UNIVERSITÀ TELEMATICA PEGASO

PROJECT WORK

Corso di Laurea Triennale in Informatica (L-31)

Elaborato

Calcolo del fattore di rischio in ambito aziendale e informatico

Studente: Mario Buongiorno

Matricola: 0312301752

Anno Accademico 2024/2025

Indice dei contenuti

1. Introduzione

Nella gestione aziendale moderna, la sicurezza riveste un ruolo sempre più importante e strategico. Non si tratta solo di tutelare l'integrità fisica e la salute dei lavoratori, ma anche di preservare la continuità operativa e garantire la conformità alle normative di settore.

Un elemento fondamentale in questa prospettiva è rappresentato dalla **valutazione dei rischi**, ovvero quell'insieme di attività che consente di individuare, analizzare e gestire i potenziali pericoli all'interno dell'organizzazione.

All'interno di tale processo, il **calcolo del fattore di rischio** svolge una funzione chiave: consente di quantificare il livello di rischio combinando la probabilità che un evento si verifichi con la gravità delle sue conseguenze. Nonostante l'apparente semplicità, questo tipo di valutazione può risultare complesso, soprattutto se non supportato da strumenti adeguati e da una conoscenza strutturata delle normative e delle buone pratiche operative.

Con l'evoluzione digitale, la sicurezza aziendale ha esteso il proprio raggio d'azione: **la protezione delle infrastrutture informatiche, la prevenzione degli attacchi informatici, la gestione delle vulnerabilità tecniche e la difesa dei dati sensibili** sono diventati elementi imprescindibili. La sicurezza, dunque, non può più essere intesa esclusivamente in termini fisici o ambientali, ma deve comprendere in modo integrato anche l'ambito informatico/cyber.

Il presente documento intende offrire una guida approfondita e strutturata al calcolo del fattore di rischio, con l'obiettivo di fornire un riferimento pratico e teorico per comprendere i principi, le formule e le metodologie più efficaci nella valutazione del rischio, con **focus specifico sulla sicurezza informatica aziendale**.

1bis. Glossario e definizioni tecniche

Nel presente glossario sono raccolti i principali termini, acronimi e concetti tecnici utilizzati all'interno del documento, con lo scopo di favorire una comprensione uniforme e precisa del contenuto, sia da parte di figure specialistiche che da lettori non esperti. Ogni voce è corredata da una definizione sintetica e, ove opportuno, da un esempio pratico.

A

Accesso non autorizzato
L'accesso a dati, sistemi o informazioni da parte di un soggetto non abilitato. È una delle minacce più comuni in ambito informatico.

Asset
Qualsiasi elemento di valore per un'organizzazione, tangibile (hardware, documenti) o intangibile (software, dati, reputazione).

Autenticazione a più fattori (MFA)
Metodo di verifica dell'identità che richiede due o più elementi di autenticazione: qualcosa che l'utente conosce (password), possiede (token) o è (impronta digitale).

B

Backup
Copia di riserva dei dati, utile per ripristinarli in caso di perdita o danneggiamento.

Brute force attack
Tecnica di attacco informatico basata sul tentativo sistematico di tutte le combinazioni possibili di password o credenziali.

C

CVE (Common Vulnerabilities and Exposures)
Database pubblico che elenca le vulnerabilità note nei software, assegnando loro un codice identificativo univoco.

Criticità
Livello di gravità associato a una vulnerabilità o a un rischio, spesso indicato su scala numerica o cromatica.

Cybersecurity
Insieme di pratiche, tecnologie e processi finalizzati a proteggere sistemi, reti e dati da attacchi informatici o accessi non autorizzati.

Cultura della sicurezza
Approccio organizzativo che promuove la consapevolezza e l'adozione di comportamenti sicuri a tutti i livelli aziendali.

D

Danno/Gravità
Effetto negativo che può derivare dal verificarsi di un evento rischioso. Nella formula R = P × G rappresenta l'impatto.

DVR (Documento di Valutazione dei Rischi)
Documento obbligatorio previsto dalla normativa italiana che raccoglie l'analisi dei rischi presenti in azienda e le misure preventive adottate.

DPIA (Data Protection Impact Assessment)
Valutazione di impatto sulla protezione dei dati, prevista dal GDPR, utile a identificare i rischi per i diritti e le libertà delle persone fisiche.

E

Esposizione (E)
Livello con cui un sistema, un'attività o un asset è soggetto a potenziali minacce. In alcune formule, funge da moltiplicatore del rischio.

Eventi di sicurezza
Ogni manifestazione anomala rilevata su un sistema informatico, che può indicare una minaccia o un attacco in corso.

F

Fattore di rischio
Condizione, comportamento o tecnologia che incrementa la probabilità o l'impatto di un evento dannoso.

Firewall
Dispositivo hardware o software che filtra il traffico di rete in ingresso e uscita, secondo regole definite, al fine di proteggere i sistemi.

Framework (di sicurezza)
Insieme strutturato di linee guida, policy e procedure che guidano la gestione del rischio e della sicurezza (es. NIST, ISO/IEC 27005).

G

Gravità/Danno
Effetto negativo che può derivare dal verificarsi di un evento rischioso. Nella formula R = P × G rappresenta l'impatto.

I

IAM (Identity and Access Management)
Sistema centralizzato per la gestione delle identità digitali e dei diritti di accesso degli utenti ai sistemi aziendali.

Impatto
Conseguenza di un evento rischioso. Sinonimo di danno, ma in alcuni modelli è considerato come grandezza separata.

Incident response
Processo strutturato per gestire e contenere gli incidenti di sicurezza informatica, con l'obiettivo di limitarne l'impatto.

Intelligenza Artificiale (AI)
Tecnologia in grado di simulare processi cognitivi umani per analizzare dati, riconoscere pattern, prendere decisioni e prevedere eventi futuri.

M

Matrice del rischio
Strumento visivo che consente di incrociare probabilità e gravità per classificare i rischi in categorie (basso, medio, alto, critico).

Mitigazione (M)
Misura o insieme di misure atte a ridurre l'impatto o la probabilità di un rischio. Spesso rappresenta una variabile sottrattiva nel calcolo del rischio residuo.

Modello predittivo
Algoritmo che stima la probabilità futura di un evento basandosi su dati storici e parametri comportamentali.

P

Pericolo

Fonte potenziale di danno. È l'origine del rischio, che diventa tale solo se può concretizzarsi in un evento dannoso.

Phishing
Tecnica fraudolenta per carpire dati sensibili, solitamente attraverso email ingannevoli.

