa o fuori ufficio. È corretto parlare, secondo le norme di diritto del lavoro di telelavoro o "lavoro da remoto".

NIS, questa normativa impone agli Stati membri di garantire un livello più adeguato di sicurezza cyber attraverso misure rigorose. È una collaborazione rafforzata a livello nazionale è tra i paesi membri, gli obiettivo principale include la protezione delle infrastrutture critiche, l'aumento della residenza degli attacchi cyber e il miglioramento della gestione del dei rischi cyber. Costituisce ulteriore punto di riferimento autorevole, non obbligatorio, il framework NIST, ente di normazione nazionale, USA, nato come risposta ad una specifica esigenza. "Il NIST sviluppa standard, linee guida, migliori pratiche e altre risorse di sicurezza informatica per soddisfare le esigenze dell'industria statunitense, delle agenzie federali e del pubblico in generale[34]". Sviluppa attività che spaziano dalla produzione di informazioni specifiche che le organizzazioni possono mettere in pratica immediatamente alla ricerca a lungo termine che anticipa i progressi tecnologici e le sfide future e promuove la comprensione e migliora la gestione dei rischi privacy e della sicurezza informatica. Le aree prioritarie del NIST includono crittografia, istruzione e forza lavoro, tecnologie emergenti, gestione del rischio, gestione dell'identità e degli accessi, misurazioni, privacy, reti affidabili e piattaforme affidabili.

Il Framework di CyberSecurity realizzato raccoglie una serie di requisiti rinviando per la loro implementazione a standard già esistenti. La sua utilità ne ha permesso

[34] Fonte: sito del NIST https://www.nist.gov/cybersecurity-measurement

la diffusione anche nel mondo finanziario e a livello internazionale. In Italia è stato recepito come cyber security framework nazionale e successivamente il NIST ha ampliato anche il privacy framework e risk management framework.

Il programma intrapreso dal NIST è mirato sulle misurazioni relative alla sicurezza informatica per supportare lo sviluppo e l'allineamento delle misurazioni tecniche per determinare l'effetto dei rischi e delle risposte alla sicurezza informatica sugli obiettivi di una qualsiasi organizzazione. Si pone il compito di supportare il top management nel processo decisione delle iniziative da adottare.

Sulla scia del framework di CyberSecurity, con team di esperti di Exprivia abbiamo lavorato per delineare un framework basato sulla AI ACT.

2.3 Il Cyber Risk

Il rischio, definito come l'effetto dell'incertezza sugli obiettivi aziendali, può tradursi in perdite economiche, danni alla reputazione e riduzione delle quote di mercato. La gestione del rischio comprende un insieme di attività che consentono alle organizzazioni di definire strategie e obiettivi, oltre a prendere decisioni consapevoli. Per mitigare i rischi, è evidente quanto sia importante applicare teorie e prassi consolidate, soprattutto nell'ambito del risk management, e in particolare nel campo della gestione del rischio cibernetico, che sono in continua evoluzione.

L'analisi degli scenari di rischio, delle minacce esterne e delle vulnerabilità interne deve essere supportata da una rete efficiente che garantisca un'interazione efficace

tra i manager e i processi aziendali, valorizzando il patrimonio informativo disponibile e attingendo a fonti esterne. Nell'era dei big data, una gestione del rischio efficace richiede l'uso di strumenti specifici e in grado di evolversi con il cambiamento delle esigenze aziendali, strumenti evolutivi e modulabili come soluzioni complete

Il Cyber Risk è, secondo Cebula, J.J e Young, L.R., "*un evento di natura operativa che si manifesta sugli asset informativi impattando la confidenzialità, la disponibilità e l'integrità dei dati o del sistema informativo stesso*."[35]

Il Cyber risk non è necessariamente la conseguenza di un attacco informatico, ma rientrano nella categoria di tali rischi anche rischi provocati da attori non malevoli o da comportamenti non intenzionali, da processi operativi che non mirano a compiere un crimine e infine disastri naturali il cui impatto si può ripercuotere sul business dell'organizzazione e sulla solidità delle informazioni da essa detenute.

Il Cyber attacco riguarda tipicamente tre aspetti essenziali della sicurezza informatica:

- confidenzialità, se le informazioni private e sensibili risultano esposte a terze parti non autorizzate

[35] Cebula, J.J. and Young, L.R. (2010) A Taxonomy of Operational Cyber Security Risks. Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University.
http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9395

- disponibilità, se i processi e le informazioni non risultano fruibili da chi ne necessita, provocando interruzioni all'accessibilità

- integrità, quando la perdita totale o parziale di componenti dell'informazione

Con l'avvento di Internet e della rete informatica, le organizzazioni, sia pubblica che privata, hanno trovato giovamento dall'uso dei processi IT, migliorando il proprio business per veicolare la propria offerta. Un qualunque danneggiamento degli asset fisici o logici lede la possibilità dell'impresa di adempiere alla sua mission. L'importanza assunta dai processi IT impone alle organizzazioni di gestire il rischio per fronteggiare le potenziali minacce. È necessario delineare e orchestrare delle strategie di prevenzione da rischi per evitare la possibilità di downtime e rallentamenti dei sistemi causati da una moltitudine di disservizi ascrivibili alle infrastrutture digitali quali attacchi esterni, intrusioni, guasti, problemi di connettività e banali errori umani nell'utilizzo degli strumenti che possono presentate la causa scatenante di blocchi che rendono indisponibili dataset, applicazioni o addirittura interi processi. Ed ecco perché è imprescindibile sviluppare una visione olistica rispetto al cyber risk, coinvolgendo nelle sessioni di assessment non soltanto tutti gli asset informatici e i processi digitali della banca, ma anche quelli dei partner e degli interlocutori di business, solo così è possibile monitorare il modo in cui vengono utilizzati. E identificati con chiarezza i fenomeni che potrebbero tradursi in fattori di rischio per la loro organizzazione.

Il rischio cyber ha trovato ampia trattazione all'interno delle più recenti normative, sia in ambito finanziario sia in ambiti trasversali a più settori. Regolamenti come il GDPR, NIS2 e DORA si risolvono le esigenze sorte in un comparto che negli ultimi anni sta affrontando una delle più grandi rivoluzioni di sempre, la digital transformation.

Si tratta di un fenomeno che genera nuove opportunità e nuovi rischi per il business: aumentano i touchpoint messi a disposizione di dipendenti e clienti, si affermano ambienti cooperativi per la creazione di modelli go to market innovativi e all'insegna della logica omnicanale, si avviano sempre più attività basate sull'analisi e l'utilizzo dei dati. Di conseguenza le minacce e nuovi elementi eventi potenzialmente avversi per la continuità operative sono all'ordine del giorno.

Il rischio cyber ha delle peculiarità che lo differenzia dai rischi legati alle normali gestioni operative, evidenziata anche nella normativa e dalle soluzioni tecniche organizzative che è necessario predisporre per mitigarlo.

2.3.1 Cyber Risk Management (ICT Risk Management)

L'ICT risk è un'attività particolarmente complessa e soprattutto estremamente dinamica in quanto deve tener conto contemporaneamente:

- Della costante evoluzione delle minacce che caratterizzano il mondo cyber;
- Dell'evoluzione normativa, sempre più attenta al presidio dei rischi ICT;

- Del contesto esterno, caratterizzato ad un ampliamento della cyber exposure come conseguenza di un sempre maggior ricorso dei clienti ai servizi on line e della gestione del lavoro da remoto.

Qualsiasi rischio correlato all'utilizzo delle tecnologie dell'informazione può interferire con le attività aziendali. Le varie tipologie di eventi o incidenti che compromettono in qualche modo l'IT o le infrastrutture fisiche e logiche su cui corrono dati e flussi di lavoro digitalizzati possono causare impatti negativi sui processi aziendali o sulla missione dell'organizzazione.

L'analisi valutativa della probabilità di verifica necessita di elaborare un elevato numero di informazioni per ipotizzare i potenziali impatti, identificando e misurando fattori che contribuiscono a facilitarne l'avverarsi, come minacce esterne, vulnerabilità interne, valore degli asset e la loro esposizione.

La complessità delle informazioni da trattare, le tempistiche eccessivamente rapide, la necessità di documentare dettagliatamente le scelte e anticipare gli eventi avversi, ha spinto gli sviluppatori di soluzioni cyber ad automatizzare e a integrare le tecnologie di risk management e cyber risk management con l'IA. Gli strumenti tecnologici integrati con IA sono in grado di:

- l’identificazione dei rischi ICT (censimento degli asset inventory, dei framework di riferimento per gli scenari delle minacce e dei framework di controllo);
- la mappatura dei rischi;
- la valutazione dei rischi;
- la mitigazione dei rischi;
- il monitoraggio dello status quo al fine di un costante potenziamento dei sistemi di gestione dell'ICT risk.

Gli indicatori di rischio sono elementi principali per monitorare i principali scenari di rischio e analizzare le tendenze sulla base della raccolta periodica dei dati e dell’applicazione di specifici algoritmi, permettendo di effettuare previsioni rispetto alle circostanze che generano rischi.

Gli sforzi e gli strumenti di misurazione della sicurezza informatica cercano di migliorare la qualità e l’utilità delle informazioni per supportare il processo decisionale tecnico e di alto livello di un’organizzazione sui rischi della sicurezza informatica e su come gestirli al meglio. Il NIST ha proposto un programma di misurazioni della sicurezza informatica che fornire alle organizzazioni gli strumenti migliori per gestire in modo mirato ed efficace i rischi legati alla sicurezza informatica. Nonostante il tema sia di estrema rilevanza a causa dell’aumento dei rischi informatici, non sono ancora creata una tassonomia standard per termini di

"misurazioni" e "metriche". Lo sviluppo di punti riferimento rappresenterebbe un progresso rilevante per la disciplina, in quanto misurare la capacità complessiva del sistema consente di *identificare, proteggere, rilevare, rispondere e recuperare* dai rischi e dalle minacce alla sicurezza informatica, obiettivo di un solido programma di misurazione della sicurezza informatica.

L'elaborazione di queste informazioni è svolta attraverso l'assessment che sottopone l'organizzazione ad una verifica, in materia di sicurezza informatica, riprendendo i principali standard normativi e linee guida relativi alla cybersecurity[36], quali ISO 27001, il NIST, il Center for Internet Security, (CIS), ISO/IEC 62443 e DORA.

La ISO 27001 è una norma che permette anche di certificare un corretto sistema di gestione della sicurezza delle informazioni implementato in tutta o in una parte dell'organizzazione; mentre la NIST propone un framework di riferimento per la gestione della sicurezza informatica in tutti i suoi aspetti, proponendo inoltre controlli più specifici con la pubblicazione di "Security and Privacy Controls for Information Systems and Organizations" noto come NIST sp800-53 rev5.

La terza linea guida di rifermento è stata rilasciata dal CIS (Center for Internet Security), organismo che propone una serie di best practices tecnologiche e di processo, mettendo a disposizione di vari vendor dei controlli organizzati sotto

[36] Rif. capitolo "Evoluzione del quadro normativo in materia di sicurezza cibernetica

forma di checklist (Benchmark). CIS fa riferimento sia al framework NIST che ai controlli proposti da ISO27001, indicando delle best practices per la loro implementazione.

Esso ha lo scopo di supportare le organizzazioni alla standardizzazione del team di lavoro, tecnologie e processi nell'ambito della riduzione del rischio cyber e della protezione del business. Tra gli standard, normative e framework esistenti

Un ulteriore supporto è fornito dalla ISO/IEC 62443 che fornisce una serie di standard che definiscono l'implementazione della sicurezza nei sistemi industriali (Operation Technology). I cybersecurity expert di Exprivia stanno lavorando per ampliare il range di normative ed includeranno anche la NIS 2. Anche se non citato, il framework fa riferimento al Regolamento europeo in materia di protezione dei dati personali, il GDPR.

L'invenzione si inserisce in un contesto in cui gli strumenti di indagine mancavano di una visione olistica delle esposizioni al rischio Cyber di un'azienda, in particolare tra diverse unità aziendali all'interno di organizzazioni più grandi e non erano in grado di collegare i rischi cyber a minacce specifiche e di identificare le aree di debolezza, fornendo allo stesso tempo raccomandazioni di miglioramento attuabili. Di conseguenza, essi non riuscivano a rappresentare contemporaneamente sia l'esposizione ai principali rischi cyber che a individuare i gap rispetto ad un livello

di maturità desiderato e ad indirizzare attività di mitigazione dei rischi pertinenti ed efficaci.

Alcune metodologie di assessment permettono, attraverso un questionario di domande basate, su diverse linee guida, generare un output dalle risposte e prendere visione e consapevolezza dei rischi e minacce cyber a cui è maggiormente esposta l'organizzazione, analizzando la postura di sicurezza ed eventuali gap da colmare, attuando azioni di mitigazione suggerite.

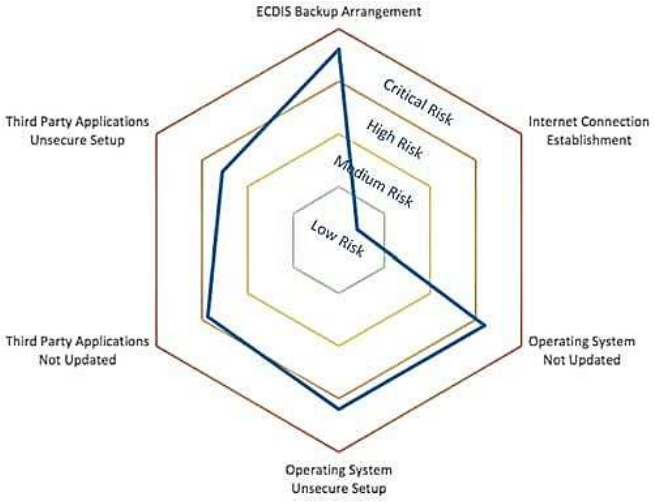
Essa fornisce un'analisi compliance di più normative e framework di riferimento, in base al set di domande sempre aggiornate e con indicazioni e spiegazioni che supportano l'utente, responsabile IT o altro professionista che conosce lo status dell'infrastruttura, a fornire la risposta più opportuna. L'assessment è configurato su un elaboratore informatico ed eseguito da un consulente umano, allo scopo di verificare il proprio rischio cyber e proteggere il proprio business in conseguenza a tale rischio.

