Guida al calcolo del fattore di rischio

Una guida operativa per la valutazione del rischio informatico nelle aziende moderne

Michele Ragone

Corso di laurea: Informatica per le Aziende Digitali L-31
Università Telematica Pegaso
Matricola: 0312301811
Anno 2024/2025

Introduzione

Nell'ambito della gestione della sicurezza sul lavoro, è fondamentale comprendere e calcolare correttamente il fattore di rischio per valutare e mitigare i potenziali pericoli. Con la crescente diffusione e sviluppo delle tecnologie digitali e l'integrazione sempre più profonda tra sistemi informatici e processi aziendali, la valutazione accurata dei rischi è diventata una priorità assoluta per qualsiasi organizzazione moderna.

Quando si parla di sicurezza aziendale, spesso si pensa esclusivamente alla protezione fisica dei dipendenti e degli ambienti di lavoro. Tuttavia, oggi il concetto include anche la tutela delle informazioni sensibili e delle infrastrutture digitali che gestiscono quotidianamente le operazioni aziendali. La mancata o errata valutazione dei rischi può comportare conseguenze gravi, come interruzioni dei processi produttivi, perdite economiche rilevanti e danni all'immagine dell'azienda.

Il rischio aziendale rappresenta la possibilità che un evento indesiderato provochi un danno o una perdita per l'organizzazione. In ambito di sicurezza aziendale, questo concetto abbraccia molteplici domini (finanziario, operativo, reputazionale ecc.), ma oggi riveste particolare importanza il rischio informatico. Con la digitalizzazione dei processi aziendali, gran parte degli asset (dati, sistemi, reti) sono esposti costantemente a minacce informatiche. Il rischio informatico è comunemente definito come la combinazione della probabilità che una minaccia si manifesti e della gravità dell'impatto derivante da tale minaccia. La gestione efficace di questi rischi è cruciale per proteggere la continuità del business, la reputazione aziendale e la confidenzialità dei dati sensibili.

Nel contesto aziendale odierno, la sicurezza informatica è diventata un pilastro centrale nella gestione complessiva del rischio. Le minacce informatiche (malware, ransomware, phishing, attacchi hacker mirati, ecc.) possono causare danni significativi agli asset aziendali. Un incidente informatico può comportare perdite finanziarie dirette, sanzioni legali e danni di immagine potenzialmente irreparabili. L'obiettivo primario della sicurezza informatica aziendale è dunque quello di salvaguardare la riservatezza, l'integrità e la disponibilità dei dati e dei sistemi durante tutto il loro ciclo di vita.

Effettuare una valutazione strutturata del rischio informatico è un passo indispensabile per ogni azienda. Senza una risk assessment accurata, l'organizzazione rischia di investire in modo inefficace nella sicurezza, ignorando minacce critiche o sovrastimando pericoli minori. L'analisi dei rischi permette di identificare sistematicamente vulnerabilità e minacce potenziali, valutandone la probabilità e l'impatto reale, per poi predisporre misure di protezione proporzionali (ibm.com). In un'epoca in cui gli attacchi informatici sono sempre più frequenti e sofisticati, una valutazione proattiva del rischio consente di mitigare in anticipo le minacce più pericolose.

Da un punto di vista economico, l'analisi del rischio informatico è motivata anche dagli elevati costi potenziali derivanti da un incidente. Il costo medio globale di una violazione di dati nel 2024 ha raggiunto 4,88 milioni di dollari (ibm.com), una cifra considerevole che evidenzia chiaramente come una singola violazione possa avere gravi impatti finanziari, oltre a danni reputazionali significativi.

Un esempio concreto dell'importanza di anticipare i rischi informatici è rappresentato dal caso del ransomware che nel 2020 ha colpito il gruppo Campari: in assenza di controlli di sicurezza adeguati, un gruppo di hacker (Ragnar Locker) riuscì a violare le difese informatiche del noto marchio, rubando oltre 2 terabyte di dati riservati. L'azienda ricevette una richiesta di riscatto pari a 15 milioni di dollari e subì la diffusione pubblica di dati personali relativi a migliaia di dipendenti ed ex dipendenti (serinf.it). Prevenire scenari simili attraverso una corretta analisi del rischio permette di evitare perdite economiche ingenti e proteggere il patrimonio informativo prima che si verifichi un danno.

Normative di riferimento

Standard internazionali e normative come **ISO/IEC 27001**, **ISO 31000** e il regolamento europeo sulla protezione dei dati (**GDPR**) forniscono linee guida e requisiti fondamentali per gestire i rischi e proteggere l'azienda.

ISO/IEC 27001

ISO/IEC 27001 è lo standard internazionale di riferimento per stabilire, mantenere e migliorare un Information Security Management System (**ISMS**). L'obiettivo principale di questa normativa è proteggere la **riservatezza**, **integrità** e **disponibilità** delle informazioni aziendali attraverso un processo continuo di valutazione e trattamento dei rischi. Tra i requisiti chiave vi sono: definire il contesto e l'ambito del ISMS, ottenere l'impegno della direzione, stabilire una politica di sicurezza, attribuire ruoli e responsabilità, eseguire la valutazione del rischio, selezionare controlli di sicurezza adeguati e attuare un ciclo di miglioramento continuo.

ISO 27001 richiede di identificare i beni informativi ed i potenziali rischi (minacce e vulnerabilità), stimando per ciascuno la probabilità di accadimento e l'impatto. Questa fase è conosciuta come la **risk assessment**, in cui l'azienda ottiene un quadro dei rischi per la sicurezza delle informazioni ed individua quelli inaccettabili. A seguire si passa al **risk treatment**: per ogni rischio inaccettabile vanno individuate e attuate misure di sicurezza (controlli) adeguate ad evitarne o ridurne l'impatto. La normativa fornisce un elenco di controlli di buona pratica nell'**Annex A** (93 controlli nella versione 2022) da utilizzare come riferimento per mitigare i rischi identificati.

Importante è redigere e mantenere aggiornati documenti come il risk assessment report, il risk treatment plan ed il Statement of Applicability (**SoA**). In ambito di sicurezza sul lavoro e sicurezza aziendale, ISO 27001 copre la dimensione della sicurezza delle informazioni sul luogo di lavoro (es. controllo degli accessi ai sistemi), contribuendo in modo essenziale alla protezione del patrimonio informativo e della continuità operativa dell'azienda.