Probabilità (P)
Valutazione della possibilità che un evento dannoso si verifichi. Può essere stimata su scala numerica (es. da 1 a 4).

R

Resilienza operativa
Capacità dell'organizzazione di adattarsi a perturbazioni (attacchi, guasti, errori) e di ripristinare rapidamente la piena operatività.

Rischio (R)
Risultato della combinazione tra probabilità di accadimento e la gravità attesa. Espressione più comune: $R = P \times G$.

Rischio residuo
Rischio rimanente dopo l'applicazione delle misure di mitigazione.

Rischio predittivo
Modello di rischio che utilizza strumenti analitici o AI per prevedere la probabilità di eventi futuri sulla base di pattern osservati.

S

SIEM (Security Information and Event Management)
Sistema centralizzato per la raccolta, correlazione e analisi in tempo reale dei dati relativi alla sicurezza informatica.

Social engineering (ingegneria sociale)
Manipolazione psicologica che induce una persona a compiere azioni o rivelare informazioni riservate.

Sicurezza by design
Principio secondo cui la sicurezza deve essere incorporata già nella fase di progettazione di un sistema, software o processo.

V

Valutazione qualitativa
Metodo descrittivo di analisi del rischio basato su categorie verbali ("basso", "medio", "alto").

Valutazione semi-quantitativa
Metodo misto che utilizza scale numeriche standard per stimare rischio in base a probabilità e gravità.

Valutazione quantitativa
Metodo rigoroso basato su dati oggettivi, simulazioni e modelli statistici.

Vulnerabilità
Debolezza intrinseca di un sistema, che può essere sfruttata da una minaccia per

causare danni.

Note: Tutti i termini indicati vengono utilizzati nel prosieguo del documento in modo coerente con le definizioni sopra riportate. La loro conoscenza è propedeutica a una piena comprensione delle metodologie di calcolo e degli scenari analizzati.

2. Obiettivi del documento

Il presente documento propone di offrire una guida completa, strutturata e multidisciplinare sul calcolo del fattore di rischio in ambito aziendale. L'impostazione è volutamente tecnica e approfondita, ma con un linguaggio accessibile e semplice anche a figure non specialistiche, affinché possa rappresentare uno strumento di riferimento concreto e funzionale, sia per la fase di analisi che per eventuali implementazioni operative e digitali.

La trattazione abbraccia la dimensione normativa, teorica, metodologica e applicativa del rischio, con dettagli al contesto della **sicurezza informatica**, oggi elemento imprescindibile nella protezione dei dati, delle infrastrutture e della continuità operativa aziendale.

Obiettivi specifici

- **Inquadrare il contesto normativo** di riferimento, analizzando in modo dettagliato sia la normativa italiana (D.Lgs. 81/2008) che le principali linee guida internazionali (ISO 45001, ISO/IEC 27005, Direttiva NIS2), al fine di fornire un quadro regolatorio aggiornato, allineato alla gestione integrata dei rischi aziendali.
- **Fornire definizioni operative e coerenti** dei concetti chiave – pericolo, rischio, fattore di rischio – chiarendone differenze e interdipendenze. Questo consente una lettura univoca dei termini tecnici utilizzati e favorisce la costruzione di modelli valutativi affidabili.
- **Illustrare le metodologie di valutazione** maggiormente diffuse, distinguendo tra approcci qualitativi, semi-quantitativi e quantitativi, e presentandone vantaggi, limiti e ambiti applicativi. Viene dato risalto alla semplicità del modello P × G e alle sue estensioni con esposizione e mitigazione.
- **Dimostrare con esempi realistici** come applicare i modelli di calcolo in situazioni operative, attraverso scenari di rischio informatico ricorrenti (es. server esposto, credenziali deboli), con calcoli dettagliati e suggerimenti pratici per la mitigazione.
- **Costruire una base concettuale e tecnica** utile allo sviluppo di strumenti informatici per la valutazione automatica del rischio, con focus su funzionalità logiche, input guidati, classificazioni automatiche e generazione di output documentale conforme.
- **Integrare aspetti organizzativi**, analizzando i ruoli coinvolti nella gestione del rischio (direzione, RSPP, CISO, DPO, HSE, IT Manager), in un'ottica collaborativa e interfunzionale, che valorizzi la cultura della prevenzione come fattore strategico.
- **Offrire una visione evolutiva e predittiva**, proponendo riflessioni sull'utilizzo

dell'intelligenza artificiale per la gestione proattiva del rischio, l'analisi predittiva degli eventi e l'automazione delle decisioni di sicurezza.

Norme internazionali

A livello internazionale, uno dei riferimenti più consolidati è la **norma ISO 45001:2018**, che definisce i requisiti per un sistema di gestione della salute e sicurezza sul lavoro **(SGSSL)**. Essa si basa su un approccio proattivo e sistemico, centrato sul miglioramento continuo, sulla prevenzione dei rischi e sul coinvolgimento dei lavoratori in tutte le fasi del processo.

Un altro punto di riferimento storico è la **Direttiva 89/391/CEE** del consiglio europeo, che ha introdotto il concetto di tutela globale dei lavoratori attraverso una gestione strutturata della prevenzione.

Questa direttiva ha fornito un modello armonizzato recepito dagli Stati membri dell'UE, costituendo il fondamento della normativa nazionale italiana.

Negli ultimi anni, il panorama normativo si è arricchito con strumenti più specifici legati alla sicurezza informatica e alla gestione del rischio digitale. Tra questi, si segnalano:

- **ISO/IEC 27005:2018** – Standard internazionale che fornisce una metodologia dettagliata per la gestione del rischio in ambito sicurezza delle informazioni. Questo documento integra e approfondisce i principi generali della famiglia ISO/IEC 27000, con riferimento all'identificazione, analisi e trattamento dei rischi legati agli asset informativi.
- **Direttiva NIS2 (EU 2022/2555)** – Evoluzione della precedente direttiva NIS, rappresenta un passo avanti nella strategia europea per la sicurezza delle reti e dei sistemi informativi. La NIS2 amplia il campo di applicazione, introducendo obblighi più stringenti per le imprese operanti in settori critici, tra cui energia, trasporti, finanza, sanità e infrastrutture digitali. La direttiva sottolinea l'importanza della valutazione del rischio come strumento di prevenzione e governance e introduce misure sanzionatorie in caso di mancata conformità.
- **Regolamento eIDAS** (Reg. UE 910/2014) – Anche se principalmente dedicato all'identificazione elettronica e ai servizi fiduciari, il regolamento ha ricadute indirette sulla gestione del rischio legata all'autenticazione e alla firma digitale, aspetti rilevanti nella protezione dei processi documentali in ambito aziendale.