Sulla base della vulnerabilità computazionale, la scansione condotta identifica e stima il cyber livello di rischio delle minacce dei sistemi, sulla base di più parametri oggetto di valutazione. L'impatto delle minacce è solitamente identificato come una grandezza di danno derivante dallo sfruttamento efficace della vulnerabilità. I livelli di impatto sono indicati come bassi, medio, mentre la probabilità delle minacce si

riferisce alla probabilità di riuscire a sfruttare la vulnerabilità. Tali tassi di probabilità sono indicati come alto, medio e basso.

Al termine del processo di analisi, i tool attualmente utilizzati sono in grado di rilasciare un report completo che presenta un grafico radar e fornisce le azioni correttive che migliorerebbe la postura di sicurezza.

Figura 2.3 Grafico Radar: strumento per l'analisi a pi variabili dei vari rischi cyber



Fonte https://www.researchgate.net/figure/Risk-level-radar-graph-of-ECDIS-cyber-threats-identified_fig5_332914204

ll grafico radar, riportato in Fig. 2.3, riporta l'assessment di un'impresa prototipo. Tre sono le minacce informatiche identificate con rischio critico: ECDIS Backup Arrangement, Operation System Not Updated e Operation System Unsecurity Setup. Nel grafico, gli elementi critici sono quelli che presentano la punta nel cerchio "critical risk". Analizzando il grafico, il rischio "Internet connection

establishment" è quello rilevato più basso, presenta un valore compreso nel range "rischio basso".

2.3.2 Modello di governance della Cyber risk management

La digital transformation è una sfida complessa, soprattutto per la velocità con la quale avvengono i cambiamenti. L'organizzazione che punta a distinguersi e si evolve con la tecnologia, deve implementare un piano per la gestione dei rischi, efficace ed efficiente, se è adattato alle caratteristiche specifiche della organizzazione ed è importante l'elaborare un modello di organizzazione.

L'intera struttura aziendale deve essere in linea con i cambiamenti per permettere una maggiore collaborazione tra le funzioni aziendali e aumentare l'elasticità aziendale di fronte al cyber risk.

Risk committee e un Audit committee, che ha poteri esecutivi e che opera attraverso le funzioni, per analizzare tutti i rischi evidenziati. Il Risk Manager è il responsabile della vigilanza del cyber risk management, coordina il gruppo, controlla e definisce, in termini di impatto e mitigazione del cyber risk, le linea guida, sistemi, processi e formazione del sistema di gestione del rischio interno, che può essere l'Enterprise Risk Management.

L'organizzazione deve predisporre nell'organigramma Cyber Risk Governance Group, composto da un Il Cyber Risk Group stabile i KPI di CyberSecurity dell'azienda, deve identificare le variabili chiave, incluse le informazioni che

sono necessarie per un efficiente gestione delle operazioni dell'aziendali e per ottenere obiettivi a breve e lungo termine.

Il Risk Manager deve effettuare l'analisi quantitativa e qualitativa del rischio per identificare e quantificare l'esposizione al rischio attraverso un'analisi finanziaria sempre, operando secondo i requisiti e vincoli di sicurezza. Egli dovrà decidere i piani strategici di prevenzione del rischio per ottimizzare il livello di sicurezza al costo minore.

Il modello riportato in Fig 2.4 prova a semplificare l'organigramma aziendale connessa alla gestione del rischio ed evidenza i diversi livelli di difesa:

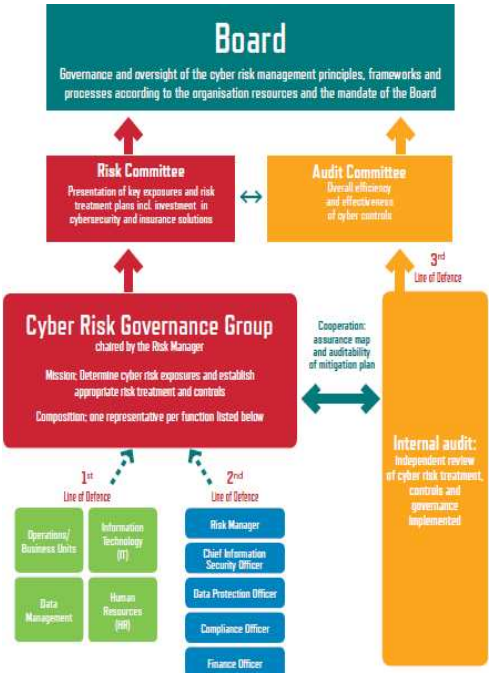
I. livello di difesa: più operativo e svolto dalle figure IT, HR, Business Unit e Data Management
II. livello difesa: rappresentato dalla figura del Risk Manager, CISO, Data Protection Officer (DPO), Compliance Officer e Finance Officer. Insieme al primo livello contribuiscono alla costituzione del Risk Committee
III. livello difesa: rappresentata dall'internal audit committee.

Nell'ambito della sicurezza informatica, una figura di spicco è Chief Information Security Officer, CISO, per le grandi imprese, nelle PMI, invece, Information Security Officer, ISO, e dal Chief Information Officer. Il compito di tali figure è selezionare ed efficientare il piano di cyber risk indicando azione ed operazioni

che spettano alle varie funzioni in accordo con la funzione IT, adattandolo alla politica aziendale.

Le figure IT hanno il compito di identificare l'esposizione al rischio, gestirlo, controllarlo e attuare azioni di remediation e di mitigazione per tenerlo al di sotto del livello di sicurezza (risk appetite) deciso dal Risk Manager. Diverse solo le risposte al rischio che possono essere impiegate per affrontare le minacce, i rischi o eventi imprevedibili. Soprattutto per i rischi negativi, l'obbiettivo primario è evitarlo, mitigarlo, ridurlo, trasferire ed elaborare piani di emergenza e per l'accettazione dei rischi. Le strategie di risposta o risk response sono decise attraverso strumenti per condividere il rischio residuo, per esempio assicurando il rischio.

Figura 2.4.: Modello di organizzazione aziendale per la gestione del rischio



Fonte: FERMA E ECIIA Framework of Corporate governance & cyber security

Realtà assicurative come UnipolSai e Allianz forniscono servizi assicurativi che coprono i rischi cyber, ovvero coprono i danni immateriali relativi alle spese che l'organizzazione dovrà sostenere per ripristinare l'accesso al proprio sistema e i dati in esso contenuto, a seguito di un attacco informatico.

Le organizzazioni, attraverso la gestione del rischio, si auspicano di massimizzare il valore e l'effetto degli investimenti effettuati, anche quelli legati alla componente di cybersecurity. I programmi, le azioni, i processi e l'ottimizzazione del potenziale rendimento sono operazioni complesse e costose, che non trovano il riscontro dei benefici associati alla riduzione del rischio. A fronte di un costo preventivo, molte organizzazioni trovano più conveniente non applicare alcuna soluzione di

CyberSecurity e rischiare di incorrere in sanzioni e incidenti, perché si confrontano scenari che differiscono in termini di costi previsti con i probabili benefici associati e alla riduzione del rischio.

L'intento dell'elaborato è sviluppare una maggiore consapevolezza dell'importanza di verificare il livello di postura aziendale e in particolare di quelle soluzioni che adottano l'Intelligenza artificiale.

2.4. Il Cyber risk nel settore finanziario: rilevamento osservazioni[37]

Nel corso del 2023, in Italia, dai dati riportati nel 'Threat Intelligence Report' elaborato dall'Osservatorio Cybersecurity di Exprivia, evidenziano un incremento degli attacchi informatici a scapito di aziende, organizzazioni e persone, con il settore finanziario che risulta tra i principali bersagli.

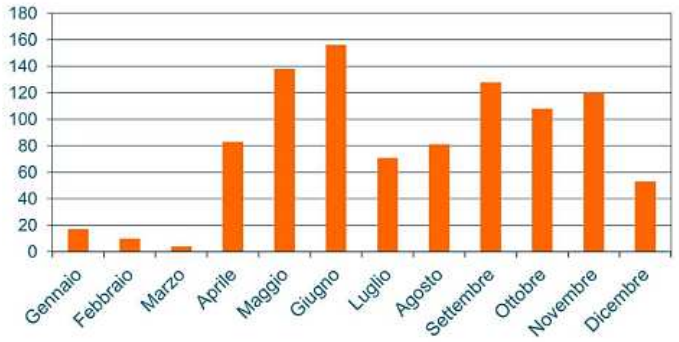
Considerando 145 fonti aperte tra siti di aziende colpite, siti pubblici di interesse nazionale, agenzie di stampa online, blog e social media, il rapporto stilato dal gruppo ICT, evidenza che si sono verificati 2.209 casi tra attacchi, incidenti e violazioni della privacy. Nello specifico, si sono verificati 1.635 attacchi (+32% rispetto ai 1.236 del 2022), 518 incidenti – più che dimezzati (-59%) rispetto al

[37] Sono riportati i dati presentati ad Aprile 2024 da Exprivia spa all'interno del report "Threat Intelligence".

2022 quando gli incidenti di sicurezza erano stati 1.236 - e 56 violazioni della privacy (-46% rispetto ai 103 fenomeni dell'anno precedente).

Nel settore finanziario, l'andamento degli attacchi registrati nel corso del precedente anno, presenta dei picchi importanti nella metà dell'anno, ed un numero di attacchi simili mese per mese, fino al calo di dicembre. Il totale degli attacchi registrati è 969, appena superiore ai 939 attacchi registrati nel 2022, anno in cui la seconda parte è stata caratterizzata da un numero di attacchi costante ed in linea tra i 40 ed i 60 attacchi, mentre nel 2023 tra settembre e novembre i numeri sono stati ben più alti, per poi subire un calo a dicembre.

Figura2.2 Analisi per singoli mesi del 2023 degli attacchi informatici



Fonte: "Threat Intelligence Report" rilasciato ad Aprile 2024 da Exprivia SpA. I dati sono raccolti ed elaborato dall'Osservatorio di Cybersecurity del gruppo.

La rapidità nell'evoluzione degli scenari e delle minacce che contraddistinguono il mondo cyber, specialmente nel mondo bancario, può essere affrontata impostando soluzioni unificate, capace di far convergere il patrimonio informativo dell'impresa su un unico punto d'attenzione, così che i è possibile anticipare gli eventi e

ottimizzare i processi operativi, facendo leva su un adeguato censimento degli indici occorsi, su attività di trading intelligence e l'uso dell'intelligenza artificiale per ipotizzare interventi correttivi tempestivi ed efficaci.

2.4.1. Cyber Risk Management nel settore bancario, finanziario e assicurativo

L’ottimizzazione delle operazioni e la rapidità nel cambiamento impongono alle banche un continuo processo di evoluzione. La velocità è la chiave per costruire la banca del futuro, in equilibrio tra trasformazione e solidità nei domini di governance, sicurezza e resilienza. Il legislatore si è pronunciato con testi regolamentari molto analitici per declinare le azioni da compiere nelle misure di sicurezza da adottare. Ha introdotto nuovi concetti, come quello della resilienza operativa, per enfatizzare le attività di prevenzione rispetto alla capacità di risposta; obbliga le società ad una gestione adeguata della grande quantità di informazioni provenienti sia dall'azienda sia dall'ambiente esterno.

Il legislatore è intervenuto in diverse occasioni per supportare il processo di digitalizzazione del settore bancario, finanziario e assicurativo, redigendo nel corso del 2023 il Regolamento Digital Operational Resilience Act, DORA, entrato in vigore il 17 gennaio 2023 e che racchiude le disposizioni da seguire nel settore finanziario per la resilienza digitale e gestione del rischio informatico.

Le banche sono un settore critico, in quanto gestiscono flussi di dati e denaro che attirano l'attenzione dei cybercriminali. Sulle priorità presentate all'evento "Banche e Sicurezza" a maggio 2024, incontro annuale sulla sicurezza fisica e digitale nel settore finance, l'aumentato della cyber exposure è stato un elemento condiviso da circa 21 banche, intervistate da ABI Lab, che hanno ampliato il budget dedicato all'area Information and Communication Technologies (ICT).[38] La priorità è rappresentata dalla gestione e mitigazione del rischio e rafforzare costantemente le misure di sicurezza e di difesa. La R&D nelle banche è focalizzate su temi della Data Governance, Intelligenza Artificiale e Cloud Computing, in linea con l'esigenza di abilitare modelli più agili nello sviluppo dei servizi.

Ogni iniziativa di digital transformation deve considerare conto della complessità dell'organizzazione: la banca è una realtà complessa in cui le dimensioni di business organizzative tecnologiche si intersecano in una rete di relazioni e interazioni. Insieme all'analisi dei rischi, è necessario applicare l'Enterprise Architecture, che rappresenta la banca con una visione organica, mettendo a disposizione mappe e strumenti metodologiche, e, soprattutto nell'ambito IT, è necessario definire policy e framework architetturali per definire gli indirizzi tecnologici e dei percorsi evolutivi che impattano anche sul governo dell'innovazione e dell'adeguamento del parco applicativo.

[38] Fonte Rapporto ABI Lab 2024 "Scenario e trend del mercato per il settore bancario"

2.4.2 Verso l'Intelligenza Artificiale: l'evoluzione del Fintech

L'intelligenza Artificiale e machine learning tecnologica rappresentano, in questo momento storico, un imperativo imprescindibile. Esse non sono le uniche che costituiscono la nuova evoluzione delle organizzazioni: un'altra importante innovazione è la blockchain[39], strumento digitale che permette di sfruttare le caratteristiche di una rete informatica di nodi e consente di gestire e aggiornare, in modo univoco e sicuro, un registro contenente dati e informazioni in maniera aperta, condivisa e distribuita senza la necessità di un'entità centrale di controllo e verifica. La blockchain nasce per essere uno strumento digitale sicuro, trasparente, decentrato e disintermediato, in risposta alla crisi finanziaria del 2008 e amplia il business del mondo finanziario, perché permette la nascita e la diffusione della moneta digitale e critpovalute.

Grazie alle suddette tecnologie, gli istituti finanziari hanno modernizzato il proprio core con il settore della tecnofinanza o Fintech e sono in grado di supportare le organizzazioni verso la digital trasformation e la nascita della start-up e delle tech companies.

Lo sviluppo del Fintech evolve e facilita i metodi tradizionali di finanza, proponendo soluzioni e servizi basati sulle tecnologie dell'informazione e

[39] Oltre a quelle citate, ricordiamo che anche il cloud computing, la stampa 3D, la realtà virtuale e il robotic process automation contribuiscono alla modernizzazione del core tecnologico delle moderne organizzazioni e degli istituti finanziari.

agevolando i servizi per i propri clienti, come pagamenti elettronici, analisi dati, mercati di capitali, immobiliare e finanza personale. L'evoluzione del Fintech ha richiesto l'aumento degli endpoint e del progressivo ampliarsi della rete, con conseguenti lacune e maggiori vulnerabilità. Se da un lato i vantaggi sono molteplici, parallelamente, i cyber criminali hanno avuto l'occasione di accedere, come mai prima d'ora, ad un numero elevato di dati, informazioni e denaro: un vantaggio evidente che si registra dall'aumento degli attacchi di cyber crime nel settore.