ISO 31000

ISO 31000 è lo standard internazionale che fornisce principi e linee guida generali per un efficace sistema di risk management. A differenza di ISO 27001 (specifico per la sicurezza delle informazioni), ISO 31000 è applicabile a qualsiasi tipo di rischio (strategico, finanziario, sicurezza informatica, ecc.) e a ogni tipo di organizzazione (techtarget.com). I **principi** di ISO 31000 enfatizzano che la gestione del rischio dovrebbe creare valore, essere parte integrante dei processi organizzativi e supportare il processo decisionale.

Dal punto di vista metodologico, ISO 31000 delinea un **processo di gestione del rischio ciclico** composta da diverse fasi principali:

- **Definizione del contesto**: si stabiliscono obiettivi, ambito, criteri di rischio e parametri di riferimento analizzando fattori esterni (es. scenario di mercato) e fattori interni (es. struttura) che influenzano il profilo di rischio dell'azienda. Vengono inoltre fissati i criteri per valutare la significatività dei rischi (es. scale di probabilità).

- **Identificazione dei rischi**: si individuano in modo sistematico le potenziali fonti di rischio, gli eventi che potrebbero avere un impatto sugli obiettivi e le relative cause e conseguenze (**riskonnect.com**). Ad esempio, in un'industria manifatturiera i rischi identificati possono includere guasti ai macchinari e attacchi informatici ai sistemi. Ogni rischio identificato viene descritto e classificato.

- **Analisi del rischio**: per ciascun rischio identificato, si analizzano le possibili **conseguenze** (gravità dell'impatto se l'evento si verifica) e la relativa **probabilità.** Inoltre, si valutano i **controlli esistenti** già in atto che potrebbero influenza quel rischio, stimandone l'efficacia attuale (**riskonnect.com**). Questa analisi può essere qualitativa (es. punteggi basso/medio/alto) sia quantitativa (es. stime economiche di perdite attese). Il risultato dell'analisi è una **stima del livello di rischio.**

- **Valutazione del rischio**: I livelli di rischio ottenuti vengono confrontati con i criteri di accettabilità definiti in precedenza, per decidere quali rischi richiedono trattamento. In pratica, si stabilisce una **priorità**: quali

rischi sono accettabili così come sono e quali invece devono essere ridotti o gestiti perché eccedono la soglia di tolleranza (**riskonnect.com**). Questo passaggio tiene conto anche di obblighi legali e normativi e delle preoccupazioni delle parti interessate.

- **Trattamento del rischio**: per i rischi inaccettabili, si scelgono e implementano opzioni di trattamento, ovvero azioni per **mitigare il rischio**. ISO 31000, in linea con le prassi generali, prevede tipicamente quattro strategie fondamentali: **evitare** il rischio (es. cessando l'attività che lo genera), **ridurre** il rischio implementando controlli che ne diminuiscano la probabilità di impatto (es. misure di sicurezza) (**advisera.com**), **condividere/trasferire** il rischio (es. stipulando assicurazioni senza eliminare però il rischio), **accettare** il rischio residuo.

- **Monitoraggio e riesame**: la gestione del rischio è un processo iterativo. ISO 31000 richiede di monitorare continuamente sia l'ambiente interno/esterno sia l'efficacia delle misure di trattamento adottate. Periodicamente, i rischi devono essere riesaminati, le valutazioni aggiornate e gli eventuali piani di azione adeguati di conseguenza.

GDPR: REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

Il **GDPR** (General Data Protection Regulation) è il regolamento UE n. 2016/679 che disciplina in maniera uniforme la protezione dei dati personali all'interno dell'Unione Europea. Entrato in vigore nel 2018, il GDPR è una **normativa cogente** e ha un impatto rilevante sulla gestione della sicurezza in azienda, in particolare per quanto riguarda la sicurezza dei dati personali di clienti, dipendenti e altri interessati. Sebbene il GDPR sia una norma legale e non uno standard tecnico, **impone requisiti specifici di sicurezza e gestione del rischio** relativi ai dati personali, avvicinandosi quindi ai temi di ISO 27001 (per la sicurezza delle informazioni) e integrandosi con un approccio di risk management (come quello di ISO 31000).

L'**art. 32 GDPR (Sicurezza del trattamento)** richiede a titolari e responsabili del trattamento di attuare misure tecniche e organizzative adeguate "tenendo conto dello stato dell'arte, dei costi di attuazione e finalità del trattamento, nonché del rischio avente probabilità e gravità diverse per i diritti e le libertà delle persone fisiche" (**gdpr-info.eu**). L'art. 32 elenca anche alcune misure esemplificative "appropriate al rischio", come la **pseudonimizzazione e cifratura** dei dati personali, la capacità di assicurare la continua **riservatezza, integrità e disponibilità** dei sistemi che trattano dati, la capacità di ripristino in caso di incidenti e procedure per testare regolarmente l'efficacia delle misure di sicurezza.

Uno degli strumenti cardine introdotti dal GDPR è la **DPIA** (**Data Protection Impact Assessment**). Si tratta di un processo strutturato per valutare i rischi specifici per i diritti e le libertà degli interessati derivanti da un certo trattamento di dati e individuare le misure per affrontare tali rischi. La DPIA è obbligatoria per i trattamenti che possono presentare un rischio elevato (es. uso di nuove tecnologie). Secondo l'art. 35, la valutazione d'impatto deve contenere: **una descrizione sistematica del trattamento e delle sue finalità, una valutazione delle necessità e proporzionalità** rispetto alle finalità, **una valutazione dei rischi per i diritti e le libertà degli interessati** e **le misure previste per mitigare tali rischi**, garantire la protezione de dati e la conformità al GDPR (**GDPR.eu**).

Un'esempio pratico: un'azienda vuole implementare un sistema di geolocalizzazione dei veicoli aziendali dei dipendenti. Tramite la DPIA valuterà i rischi per la privacy dei lavoratori, stimerà la probabilità e gravità di impatti negativi sui loro diritti e studierà misure come limitare la raccolta ai soli dati indispensabili. Se dalla DPIA risultasse che i rischi residui restano **altissimi** nonostante le mitigazioni, l'azienda dovrebbe consultare l'autorità Garante prima di procedere con il trattamento (obbligo di consultazione preventiva).