I riferimenti normativi citati, pur distinti per ambito applicativo, convergono verso un principio comune: **la gestione del rischio non è più confinata alla sicurezza fisica o operativa**, ma deve includere anche la dimensione **digitale**, in una logica di protezione integrata e multilivello.

Applicabilità informatica

Dal punto di vista informatico, queste normative rappresentano un modello concettuale perfettamente traducibile in logica software. Ogni elemento normativo — come le categorie di pericolo, le scale di probabilità e gravità, le soglie di rischio e le misure correttive — può essere formalizzato in strutture dati, algoritmi e interfacce utente.

Questa trasformazione è alla base della progettazione di strumenti digitali per la valutazione del rischio, in grado di:

- Guidare l’utente nella compilazione dei dati
- Calcolare automaticamente i livelli di rischio in base alle variabili scelte
- Generare report conformi ai requisiti di legge

In questo modo, il software non si limita a semplificare un’attività complessa, ma diventa **strumento di compliance**, supporto decisionale e garanzia di tracciabilità documentale.

4. Definizione di rischio e fattore di rischio

Nella sicurezza aziendale è fondamentale distinguere con chiarezza i concetti di **pericolo**, **rischio** e **fattore di rischio**.
Questi termini, pur essendo spesso utilizzati in modo intercambiabile nella comunicazione quotidiana, hanno **valenze tecniche distinte** e rivestono ruoli specifici all’interno del processo di valutazione della sicurezza.
La corretta comprensione e applicazione di tali concetti è un prerequisito essenziale per ogni sistema di gestione del rischio che voglia essere solido, replicabile e conforme alle normative vigenti.

Pericolo

Il **pericolo** (*hazard*, secondo la terminologia internazionale) rappresenta una **caratteristica intrinseca** di un agente, un’attività o una condizione che ha il **potenziale di causare un danno**.
Si tratta di un concetto oggettivo, indipendente dal contesto o dalle circostanze specifiche. Un pericolo esiste a prescindere dalla probabilità che si manifesti: ciò che cambia è il rischio, non la presenza del pericolo.

Esempi classici:

- Una macchina in movimento all’interno di un capannone industriale
- Una sostanza chimica tossica mal gestita
- Un pavimento bagnato o con scarsa segnaletica
- Un cavo scoperto in un ambiente di lavoro

In ambito informatico:

- Un'applicazione con codice vulnerabile è **un pericolo**, anche se non ancora attaccata
- Un file eseguibile scaricato da fonte non attendibile
- Un'interfaccia aperta su Internet priva di autenticazione

Nota: Il pericolo è quindi una **condizione latente**. Il rischio ne misura l’attualizzazione possibile.

Rischio

Il **rischio** è la **combinazione della probabilità di accadimento di un evento dannoso e delle sue conseguenze**.
Nella maggior parte dei contesti normativi (inclusi ISO 31000 e D.Lgs. 81/08), è definito come l’effetto dell’incertezza su obiettivi specifici, dove l’incertezza riguarda sia **la**

probabilità che **la gravità del danno**.

Formula più diffusa:

$$R = P \times G$$

Dove:

- **P** = Probabilità (scala 1–4)
- **G** = Gravità del danno (scala 1–4)

Esempi:

- Un rischio con P = 1 e G = 4 può sembrare meno urgente di P = 3 e G = 2, ma dipende dalla soglia di rischio aziendale.
- Il rischio **non è statico**: varia nel tempo in base all'esposizione, all'ambiente, all'aggiornamento delle contromisure.

Concetti correlati:

- **Rischio accettabile**: soglia sotto la quale il rischio può essere tollerato.
- **Rischio trascurabile**: valore talmente basso da non richiedere interventi.
- **Rischio residuo**: ciò che resta dopo l'applicazione delle misure di mitigazione.
- **Rischio sistemico**: rischio che, se si verifica, ha effetti su più componenti aziendali.

In ambito informatico:

- Il rischio legato a un ransomware è alto se la probabilità (alta esposizione) e il danno (perdita dati) sono entrambi significativi.
- L'accesso a sistemi critici senza autenticazione MFA moltiplica il rischio anche in presenza di utenti interni.

Fattore di rischio

Il **fattore di rischio** rappresenta ogni **componente, condizione o variabile che agisce come amplificatore del rischio**, aumentando la probabilità o la severità di un danno. Diversamente dal pericolo (che è intrinseco) e dal rischio (che è calcolato), il fattore di rischio è **relazionale**: modifica lo scenario e può essere **gestito attivamente** attraverso misure di controllo.

Classificazione ampliata:

- **Fattori ambientali** → polveri, scarsa ventilazione, illuminazione insufficiente
- **Fattori organizzativi** → carichi di lavoro eccessivi, mancanza di formazione continua, ambiguità nei ruoli
- **Fattori comportamentali** → negligenza, mancato rispetto delle procedure, resistenza al cambiamento
- **Fattori tecnologici** → dispositivi non aggiornati, assenza di ridondanza, mancanza di audit trail

Esempi in contesto aziendale:

- La **mancanza di cultura della sicurezza** è un fattore di rischio trasversale

- L’**obsolescenza dei sistemi ERP** può aumentare l’impatto potenziale di un attacco informatico

Estensione al contesto informatico

Nel ICT, i fattori di rischio si moltiplicano e assumono caratteristiche specifiche. Le tecnologie digitali introducono **nuove superfici d’attacco**, **minacce dinamiche** e un **alto grado di interconnessione**, che amplificano l’effetto di ogni vulnerabilità.

Esempi aggiornati di fattori di rischio informatici:

- Utilizzo di sistemi operativi non supportati
- Applicazione di patch critiche in ritardo o in modo parziale
- Gestione manuale e non tracciata delle credenziali
- Assenza di network segmentation in ambienti cloud-ibridi
- Mancanza di sistemi di log, auditing e alerting in tempo reale

Esempio pratico (cybersecurity)

Una rete aziendale esposta direttamente a Internet e priva di un firewall aggiornato costituisce un fattore di rischio elevato.
Se un attacco ransomware ha una probabilità stimata di 3 su 4 e può causare un danno classificabile come 4 su 4, il rischio risultante sarà:

$$R = P \times G = 3 \times 4 = 12$$

Secondo le scale di classificazione standard, un valore di 12 rappresenta un **livello di rischio alto**, che richiede interventi urgenti di mitigazione, come l’implementazione di un firewall, l’attivazione di sistemi di backup e il rafforzamento delle credenziali di accesso.