La conclusione dell'evidenza è riscontrabile nella massiva riformulazione della regolamentazione nel settore: il Consiglio europeo, per introdurre una maggiore consapevolezza, ha deliberato solo nel 2023 due documenti, la NIS 2 e il Regolamento Digital Operational Resilience Act (DORA), e nel 2024 ha approvato la legge sull'IA. L'urgenza di quantificare i rischi potenziali è cruciale, non solo nel settore finanziario, dove la criticità strutturale è elevata, e questi possono essere esaminati utilizzando framework condivisi e standardizzati, basati sulle appropriate misure di sicurezza e di regolamentazione.

Capitolo 3 Cyber risk con l'intelligenza artificiale

3.1 Introduzione: Analisi del contesto storico ed esigenza (linea temporale, tappe più importanti fino ad oggi per motivare il perché nasce l'esigenza di una normativa)

L'Intelligenza Artificiale o IA, nell'immaginario fantascientifico creato dalla letteratura e dalla cinematografia, era attesa sottoforma di robot antropomorfi. Anche se non si sono ancora diffusi robot stile Blade Runner, oggi l'IA è già diffusa e accessibile a tutti. La capacità comunicativa, che da sempre contraddistingue gli esseri umani dagli animali, oggi appartiene anche ad entità che sono in grado di dialogare, commentare, rispondere e imparare.

Dal primo dopoguerra, assistiamo all'evoluzione di macchine pensanti.

Per la precisione, nell'Ottocento, Augusta Ada Byron, una pioniera della scienza informatica e riconosciuta universalmente come la prima programmatrice della storia, in un suo trattato del 1843, riportava le sue intuizioni sulle potenzialità dell'Analytical Engine che andavano ben oltre il semplice calcolo numerico. Infatti, lei previde che, trattando i numeri come simboli, la macchina avrebbe potuto manipolare anche lettere o note musicali, aprendo la strada a una vasta gamma di applicazioni. Mentre Babbage vedeva la sua invenzione principalmente come uno

strumento per il calcolo algebrico, Ada intuì che poteva essere usata per elaborare qualsiasi tipo di informazione codificata.

Un altro importante contributo da citare ai fini introduttivi del seguente elaborato è stato realizzato da Alan Turing nel 1950, che grazie al suo articolo sul "Computing Machinery and Intelligence" è definito il "padre dell'IA". Nell'articolo, ha introdotto il test di Turing, un criterio per determinare se una macchina è capace di un comportamento intelligente.

L'Artificial Intelligence si manifesta in molteplici forme e modi: è in grado di imitare comportamenti umani, risolvere problemi, creare prodotti innovativi e automatizzare i processi. Grazie alla sua valida applicabilità, è adottata in diversi settori come marketing, assistenza sanitaria, finanza, logistica, sicurezza informatica e attacchi informatici. Il suo ampio utilizzo ha spinto il Parlamento Europeo ad interrogarsi sui suoi rischi e impatti sugli utenti e, con lo scopo di tutelare i diritti digitali degli europei, il 17 gennaio 2024 viene approvata la normativa sull'Intelligenza artificiale, la c.d. IA ACT.

La IA Act si pone come obiettivo quello di sviluppare un quadro normativo che favorisca il buon funzionamento del mercato unico digitale e lo sviluppo e prodotti basati sull'IA. L'esigenza di regolamentare il settore delle tecnologie costituite da IA è nata dopo gli importanti sviluppi che hanno impattato sulla società e su diversi settori. Infatti, l'hype relativo all'IA generativa, in particolare con piattaforma con

ChatGpt e Gemini, è diventato un fenomeno di massa, suscitando l'interesse di studiosi.

La concretezza della proposta di regolamentazione nel settore è stata raggiunta nel febbraio 2024 e verrà recepita il 13 luglio 2024 in tutti gli Stati membri dell'Unione Europea. Il testo impone obblighi legislativi in tutte le fasi del ciclo di vita di un sistema IA: dall'idealizzazione, formazione, test, valutazione di conformità ai rischi, validazione e monitoraggio continuo post-vendita. Tra le previsioni contenute del documento è effettuata una distinzione tra sistemi di Intelligenza artificiale generativa, GenIA, a "rischio sistemico", sottoposti a maggiori vincoli e controlli, e a quelli "non a rischio sistemico", per i quali le regole sono meno stringenti.

In seno al Consiglio Europeo è stato istituito un Consiglio AI, che permetta un confronto costante tra rappresentanti dei governi, esperti di settore e stakeholder delle aziende e supportare le organizzazioni nella gestione dei rischi. L'AI ACT introduce, inoltre, un sistema sanzionatorio progressivo che impatterà in misura variabile tra l'1% e il 7% del fatturato dell'azienda e calibrate in base a parametri che indicano la gravità della violazione e alla natura, dimensione dell'organizzazione. Le norme sono destinate a proteggere dai rischi, ma non sono in grado di prevedere scenari tecnologici futuri. Per tale ragione, le organizzazioni

sono chiamate ad ampliare il livello di postura di sicurezza informatica e la cyber resilience[40].

Il compito dell'elaborato è portare a una lettura della normativa e presentare il framework realizzato per valutare l'impatto della GenIA e supportare le organizzazioni che sono chiamate a rivedere le proprie impostazioni operative sulla base dei requisiti, sia in termini di policy e in relazione alle configurazioni organizzative e agli impianti di controllo e di governo dei rischi.

3.1.1. L'impatto dell'Intelligenza Artificiale sulle imprese

I tradizionali strumenti di CyberSecurity non sono in grado di fronteggiare all'aumento di numero e di gravità delle minacce informatiche. L'evoluzione delle tecniche di hackeraggio, la continua esigenza di tutelarsi e l'evoluzione tecnologica, hanno consentito a team di società sviluppatrici di software di integrare le soluzioni di sicurezza informatica con l'Intelligenza Artificiale, allo scopo di supportare anche i team tecnici nell'individuazione degli incidenti, della business continuity e ottenere un vantaggio competitivo sui criminali informatici.

L'IA sarà una componente critica non solo per la difesa, ma anche per sviluppo di tecnologie[41].

[40] La cyber resilience è la capacità recuperare dati post incidente informatico.
[41] L'IA è già utilizzata in diversi dispositivi di IoT, ChatBot e altri strumenti alla portata di tutti. Anche i criminali informatici adottano tale tecnologia per rilasciare attacchi mirati, pervasi e automatici.

Il legislatore EU conscio dell'importanza, del potere e delle minacce della tecnologia basata su AI e Machine Learning, ha emanato la normativa AI Act.: la prima normativa sulle soluzioni che adottano l'intelligenza artificiale e con lo scopo di tutelare gli utilizzatori e fornire alle organizzazioni sviluppatrici di soluzioni di IA delle indicazioni per evitare condotte scorrette.

Le organizzazioni stanno traendo vantaggio dalle potenzialità della AI, per velocizzare i processi, abbassare i costi a fronte di fatturati più elevati. Esse avranno accesso a una notevole quantità di dati, che, se ben studiati possono portare un vantaggio competitivo importante nello scenario dell'economia mondiale. L'IA non ha darà vantaggi solo ad aziende di grandi dimensioni del settore informatico, ma qualsiasi tipologia di azienda può utilizzarla per testare i propri prodotti, creare contenuti e gestire processi interni di assistenza cliente. Un case use molto interessante è stato realizzato dall'azienda Nike, nota nel settore abbigliamento e calzaturiero sportivo. Essa, per velocizzare la messa in commercio delle sue scarpe, ha introdotto un processo basato sull'Intelligenza Artificiale che testa i prototipi. L'IA sta supportando anche la gestione dei rischi e nel rilevamento delle frodi, perché è in grado di individuarli prima del tempo e supporta le organizzazioni nel processo decisionale, perché in grado di analizzare miliardi di informazioni al nano secondo. La soluzione agevola e migliora le previsioni e identifica nuove opportuni

di mercato e sviluppo del business, senza l'influenza dell'elemento di soggettività del decisore.

L'approccio da adottare nell'introdurre l'IA all'interno della propria organizzazione deve essere critico, ma non intimorito. I suoi sviluppi futuri saranno notevoli e a breve, forse, non sarà più possibile farne a meno, perché l'AI è la tecnologia che ha il potenziale per apportare notevoli benefici all'industria e alla società, ma è importante anche riconoscere che ci sono molte sfide da superare e bisogna garantire che gli utilizzatori e sviluppatori di AI siano effettuati in modo responsabile e sostenibile e l'AI ACT è la prima normativa che si è posta l'obiettivo di disciplinare il settore.

3.2. Analisi del testo normativo, considerazioni e analisi di prospetti del cambiamento dopo che la legge entrerà in vigore

La definizione di intelligenza artificiale è al centro dei dibattiti politici e giuridici: nel 2024, è nell'agenda del Gruppo dei sette paesi (Italia, Canada, Francia, Germania, Giappone, Regno Unito e Stati Uniti), noto come G7, in vista dell'approvazione dell'AI ACT, che si applica, secondo l'art. 3 n.1, a qualsiasi " *sistema basato su macchina progettato per funzionare con diversi livelli di autonomia e che può, per obiettivi espliciti o impliciti, generare output come previsioni, raccomandazioni o decisioni che influenzano ambienti fisici o virtuali* ".

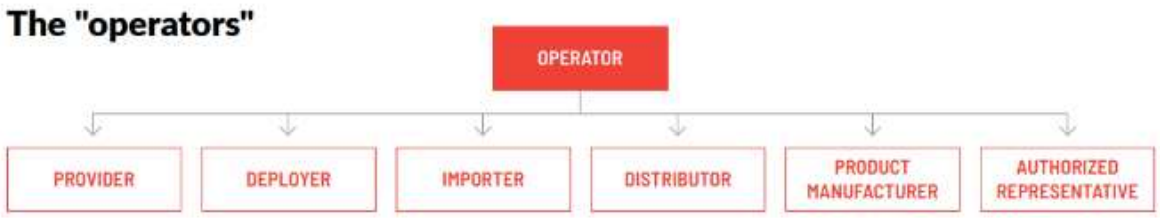
La normativa, quindi, fornisce una delucidazione del campo di applicazione materiale della stessa, ma fatica a fornire una definizione di AI. Lo scopo, invece, è ben chiaro ed è quello di promuovere il progresso e lo sviluppo nelle nostre società. Essa si impegna a promuovere la diffusione di sistemi di IA sicuri, protetti e affidabili raccogliendo, per massimizzare la trasformazione digitale, rafforzare la crescita economica e lo sviluppo sostenibile, traendo i miglior benefici e gestendo al meglio i rischi, nel rispetto soprattutto dei diritti umani, dei minori e delle persone più deboli e sensibili.

Il Consiglio Europeo ha inserito tra gli obbiettivi della normativa il miglioramento dell'interoperabilità degli approcci alla governance dell'IA e promuovere maggiore certezza, trasparenza e responsabilità, adottando un approccio basato sul rischio all'interno di una più vasta promozione dell'innovazione e di una crescita forte, inclusiva e sostenibile attraverso quadri normativi, condivisione di buone pratiche e consultazioni regolari.

L'analisi dei singoli articoli della legge UE sull'Intelligenza Artificiale ha permesso di individuare i sei operatori sui quali impatta la normativa. Essi sono: provider o fornitori, deployer, importatori, distributori, produttori di manufacturing e rappresentanti autorizzati. Ad ognuno di essi, il legislatore ha indicato specifici obblighi da seguire per la conformità normativa. Dall'elenco sono esclusi, a norma

dell'articolo 2[42], paragrafo 3, i sistemi di IA per fini militari, di difesa o sicurezza nazionale.

Tabella 3.1 Gli operatori sui quali impatta l'IA



Fonte EU AI ACT Compliance Matrix, by IAPP Principal Researcher, Privacy Law and Policy, Muge Fazlioglu, CIPP/e, CIPP/US

Secondo l'art.3 par 3, è individuato come providers o fornitore una "*persona fisica o giuridica, autorità pubblica, agenzia o altro organismo che sviluppa un sistema di IA o un modello di IA per scopi generali o che dispone di un sistema di IA o di un modello di IA per scopi generali*". Il sistema di IA è sviluppato, o immesso sul mercato o in servizio con il proprio nome o marchio del fornitore. La distribuzione può essere a pagamento o gratuitamente. Secondo l'articolo 2, paragrafo 1, lettera a/c, i fornitori possono essere stabiliti o ubicati all'interno dell'UE o in un paese

[42] Riferimento art 2 "*se e nella misura in cui sono immessi sul mercato, messi in servizio o utilizzati con o senza modifiche esclusivamente per scopi militari, di difesa o di sicurezza nazionale, indipendentemente dal tipo di entità che svolge tali attività. Il presente regolamento non si applica ai sistemi di IA che non sono immessi sul mercato o messi in servizio nell'Unione, qualora l'output sia utilizzato nell'Unione esclusivamente per scopi militari, di difesa o di sicurezza nazionale, indipendentemente dal tipo di entità che svolge tali attività*"

terzo se immettono un sistema di IA sul mercato o lo mettono in servizio nell'UE, o se l'output prodotto dal sistema di intelligenza artificiale è utilizzato nell'UE.

Invece, il distributore è, secondo l'articolo 3, paragrafo 7, "una persona fisica o giuridica nella catena di fornitura, diversa dal fornitore o dall'importatore, che mette a disposizione un sistema di IA sul mercato dell'Unione".

Altro operatore disciplinato dalla normativa sono i produttori manufacturing, che secondo l'articolo 2, paragrafo 1, lettera e), ovvero coloro che immettono un sistema di IA sul mercato o lo mettono in servizio con il proprio prodotto e con il proprio nome o marchio. Nel caso di sistemi di IA ad alto rischio, che sono componenti di sicurezza di prodotti disciplinati dalla normativa di armonizzazione dell'UE elencati nell'allegato I, sezione A, il fabbricante del prodotto è considerato il fornitore del sistema di IA ad alto rischio. Sono soggetti agli obblighi di cui all'articolo 16, se il sistema ad alto rischio viene immesso sul mercato con il prodotto sotto il nome o il marchio del fabbricante del prodotto o messo in servizio sotto il nome o il marchio del fabbricante dopo l'immissione del prodotto sul mercato, ai sensi dell'articolo 25, paragrafo 3.