Oltre alla DPIA, il GDPR introduce altri requisiti di sicurezza: l'adozione di principi di **Privacy by Design e by Default** (art. 25), ossia considerare la protezione dei dati fin dalla progettazione di processi e sistemi e impostare configurazioni predefinite rispettose dalla privacy; la **formazione e sensibilizzazione** del personale che tratta dati personali; la **gestione dei data breach** (violazioni di sicurezza) con obbligo di notifica entro 72 ore all'autorità con comunicazione agli interessati (art. 33 e 34); la tenuta di un **registro dei trattamenti** (art. 30) che consenta di conoscere e tenere sotto controllo i flussi di dati; nonché la designazione di un **DPO (Data Protection Officer**) per sorvegliare la conformità privacy, nei casi previsti.

Metodologie e formule

Secondo gli standard internazionali, il rischio viene tipicamente espresso come **combinazione delle probabilità** che si verifichi un evento e **delle conseguenze/impatti** associati (sciencedirect.com). In generale, il **rischio** può essere quantificato come: **Rischio = Probabilità x Impatto**.

Le **normative di riferimento** danno grande enfasi a un approccio basato sul rischio. *ISO 31000* fornisce principi e linee guida generali per gestire qualunque tipo di rischio, delineando un processo iterativo di identificazione, analisi, valutazione e trattamento dei rischi. *ISO 27001* richiede alle organizzazioni di individuare i rischi per la sicurezza delle informazioni (minacce ai sistemi, ai dati e ai processi) e di determinarne **probabilità di occorrenza e impatto potenziale** (adivsera.com), per decidere come mitigare le minacce più gravi. Allo stesso modo il *GDPR* (Regolamento UE 2016/679) adotta un approccio proporzionato al rischio: impone valutazioni d'impatto sulla protezione dei dati (DPIA) quando un trattamento può presentare *rischi elevati per i diritti e le libertà delle persone*. Tali valutazioni devono considerare sia la **probabilità che si verifichi un impatto negativo, sia la gravità dell'impatto** stesso sugli individui (ico.org.uk).

Approccio qualitativo e quantitativo

Nel *risk management* esistono due approcci principali per valutare il rischio: **qualitativo** e **quantitativo**. Entrambi mirano a stimare la combinazione di probabilità e impatto di un evento rischioso, ma differiscono per metodo di calcolo, livello di dettaglio e ambito di utilizzo.

- **Analisi Qualitativa**: si basa su giudizi descrittivi e categorizzazione soggettiva dei rischi, piuttosto che su dati numerici precisi. Tipicamente, a probabilità e impatto vengono assegnati livelli qualitativi (es. basso, medio, alto, oppure punteggi su scala limitata come 1-5) invece di valori numerici assoluti. Questo metodo sfrutta l'esperienza e il giudizio degli esperti per classificare ogni rischio in termini comprensibili. Un esempio classico è l'uso di **etichette** o **codici colore** (verde, giallo, rosso) per indicare il livello di rischio. L'analisi qualitativa è *rapida* e *intuitiva;* di solito è l'approccio iniziale preferito per la sua **semplicità** e perché **richiede meno risorse** rispetto a quello quantitativo. Tuttavia, ha anche dei limiti: essendo basata su percezioni soggettive, può introdurre incongruenze di giudizio tra valutatore diversi. Produce inoltre risultati espressi in categorie che, pur utili per proritizzare, **non forniscono un valore numerico preciso** del rischio

- **Analisi Quantitativa**:mira ad assegnare ai componenti del rischio dei **valori numeri** misurabili, come probabilità percentuali e impatti monetari. In altre parole, si cerca di *quantificare* il rischio in termini di metriche oggettive (es. euro di perdita attesa all'anno, percentuale di frequenza annua di un evento, ecc.). Questo approccio richiede di disporre di **dati affidabili** sul passato o stime quantitative plausibili (frequenza di incidenti, costi dei danni, ecc), oltre a strumenti analitici e competenze statistiche. Il vantaggio è che il risultato è molto più **specifico** e **oggettivo**: si ottengono indicatori numerici con cui è possibile valutare con precisione l'esposizione al rischio e prendere decisioni più informate (**isaca.org**). Ad esempio, una valutazione quantitativa potrebbe stimare che un certo tipo di cyber-attacco ha una probabilità del 10% annuo e causerebbe 50.000 € di danno; da ciò si può inferire un costo annuo atteso di 5.000 €. Queste analisi permettono di condurre **analisi costi-benefici rigorose**, giustificando investimenti in sicurezza con dati. Di contro, la metodologia quantitativa può essere **onerosa e complessa** da applicare: spesso mancano dati statistici sufficienti per stimare accuratamente probabilità o impatti.

È prassi comune **combinare i due approcci**: iniziare con una valutazione qualitativa per screening generale e, successivamente, condurre analisi quantitative più approfondite sui rischi a più a alta priorità che richiedono dati oggettivi aggiuntivi.

Matrice di Rischio (qualitativa)

Uno degli strumenti più diffusi per condurre valutazioni qualitative è la **matrice di rischio**. Si tratta di una rappresentazione tabellare a doppia entrata che incrocia su un asse la **probabilità** di un evento e sull'altro asse la **gravità dell'impatto** qualora l'evento di verifichi (**vanta.com**). La matrice consente di collocare ciascun rischio i una cella a seconda dei valori attribuiti a queste due dimensioni, ottenendo un **punteggio di rischio** combinato. Generalmente, le celle della matrice sono colorate per indicare in modo visivo il livello di criticità: ad esempio **verde** per rischio basso, **giallo/arancione** per rischio medio, **rosso** per rischio elevato.

In una tipica matrice, la **scala dei valori** per probabilità e impatto può variare a seconda delle esigente. La matrice spesso utilizza la **moltiplicazione** di indici numeri associati a probabilità e impatto per calcolare un *punteggio di rischio* sottostante. Questi punteggi permettono di **ordinare** i **rischi** e di stabilire soglie di attenzione.

ALE, SLE, ARO (quantitativa)

Quando si adotta un approccio quantitativo, si introducono **metriche numeriche** per esprimere sia la probabilità sia l'impatto dei rischi. Nel campo della **sicurezza informatica** e della gestione del rischio aziendale, un insieme di parametri molto utilizzato per quantificare le perdite attese è dato dalle formule **SLE**, **ARO**, e **ALE**:

- **SLE (Single Loss Expectancy)** - *Perdita Singola Attesa*: rappresenta l'**impatto economico** (perdita) atteso **per un singolo evento** avverso. In pratica, è la stima del danno che un singolo episodio (es. un singolo incidente di sicurezza) causerebbe. La **formula** generalmente usata è: SLE = Asset Value (AV) x Exposure Factor (EF) (**infosecinstitute.com**). L'**Asset Value** è il valore dell'asset coinvolto, mentre l'**Exposure Factor** è la frazione (percentuale) di valore che verrebbe persa se quell'evento si verifica.