5. Metodologie di valutazione

La valutazione del rischio è un processo sistematico volto a identificare i pericoli, stimare le potenziali conseguenze e definire misure preventive e protettive appropriate. A seconda del grado di approfondimento e della natura dei dati impiegati, le metodologie possono essere classificate in **qualitative**, **semi-quantitative** o **quantitative**.

Valutazione qualitativa

Questo approccio si basa su criteri descrittivi e giudizi soggettivi. È comunemente adottato quando mancano dati storici affidabili o nei casi in cui si richieda una prima valutazione generale dei rischi.

- Il rischio viene descritto mediante **categorie verbali** come “basso”, “moderato”, “alto”.
- È una metodologia **rapida e intuitiva**, ma meno accurata.
- La sua efficacia dipende in larga misura **dall’esperienza e dalla percezione** del valutatore.

Valutazione semi-quantitativa

È il metodo più diffuso in ambito aziendale. Combina la semplicità della classificazione qualitativa con l'impiego di **valori numerici standardizzati**, attribuiti a:

- **Probabilità di accadimento** (es. scala da 1 a 4)
- **Gravità del danno** (es. scala da 1 a 4)

Il rischio viene quindi calcolato come **prodotto tra questi due valori** (la formula verrà presentata nella sezione successiva).

Questo approccio è particolarmente adatto all'**implementazione software**, poiché consente di trasformare le valutazioni soggettive in dati numerici gestibili da algoritmi.

Inoltre, può essere integrato facilmente in interfacce utente con input guidati e report automatizzati.

Valutazione quantitativa

Si tratta della metodologia più complessa e precisa. Fa uso di dati oggettivi come **statistiche storiche**, **analisi probabilistiche**, **simulazioni numeriche** e **modelli predittivi**.

- È spesso utilizzata in contesti ad elevato rischio o criticità (es. sanità, trasporto aereo, industria nucleare).
- Richiede competenze avanzate e strumenti di calcolo specifici.
- Fornisce un'**analisi altamente accurata**, ma può risultare onerosa in termini di tempo e risorse.

Tecniche di supporto comuni

Per facilitare il processo valutativo, esistono strumenti e rappresentazioni standardizzate:

- **Matrice del rischio**
  Rappresentazione grafica che incrocia le dimensioni di probabilità e gravità, consentendo di visualizzare rapidamente il livello di rischio associato a ciascun pericolo.
- **Checklist operative**
  Liste di controllo precompilate che guidano l'utente nella valutazione sistematica di tutti i possibili fattori di rischio (es. modelli INAIL, OT23).
- **Tool informatici dedicati**
  Applicazioni che implementano le metodologie sopra descritte e consentono la **valutazione digitale del rischio**, integrando calcolo, archiviazione e generazione automatica della documentazione.

Integrazione informatica

Queste metodologie costituiscono la base logica per la progettazione di **strumenti software di supporto decisionale**, in grado di trasformare le valutazioni soggettive in **output numerici, visivi e standardizzati**, rendendo il processo di gestione del rischio più oggettivo, tracciabile e ripetibile.

Criteri di scelta della metodologia

La selezione della metodologia più idonea per la valutazione del rischio non è un

processo neutro, ma deve tener conto di numerosi fattori contestuali. Tra i principali:

- **Qualità e quantità dei dati disponibili**: in assenza di storicità affidabile, si tende a privilegiare approcci qualitativi o semi-quantitativi;
- **Criticità del processo da analizzare**: più è elevato il potenziale impatto di un evento, maggiore sarà la necessità di adottare metodi quantitativi e modelli predittivi;
- **Maturità organizzativa**: realtà aziendali con sistemi gestionali strutturati (es. certificazioni ISO) tendono a integrare valutazioni quantitative in un'ottica di miglioramento continuo;
- **Risorse disponibili**: strumenti, competenze e tempi condizionano la scelta tra modelli semplici e approcci analitici più avanzati.

Nella pratica, molti gruppi adottano approcci **ibridi**, che bilanciano efficacia, semplicità operativa e precisione del risultato.

Limiti e affidabilità dei modelli

Sebbene ciascun approccio presenti vantaggi specifici, è importante considerarne anche le **debolezze strutturali**:

- Le **valutazioni qualitative** risultano fortemente influenzate dalla percezione individuale, con possibili variazioni tra diversi analisti.
- I modelli **semi-quantitativi**, se non supportati da scale ben definite, possono indurre in errore simulando una precisione non reale.
- Le analisi **quantitative**, pur più robuste, sono spesso limitate dalla **reperibilità e qualità dei dati**, oltre che dalla loro complessità implementativa.

Per questo motivo, è raccomandabile affiancare alle metodologie **meccanismi di validazione e revisione periodica**, in modo da garantire l'aderenza delle valutazioni al contesto reale in continua evoluzione.

La valutazione del rischio come processo dinamico

Infine, è fondamentale ricordare che la valutazione del rischio **non è un'attività statica**, ma un processo **continuo e adattivo**. Ogni cambiamento organizzativo, tecnologico o normativo può influire sul profilo di rischio e richiedere un aggiornamento della valutazione iniziale.

Per questo, le best practices suggeriscono di pianificare **revisioni periodiche** o **riesami straordinari** nei seguenti casi:

- introduzione di nuove tecnologie o procedure operative
- riorganizzazioni aziendali
- rilevamento di incidenti o near miss significativi,
- aggiornamenti normativi impattanti

Questa visione dinamica consente di mantenere l'efficacia delle misure di controllo, migliorare la reattività organizzativa e sviluppare una **cultura della sicurezza** fondata sulla consapevolezza e sulla responsabilità diffusa.

6. Formula del calcolo del rischio

Il calcolo del rischio avviene tramite una formula semplice ma estremamente efficace, che combina due variabili fondamentali: la **probabilità di accadimento** di un evento e la **gravità del danno** che potrebbe derivarne.

$$R=P\times G$$

Dove:

- **R** = Rischio complessivo
- **P** = Probabilità che l'evento si verifichi
- **G** = Gravità potenziale conseguente all'evento

Questa espressione, pur nella sua semplicità, è largamente utilizzata in diversi settori — dall'industria alla sanità, fino alla **sicurezza informatica** — per la sua **efficacia pratica** e la facilità con cui può essere integrata all'interno di strumenti digitali.