Un operatore è definito all'articolo 3, paragrafo 4, come "una persona fisica o giuridica, un'autorità pubblica, un'agenzia o altro organismo che utilizza un sistema di IA sotto la sua autorità". Non include "le persone fisiche che utilizzano sistemi di IA nel corso di un'attività puramente personale e non professionale", come

indicato nell'articolo 2, paragrafo 10. A norma dell'articolo 2, paragrafo 1, lettera bbc), gli operatori possono essere stabiliti o ubicati all'interno dell'UE o in un paese terzo, se i risultati prodotti dal sistema di IA sono utilizzati nell'UE.

Secondo l'articolo 3, paragrafo 5, un rappresentante autorizzato è "una persona fisica o giuridica situata o stabilita nell'Unione che ha ricevuto e accettato un mandato scritto da un fornitore di un sistema di IA o di un modello di IA generale rispettivamente per eseguire per suo conto gli obblighi e le procedure" stabiliti dalla legge AI.

Infine, l'importatore, secondo l'articolo 3, paragrafo 6, è "una persona fisica o giuridica situata o stabilita nell'Unione che immette sul mercato un sistema di IA che porta il nome o il marchio di una persona fisica o giuridica stabilita in un paese terzo.

3.2.1 Attuazione e applicazione della legge sull'AI[43]

Claudio Novelli, Philipp Hacker, Jessica Morley, Jarle Trondal e Luciano Floridi, esperti ricercatori del digital e della giurisprudenza, hanno pubblicato un articolo con lo scopo di spiegare il quadro di governance dell'AI ACT e fornire raccomandazioni per garantire l'esecuzione uniforme e coordinata. La pubblicazione si concentra sulla classificazione di "General Purpose AI Model",

[43] approfondimenti e punti salienti elaborati da Novelli et al. (2024)

GPAI, definiti nell'art 44 AI ACT come modelli informatici che, tramite la grande mole di dati, possono essere usati a diversi scopi, singolarmente o inseriti come componenti di un sistema IA.

Tabella 3.1 Matrice di compliance per i GPAIM

GENERAL-PURPOSE AI MODELS

Article	Providers	Deployers	Product manufacturers	Authorized representatives	Importers	Distributors
Article 41 Common specifications → Lays out requirements for providers to comply with common specifications adopted by the Commission.	✓					
Article 51 Classification of general-purpose AI models as general-purpose AI models with systemic risk → Lays out the conditions under which a general-purpose AI model should be classified as a "general-purpose AI model with systemic risk."	✓					
Article 52 Procedure → Establishes procedures for the providers of general-purpose AI models that meet the conditions of Article 51, such as notifying the Commission or requesting reassessment.	✓					
Article 53 Obligations for providers of general-purpose AI models → Establishes requirements for drawing up and updating technical documentation regarding a model's training, testing, evaluation and integration with AI systems.	✓					

GENERAL-PURPOSE AI MODELS

Article	Providers	Deployers	Product manufacturers	Authorized representatives	Importers	Distributors
Article 54 Authorized representatives of providers of general-purpose AI models → Lays out rules for providers established in third countries to appoint an authorized representative in the EU.	✓			✓		
Article 55 Obligations for providers of general-purpose AI models with systemic risk → Requires providers of general-purpose AI models with systemic risk to perform model evaluations and assess and mitigate possible systemic risks.	✓					
Article 56 Codes of practice → Outlines procedures for providers of general-purpose AI models and downstream providers to participate in drawing up codes of practice and adhere to them.	✓					
Article 89 Monitoring actions → Enables downstream providers to lodge complaints alleging infringement of the AI Act.	✓					

Fonte EU AI ACT Compliance Matrix, by IAPP Principal Researcher, Privacy Law and Policy, Muge Fazlioglu, CIPP/e, CIPP/US

La Commissione ha distinto i modelli GPAI in sistemici e generici, dove i primi sono soggetti ad una regolamentazione più pervasiva. Infatti, essi sono soggetti a standard di sicurezza dell'IA molto rigidi, che riguardano la valutazione e il red teaming, la valutazione globale e la mitigazione del rischio, la segnalazione degli incidenti e la sicurezza informatica. I fornitori di GPAI, secondo l'art 52 AI ACT, potranno contestare la decisione di classificazione di rischio se i modelli sono addestrati

con dimensione 10^{25} Flop[44], mentre quelli già esistenti avranno tempo di garanzia di 24 mesi prima di dover rispondere pienamente all'AI ACT.

Novelli et al. hanno elaborato una tabella semplificativa dei compiti e responsabilità della commissione. La tabella è stata riportata per completare l'approfondimento sull'attuazione e applicazione della legge AI ACT.

Tabella 3. 2 Attuazione e applicazione della legge sull'AI: i restanti passi per la Commissione

Aspetti chiave	**Compiti e responsabilità della Commissione**
a) Procedure	• Istituire e collaborare con l'Ufficio AI e il Comitato AI per sviluppare atti di esecuzione e delegati • Condurre la procedura di comitatologia con gli Stati membri per l'adozione e gli atti di esecuzione • Gestire l'adozione degli atti delegati, consultando esperti e sottoposti al controllo del Parlamento europeo e del Consiglio
b) Linee guida	• Pubblicare linee guida sull'applicazione della definizione di un sistema di IA e regole di classificazione per i sistemi ad alto rischio • Creare metodi di valutazione del rischio per identificare e mitigare i rischi • Definire regole per "modifiche significative" che alterano il livello di rischio di un sistema ad alto rischio
c) Classificazione	• Aggiornare allegato III per aggiungere o rimuovere casi d'uso dei sistemi di IA ad alto rischio attraverso atti delegati • Classificare la General Purpose AI Model, GPAI come a rischio sistemico sulla base di criteri quali FLOP e capacità ad alto impatto • Adeguare i parametri normativi (soglie, parametri di riferimento) per la classificazione GPAI attraverso atti delegati
d) Sistemi vietati	• Sviluppare linee guida sulle pratiche di IA vietate ai sensi art. 5 • Stabilire standard e migliori pratiche per contrastare le tecniche e i rischi di manipolazione • Definire criteri per le eccezioni ai divieti, ad esempio, per l'uso da parte delle forze dell'ordine dell'identificazione biometrica remota in tempo reale

[44] Unità di misura della grandezza di un software

Aspetti chiave	Compiti e responsabilità della Commissione
e) Norme armonizzate e obblighi ad alto rischio	• Definire norme e obblighi armonizzati per i fornitori di sistemi ad alto rischio, compreso il sistema di gestione del rischio interno, art 9 • Standardizzare i requisiti di documentazione tecnica e aggiornare l'allegato IV tramite atti delegati, se necessario • Approvare codici di condotta, art 56, comma 6, AIA)
f) Informazione e Trasparenza	• Stabilire obblighi di informazione per i fornitori di sistemi ad alto rischio lungo tutta la catena del valore dell'IA • Pubblicare linee guida per garantire la conformità ai requisiti di trasparenza, in particolare per i General Purpose AI Model GPAI
g) Esecuzione	• Chiarire l'interazione tra l'AIA e altri quadri legislativi dell'UE • Regolamentare i sandbox normativi e le funzioni di supervisione • Supervisionare l'impostazione da parte degli Stati membri di sanzioni e misure di applicazione che siano efficaci, proporzionate e deterrenti

Fonte 1 Novelli et al. (2024)

3.3 IA: opportunità e gestione dei rischi

L'Intelligenza Artificiale fornisce opportunità elevate allo sviluppo del business: numerosi sono le potenzialità che possono essere sfruttate dalle organizzazioni, ma è indispensabile tener ben presenti gli aspetti legati all'etica, alla conformità normativa e alla governance. La preoccupazione principale della tecnologia è che ha capacità GenIA, ovvero è in grado da sola di generare codici, dati, immagini e falsi che assomigliano alla realtà. La complessità e potenzialità della tecnologia destano sospetti che nel breve futuro queste saranno sempre più elevate, rendendo sempre più difficile distinguere un output umano da quello di IA e si diffonderanno criticità legate alla sicurezza, all'applicazione in campo militare, al copyright dei

contenuti e alla gestione della proprietà intellettuale. La giurisdizione è oggi chiamata a elaborare nuovamente norme a tutela dei cittadini e dei soggetti giuridici. Infatti, oltre alla AI ACT, nell'autunno del 2023 sono stati emessi due documenti: le linee guida del G7 e l'Executive Order del Presidente USA Joe Biden[45].

Il dibatti sui rischi connessi alla tecnologia GenIA richiama le aziende a adottare le misure in tempi brevi per ridurre i danni reputazionali e patrimoniali associati ad utilizzi impropri o che violino i diritti di soggetti.

3.4 I rischi connessi all'Intelligenza Artificiale

Lo sviluppo e l'evoluzione delle economie mondiali, comprese quelle più solide, quale quella statunitense ed europea, sono legate allo sfruttamento delle tecnologie e della IA.

Le opportunità sono bene evidenti nell'industria digitale e nelle applicazioni business-to-business, ma non dobbiamo dimenticare che ad usufruirne sono anche i cittadini, che hanno ottenuto una maggiore rapidità nell'accesso ai servizi della PA e una maggiore assistenza, tramite le chatbot. Come evidenziato, l'uso crescente di sistemi di IA comporta dei rischi, di tipo etico, morale, lesioni ai diritti fondamentali

[45] Giacomo Borgognese, Anna Cataleta, Intelligenza Artificiale più sicura, i paletti del G7 e di Biden, www.cybersecurity360.it

e alla democrazia ed economico; di conseguente per evitare l'uso improprio è necessario porre delle indicazioni prima di rilasciare la tecnologia sul mercato.

I rischi sono connessi alla salute dei cittadini, perché in caso di applicazioni di IA a contatto o integrate nel corpo umano potrebbero essere pericolose se mal progettate, mal utilizzare o hackerate. Quest'ultimo è quello attualmente più preoccupante, perché potrebbe comportare una maggiore proliferazione di dati all'interno del Dark Web, un gruppo di siti web, nascosti e raggiungibili solo attraverso browser specifici, all'interno del quale non vi è nessuno a gestire ed è dove si svolgono attività illegali, quali la vendita di dati e informazioni di vario genere.

Oltre alle minacce sulla sicurezza informatica, l'IA, essendo in grado di progettare da sola, potrebbe essere in grado di mettere insieme informazioni acquisite senza l'autorizzazione del soggetto, oppure realizzare contenuti falsi. Infatti, essa ha già creato dei contenuti, dati dall'interazione con gli utenti, che hanno acceso ampi dibattiti, perché non etici, non veritieri e lesivi della dignità umana[46]. I contenuti falsi, ma estremamente realistici, noti come deepfake, sono stati usati anche per truffare, rovinare la reputazione di persone fisiche e giuridiche, incidendo sia su fatturati che sui diritti umani. Senza l'uso dell'IA, Cambrige analytica, società britannica con la mission di occuparsi delle strategie di comunicazione politica per

[46] Ad aprile 2024, numerosi sono stati i casi di contenuti immagini realizzati con IA sulla storia mai esistiti oppure contenuti video cortometraggi con personaggi famoso mischiati (volto di uno sul corpo di un altro)

finalità elettorali, è stata in grado di sviluppare un sistema di microtargeting psicografico. Essa, attraverso la raccolta di dati provenienti da Facebook, social media più diffuso, è stata in grado di influenzare il giudizio di utenti aventi diritto al voto in occasione delle votazioni presidenziali negli stati uniti nel 2016, in quelle della Brexit in Inghilterra. Con l'avvento dell'IA, la stessa operazione avrebbe potuto essere più automatizzata e con conseguenza ancora più rilevanti.

Inoltre, anche la concorrenza potrebbe essere distorta, in quanto le diverse parti potrebbe aver accesso ad informazioni differenti che comporterebbe un vantaggio rispetto all'altro.

L'evidente problema di trasparenza potrebbe rendere poco chiaro all'utente se l'interazione è con umano o con un sistema di intelligenza artificiale.

Capitolo 4 Sviluppo di un framework per la gestione dei rischi dei sistemi di IA

4.1. Introduzione

Il lettore a questo punto della narrazione del seguente elaborato avrà avuto modo di interrogarsi sull'excursus fino ad ora presentato: da un aspetto generale, quale i rischi aziendali, è stata effettuata l'analisi di uno dei rischi più impattanti oggi, quello cyber, e infine, è stata effettuata l'introduzione alla normativa AI ACT, quale strumento di tutela per quei sistemi che adottano l'Intelligenza Artificiale.

Il titolo della tesi elaborata, però, è "AI Risk Control Framework: assessment di risk management su software che utilizzano l'intelligenza artificiale", perché l'obiettivo è la produzione di un framework che sia in grado di supportare le organizzazioni nello sviluppo compliance di sistemi IA. La prime due parti hanno preparato il lettore a comprendere il modus di operare: indipendentemente da quale rischio l'azienda si trova ad affrontare, deve utilizzare gli strumenti di valutazione preliminare, al fine di prevenirli e abbatterli. Considerando che il rischio cyber è in costante crescita, l'introduzione di sistemi dotati di IA e machine learning, potrebbe, da un lato supportare l'automazione della gestione dei rischi, anche cyber, ma allo stesso tempo provocare un innalzamento delle vulnerabilità delle infrastrutture informatiche delle organizzazioni. Gli stessi sistemi IA non sono esenti da rischi e, come delineato nella legge, è necessario analizzare i diversi

sistemi sulla base anche delle loro destinazioni, finalità, utilizzatori e output prodotti.

Una delle sfide richieste oggi è determinare chi sia responsabile per i danni causati da un dispositivo o servizio azionato dall'intelligenza artificiale. I produttori e divulgatori di applicativi IA devono fin da oggi tutelare gli utenti e tutelarsi. In un futuro, come nella serie tv "Upload"[47]sarà necessario per la società assicuratrice intervenire in un incidente in cui è coinvolta un'auto a guida autonoma e comprendere da chi dovranno essere ripagati i danni se dal proprietario, che però non guidava, dal costruttore o dal programmatore.