  Ad esempio, supponiamo di avere un asset informatico (come un insieme di dati o un sistema IT) dal valore di 100.000 €. Se stimiamo che un certo incidente (es. guasto non recuperabile al server) potrebbe distruggere circa il 30% di tale asset (perdita di dati parziale, costi di ripristino, ecc.), allora **EF= 30% = 0,3.** In tal caso la SLE sarebbe: SLE = 100.000 € x 0,3 = 30.000 €. Significa che ogni volta che si verifica quell'evento, ci aspettiamo una perdita di 30.000 €.

- **ARO (Annual Rate of Occurrence)** - *Tasso Annuale di Occorrenza*: è la stima della **frequenza** con cui un dato evento rischioso si verifica in un anno. Può essere espresso come un numero oppure come percentuale/probabilità annua. Nel nostro esempio, se valutiamo che il guasto grave al server potrebbe avvenire una volta ogni 2 anni, avremo ARO = 0,5 (ovvero 50% di probabilità annua di almeno un evento).

- **ALE (Annual Rate of Occurrence)** - *Perdita Annuale Attesa*: è il **valore di perdita attesa su base annua** legato a un determinato tipo di rischio. Si calcola combinando le due metriche precedenti: **ALE = SLE x ARO**. (**infosecinstitute.com**)

  Proseguendo l'esempio, con SLE = 30.000 € e ARO = 0,5, si ottiene ALE = 30.000 € x 0,5 = 15.000 €. Questo risultato indica che, **in media**, ci si può aspettare una perdita di 15.000 € all'anno a causa del rischio considerato. Naturalmente, nella realtà l'evento non accadrà ogni anno con regolarità matematica - alcuni anni potrebbe non succedere affatto, altri anni magari accade più di una volta - ma ALE fornisce una *media annualizzata* utile per fare pianificazione.

Vale la pena notare che le formule **ALE**, **ARO**, **SLE** sono ampiamente utilizzate nel campo della **cybersecurity** e della gestione del rischio IT.

Procedure operative e applicazioni

Identificazione degli asset aziendali

In un azienda informatica, il primo passo consiste nel **censire e classificare gli asset informatici**. Gli asset includono non solo hardware (server, PC, infrastrutture di rete) e software (applicazioni, sistemi operativi, cloud), ma anche i **dati** (basi di dati clienti, documenti riservati, proprietà intellettuale) e i **processi** critici di business supportati da tali risorse (itgovernance.co.uk). Ogni asset viene poi valutato in termini di **importanza, sensibilità e valore economico**: ad esempio, si attribuisce un livello di sensibilità ai dati contenuti (pubblici, interni, confidenziali, critici) e si stima l'impatto economico in caso di perdita o indisponibilità dell'asset. In ambito ISO 27001 (Annex A.8 Asset Management) ciò corrisponde alla classificazione delle informazioni n base ai requisiti di **confidenzialità, integrità e disponibilità (triade CIA)** (isaca.org).

Il **valore di un asset** può essere determinato valutando il contributo che fornisce all'azienda e le conseguenze di una sua compromissione sui requisiti di sicurezza: ad esempio, secondo un modello di valutazione, si può sommare un punteggio da 1 a 3 per ciascuna dimensione CIA (1= impatto basso, 3 = impatto alto) per ottenere un punteggio complessivo di criticità dell'asset.

Identificazione delle minacce e delle vulnerabilità

Una volta noti gli asset e la loro importanza, si procede a **identificare le minacce potenziali** e le **vulnerabilità** esistenti per ciascun asset. Le *minacce* sono eventi o agenti in grado di causare danni: esempi comuni includono attacchi informatici esterni (malware, phishing, attacchi DDoS), minacce interne (errore umano, ecc.), guasti tecnici o disastri fisici. Le *vulnerabilità* sono le debolezze o lacune di sicurezza che potrebbero essere sfruttate da una minaccia: ad esempio software non aggiornato, configurazioni errate, mancanza di controlli di accesso. Per rilevare minacce e vulnerabilità si usano varie tecniche e strumenti operativi.

Checklist e audit di sicurezza permettono di verificare la presenza dei controlli richiesti dalle norme e identificare gap (ad esempio l'assenza di politiche, mancata formazione). Strumenti automatizzati come i **vulnerability scanner** eseguono scansioni della rete e dei sistemi per individuare debolezze tecniche note (porte aperte non necessarie, patch mancanti, configurazioni deboli) (**halock.com**). I risultati di queste scansioni classificano le vulnerabilità per gravità, fornendo un elenco di problemi da valutare.

In aggiunta, si effettuano **penetration test** periodici, ossia simulazioni controllate di attacchi da parte di esperti, al fine di scoprire percorsi di exploit reali: il penetration testing consiste nel simulare un attacco informatico contro un sistema o applicazione aziendale per identificare quali vulnerabilità possono essere effettivamente sfruttate da un aggressore (**jit.io**). A differenza del semplice scan (che elenca possibili falle), il penetration test permette di capire fino a che punto un attacco potrebbe compromettere l'asset, fornendo contesto sul rischio reale di ogni vulnerabilità identificata. Ad esempio, per un server web (asset) si potrà annotare la minaccia "attacco SQL injection" con la vulnerabilità "input validation mancante sull'applicazione web", oppure per un database di clienti si consideri la minaccia "accesso non autorizzato" con vulnerabilità "password deboli" o "mancata crittografia dei dati a riposo".

Questa attività di identificazione corrisponde alla fase di **risk identification** prevista sia da ISO 27001 che dal framework ISO 31000, e produce un elenco strutturato *asset-minaccia*-vulnerabilità (**advisera.com**). Il risultato finale della base di identificazione è un registro dei rischi grezzi in cui per ciascun asset critico si hanno alcune possibili minacce, ciascuna con le vulnerabilità corrispondenti.

Applicazione operativa della valutazione qualitativa

La **valutazione qualitativa del rischio** mira a stimare in modo descrittivo o categorizzato la gravità di ciascun rischio identificato, al fine di poterli comparare e prioritizzare. Operativamente, lo strumento più diffuso per la valutazione qualitativa è la **matrice del rischio** (**auditboard.com**). Si costruisce definendo una scala qualitativa (tipicamente numerica) sia per la *probabilità* di occorrenza della minaccia, sia per l'*impatto* (o severità) sul business in caso di accadimento.