Scale di riferimento (valori tipici)

Probabilità (P)

Valore	Significato
1	Evento improbabile
2	Possibile
3	Probabile
4	Molto probabile

Gravità del danno (G)

Valore	Significato
1	Danno lieve
2	Danno moderato
3	Danno grave
4	Danno gravissimo / catastrofico

Classificazione dei livelli di rischio

R (P × D)	Livello di rischio	Azione suggerita
1 – 4	Basso	Monitoraggio, misure minime
5 – 8	Medio	Interventi pianificati, mitigazione
9 – 12	Alto	Azioni correttive urgenti
13 – 16	Critico	Intervento immediato, possibile stop attività

Questa classificazione, basata su soglie numeriche predefinite, è **perfettamente automatizzabile**.

Un software può associare automaticamente il livello di rischio a ciascuna combinazione di valori, fornendo all'utente **output immediati e facilmente interpretabili**.

Applicazione pratica nel software

All'interno del progetto, l'utente avrà la possibilità di:

- **Selezionare il tipo di rischio o scenario** da valutare (es. "software non aggiornato", "accesso remoto non protetto");
- **Attribuire i valori di probabilità e gravità**;
- **Ottenere in tempo reale il valore del rischio** calcolato;
- Visualizzare **il livello di rischio corrispondente** e ricevere **indicazioni operative** per la mitigazione.

Formula del calcolo del rischio (estesa)

Oltre alla formula classica, esistono varianti più sofisticate pensate per contesti più complessi — come la **cybersecurity** — dove entrano in gioco ulteriori fattori.

Formula con esposizione (R = P × D × E)

$$R=P\times D\times E$$

Dove **E** rappresenta il livello di **esposizione** o vulnerabilità del sistema:

Esempio: un server accessibile da Internet, privo di aggiornamenti e con credenziali deboli, ha un'esposizione **E = 3** su una scala da 1 a 3.

Formula con mitigazione (R = (P × I) – M)

$$R=(P\times I)-M$$

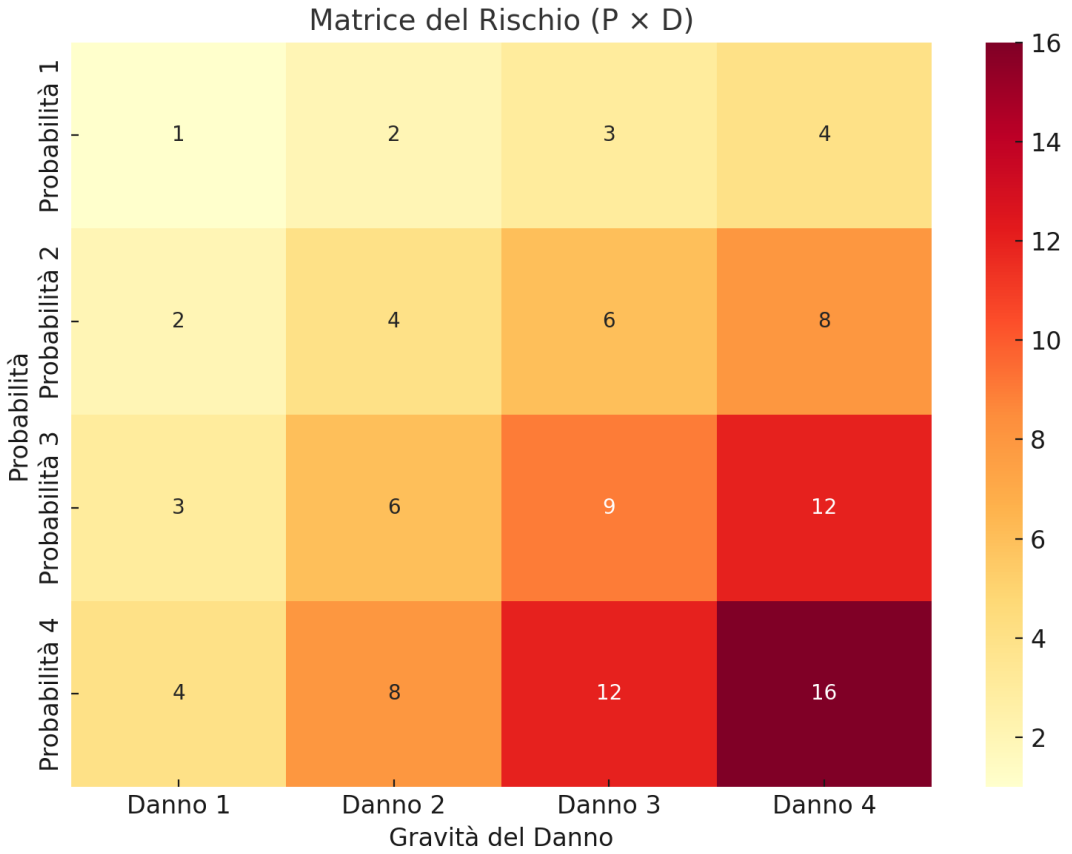
I = Impatto complessivo (dimensione della gravità attesa)

M = Mitigazioni già in atto (es. firewall, backup, antivirus)

Questo modello consente di calcolare il **rischio residuo**, ovvero il rischio effettivamente presente anche dopo aver applicato misure di sicurezza.

Visualizzazione: Matrice del rischio

Per facilitare l'interpretazione, i valori possono essere rappresentati in una **matrice bidimensionale**, dove righe e colonne corrispondono rispettivamente a **probabilità** e **gravità**.
Ogni cella della matrice restituisce un valore di rischio, visibile anche **tramite codifica cromatica**.



Nota: Questo tipo di rappresentazione è utile per evidenziare visivamente le aree più critiche e per supportare le decisioni a livello gestionale.

Approfondimento sulle variabili del modello

Le formule di calcolo del rischio si basano su variabili che, pur apparentemente semplici, richiedono un'attenta definizione e calibrazione per essere significative dal punto di vista operativo.

- **Probabilità (P)**: può essere stimata tramite dati storici, analisi esperta, modelli di previsione o osservazioni qualitative. In contesti ad alto dinamismo tecnologico, è preferibile affiancare valutazioni soggettive a indicatori quantitativi aggiornati in tempo reale (es. tassi di vulnerabilità, log di attacco).
- **Gravità (G)**: dipende dal tipo di asset coinvolto e dalle conseguenze potenziali (economiche, legali, reputazionali). In ambito ICT, la gravità del danno può includere perdita di dati, interruzione dei servizi, sanzioni normative o compromissione della reputazione aziendale.
- **Esposizione (E)**: misura quanto un asset è accessibile o vulnerabile a minacce. Può essere valutata in base a fattori come la presenza di controlli attivi, la segmentazione di rete, la superficie d'attacco.
- **Impatto (I)**: spesso usato in alternativa o complemento al "danno", può rappresentare una grandezza aggregata che considera anche l'effetto sistemico o la criticità del processo colpito.
- **Mitigazione (M)**: rappresenta l'efficacia delle misure tecniche e organizzative già attuate. Una sovrastima del valore di mitigazione può portare a una sottovalutazione pericolosa del rischio residuo.