4.2. Sviluppo di un framework per l'analisi dei rischi dei sistemi IA per i proveder

La consapevolezza che i rischi connessi ai sistemi IA sono elevati e in grado di ledere i diritti dei cittadini è il motivo per il quale è stato sviluppato un framework[48] per supportare i proveder nel valutarli prima della commercializzazione. Il framework è stato elaborato e testato allo scopo di analizzare i rischi relativi ai sistemi di IA e quali sono gli obblighi, ad oggi, per i fornitori che sviluppano strumenti di IA. Lo strumento è solo in una primissima versione ed è stato testato

[47] Il capitolo è un'introduzione per spiegare perché l'elaborato ha posto un accento notevole sui rischi in generale, citato numerosi soggetti. Tutti i citati sono parte di un ecosistema in evoluzione e su tutti loro ricadono le potenziali conseguenze dell'introduzione di un sistema IA non conforme a normativa. È stata inoltre proposto un esempio fantascientifico al solo scopo semplificativo.
[48] Si ringrazia l'Ing. Alessandro de Bartolo e Ing. Michele Cortese che hanno contribuito allo sviluppo del framework.

su cinque providers, per realizzare il seguente progetto di ricerca, ma sarà oggetto di ampliamento sia per le altre figure che sono delineate all'interno della normativa, che fruibile per un numero più elevato di sviluppatori di sistemi di IA. Come da specifica normativa, gli obblighi presentati dalla AI ACT si applicheranno a livello globale dopo 12 mesi e le norme per i sistemi di AI integrati nei prodotti saranno regolamentati dopo 36 mesi e, quindi, è necessario iniziare divulgare l'importanza dell'adeguamento e avviare un processo di assessment. Il framework realizzato ha proprio il fine di sensibilizzare la conoscenza della legge e diventare uno strumento di analisi dei rischi della tecnologia sviluppata.

Il modello è basato sulle azioni che i providers sono chiamati ad intraprendere e sono: sensibilizzazione e linee guida, risk assessment, definizione di AI Control Framework e analisi sanzionatoria.

La prima fase è caratterizzata dalla diffusione dell'importanza, alla sensibilizzazione della tematica e a fornire linee guida per i fornitori di sistemi IA, che possono guidare alla realizzazione, al test e al monitoraggio.

L'assessment avrà lo scopo di individuare uno score di compliance del sistema IA e verrà rilasciata una stima della potenziale somma sanzionatoria a cui si potrebbe andare incontro. Il vantaggio è di assicurarsi che i rischi associati allo sviluppo siano contenuti e compliance. Infatti, come da normativa, ogni applicativo dovrà essere sottoposta alla valutazione dei rischi e identificarlo nella categoria indicata

dalla norma (inaccettabile, alto, accettabile e minimo). Il framework di Exprivia è in grado di fornire un risultato valutativo e di determinare a quali condizioni deve essere sottoposto l'applicativo.

La gestione dei rischi richiede l'individuazione di regole, procedure e strutture organizzative che permettono di identificare, misurare e gestire il percorso dei rischi legati alla IA ed è elaborata dal tool AI Risk Control.

Infine, abbiamo ritenuto opportuno basare l'intero modello con un approccio da sanzionatore, perché, in attesa della definizione più chiara della normativa, le organizzazioni necessitano di una guida per verificare il livello di rischio e per sensibilizzare la consapevolezza dei pericoli della tecnologia. In particolare, lo sviluppo di un piano di awareness è necessario per tutti i dipendenti. Infatti, l'utilizzo di chat intelligenti, quali chatGpT, hanno fin da subito raccolto l'entusiasmo di diverse aree aziendali, come il Marketing, perché capace di sviluppare contenuti in poco tempo e di ottima qualità.

Nella prassi, le linee guida illustrano le caratteristiche della tecnologia e le modalità con le quali può essere utilizzata, specificando che qualsiasi output generato da modelli generativi, deve essere oggetto di attenta analisi, prima del suo impiego.

In questa primissima fase, gli operatori indicati della normativa devono identificare una o più figure tra coloro che gestiscono il rischio oppure un consulente esterno, con il compito di intervenire per ogni aspetto di natura legale, regolamentare e di

gestione del rischio correlato all'uso e al potenziale uso degli applicativi IA. La gestione della parte operativa dell'help desk interno dovrebbe essere affidata ad esperti IT, che esaminano, progettano e sviluppano le soluzioni in relazioni alle esigenze interne e di mercato. Essi sono stati individuati come la figura di interfaccia per rispondere alle domande del questionario del AI Risk Control Assessment.

4.2.1. AI Risk Control Assessment

L'analisi dei 113 articoli più 13 allegati ha portato all'elaborazione di 80 domande inerenti ai rischi, obblighi e sanzioni, per analizzare e verificare il livello di rischio dei sistemi IA. Le domande sono state sviluppate per essere rivolte al team tecnico che sviluppa l'applicativo di IA di organizzazioni proveder, uno degli operatori indicati nella normativa. Esse sono state inserite all'interno di una matrice su foglio di calcolo Excel.

Tabella 4.1: EU AI ACT Compliance ACT

HIGH-RISK AI SYSTEMS

Article	Providers	Deployers	Product manufacturers	Authorized representatives	Importers	Distributors
Article 6 **Classification rules for high-risk AI systems** → Provides a set of conditions for use in determining whether an AI system is high-risk, as well as documentation requirements for certain providers.	✓					
Article 8 **Compliance with the requirements** → Lays out how providers of high-risk AI systems may demonstrate compliance with their obligations.	✓					
Article 9 **Risk management system** → Outlines steps for the establishment, implementation, documentation and maintenance of risk management systems.	✓					
Article 10 **Data and data governance** → Establishes requirements for training, validation and testing datasets.	✓					
Article 11 **Technical documentation** → Establishes requirements for the drawing up of technical documentation before a high-risk AI system can be placed on the market.	✓					

HIGH-RISK AI SYSTEMS

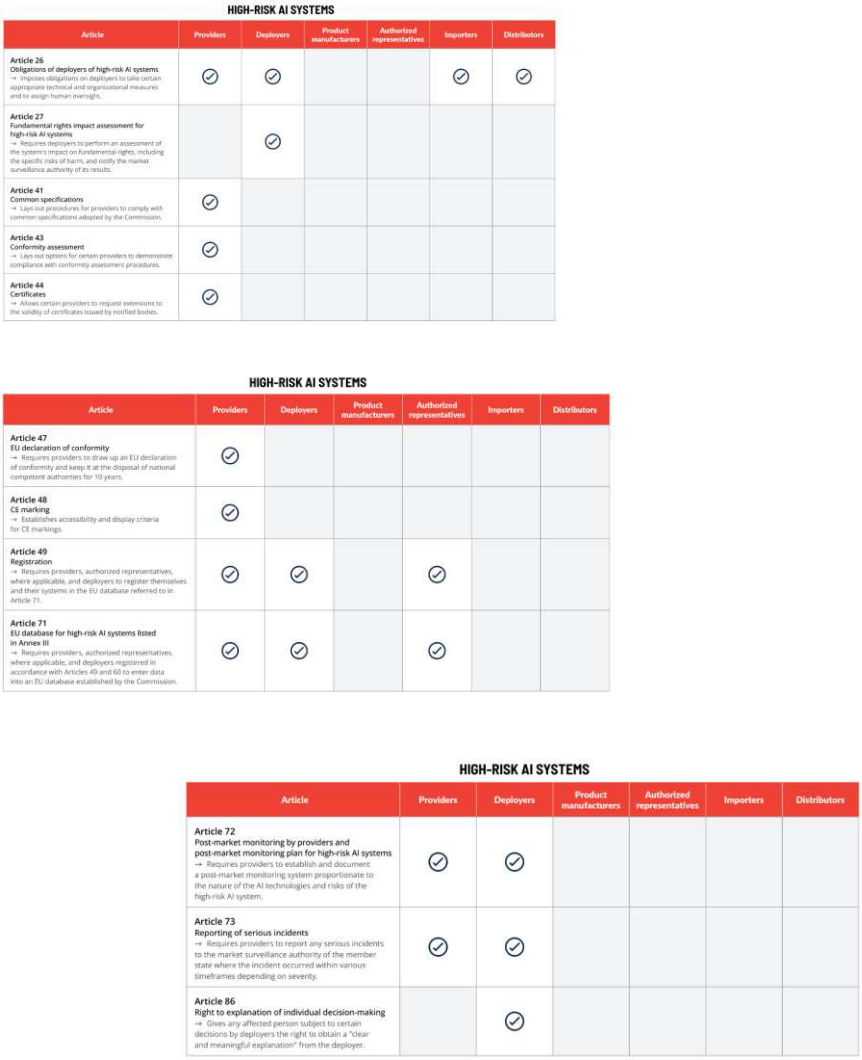
Article	Providers	Deployers	Product manufacturers	Authorized representatives	Importers	Distributors
Article 12 **Record-keeping** → Establishes rules for the automatic recording of events, or logs, over the lifetime of a system.	✓					
Article 13 **Transparency and provision of information to deployers** → Establishes requirements for what "instructions for use" should contain and how they should be made transparent to deployers.	✓	✓		✓		
Article 14 **Human oversight** → Creates rules for oversight measures commensurate with the risk, level of autonomy and context of use of high-risk AI systems.	✓	✓				
Article 15 **Accuracy, robustness and cybersecurity** → Establishes technical rules for the design of high-risk AI systems to achieve accuracy, robustness and cybersecurity throughout their life cycle.	✓					
Article 16 **Obligations of providers of high-risk AI systems** → Clarifies requirements around documentation, quality management, conformity assessment, registration and other obligations.	✓					

HIGH-RISK AI SYSTEMS

Article	Providers	Deployers	Product manufacturers	Authorized representatives	Importers	Distributors
Article 17 **Quality management system** → Establishes rules around the policies, procedures and instructions for implementing quality management systems.	✓					
Article 18 **Documentation keeping** → Ensures providers keep the documentation required by Article 11 at the disposal of national competent authorities for a period of at least 10 years.	✓			✓		
Article 19 **Automatically generated logs** → Ensures providers keep the logs referred to in Article 12 for at least six months.	✓					
Article 20 **Corrective actions and duty of information** → Requires providers to take corrective actions, withdraw, disable or recall high-risk AI systems that are not in conformity.	✓	✓		✓	✓	✓
Article 21 **Cooperation with competent authorities** → Following a reasoned request, requires providers to supply information and documentation to demonstrate conformity to a competent authority.	✓					

HIGH-RISK AI SYSTEMS

Article	Providers	Deployers	Product manufacturers	Authorized representatives	Importers	Distributors
Article 22 **Authorized representatives of providers of high-risk AI systems** → Requires providers established in third countries to appoint an authorized representative in the EU to perform certain tasks.	✓			✓		
Article 23 **Obligations of importers** → Imposes obligations on importers to ensure providers have complied with certain requirements, such as the conformity assessments in Article 43 and technical documentation in Article 11.	✓			✓	✓	
Article 24 **Obligations of distributors** → Imposes obligations on distributors to ensure providers and importers have complied with their obligations in Article 16 and Article 23.	✓				✓	✓
Article 25 **Responsibilities along the AI value chain** → Establishes certain conditions under which a distributor, importer, deployer or other third party may be considered a provider of a high-risk AI system.	✓	✓	✓		✓	✓



HIGH-RISK AI SYSTEMS

Article	Providers	Deployers	Product manufacturers	Authorized representatives	Importers	Distributors
Article 26 Obligations of deployers of high-risk AI systems → Imposes obligations on deployers to take certain appropriate technical and organizational measures and to assign human oversight.	✓	✓			✓	✓
Article 27 Fundamental rights impact assessment for high-risk AI systems → Requires deployers to perform an assessment of the system's impact on fundamental rights, including the specific risks of harm, and notify the market surveillance authority of its results.		✓				
Article 41 Common specifications → Lays out procedures for providers to comply with common specifications adopted by the Commission.	✓					
Article 43 Conformity assessment → Lays out options for certain providers to demonstrate compliance with conformity assessment procedures.	✓					
Article 44 Certificates → Allows certain providers to request extensions to the validity of certificates issued by notified bodies.	✓					

HIGH-RISK AI SYSTEMS

Article	Providers	Deployers	Product manufacturers	Authorized representatives	Importers	Distributors
Article 47 EU declaration of conformity → Requires providers to draw up an EU declaration of conformity and keep it at the disposal of national competent authorities for 10 years.	✓					
Article 48 CE marking → Establishes accessibility and display criteria for CE markings.	✓					
Article 49 Registration → Requires providers, authorized representatives, where applicable, and deployers to register themselves and their systems in the EU database referred to in Article 71.	✓	✓		✓		
Article 71 EU database for high-risk AI systems listed in Annex III → Requires providers, authorized representatives, where applicable, and deployers registered in accordance with Articles 49 and 60 to enter data into an EU database established by the Commission.	✓	✓		✓		

HIGH-RISK AI SYSTEMS

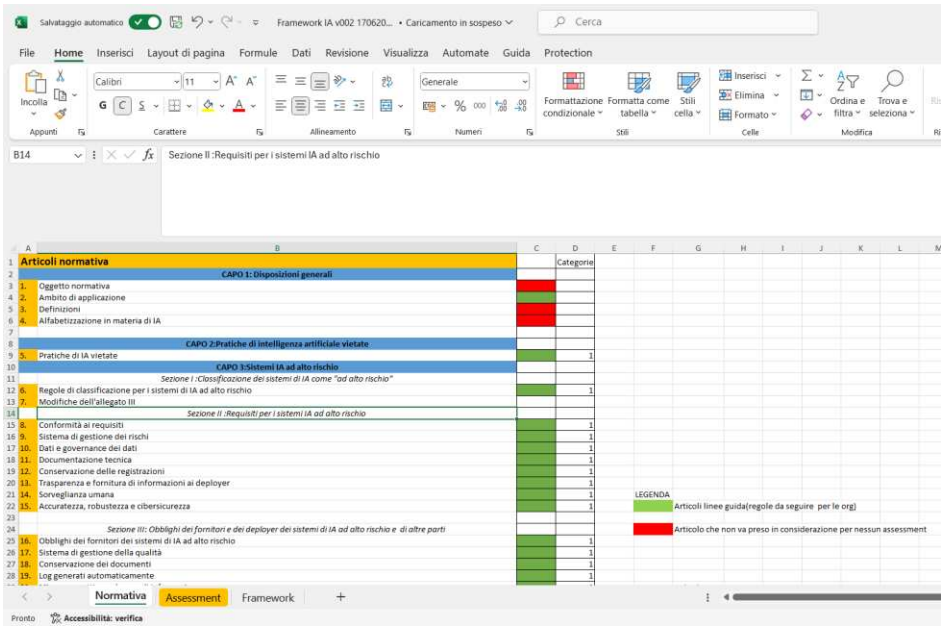
Article	Providers	Deployers	Product manufacturers	Authorized representatives	Importers	Distributors
Article 72 Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems → Requires providers to establish and document a post-market monitoring system proportionate to the nature of the AI technologies and risks of the high-risk AI system.	✓	✓				
Article 73 Reporting of serious incidents → Requires providers to report any serious incidents to the market surveillance authority of the member state where the incident occurred within various timeframes depending on severity.	✓	✓				
Article 86 Right to explanation of individual decision-making → Gives any affected person subject to certain decisions by deployers the right to obtain a "clear and meaningful explanation" from the deployer.		✓				

Fonte 2 Fonte EU AI ACT Compliance Matrix, by IAPP Principal Researcher, Privacy Law and Policy, Muge Fazlioglu, CIPP/e, CIPP/US

Nella prima interfaccia del Framework è presenta la normativa, divisa per capo e sezione. Nella colonna C, vicino ad ogni articolo, le celle sono evidenziate con colori differenti: rosso o verde, ad indicare nel caso verde, di interesse per la

realizzazione dell'assessment risk, rosso legge che non fornisce alcuna indicazione necessaria per la realizzazione del questionario.