Ad esempio, la scala della **probabilità** può andare da 1 = raro a 5 = quasi certo. Analogamente, la scala dell'**impatto** può essere definita come: 1 = trascurabile, 5 = catastrofico. Tali definizioni dovrebbero essere adattate al contesto specifico dell'azienda e approvate dal management.

Nella valutazione qualitativa, per ciascun rischio si assegna un valore di probabilità **P** e un valore di impatto **I** secondo le scale definite. Si può quindi calcolare un **livello di rischio** come il prodotto **P x I** (**safetyculture.com**), ottenendo uno *score* numerico. L'importante è **definire soglie e criteri** coerenti con la propria *politica di gestione del rischio.* ISO 27001 richiede infatti che l'organizzazione stabilisce criteri specifici per valutare quando un rischio è accettabile e quando necessita trattamento (**itgovernance.co.uk**).

Una volta attribuiti punteggi di probabilità e impatto a tutti i rischi individuati, si popolano i valori nella matrice del rischio. Questo consente di **classificare i rischi** in ordine di gravità. Spesso i risultati vengono rappresentati con codici colore o mappe di calore: i rischi a punteggio più alto appariranno in area rossa (alto rischio), quelli intermedi in giallo, quelli bassi in verde (**safetyculture.com**). Queste classificazioni permettono al management di **visualizzare rapidamente la mappa dei rischi**; tipicamente, si concentra l'attenzione sui rischi in zona rossa (inaccettabili), da mitigare con priorità, e secondariamente su quelli gialli (da tenere sotto controllo).

La matrice del rischio qualitativa diventa così uno strumento decisionale: aiuta a **guidare le decisioni** sul trattamento, mostrando quali rischi minacciano maggiormente gli obiettivi aziendali (**auditboard.com**). Inoltre, è un mezzo di comunicazione efficace verso la direzione: anche senza approfondite conoscenze tecniche, i dirigenti possono comprendere dal grafico quali scenari rappresentano le maggiori minacce e richiedono investimenti o interventi urgenti.

Applicazione operativa della valutazione quantitativa

Accanto all'analisi qualitativa, un'azienda può voler approfondire alcuni scenari con una **valutazione quantitativa del rischio**, allo scopo di ottenere misure più oggettive in termini finanziari. La valutazione quantitativa comporta l'assegnazione di valori numerici (monetari o statistici) agli elementi del rischio, e fa uso di metriche come l'**Asset Value (AV)**, l'**Exposure Factor (EF)**, l'**Annualized Rate of Occurrence (ARO)** e il calcolo della **Annualized Loss Expectancy (ALE)** (**infosecinstitute.com**).

Per ogni rischio, si procede così:

- **Determinare l'Asset Value (AV):** il valore dell'asset impattato, espresso tipicamente in termini monetari. Può corrispondere al costo di sostituzione dell'asset o al danno economico potenziale massimo.

- **Stimare l'Exposure Factor (EF):** ossia la *percentuale di valore* che si perderebbe in un singolo incidente. Nel nostro esempio del database da 100k€, se un singolo data breach causasse una perdita stimata del 30% del valore (ad esempio per sanzioni o clienti persi), allora **SLE (Single Loss Expectancy)** = 100.000 € x 0,3 = **30.000 €** (**infosecinstitute.com**). La SLE rappresenta la perdita economica attesa per *un singolo incidente* di quel tipo.

- **Determinare l'Annualized Rate of Occurrence (ARO)**: è la frequenza attesa di occorrenza del sinistro, espressa in numero di volte per anno. Ad esempio, ARO = 0,5 significa che l'evento si stima avvenga una volta ogni due anni (50% di probabilità annua). ARO può essere stimato da dati storici (della propria azienda o del settore), da statistiche di industria o tramite il giudizio di esperti. È qui che la collaborazione tra team tecnici e management è importante: gli esperti di sicurezza possono stimare la probabilità di un certo attacco sulla base delle minacce attuali, mentre il business deve validare la sequenza in base all'esposizione e contesto aziendale.

- **Calcolare l'Annualized Loss Expectancy (ALE)**: è il valore atteso di perdita annuale per quel rischio, ottenuto moltiplicando SLE x ARO. Segundo l'esempio: SLE = 30.000 € e ARO = 0.5, quindi **ALE = 15.000 €.** Ciò significa che, in media, quel rischio comporta una perdita di 15 mila euro l'anno. Questo numero può essere interpretato come il "costo del rischio" e diventa molto utile in fase di pianificazione. Ad esempio, se si considera l'implementazione di un controllo di sicurezza per mitigare questo rischio, tale controllo **non dovrebbe costare più di 15.000 € all'anno**, altrimenti economicamente non sarebbe giustificato. Questo principio di *cost/benefit analysis* aiuta a decidere le contromisure: l'ALE fornisce un tetto massimo all'investimento ragionevole per mitigare quel rischio.

- **Esempio numerico integrativo**: supponiamo che una PMI valuti il rischio "perdita di dati per guardo ad un server non ridondato". Asset: file server con dati di progetto, AV = 50.000 € (stima del costo per ripristino e perdita produttività). Vulnerabilità: assenza di backup recenti, Threat: guasto hardware (es. rottura disco). EF stimato = 0,5 (perdita del 50% dei dati prima di riuscire a ripristinare da copie parziali) quindi SLE = 25.000 €. ARO: si valuta che il guasto grave possa avvenire una volta ogni 4 anni quindi ARO = 0,25.

  ALE = 25.000 x 0,25 = **6.250 €**/anno.

  Se per mitigare questo rischio si propone l'implementazione di un sistema di backup ridondante dal costo di 10.000 € annui, si può vedere che il costo del del controllo (10k) supera l'ALE (6,25k). Quindi non è economicamente conveniente - l'azienda potrebbe valutare di accettare il rischio residuo o cercare una soluzione più economica. Se invece la stima di ARO fosse maggiore (diciamo 0,5), ALE diventerebbe 12.500 € e un backup da 10k annui sarebbe giustificabile (*ridurre il rischio costa meno del rischio stesso*). Queste analisi quantitative supportano dunque le decisioni in modo oggettivo, traducendo il linguaggio tecnico in **impatto economico**.