Nota: Le scale numeriche (1–4, 1–5 o 1–10) devono essere definite in modo coerente e condiviso all'interno dell'organizzazione, per evitare discrepanze e garantire l'affidabilità delle valutazioni.

Rischi interpretativi e limiti applicativi

Nonostante la loro semplicità, le formule standard di calcolo del rischio presentano **alcuni limiti intrinseci**, soprattutto in contesti digitali complessi:

- **Falsa precisione**: l'attribuzione numerica a variabili soggettive può generare un'illusione di oggettività, se non accompagnata da una riflessione critica.
- **Eccessiva semplificazione**: scenari articolati possono essere mal rappresentati da un singolo valore numerico, che non tiene conto di fattori contestuali o interdipendenze tra asset.
- **Valori estremi**: nei modelli estesi, il prodotto tra P, G ed E può generare valori elevatissimi e poco gestibili, mentre una M sovrastimata può azzerare artificialmente il rischio residuo.

Per questo motivo, è raccomandabile accompagnare ogni valutazione numerica con **una descrizione qualitativa**, utile per contestualizzare il rischio e supportare le decisioni manageriali.

Verso una valutazione dinamica con AI e logica adattiva

Le moderne soluzioni software di **risk assesment** stanno evolvendo verso modelli **adattivi e intelligenti**, in cui i parametri di calcolo vengono aggiornati dinamicamente sulla base di:

- Log di sistema e attività degli utenti
- Eventi di sicurezza rilevati da SIEM e sistemi IDS/IPS
- Indicatori di rischio aggregati (es. threat intelligence, CVSS score, audit interni)

In questi contesti, le variabili P, G, E e M non sono più fissate a priori, ma **calcolate automaticamente da algoritmi di machine learning** che apprendono dall'ambiente operativo e dalle condizioni reali.

L'introduzione dell'**intelligenza artificiale nella valutazione del rischio** consente quindi una gestione predittiva e proattiva, capace di reagire in tempo reale a variazioni del contesto o a nuove minacce emergenti.

7. Esempi pratici

Per comprendere in modo concreto l'applicazione delle metodologie e formule illustrate nelle sezioni precedenti, vengono di seguito presentati due **scenari realistici** in ambito **cybersecurity aziendale**, ciascuno analizzato attraverso i modelli di calcolo del rischio.
Gli esempi sono progettati per essere **direttamente implementabili in ambiente software**, rendendo possibile l'automazione del processo valutativo.

Scenario 1: Server aziendale esposto

Contesto

Il server web aziendale è accessibile dall'esterno tramite rete pubblica. Non è presente un sistema di autenticazione forte (MFA) e il software installato non risulta aggiornato.

Minaccia
Sfruttamento di vulnerabilità note (es. CVE pubbliche) o attacchi di tipo brute force.

Conseguenza
Accesso non autorizzato al database clienti, possibile furto di dati sensibili, danni reputazionali e impatto legale.

Parametri di input

Parametro	Valore	Descrizione
P (Probabilità)	4	Evento altamente probabile
G (Gravità)	4	Impatto elevato (dati sensibili)
E (Esposizione)	3	Infrastruttura altamente vulnerabile
M (Mitigazione)	0	Nessuna misura di protezione attiva

Calcolo

- **Rischio base**: *4×4=16*
- **Rischio esteso**: *4×4×3=48*
- **Rischio residuo**: *48−0=48* → **Critico**

Azioni raccomandate

- Abilitazione dell'autenticazione a più fattori (MFA)
- Aggiornamento tempestivo del sistema operativo e del software
- Limitazione degli accessi tramite regole firewall e IP autorizzati

Scenario 2: Password debole su account utente

Contesto
Un dipendente accede a una piattaforma interna utilizzando una password debole. Il sistema in uso è non critico, ma collegato alla rete aziendale.

Minaccia
Accesso non autorizzato tramite tentativi automatici (password guessing).

Conseguenza
Possibile consultazione non autorizzata di contenuti, con impatto minimo sull'infrastruttura complessiva.

Parametri di input

Parametro	Valore	Descrizione
P (Probabilità)	2	Evento possibile

G (Gravità)	2	Gravità limitata
E (Esposizione)	2	Rischio moderato (accesso interno)
M (Mitigazione)	10	Policy attive e monitoraggio

Calcolo

- **Rischio base**: *2×2=4*
- **Rischio esteso**: *2×2×2=8*
- **Rischio residuo**: *8−10*=0 → **Trascurabile**

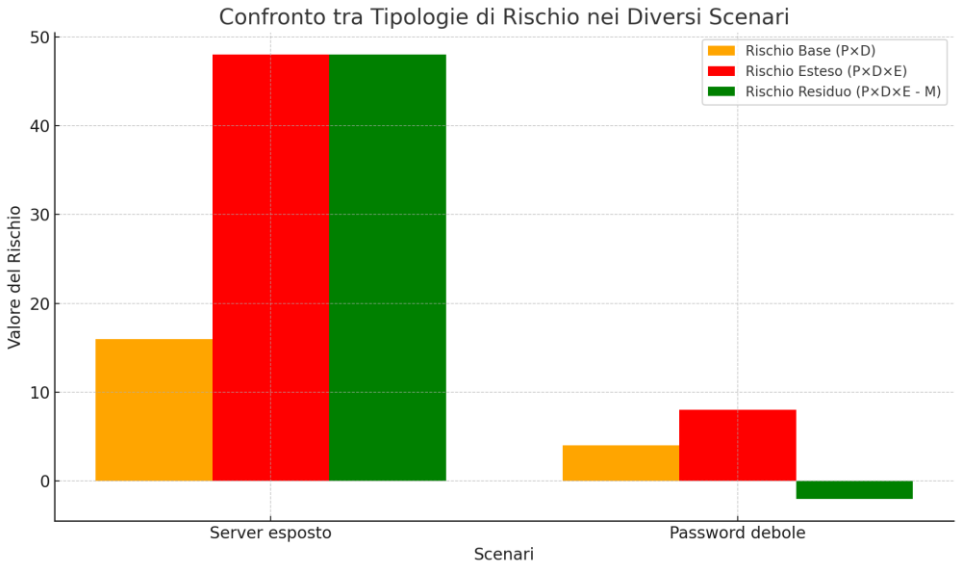
Azioni raccomandate

- Proseguire con la formazione degli utenti su pratiche di sicurezza
- Mantenere attive le policy esistenti (blocco account, avvisi, logging)
- Eventuale integrazione con autenticazione a due fattori

Confronto visivo tra scenari

Il confronto tra i due casi evidenzia chiaramente come:

- Lo **stesso evento** (accesso non autorizzato) possa avere impatti radicalmente diversi in base al contesto;
- Le **misure di mitigazione** attuate (M) possono ridurre drasticamente il rischio residuo;
- La rappresentazione numerica del rischio consente una **valutazione oggettiva e comparabile**, ideale per essere elaborata e visualizzata all'interno di un software.