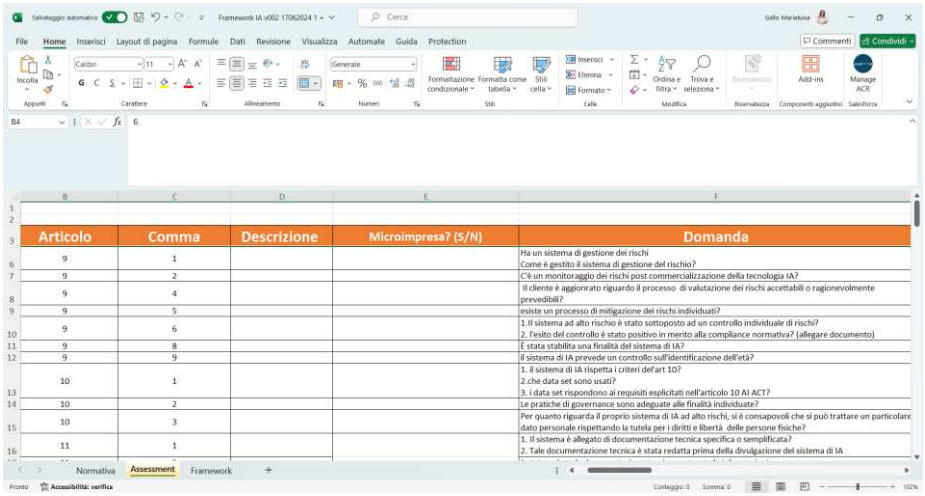
Figura 4.1 Interfaccia grafica 1 foglio Excel: la normativa



Fonte: Nostra elaborazione

La seconda interfaccia del foglio di lavoro Excel è caratterizzata dall'assessment. La suddivisione della matrice realizzata è composta da articolo, comma di riferimento, descrizione, domanda, peso della domanda, risposta del fornitore.

Figura 4.2: Interfaccia grafica 1 foglio Excel: l'assessment



Articolo	Comma	Descrizione	Microimpresa? (S/N)	Domanda
9	1			Ha un sistema di gestione dei rischi Come è gestito il sistema di gestione del rischio?
9	2			C'è un monitoraggio dei rischi post commercializzazione della tecnologia IA?
9	4			Il cliente è aggiornato riguardo il processo di valutazione dei rischi accettabili o ragionevolmente prevedibili?
9	5			esiste un processo di mitigazione dei rischi individuati?
9	6			1.Il sistema ad alto rischio è stato sottoposto ad un controllo individuale di rischi? 2. l'esito del controllo è stato positivo in merito alla compliance normativa? (allegare documento)
9	8			È stata stabilita una finalità del sistema di IA?
9	9			Il sistema di IA prevede un controllo sull'identificazione dell'età?
10	1			1. il sistema di IA rispetta i criteri del'art 10? 2.che data set sono usati? 3. i data set rispondono ai requisiti esplicitati nell'articolo 10 AI ACT?
10	2			Le pratiche di governance sono adeguate alle finalità individuate?
10	3			Per quanto riguarda il proprio sistema di IA ad alto rischi, si è consapovoli che si può trattare un particolare dato personale rispettando la tutela per i diritti e libertà delle persone fisiche?
11	1			1. Il sistema è allegato di documentazione tecnica specifica o semplificata? 2. Tale documentazione tecnica è stata redatta prima della divulgazione del sistema di IA

Fonte: Nostra elaborazione

La pluralità di domande è stata sottoposta ad una figura appartenete all'organizzazione, il metodo prevede di ricevere le risposte a tali domande e memorizza il tutto in un supporto di archiviazione. Per facilitare il rispostare e semplificare la fase della misurazione, il framework segue la formula delle risposte con:

• SI: se l'organizzazione soddisfa pienamente il requisito indicato nella domanda;

• NO: se l'organizzazione non soddisfa il requisito indicato nella domanda;

• In parte: se l'organizzazione soddisfa parzialmente il requisito indicato nella domanda.

L’approccio consente vantaggiosamente di disaccoppiare le domande e le risposte ricevute rispetto alla generazione dei risultati e verifica se è stata rispettata la legge UE sull'intelligenza artificiale, fornendo una panoramica di alto livello dei suoi requisiti chiave per le organizzazioni. Dopo la recezione delle domande si fornisce uno score dell’analisi effettuale e attraverso il range definito è possibile individuare anche la potenziale somma pecuniaria alla quale l’organizzazione potrebbe andar incontro.

Ottenute le risposte alle singole domande si assegna un punteggio numerico G con la seguente logica:

- SI: valore 1;
- NO: valore 0;
- In parte: valore 0.5.

Una volta assegnato ad ogni risposta uno specifico punteggio numerico G, il metodo dell’invenzione prevede, di assegnare un peso di importanza P di ciascuna domanda del sottoinsieme, per ciascun elemento di rischio appartenente all’assessment di sicurezza che si intende valutare. Il valore di ciascuno dei pesi di importanza P assegnato a ciascuna delle domande del sottoinsieme, per ciascuno degli elementi

di rischio i appartenenti allo specifico assessment, è ottenuto assegnando alla domanda, per ciascuno degli elementi di rischio i, un valore di importanza xi compreso tra 0 e 10, e successivamente calcolando il valore del peso di importanza P mediante la formula:

$$P_{i=\frac{x_i}{\sum_{i=1}^{N} x_i}}$$

laddove N è il numero totale degli elementi di rischio i appartenenti all'assessment e laddove:

$$\sum_{i=1}^{N} P_{i=1}$$

Definiti i punteggi numerici G delle risposte e i pesi di importanza P di ciascuna domanda per ciascun elemento di rischio i, si calcola il valore di esposizione al rischio O che si intende valutare, in funzione del peso di importanza P assegnato a ciascuna delle domande del sottoinsieme e in base al punteggio numerico G assegnato alla relativa risposta. Preferibilmente, tale funzione di calcolo per definite il valore di esposizione al rischio O per ciascuno degli elementi di rischio i appartenenti allo specifico assessment di sicurezza è la seguente:

$$0 = \sum_{i=1}^{N} (P_i * G_i)$$

Con 0: [0:5] ∈ ℕ

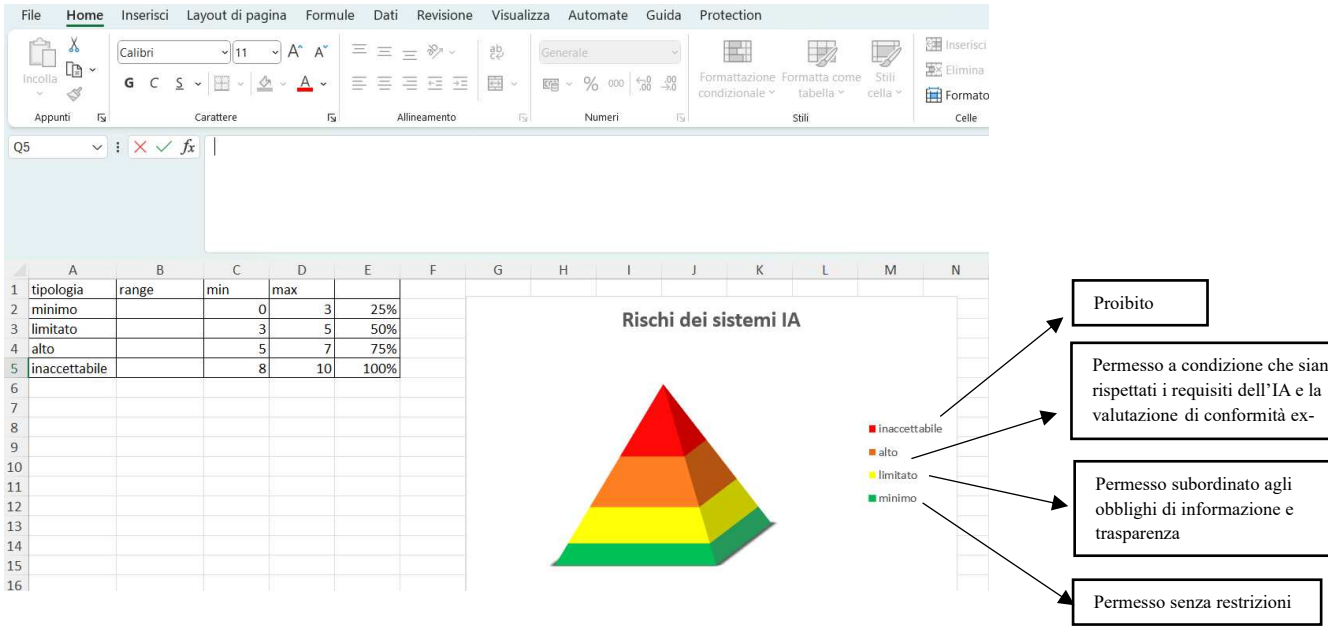
$$y \in o \ni \begin{cases} y > 5 \Longrightarrow 0 = 5 \\ y = 0 \Longrightarrow 0 = 0 \\ 0 < y \leq 5 \Longrightarrow 0 = [0;5] \end{cases}$$

Infine, si rappresentare graficamente il risultato della valutazione in base ai valori di esposizione al rischio O calcolati per gli elementi di rischio i. Il grafico è una tabella di score a colori rosso, arancione, giallo e verde, ognuno dei quali è assegnato un range di valori.

Il grafico fornisce un'utile e rapida visualizzazione del rischio a cui il sistema di IA è esposto e quanto risponde ai requisiti.

Una volta ultimato l'assessment, l'utente può osservare sia i progressi fatti, che prendere visione sui motivi per il quale risulta essere carente (quelli determinati dal punteggio basso) su un determinato elemento di rischio.

Figura 4.5 Modello di riferimento dei quattro livelli di rischio previsti dall'AI ACT



Fonte Nostra elaborazione

L'analisi della valutazione dei rischi ottenuta dalle risposte alle domande sottoposte al fornitore rilascia informazioni sullo stato di rischio. Abbiamo individuato quattro livelli: rischio inaccettabile, rischio alto, rischio limitato e rischio minimo, come presentato nella Fig.4.5.

Il sistema di IA sarà definito inaccettabile se il valore raggiunto dalla somma di tutte le domande per il peso attribuito ad ogni singola domanda è inferiore al 0.0047. Il valore si ottiene dividendo il massimo valore ottenibile (punteggio 10 su tutte le 81 domande) diviso quello ottenuto. Il seguente rischio viola i valori europei e dunque, sarà, vietato all'interno dei confini dell'Unione.

Il rischio alto sarà identificato nella sezione arancione e, in questo caso, i sistemi hanno o potranno avere un impatto controverso sulla sicurezza e sui diritti delle persone, non sono vietati, ma il provider ed eventuali distributori sono responsabili e dovranno rispondere direttamente in caso di mal funzionamento e/o danno.

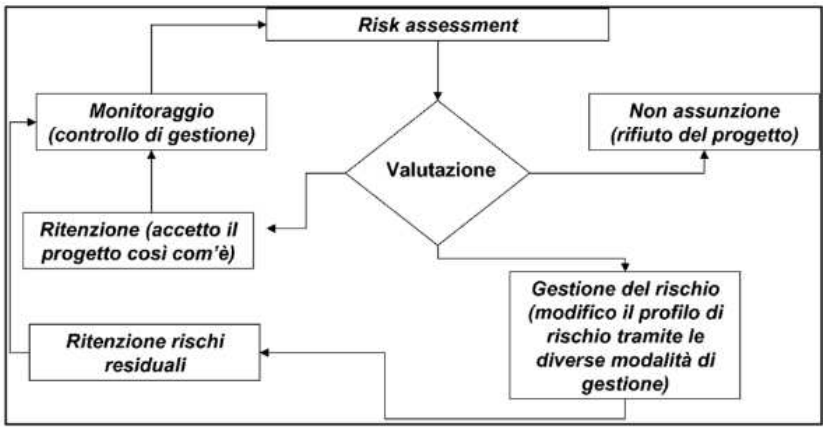
Invece, per le applicazioni che non comportano considerevoli rischi, rientrano nel segmento giallo. Il sistema che si inserisce in questo range (tra 5 e 7) non ha particolari difficoltà e al proveder è richiesto di assicurare un set limitato di requisiti, quali la trasparenza e rivelare in modo evidente l'utilizzo dell'intelligenza artificiale.

Infine, non sono ancora state definiti obblighi di legge per i sistemi con rischio minimo e sono identificati, all'interno della piramide, dalla porzione di colore verde.

4.2.2. Ragionamento del framework di assessment risk di sistemi IA

Il framework sviluppato, si basa sul processo di valutazione del rischio, riportato in Fig. 4.3: dopo l'assessment si avvia la fase continua di monitoraggio che consente di gestire il rischio, modificando il progetto, ovvero l'applicativo IA ove necessario per renderlo compliance. Il fornitore ha la possibilità di modificare le risposte, in base agli aggiornamenti effettuati, e visualizzare immediatamente il nuovo risultato.

Figura 4.3: La valutazione dei rischi di un progetto



Fonte immagine tratta da "Enterprise Risk Management. I rischi aziendali e il processo di risk management" di Alberto Floreani

La variazione di una risposta, fa modificare i valori ottenuti e, di conseguenza il punteggio raggiunto potrebbe modificarsi al punto tale da posizionare l'azienda analizzata su un'altra sezione della piramide dei rischi.

Una volta individuato il tipo di rischio, il framwork è in grado di associare il valore di sanzione, se sussiste, sulla base della normativa AI ACT.