Dal punto di vista operativo, l'**integrazione della valutazione quantitativa nella pianificazione** aziendale avviene collegando i risultati ALE con i budget e i piani di trattamento del rischio. ISO 27001 non impone di usare l'analisi quantitativa, ma la **ISO 31000** incoraggia l'uso di metodi appropriati di misura del rischio. In molti casi, la PMI userà l'analisi qualitativa per la maggior parte dei rischi (è più semplice e "veloce"), e riserverà la quantificazione dettagliata ai rischi più critici o a quelli per cui occorre giustificare spese ingenti.

In aggiunta, l'analisi quantitativa produce metriche che possono essere monitorate nel tempo: se l'ALE di un certo scenario aumenta anno su anno (magari perché cresce l'ARO a causa di nuoce minacce), ciò segnala al management un aggravarsi del profilo di rischio e la necessità di intervento. Va sottolineato che la quantificazione si basa comunque su stime e assunzioni: è importante documentare le ipotesi fatte (es. criteri per ARO, per EF) e aggiornare i valori quando is dispone di dati migliori.

Definizione di azioni di mitigazione (Risk Treatment Plan)

Dopo aver valutato i rischi, l'azienda deve decidere come **trattare ciascun rischio** identificato, formulando un **Piano di trattamento del rischio** (Risk Treatment Plan) concreto. Secondo ISO 27001 e ISO 31000, le possibili strategie di trattamento (risk treatment) rientrano in quattro categorie principali (**itgovernance.co.uk**):

- **Evitare il rischio (risk avoidance)**: eliminare completamente la situazione che genera il rischio, ad esempio cessando un'attività pericolosa

- **Mitigare o ridurre il rischio (risk reduction)**: implementare contromisure e controlli di sicurezza per abbassare la probabilità di accadimento e/o l'impatto. Questa è la strategia più comune in cybersecurity.

- **Condividere o trasferire il rischio (risk sharing/transfer)**: trasferire una parte del rischio a terzi, ad esempio stipulando un'assicurazione che copra le perdite in caso di incidente, oppure esternalizzando servizi a un fornitore contrattualmente responsabile di certi rischi. Va notato che il trasferimento *finanziario* del rischio non elimina il rischio di sicurezza in sé, ma ne sposta gli effetti economici.

- **Accettare il rischio (risk acceptance)**: decidere di non intervenire ulteriormente e tollerare il rischio residuo, tipicamente perché ritenuto basso o perché i costi di mitigazione superano i benefici. L'accettazione deve essere deliberata e documentata, e implica che il management ha consapevolezza del rischio e lo considera entro la propria **risk appetite**.

Nel definire le azioni di mitigazione, l'azienda deve partire dalla **gravità del rischio** (valutazione precedente) e dal confronto con i criteri di accettabilità stabili. Per ogni rischio intollerabile (oltre la soglia di rischio accettabile), si individua almeno un intervento di trattamento. Alcuni **esempi di contromisure** sono: *contromisure tecniche* (es. installazione o potenziamento di firewall, adorazione della multi-facto authentication per accessi critici, ecc.), *contromisure organizzative/procedurali* (es. controllo fisici, formazione per il personale, ecc.).

Durante questa fase, conviene aggiornare la **matrice del rischio** con una seconda valutazione detta *residuale*, stimando come i livelli di *probabilità P* e *impatto I* cambierebbero dopo l'implementazione dei controlli proposti.

Tutte le decisioni prese vanno consolidate in un **Risk Treatment Plan (RTP)**, documento (o tabella) che per **ogni rischio** riporti: le azioni di trattamento decise, i **controlli specifici** da implementare, la scelta tra le 4 strategie di cui sopra, la persona responsabile dell'implementazione e una **timeline** di attuazione (**hyqoo.com**). Il piano di trattamento è sostanzialmente un **piano operativo di sicurezza**: dovrebbe indicare anche le risorse stimate (budget, personale, strumenti) per ogni azione, in modo che la direzione possa approvarne l'esecuzione.

È fondamentale che il RTP abbia obiettivi **misurabili** e tempi definiti, in quanto sarà poi verificato nell'ambito sia di audit interni che durante i **riesami della direzione** (ISO 27001 richiede di verificare l'efficacia dei trattamenti intrapresi). Idealmente ogni azione di mitigazione dovrebbe ridurre il rischio a un livello target specificato (es. "portare rischio X da alto a basso entro 6 mesi"). Spesso, nell'ambito di ISO 27001, viene prodotto anche un **Statement of Applicability (SoA)** che elenca tutti i controlli applicabili e implementati, con giustificazione (**itgovernance.co.uk**).

Procedure operative di monitoraggio e aggiornamento

La gestione del rischio di cybersecurity non si esaurisce con l'implementazione delle contromisure: secondo il principio di **miglioramento continuo** di ISO 27001, l'azienda deve prevedere **procedure di monitoraggio, revisione e aggiornamento periodico** dei rischi e dei controlli.

Tramite il **monitoraggio continuo della sicurezza**, l'azienda dovrebbe sorvegliare costantemente lo stato di attuazione dei controlli e l'emergere di nuove minacce. Strumenti di **SIEM (Security Information and Event Management)** possono raccogliere e analizzare in tempo reale log e dati di sicurezza da varie fonti (firewall, sistemi, applicazioni) per individuare comportamenti anomali, tentativi di intrusione o indicatori di compromissione (**bitsight.com**). Un SIEM, integrato magari con soluzioni di monitoraggio di integrità (FIM) e di rilevamento endpoint (EDR), permette di avere un quadro aggiornato del livello di rischio effettivo, emettendo allarmi verso il team di sicurezza. Parallelamente, strumenti di **GRC (Governance, Risk & Compliance)** o piattaforme di gestione del rischio informatico possono aiutare a tracciare lo stato dei rischi nel tempo.

Per quanto riguarda le **revisioni periodiche del rischio**, è consigliabile condurre un **riesame del rischio a cadenza regolare**, tipicamente **annuale** (**community.advisera.com**). Durante queste revisioni periodiche si rivedono tutti i rischi nel registro: si verifica se le probabilità o gli impatti stimati sono cambiati (ad esempio per variazioni nel contesto aziendale, nuove vulnerabilità scoperte, variazione nel valore degli asset), si controlla lo stato delle azioni di trattamento previste e si aggiungono eventuali **nuovi rischi** emersi. ISO 27001 enfatizza la necessità di assicurare che i risultati delle valutazioni del rischio rimangano **validi e aggiornati nel tempo**.