(Il grafico incluso in questa sezione mostra le differenze di rischio base, esteso e residuo.)

Integrazione nel software

Ciascuno di questi scenari può essere rappresentato e calcolato in modo automatico attraverso il software previsto dal project work.
Il sistema potrà includere:

- **Maschere di inserimento** per P, G, E e M
- **Calcolo dinamico** dei tre livelli di rischio (base, esteso, residuo)
- **Visualizzazione automatica del risultato** con etichettatura del livello di criticità

8. Come le aziende informatiche gestiscono oggi il rischio

Le aziende, oggi, operanti nel settore informatico si trovano a fronteggiare un numero crescente di minacce digitali, vulnerabilità tecniche e rischi legati alla protezione dei dati, dei sistemi e delle infrastrutture. Per far fronte a tali sfide, adottano **approcci strutturati**, basati su framework riconosciuti, tecnologie avanzate e politiche di sicurezza proattive, finalizzate a contenere e mitigare il rischio informatico.

Approcci e strumenti adottati

Tra le strategie maggiormente diffuse, si evidenziano:

- **Framework internazionali**, come il **NIST Cybersecurity Framework** e la **norma ISO/IEC 27005**, che forniscono linee guida per l'identificazione, analisi, trattamento e monitoraggio del rischio cyber.
- **Strumenti di vulnerability assessment**, come **Nessus**, **Qualys** e **OpenVAS**, impiegati per l'analisi automatizzata delle vulnerabilità presenti su reti, sistemi e applicazioni.
- **Sistemi SIEM (Security Information and Event Management)**, come **Splunk**, **Elastic Security** o **IBM QRadar**, che consentono di centralizzare la raccolta e l'analisi degli eventi di sicurezza in tempo reale.
- **Soluzioni di IT Risk Management (ITRM)**, che assegnano punteggi di rischio agli asset aziendali, basandosi su metriche come esposizione, criticità e impatto potenziale.
- **DevSecOps**, ovvero l'integrazione della sicurezza nel ciclo di vita dello sviluppo software, mediante test automatizzati, scansioni del codice e strumenti di sicurezza continua.
- **Sistema di scoring delle vulnerabilità**, come il **CVSS (Common Vulnerability Scoring System)**, utilizzato per classificare e prioritizzare le criticità rilevate nei sistemi informatici.

Gestione delle credenziali e degli accessi

Uno degli aspetti più delicati nella riduzione del rischio è il controllo sugli accessi ai sistemi. Le aziende informatiche applicano policy avanzate di **Identity & Access Management (IAM)**, che includono:

- **Rotazione periodica delle credenziali**, con scadenze imposte (es. ogni 90 o 180 giorni) per ridurre il rischio legato a credenziali compromesse.
- **Requisiti di complessità delle password**, che prevedono lunghezza minima,

caratteri speciali, maiuscole/minuscole e numeri.
- **Blocco automatico dell'account** dopo tentativi consecutivi falliti, come protezione contro attacchi brute force.
- **Autenticazione a più fattori (2FA)**, implementata tramite app mobili (Microsoft Authenticator, Google Authenticator) o dispositivi fisici (token hardware).
- **Soluzioni IAM** per la gestione centralizzata di ruoli, permessi e cicli di vita degli utenti (creazione, modifica, revoca).

Queste pratiche consentono di **limitare drasticamente la superficie di attacco**, migliorando la resilienza del sistema informativo.

Cultura della prevenzione e monitoraggio continuo

Oltre agli strumenti tecnologici, le aziende pongono attenzione anche alla dimensione **organizzativa e culturale** della sicurezza:

- **Formazione continua del personale**, per aumentare la consapevolezza sui rischi informatici (phishing, ingegneria sociale, frodi digitali).
- **Attività di red teaming e penetration testing**, per simulare attacchi reali e individuare debolezze nella difesa.
- **Piani di backup e disaster recovery** automatizzati, per garantire la continuità operativa in caso di incidenti o perdita di dati.

L'approccio più moderno prevede un passaggio da una gestione **reattiva** del rischio a una **predittiva e adattiva**, in cui la valutazione è continua, contestuale e supportata da dati aggiornati.

Ruoli organizzativi nella gestione del rischio

La gestione efficace del rischio richiede non solo l'adozione di metodologie e strumenti adeguati, ma anche il coinvolgimento attivo di più ***figure professionali*** all'interno dell'organizzazione.

Ogni funzione aziendale, a vario titolo, partecipa al processo di identificazione, valutazione, mitigazione e monitoraggio dei rischi, contribuendo in modo sinergico alla protezione degli asset materiali e immateriali dell'impresa.

Di seguito individueremo i principali attori coinvolti e delinearne i rispettivi ruoli e responsabilità operative.

Datore di lavoro / Direzione generale

Ha la **responsabilità primaria e non delegabile** della valutazione dei rischi, come previsto dalla normativa italiana (D.Lgs. 81/08, art. 17).
A livello pratico, deve:

- definire le **strategie di prevenzione e protezione**;
- garantire risorse adeguate (tecnologiche, umane e finanziarie);
- approvare il **Documento di Valutazione dei Rischi (DVR)** e gli aggiornamenti periodici.

Nel contesto digitale, è chiamato a promuovere un approccio integrato alla sicurezza, in cui la componente informatica sia trattata al pari di quella fisica e organizzativa.

RSPP – Responsabile del servizio di prevenzione e protezione

Figura tecnica incaricata di:

- individuare i fattori di rischio presenti nei luoghi di lavoro;
- proporre misure tecniche e organizzative per ridurre l'esposizione al rischio;
- collaborare alla redazione del DVR.