La norma specifica che le violazioni variano da 7,5 milioni di euro, l'1,5% del fatturato o 35 milioni di euro o il 7% del fatturato globale, a seconda del tipo di infrazione compiuto. Il framework fornisce un potenziale valore che la Commissione potrebbe attribuire nel caso di specie.

La valutazione effettuata è una valutazione di risk severity che è filtrata e bilanciata con ulteriori due livelli di analisi: la risk likelihood e la risk mitigation. Esse contribuiscono a definire le azioni di mitigazione del rischio. L'esito raggiunto dalla valutazione del risk assessment consente di avere un quadro esaustivo delle implicazioni derivanti dal potenziale uso del tool AI realizzato. Le informazioni raccolte permettono di realizzare indicare la potenziale sanzione che gli operatori indicati dalla IA ACT potrebbero incorrere. Infine, in caso di sistema IA con rischio inaccettabile, alto e minimo, si presenta una matrice che raccoglie consigli, azioni e mitigazioni per abbassare il livello di rischio della tecnologia.

4.3 Realizzazione di sistemi IA responsabili

Il framework sviluppato vuole favorire lo sviluppo della IA responsabile e si vuole accompagnare, in primis i proveder e poi anche gli altri operatori delineati dalla legge, a disegnare una strategia e definire il modello di governance, mantenendo l'attenzione sullo sviluppo ragionevole dell'IA.

La realizzazione di IA responsabile si compone di quattro dimensioni: la strategia, il controllo, le pratiche responsabili e le pratiche core

Il processo di sviluppo, messa in commercio e uso dell'IA deve essere valutato in fase di design e tener conto delle possibili implicazioni morali legati anche al potenziale uso scorretto dell'applicativo. Lo sviluppatore e divulgatore sono potenzialmente responsabili di impiego non conforme e rischiano danni reputazionali, sanzionatori ed economici. L'elemento "strategia" è variabile nel tempo perché deve tener conto dell'evoluzione sia

della normativa, ma anche della tecnologia e, accanto, è necessario affiancare un attento monitoraggio delle politiche e dei regolamenti generali e verticali sul settore.

L'adozione della strategia etica per l'uso responsabile dell'AI permette di definire la seconda dimensione, la governance e i meccanismi di controllo. L'attività è fondamentale per coinvolgere tutti i livelli dell'azienda e ha l'obiettivo di definire, pianificare, implementare e monitorare tutti i processi e attività interne.

La definizione della strategia e dei meccanismi di controllo comporta la stesura di pratiche responsabili da attuare per garantire l trasparenza del modello decisionale. Il sistema IA sviluppato deve essere interpretabile, ripercorribile e spiegabile, non sono agli sviluppatori e tutti i potenziali utilizzatori o chiunque ne venga in contatto[49]. Il modello deve essere comprensibile, robusto, sostenibile e accessibile e riportato all'interno del documento tecnico, anch'esso disponibile sia per le autorità che per gli utenti. Il sistema IA dovrà garantire alte prestazioni, un elevato livello di affidabilità ed esente da bias, cioè da anomalie derivanti da basi dati che riflettono eventuali pregiudizi umani.

L'ultimo tassello dell'output che realizzerà il framework è rappresentato dalle best practices e continuous improvement: verranno rilasciati all'interno del report dei consigli e delle regole di condotta corretta sullo sviluppo, potenziamento e aggiornamento del sistema IA. La finalità è garantire che l'applicativo risulti sempre conforme agli standard.

[49] Le tecnologie IA interagiscono anche con chi non le sta utilizzando.

Capitolo 6 Conclusione

L’evoluzione tecnologica è in continuo e rapido mutamento, rendendo difficile il controllo degli effetti. Il momento attuale è solo l’inizio di un processo che modificherà il nostro modo di formarci, di lavorare, di condivider e il tempo con gli altri. I componenti di IoT, per esempio, interagiscono con gli utenti, facilitando le sue azioni quotidiane.

Robot, droni, dispositivi indossabili sono solo i primi di una lunga serie di sistemi che invaderanno la quotidianità, lavorativa e privata, delle persone, nei quali l’IA è centrale.

Le organizzazioni stanno vivendo seri cambiamenti grazie ad algoritmi che apprendono le necessità dei consumatori e i dati ISTAT rilevano che nel 2025 la cifra stimata è di circa 60 miliardi di euro di investimenti globali.

La sfida di assicurarsi il vantaggio competitivo è evidente anche tra gli Stati: la Cina, punta entro il 2030 ad essere il vincitore. L’UE presenta più difficoltà rispetto ad altre realtà, ma il suo impegno è evidente attraverso numerose pubblicazioni, normative e enti istituiti per l’intelligenza artificiale, la cybersecurity e la robotica. Gli obiettivi dell’UE riguardano l’incremento sostenibile della capacità tecnologica e industriale, in vari settori, sia pubblico che privato, includendo numerosi investimenti per supportare la ricerca e l’innovazione. Essa si impegna a preparare gli Stati membri al cambiamento

socio-economico, favorendo lo sviluppo dei talenti[50], anticipando i cambiamenti del mercato del lavoro. Inoltre, la Commissione vuole assicurare che lo sviluppo tecnologico sia sempre etico e legale, basato sui valori delineati dalla Carta dei Diritti Fondamentali dell'Unione Europea e dalle normative di settore, come DORA e GDPR.

L'UE suppone che la trasformazione digitale comporterà una sociale e, quest'ultima, dovrà essere guidata e controllata con un approccio multidimensionale che consideri gli aspetti etici e sociali, legali, educativi e formativi, economici, la disponibilità di dati, le possibili intrusioni nella vita privata e relativa Cyber-security, i rischi di discriminazione ed esclusione e la resilienza sociale. La cybersecurity sarà la "compagna" di viaggio dell'IA, per prevenire i rischi derivanti dall'utilizzo improprio o sviluppo non conforme. Il processo di risk management dovrà essere ampliato e considerare oltre alla cyber resilience, anche l'IA resilience, partendo dal processo di awareness per sensibilizzare gli utenti ai rischi e pericoli insiti nel mondo digitale.

L'incentivare fin da subito l'adozione di pratiche di sicurezza potranno avviare a una digital transformation meno imprudente e, per questo, le organizzazioni devono dotarsi di flessibilità operativa e di conformità agli standard e alle normative, verificando periodicamente il proprio livello di maturità nei confronti delle tecniche di mitigazione adeguati e stabilendo programmi di formazione alla sicurezza informatica e all'uso corretto dell'IA. Il processo deve partire anche dagli stessi

[50] Si prevede che le nuove generazioni avranno orari più flessibili, competenze più elevate e maggiore dignità sul lavoro.

produttori, che, essendo i primi coinvolti, devono essere consapevoli delle potenzialità del proprio prodotto.

La tecnica di un framework di assessment è attualmente il tool per eccellenza per l'analisi valutativa dei rischi. Lo strumento realizzato vuole essere una prima guida ai cambiamenti e all'attuazione normativa: l'impatto della tecnologia è sulle persone e in particolare i minori. Il dovere delle istituzioni e delle società informatiche è trovare soluzioni di difesa, dal momento che numerose sono le minacce correlate alla tecnologia e ai cyber attack. Nel corso dei prossimi anni, l'evoluzione dovrà portare con sé anche l'introduzione di standard più chiari e rigidi, per fornire tutale in ogni livello, sia al produttore, che ai distributori e ovviamente agli utilizzatori.

Allegati

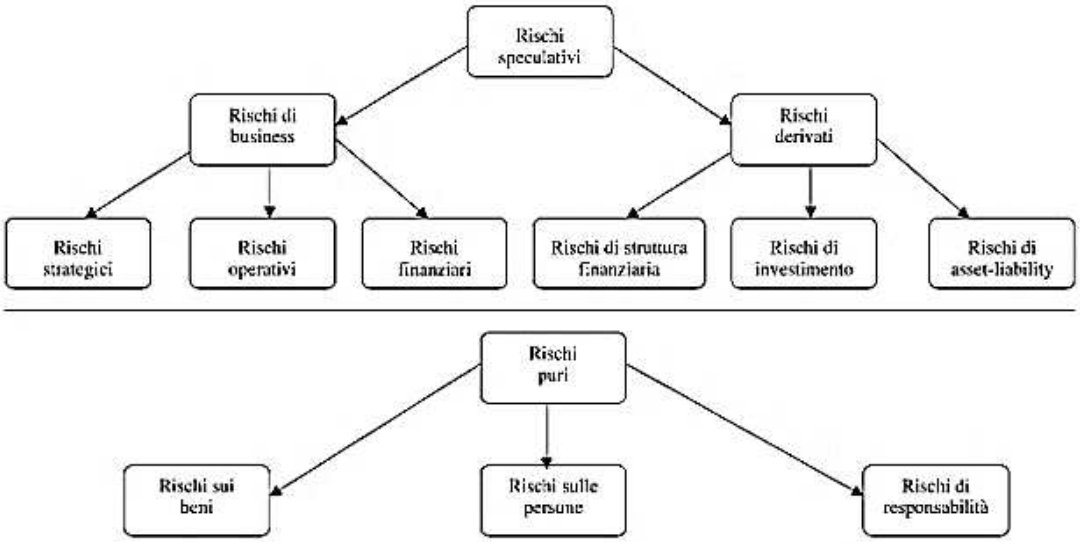
Allegato I: Classificazione dei rischi

Il seguente allegato approfondisce l'aspetto legato alla classificazione dei rischi. Esistono numerose classificazioni dei rischi, la prima che si considera è quella in base al segno dell'impatto.

In primis, i rischi si distinguono in puri e rischi speculativi: i primi sono eventi che possono generare solo danni per l'azienda, mentre ai secondi è possibile associare sia uno scostamento positivo che negativo dai risultati attesi.

La classificazione dei rischi è visibile nel grafico Fig I:

Figura.I. Classificazione dei rischi aziendali



Fonte immagine tratta da "Enterprise Risk Management. I rischi aziendali e il processo di risk management" di Alberto Floreani

I rischi speculativi si dividono a loro volta in rischi di business e rischi derivati:

i primi sono, inerenti alla gestione aziendale, mentre i secondi sono secondari ai primi.

Ulteriormente è possibile distinguere i rischi di business in strategici, operativi, di reporting e di compliance. La tipologia degli strategici comporta un peggioramento della qualità della strategia a seguito di una riduzione della capacità competitiva di un'azienda a lungo termine. Il rischio strategico è legato al tipo di vantaggio competitivo che l'azienda persegue all'interno del settore.

Gli eventi che, invece, producono una diminuzione in termini di efficacia ed efficienza ed economicità di un processo operativo sono definiti rischi operativi

I rischi di reporting riguardano l'attività di reporting sia esterna che interna e sono legati a problemi che possono riguardare ritardi, scarsa accuratezza, sovrabbondanza o assenza delle informazioni.

Infine, per rischi di compliance si intendono tutti quegli eventi che possono determinare uno scostamento da ciò che regolamenti, leggi e disposizioni normative prevedono.

I rischi derivati possono alloro volta essere distinti in: rischi di struttura finanziaria, rischi di investimento e rischi di asset-liability. Tra i rischi derivati si inserisce anche il rischio di reputazione che dipende dal manifestarsi di altri rischi, principalmente da quelli di compliance e riguarda il verificarsi di un danno di immagine dell'azienda portando a delle conseguenze negative in termini di risultati economici.

ed infine per rischio strutturale intendiamo il grado di flessibilità dell'azienda.

I rischi possono essere classificati anche in rischi finanziari, che influenzano alla gestione finanziaria, e operativi. I tre rischi finanziari sono: rischi di mercato, di credito e di liquidità. L'azienda, per monitorare i rischi finanziari dovrà cercare di diversificare il proprio portafoglio di clienti.

I rischi operativi, invece, altri caratterizzano i processi operativi di un'azienda che impattano sui processi di approvvigionamento, di produzione, di vendita, legati alla gestione delle risorse umane e quindi principalmente sul Reddito Operativo. Tre sono le tipologie di rischi operativi: di settore, strategico e strutturale.

Quando si parla di rischiosità settoriale, si intendono le caratteristiche del settore all'interno del quale l'azienda opera e che comportano diversi rischi di natura operativa; mentre il rischio di mercato è legato agli imprevisti delle attività e passività. Legato ai rischi di mercati, troviamo i rischi di cambio, di tasso e di prezzo.

Infine, il rischio di credito si ha nel momento in cui una parte del contratto risulta inadempiente.

L'ultimo criterio di classificazione che possiamo utilizzare è quello che distingue i rischi sulla base della loro universalità o specificità e distinguiamo rischio sistematico e quello specifico.

Il rischio sistematico influisce su tutto il sistema ed è legato a variabili

macroeconomiche, non facilmente governabile dall'azienda e non è semplice gestirlo. Infatti, esso non può essere eliminato nemmeno con le strategie di diversificazione e dipende da dove l'azienda opera, dal modello di business e dal settore.

Infine, quello specifico è collegato a variabili specifiche dell'azienda e può essere contenuto attraverso una diversificazione degli investimenti.

I rischi puri invece possono impattare sulle cose, persone e responsabilità.

Allegato II: Classificazione delle minacce informatiche

Il seguente allegato vuole riportare alcune delle principali minacce informatiche: riconoscerle permette di comprendere che l'introduzione dell'IA può renderli più pericolosi. La prima minacce che ha colpito quasi tutti gli utenti in rete è il phishing, pratica molto diffusa, che consiste nell'inviare e-mail fraudolente che assomigliano a quelle provenienti da fonti affidabili. L'obiettivo è quello di sottrarre dati sensibili, come i numeri delle carte di credito e le informazioni di accesso. L'evoluzione ha portato anche ad azioni che vengono svolte via sms o chiamata telefonica.

Un altro tipo di attacco è quello di tipo ransomware, un tipo di software dannoso progettato per estorcere denaro bloccando l'accesso ai file o al sistema informatico fino al pagamento del riscatto. Il pagamento del riscatto non garantisce che i file verranno recuperati o che il sistema venga ripristinato, anzi, il più delle volte,

nonostante il pagamento, i dati non vengono sbloccati. Esso è utilizzato non solo a scopo di estorsione, ma anche per scopi etici e politici.

Un altro software progettato per ottenere un accesso non autorizzato o per causare danni a un computer è il malware.

Infine, il social engineering è una tattica, più recente, utilizzata per indurre l'utente a rivelare informazioni sensibili. Gli Hacker criminali richiedere un pagamento in denaro oppure ottenere l'accesso ai dati riservati. Il social engineering può associarsi ad altre minacce per rendere l’utente più propenso a fare clic sui link o scaricare il malware.