Oltre alla frequenza periodica, il processo deve prevedere **revisioni straordinarie post-incidente o cambiamento**. In particolare, dopo un **incidente di sicurezza significativo**, è fondamentale svolgere un'analisi a posteriori per capire cosa è andato storto. Ad esempio, se l'azienda subisce un attacco pishing andato a buon fine, quel rischio (forse precedentemente sottovalutato) deve essere ricalibrato e trattato (es. intensificando la formazione o implementando filtri migliori). Allo stesso modo, **cambiamenti sostanziali** nell'infastruttura devono innescare un aggiornamento.

Ogni modifica apportata (nuovo rischio, modifica del livello, chiusura di un rischio perché eliminato l'asset) va **documentata** nel registro dei rischi, mantenendo traccia delle versioni (**community.advisera.com**). ISO 27001 non prescrive una modalità fissa, ma chiede evidenza che il processo sia controllato. Contestualmente al monitoraggio dei rischi, l'azienda deve monitorare se le contromisure implementate funzionano come previsto. Ciò include attività come test periodici di backup (per assicurarsi che i dati si recuperino davvero), scanni di vulnerabilità ricorrenti per vedere se le falle note sono state effettivamente risolte. Molte organizzazioni adottano **indicatori KPI/KRI** (Key Risk Indicators, Key Performance Indicators) per misurare aspetti del rischio e della sicurezza nel tempo - ad esempio numero di incidenti occorsi per tipo, tempo medio di risoluzione, ecc. - così da avere metriche oggettive per valutare l'andamento della postura di sicurezza.

Le attività di monitoraggio culminano nei **controlli periodici** (audit interno ISO 27001, audit di terza parte per la certificazione, verifiche GDPR) che valutano se il processo di risk management è efficace. La sicurezza informatica è un moving target: nuove minacce emergono costantemente, quindi il modello di rischio va *adattato dinamicamente*. I principi ISO 31000 enfatizzano proprio questo adattamento continuo: considerare feedback, contesto e apprendimento dagli incidenti per affinare criteri e trattamenti (**isms.online**).

Integrazione con il GDPR

Nell'ambito europeo, la **gestione del rischio cybersecurity** in un'azienda informatica deve necessariamente tenere conto anche del **rischio privacy** regolato dal Regolamento Generale sulla Protezione dei Dati (**GDPR**). Il GDPR infatti adotta un approccio basato sul rischio per la tutela dei dati personali, introducendo requisiti specifici come la **DPIA** (**Data Protection Impact Assessment**) e il principio di **Privacy by Design**. È importante integrare questi aspetti nel processo di risk management aziendale, per evitare duplicazioni e garantire conformità legale.

L'articolo 35 GDPR obbliga le organizzazioni a effettuare una DPIA ogni volta che un trattamento di dati personali "possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche". In termini operativi, una DPIA è una valutazione struttura del rischio mirata alla protezione dei dati personali e della privacy degli interessanti. Essa mira a identificare "quali impatti" (es. divulgazione non autorizzata di informazioni personali, discriminazione, danno economico, violazione di diritti) potrebbero subire gli individui a causa di determinati trattamenti di dati, e *quanto sono probabili* tali impatti. Di fatto, la DPIA è un sotto-processo di risk assessment focalizzato sul rischio per la privacy individuale (scytale.ai).

La DPIA segue step analoghi alla valutazione classica: descrizione del trattamento e dei suoi scopi, identificazione dei dati personali coinvolti e delle misure di sicurezza esistenti, valutazione di necessità e proporzionalità, individuazione dei rischi per i diritti degli interessanti, identificazione di misure per mitigare quei rischi. L'output è un documento che riporta i rischi privacy e le contromisure. È fondamentale che i **risultati della DPIA confluiscano nella matrice del rischio** generale: questo crea un collegamento tra *rischio tecnologico e rischio regolamentare*. In altre parole, un rischio elevato in DPIA implica che l'azienda non può avviare quel trattamento finché non lo riduce a un livello accettabile.

Nel valutare impatto e probabilità, la prospettiva GDPR introduce elementi aggiuntivi. L'**impatto** di un incidente di sicurezza non va visto solo come danno per l'azienda, ma anche come **danno per gli individui** coinvolti (gli *interessati*). Spesso, in sede di DPIA, l'impatto è valutato proprio in termini di **gravità per l'interessato** (nessun impatto, limitato, significativo, massimo). Un altro concetto chiave del GDPR è il **rischio residuale per gli interessati**: se dopo le contromisure rimane *ancora* alto, va consultata l'autorità Garante. Quindi il Risk Treatment Plan deve esplicitare se una misura di sicurezza abbassa sufficientemente anche il rischio privacy.

Il GDPR all'Art.25 introduce i principi di **Privacy by Design e by Default**, che impongono di incorporare fin dall'inizio appropriate misure di tutela dei dati personali nei sistemi e nei processi. In termini operativi di risk management, *privacy by design* significa che **nella fase di definizione dei requisiti e progettazione di un nuovo sistema/prodotto, si effettua subito un'analisi del rischio privacy e si scelgono controlli adeguati** (**isms.online**). L'implementazione di privacy by design dovrebbe essere verificata come parte del processo di gestione rischi: ad esempio, nel **risk assessment di progetto** si aggiunge un checkpoint per la privacy. In sede di monitoraggio, oltre agli indicatori di sicurezza, si tengono d'occhio KPI di compliance privacy (es. numero di richieste diritti esercitati, incidenti privacy, ecc.). Un altro aspetto critico è la **gestione dei data breach**: l'Art. 33 GDPR obbliga a notificare le violazioni di sicurezza sui dati personali all'autorità entro 72 ore dall'accertamento, e l'Art. 34 a comunicare agli interessati se c'è alto rischio per i loro diritti.

Pertanto, le procedure di incident response dell'azienda (che rientrano nel risk treatment plan per mitigare l'impatto) devono includere **step specifici per il GDPR**: identificazione immediata se l'incidente riguarda dati personali, coinvolgimento del DPO (Data Protection Officer) o legale, valutazione rapida del livello di rischio per gli interessati (che è proprio un micro-processo di risk assessment durante l'incidente), decisione sulla notifica al Garante e agli utenti. Questo significa che il piano di risposta agli incidenti (che è un controllo di mitigazione di impatto) sia strettamente collegato con la valutazione del rischio privacy: prima dell'incidente, in fase di analisi del rischio, l'azienda dovrebbe già aver stabilito criteri su quali tipi di incidenti costituirebbero data breach da notificare.