Bibliografia

Popoli, "*Outsourcing risk management*", 2008

Alberto Floreani, *Enterprise Risk Management. I rischi aziendali e il processo di risk management"*

Parlamento europeo e del consiglio regolamento (UE) 2022/2554 del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011

Parlamento e Consiglio Europeo, Regolamento (UE), Regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (legge sull'intelligenza artificiale), 2024

Floreani, Introduzione al Risk Management, 2005

Nassim Nicholas Tales, "Il cigno nero"

Commissione europea, Cybersecurity. Resilience, deterrence and defence. Building strong cybersecurity in Europe, 2017

Banca d'Italia, Disposizioni di vigilanza per le banche Circolare n. 285 del 17 dicembre 2013, Titolo II - Capitolo 5, e nel recepire gli accordi di Basilea, ha definito il rischio operativo come la possibilità "*di subire perdite derivanti dall'inadeguatezza o dalla*

disfunzione di procedure, risorse umane e sistemi interni, oppure da eventi esogeni. Rientrano in tale tipologia, tra l'altro, le perdite derivanti da frodi, errori umani, interruzioni dell'operatività, indisponibilità dei sistemi, inadempienze contrattuali, catastrofi naturali

Parlamento e Consiglio Europeo, General data protection regulation. "Regulation eu 2016/679 of the euro- pean parliament and of the council of 27 april 2016", 2016

Parlamento e Consiglio Europeo, Regolamento (UE), Regolamento (UE) n. 575/2013 relativo ai requisiti prudenziali per gli enti creditizi e le imprese di investimento, 2016

Parlamento europeo e del consiglio Direttiva 2013/36/ue del del 26 giugno 2013 sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento, 2013.

ECB, Revised oversight framework for retail payment systems.

ECB, Cyber resilience oversight expectations for financial market infrastruc- tures. Rapp. Tecn. Banca centrale europea, 2018.

Giacomo Borgognese, Anna Cataleta, Intelligenza Artificiale più sicura, i paletti del G7 e di Biden, www.cybersecurity360.it

Il sistema di controllo interno nella prospettiva del risk management, Giuseppe D'Onza

Introduzione allo studio dei rischi nell'economia aziendale, Umberto Bertini

Scritti di politica aziendale, Umberto Bertini

Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards and Technology

Italian Cyber Security report, un framework nazionale per la cyber security, a cura di Roberto Baldoni e Luca Montanari, CINI Cyber Security National Lab

2016 Italian Cybersecurity Report Controlli Essenziali di Cybersecurity Research Center of Cyber Intelligence and Information Security, Sapienza Università di Roma

Il "Paese Internet" nella società del rischio, Massimiliano Cannata, Maria Sabina Guerra, Rocco Mammoliti.

Il Futuro della Cyber Security in Italia, Laboratorio Nazionale di Cyber Security, Consorzio Interuniversitario Nazionale per

l'Informatica, A cura di Roberto Baldoni, Università degli Studi di Roma "La Sapienza"

Rocco De Nicola, IMT, Institute for Advanced Studies, Lucca

L'evoluzione del ruolo del CISO in azienda, Aipsa, Raoul Savastano

Cybersecurity Management in the States: The Emerging Role of Chief Information Security Officers, IBM center for the business of government, Marilu Goodyear, Holly T. Goerdel, Shannon Portillo, Linda Williams.

At the juction of corporate governance & cyber security, FERMA e ECIIA.

Cyber Risk Management Italia v1.0 - Modelli di governance dei rischi

Cyber e raccomandazioni di sviluppo per le aziende italiane, Cyber Risk Management Survey 2015, Deloitte e The Innovation Group

Clusit, Supply chain security. L'importanza di conoscere e gestire i rischi della catena della fornitura, 2023

Exprivia, Threat Intelligence Report 2023

Tesi di Laurea Enterprise Risk Management e struttura organizzativa: analisi dello scenario Europeo, di Olimpia Mashio, Relatrice Prof Gloria Gardenal

Tesi di laurea, Risk Management: caratteristiche generali, applicazioni all'ICT, tool di gestione, realizzazione di un case study nell'ambito della cyber security, di Claudia Bolognino, Relatore Prof. Domenico Ursino.

Tesi di Laurea, Cyber Risk: un nuovo approccio alla valutazione, di Matteo Tiscornia, Relatore Prof Danilo Montesi.

Tesi di Laurea, Cyber Risk Management: un'analisi empirica sui comportamenti delle aziende di Alessandra Rigolini, Relatore Alessandra Regoli

PWC, AI la grande ricerca. L'equilibrio sostenibile tra opportunità e gestione dei rischi, 2024

Thomas, H. Davenpot, Nitin Mittal, *Scacco matto con l'IA. Come le aziende all'avanguardia stravincono con l'intelligenza Artificiale*, 2024

Sitologia

Agenda digitale: https://www.agendadigitale.eu/sicurezza/privacy/ai-act-ecco-il-testo-definitivo-gli-impatti/

Agenda digitale https://www.agendadigitale.eu/sicurezza/privacy/ai-act-ecco-il-testo-definitivo-gli-impatti/

Agicap:https://agicap.com/it/articolo/rischio-aziendale/#:~:text=Quando%20si%20parla%20di%20rischio,caso%20peggiore%2C%20portare%20al%20fallimento.

Augeos: https://blog.augeos.it/ict-risk-migliora-la-gestione-dei-rischi-informatici-con-augeos

Diritto al digitale: https://dirittoaldigitale.com/2023/10/16/cybersicurezza-direttiva-nis/

Augeos:https://blog.augeos.it/compliance-risk-governance-come-minimizzare-il-rischio-nelle-esternalizzazioni

Augeos:https://blog.augeos.it/rischio-operativo-come-evitare-perdite-correggendo-in-anticipo-i-processi

Avvocloud:https://avvocloud.net/blog/diritto-nuove-tecnologie/regolamento-europeo-intelligenza-artificiale

Avvocloud:https://avvocloud.net/blog/diritto-nuove-tecnologie/regolamento-europeo-intelligenza-artificiale

Avvocloud:https://avvocloud.net/blog/diritto-nuove-tecnologie/regolamento-europeo-intelligenza-artificiale#scopi

AWMS:https://www.awms-system.com/blog/prodotto/risk-management-significato-fasi-e-strategie/

BCG: https://www.bcg.com/press/10january2024-imprese-e-gestione-del-rischio-non-e-il-momento-di-tagliare-i-fondi

Cronaca Bianca: Intelligenza artificiale: tre incontri per gli studenti in Assemblea legislativa. Aperte le iscrizioni | Cronaca Bianca

Commissione Europea: https://www.bankingsupervision.europa.eu/press/publications/newsletter/2019/html/ssm.nl190213_4.en.html.

Commissione Europea: https://digital-strategy.ec.europa.eu/it/policies/regulatory-framework-ai

Commissione Europea: https://eurlex.europa.eu/legalcontent/IT/TXT/?uri=celex%3A52021PC0206

Commissione Europea: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0006.02/DOC_1&format=PDF

Cybersecurity360:https://www.cybersecurity360.it/legal/iso-iec-420012023-lo-standard-per-il-sistema-di-gestione-dellintelligenza-artificiale-le-finalita/

Deloitte:https://www2.deloitte.com/dl/en/pages/legal/articles/ki-verordnung-eu.html

Europarlamento Europeo:https://www.europarl.europa.eu/topics/it/article/20200918STO87404/quali-sono-i-rischi-e-i-vantaggi-dell-intelligenza-artificiale

Europarlamento Europeo:https://www.europarl.europa.eu/doceo/document/A-9-2023-0188-AM-808-808_IT.pdf

Exprivia: https://www.exprivia.it/wp-content/uploads/2024/03/CS-Exprivia-Report-Cybersecurity-2023.pdf

GEP:https://www.gepinformatica.it/lezioni-di-logistica/ada-lovelace-pioniera-dellinformatica-e-ispirazione-per-la-festa-della-donna/

GEP:https://www.gepinformatica.it/lezioni-di-logistica/ada-lovelace-pioniera-dellinformatica-e-ispirazione-per-la-festa-della-donna/

Headvisor:https://www.headvisor.it/risk-management-gestione-del-rischio#:~:text=La%20definizione%20di%20Risk%20Management,disparati%2C%20sia%20interni%20che%20esterni.

IBM: https://it.newsroom.ibm.com/aicambierailmondo?sf187522610=1

IBM: https://www.ibm.com/it-it/ai-cybersecurity

IBM: https://www.ibm.com/it-it/security

IBM:https://www.ibm.com/it-it/topics/nist#:~:text=Il%20NIST%20(National%20Institute%20of,e%20della%20tecnologia%20delle%20misurazioni

IBM:https://www.ibm.com/account/reg/it-it/signup?formid=urx-52506

Intelligenza artificiale: https://www.intelligenzaartificialeitalia.net/post/alan-turing-il-padre-dell-intelligenza-artificiale-ia#:~:text=Alan%20Turing%20era%20un%20matematico,Universit%C3%A0%20di%20Cambridge%20nel%201931.

INSIC:https://www.insic.it/privacy-e-sicurezza/information-security/ai-act-regolamento-europeo-intelligenza-artificiale/#:~:text=Oggi%2C%2021%20maggio%202024%2C%20il,'utilizzo%20dell'intelligenza%20artificiale

ISO: https://shahrdevelopment.ir/wp-content/uploads/2020/03/ISO-31000.pdf

ISO: https://www.iso.org/directives-and-policies.html

ISP: https://www.ispionline.it/it/pubblicazione/ai-act-la-sfida-europea-136317

Microsoft:https://info.microsoft.com/rs/157-GQE-382/images/IT-WBNR-SlideDeck-SRGCM11892.pdf?version=0

More globant:https://more.globant.com/it/ia-generativa-nel-settore-finanziario-assicurativo?utm_source=lin&utm_medium=soc&utm_campaign=a-mkt-r-eur-bo-it-cn-genaiemeait-s-lin-me-soc-o-wpd-bi-nap-f-lik-y-2024-m-3-ac-tl-t-genaiinfsitalia

MYR: https://www.myr.it/norma-iso-31000-cose-e-come-la-utilizziamo/

Osservatori: https://blog.osservatori.net/it_it/storia-intelligenza-artificiale

Parlamento Europeo: Il Parlamento europeo approva la legge sull'intelligenza artificiale | Attualità | Parlamento europeo (europa.eu)

Ringraziamenti

Mi accingo a scrivere i ringraziamenti della mia tesi Magistrale e vorrei manifestare la gratitudine verso chi mi ha sostenuta in questo percorso.

Desidero ringraziare la Professoressa Lucarelli, non solo per essere la mia relatrice, ma soprattutto per le sue lezioni, perché fonti di ispirazioni. Sono rari i docenti che sono in grado di trasmettere la passione ai propri studenti ed è solo grazie ai seminari organizzati dalla docente Lucarelli che ho avuto l'opportunità di scoprire la cybersecurity e di farne la mia professione di vita.

Doverosi i ringraziamenti per Ing. Alessandro de Bartolo e l'Ing Michele Cortese, colleghi nel mio percorso in Exprivia e nello sviluppo del framework realizzato per il seguente elaborato. Oltre all'intero team di lavoro, vorrei cogliere oggi l'occasione per ringraziare i miei colleghi e i miei responsabili, Dott. Daniele Urbano e Ing.Domenico Raguseo, professionisti che hanno creduto in me e mi hanno portata a bordo di una realtà ancora in evoluzione.

Ringrazio il Dott. Antonio Galliano, il mio primo mentor e guida di vita professionale. È stato un vero piacere affrontare le numerose sfide che insieme abbiamo affrontato.

I ringraziamenti professionali non sono ancora conclusi, perché grazie ad Exprivia Women, team di inclusion, ho avuto l'opportunità di conoscere Serena Pistillo. Fin

dà subito ha riposto in me fiducia e mi sta insegnando a credere in me. La ringrazio per il sostegno che mi ha accompagnata verso questo traguardo e per essere un esempio di coraggio. Serena è la mia coach di vita, ma anche un'amica e spero che ci saranno sempre nuove opportunità di condividere con lei idee, passioni e progetti.

Chi mi conosce sa che non sono molto comunicativa e difficilmente sono in grado di esprimere i miei sentimenti, ma vorrei anche ringraziare tutti coloro che mi hanno accompagnata in questo percorso, sostenendomi moralmente nelle sconfitte, festeggiando ad ogni vittoria e ascoltandomi ripetere.

Ringrazio la mia famiglia, i miei genitori e vorrei dedicare questo momento a loro, nell'augurio che saranno orgogliosi del mio percorso professionale. So che il mio percorso non è stato lineare e uguale a quello dei miei coetanei, ma è stato il mio e nonostante le difficoltà, il lavoro, i trasferimenti, oggi sono riuscita a raggiungere un risultato che è anche vostro. Grazie.

Vorrei ringraziare Elisa, per essere un'amica che mi ha incoraggiata e sostenuta nei momenti difficili di questo percorso. Insieme a lei, colgo l'occasione per dire "grazie" a tutte le coinquiline di via Frediani, Alessandra, Federico e tutti gli amici che festeggeranno con me questo momento.

L'ultimo anno è stato impegnativo e vorrei ringraziare chi mi è stato accanto, giorno dopo giorno, chi mi ha ascoltata e supportata, anche in piena notte, quando ancora

ero intenta a studiare. Ringrazio per le lacrime asciugate, per gli scherzi e le risate, ringrazio per i sacrifici vissuti insieme e per aver avuto sempre il coraggio di cominciare insieme il nostro percorso di vita. "*Tutte le volte che sono insieme a te, è come un evento rivoluzionario, scisma potente e crollo di Cartagine"*

Il mio percorso professionale non si conclude in Exprivia, ma ho scelto di essere un arbitro di calcio ed è un onore per me far parte dell'Associazione Arbitri Italiani, una palestra fisica e mentale, per mantenere la concentrazione e la performace per 45 minuti.

Infine, questo traguardo voglio dedicarlo a me e vorrei darmi finalmente "quella bacca sulla spalla" che spesso non mi concedo. Oggi voglio finalmente pensare e respirare, ringraziarmi perché oggi sono qui e non sono diversa da chi insieme a me conseguirà il titolo, solo perché sono più grande di età. Conseguo il titolo di Laurea Magistrale, perché credo nella formazione universitaria e, nonostante le difficoltà di conciliare lavoro e studio, ho scelto di concludere il percorso per la mia carriera e la mia crescita personale.

Grazie a tutte le persone speciali che hanno reso e rendono ogni giorno la mia vita speciale.