Linee Guida Operative

Sulla base delle analisi svolte, si possono individuare alcune **best practice** fondamentali per una gestione efficace del rischio informatico in ambito aziendale. Queste line guida, riprendono i concetti chiave trattati (valutazione qualitativa/quantitativa del rischio, standard ISO 27001/ISO 31000, GDPR, ciclo di vita del rischio) e integrano raccomandazioni sia tecnico-operative sia organizzative e culturali. I principali pilastri da adottare includono:

1. **Adozione di framework riconosciuti e conformità normativa:** Implementare un solido framework di **risk management** (ad es. ISO 31000 e ISO 27001) per assicurare un processo strutturato e allineato alle linee guida internazionali (cybersecurity360.it). Tali standard forniscono principi, requisiti e persino raccolte di **best practices** per proteggere le risorse informative (docenti.unimc.it), promuovendo un approccio sistematico e ciclico alla gestione del rischio. Contestualmente, è essenziale garantire la **conformità alle normative** di settore (come il GDPR), in particolare abbracciando il principio di *accountability* che impone di valutare e mitigare produttivamente i rischi per i dati personali, documentando razionalmente le misure tecnico-organizzative adottate.

2. **Valutazione regolare e completa del rischio (qualitativa e quantitativa)**: Condurre periodicamente una **analisi dei rischi** approfondita, combinando metodi qualitativi e quantitativi, in modo da identificare le minacce e valutarne sia la probabilità sia il potenziale impatto in termini oggettivi. È importante stimare i rischi *quantitativamente* e *qualitativamente* per poi capire come introdurre azioni mirate a mitigarne gli impatti e le conseguenze. L'utilizzo congiunto di valutazioni **qualitative** (es. matrici di rischio, categorie basso/medio/alto) e **quantitative** (es. calcolo di metriche come *Single Loss Expectancy* e *Annualized Loss Expectancy*) permette infatti di misurare con maggiore precisione la frequenza e la gravità degli eventi, fornendo basi solide per prioritizzare i rischi e allocare le risorse di conseguenza.

3. **Processo continuo di gestione del rischio (monitoraggio e revisione costante)**: Trattare la gestione del rischio come un **ciclo di miglioramento continuo** anziché un esercizio occasionale. Il processo deve essere **circolare e proattivo**: dopo l'identificazione e valutazione iniziale, occorre pianificare e implementare le opportune **azioni di trattamento** del rischio, per poi **monitorarne** l'efficacia nel tempo e **rivedere** periodicamente strategia e controlli. Questo approccio dinamico consente di adattare la postura di sicurezza all'evoluzione delle minacce, dei requisiti di business e delle normative. La ciclicità delle fasi (identificazione, trattamento, monitoraggio, revisione) assicura inoltre il **miglioramento continuo** del sistema di risk management. Ciò si traduce nell'aggiornamento regolare del registro dei rischi, in audit e test periodici (es. simulazioni di attacco, revisioni di compliance) e nel perfezionamento costante delle misure adottate sulla base di lezioni apprese e cambiamenti del contesto.

4. **Implementazione di controlli di sicurezza adeguati e aggiornati**: La riduzione del rischio passa attraverso l'adozione di robuste **misure tecnico-operative** proporzionate alle minacce individuate. È fondamentale mantenere sistemi e software costantemente **aggiornati** (efficace *patch management*), dal momento che l'applicazione tempestiva delle patch può prevenire fino all'85% degli attacchi informatici noti (**metacompliance.com**). In parallelo, occorre gestire attivamente le **vulnerabilità** (identificazione e valutazione) e predisporre efficaci misure di **monitoraggio**: ad esempio, l'implementazione di sistemi SIEM (*Security Information and Event Management*) e di strumenti di rilevamento intrusioni permette un controllo in tempo reale dell'ambiente IT, condizione necessaria per individuare tempestivamente incidenti e anomalie. Un ulteriore pilastro tecnico-operativo è rappresentato da un solido piano di **backup e disaster ricovery:** eseguire backup regolari (idealmente anche **offline**) garantisce la resilienza dei dati e la continuità operativa in caso di guasti o attacchi gravi come i ransomware (**artser.it**).

5. **Coinvolgimento del top management e governance del rischio:** Un'efficace gestione del rischio informatico richiede un forte **committente della direzione aziendale**. La cybersecuriy deve partire dall'alto: il top management dovrebbe promuovere attivamente una cultura orientata alla sicurezza come parte integrante della governance organizzativa. Ciò significa che i vertici aziendali devono sostenere e indirizzare le iniziative di risk management, assicurando che vi siano risorse adeguate, obiettivi chiari e una sponsorship visibile. Dunque, il consiglio di amministrazione e i dirigenti dovrebbero definire la **strategia di rischio** (inclusa la determinazione della *risk appetite* più idonea e delle tolleranze al rischio accettabili) e supervisionare l'implementazione delle politiche e controlli di sicurezza. Il coinvolgimento della leadership, enfatizzato anche dagli standard internazionali, garantisce inoltre che la gestione del rischio rimanga allineata agli obiettivi di business e che la cultura del rischio permei efficacemente tutti i

livelli organizzativi.

6. **Formazione, consapevolezza e responsabilizzazione diffusa:** Investire sul **fattore umano** è una best practice imprescindibile, poiché anche le migliori politiche e tecnologie possono fallire senza personale adeguatamente formato. Studi evidenziano che fino al *90% degli attacchi informatici riusciti* dipendono in qualche misura da un errore umano o dalla mancanza di consapevolezza dei dipendenti (**metacompliance.com**). È dunque essenziale attirare programmi di **formazione continua** e aggiornamento in materia di sicurezza informatica per tutti i livelli aziendali, dal top management ai nuovi assunti, con particolare attenzione a chi gestisce informazioni critiche. Attraverso campagne di sensibilizzazione periodiche, simulazioni (es. pishing test) e corsi mirati, i dipendenti apprendono a riconoscere le minacce e ad adottare le **buone pratiche** di sicurezza nel lavoro quotidiano. Parallelamente, va promossa una chiara **accountablity** individuale: ogni membro dell'organizzazione deve comprendere le proprie responsabilità nella protezione delle informazioni e aderire alle policy di sicurezza, Una cultura aziendale fortemente consapevole dei rischi, in cui la sicurezza sia valorizzata e condivisa come obiettivo comune, costituisce uno dei deterrenti più efficaci contro gli incidenti e favorisce il successo di tutte le altre iniziative di risk management.