Anche se storicamente focalizzato sugli ambienti fisici e operativi, il RSPP deve oggi interfacciarsi con i responsabili ICT per comprendere e valutare i rischi digitali, contribuendo a una visione unitaria del rischio aziendale.

Dipartimento HSE – Health, Safety & Environment

Il Dipartimento HSE (o Salute, Sicurezza e Ambiente) svolge un ruolo centrale nella valutazione e nella gestione dei rischi, con una visione trasversale che abbraccia sia gli **aspetti normativi sia quelli operativi.**

Le principali responsabilità includono:

- monitoraggio dei rischi legati alla salute dei lavoratori e alla sicurezza ambientale;
- supervisione delle misure di prevenzione e protezione collettiva e individuale;
- gestione degli adempimenti normativi e delle relazioni con enti ispettivi;
- partecipazione alla stesura e aggiornamento del DVR in collaborazione con RSPP e direzione aziendale.

Nei contesti aziendali in cui la sicurezza informatica si interseca con i processi produttivi (es. fabbriche automatizzate, logistica integrata, sistemi IoT), il dipartimento HSE collabora attivamente con **l'IT** e la **funzione security** per valutare rischi ibridi, che coinvolgono contemporaneamente **persone, impianti e tecnologie**.

CISO – Chief Information Security Officer

È il responsabile della **sicurezza informatica aziendale**. In particolare:

- coordina le attività di **identificazione delle minacce IT**;
- gestisce i processi di **analisi del rischio cyber**;
- definisce le politiche di accesso, monitoraggio, cifratura e risposta agli incidenti.

Nel processo di valutazione del fattore di rischio, il CISO fornisce i dati tecnici relativi a vulnerabilità, probabilità di attacco e impatti potenziali.

DPO – Data Protection Officer

Figura prevista dal Regolamento UE 2016/679 (GDPR), è incaricata della **tutela dei dati personali**. In ambito rischio, il DPO:

- valuta i rischi legati al trattamento dei dati;
- partecipa alle **DPIA** (valutazioni di impatto sulla protezione dei dati);
- suggerisce misure organizzative e tecniche per la riduzione del rischio privacy.

Collabora strettamente con il CISO e con il RSPP per armonizzare le strategie di protezione tra sicurezza informatica e protezione dati.

IT Manager / Responsabile sistemi informativi

Gestisce l'infrastruttura tecnologica aziendale e garantisce il funzionamento sicuro dei sistemi. Contribuisce alla gestione del rischio informatico attraverso:

- il monitoraggio delle vulnerabilità software e hardware;
- la supervisione degli aggiornamenti di sicurezza;
- l'applicazione delle policy aziendali relative a backup, accessi, log e firewall.

Fornisce al CISO e al team di valutazione del rischio tutte le informazioni utili sui sistemi in uso e sui livelli di esposizione tecnica.

Altri attori coinvolti

In base alla dimensione e alla struttura dell'azienda, possono essere coinvolte anche altre figure chiave:

- **HR Manager** – per la gestione dei rischi legati al comportamento degli utenti e alla formazione del personale;
- **Compliance Officer** – per l'allineamento tra processi aziendali e normative di settore;
- **Auditor interni** – per la verifica periodica dell'efficacia delle misure di mitigazione adottate.

Modello collaborativo e responsabilità condivisa

La gestione del rischio aziendale non può essere confinata a un singolo dipartimento. L'approccio più efficace è quello **multidisciplinare**, dove ogni funzione mette a disposizione le proprie competenze per raggiungere un obiettivo comune: *la protezione integrata dell'organizzazione*.

Questo modello prevede:

- **comunicazione costante** tra ruoli tecnici, manageriali e operativi;
- **condivisione dei dati di rischio** su piattaforme centralizzate;
- **riunioni periodiche interfunzionali** per aggiornare le valutazioni;
- **formazione trasversale** per diffondere la cultura della prevenzione.

9. Bibliografia e riferimenti

Normative e standard

- **D.Lgs. 9 aprile 2008, n. 81** – Testo Unico sulla Salute e Sicurezza sul Lavoro https://www.normattiva.it
- **ISO 45001:2018** – Sistemi di gestione per la salute e sicurezza sul lavoro https://www.iso.org/standard/63787.html
- **Direttiva 89/391/CEE** – Direttiva quadro europea sulla sicurezza e salute dei lavoratori https://eur-lex.europa.eu
- **ISO/IEC 27005:2018** – Gestione del rischio per la sicurezza delle informazioni https://www.iso.org/standard/75281.html
- **Direttiva (UE) 2022/2555 – NIS2** – Misure per un elevato livello comune di cybersicurezza nell'Unione

https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32022L2555

- **Regolamento eIDAS (UE) 910/2014** – Identificazione elettronica e servizi fiduciari per le transazioni elettroniche
  https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32014R0910

Enti istituzionali e risorse tecniche

- **INAIL** – Istituto Nazionale per l'Assicurazione contro gli Infortuni sul Lavoro
  https://www.inail.it
  → Sezioni consigliate: *Prevenzione*, *Valutazione dei rischi*, *Modelli OT23*
- **Ministero del Lavoro e delle Politiche Sociali**
  https://www.lavoro.gov.it
- **UNI – Ente Italiano di Normazione**
  https://www.uni.com
- **PuntoSicuro.it** – Quotidiano digitale sulla sicurezza sul lavoro
  https://www.puntosicuro.it

Sicurezza informatica

- **ENISA** – Agenzia dell'Unione Europea per la cybersicurezza
  https://www.enisa.europa.eu
- **OWASP** – Open Web Application Security Project
  https://owasp.org
  → Raccolta aggiornata di best practice per la sicurezza applicativa (es. *OWASP Top 10*)
- **NIST – National Institute of Standards and Technology**
  https://www.nist.gov
  → *NIST Cybersecurity Framework*, *SP 800-30*, *SP 800-53*
- **MITRE ATT&CK Framework** – Knowledge base di tecniche e tattiche di attacco
  https://attack.mitre.org

Conclusioni e plus finali

La gestione del rischio costituisce una leva fondamentale per la tutela e lo sviluppo sostenibile delle organizzazioni moderne.

Rappresenta un approccio sistemico volto a garantire la continuità operativa, la protezione degli asset aziendali e la conformità alle normative di riferimento.

Nel corso del presente documento è stata delineata una **panoramica completa e operativa sul calcolo del fattore di rischio**, partendo dall'inquadramento normativo, passando per la definizione concettuale di pericolo, rischio e fattore di rischio, fino ad arrivare alle metodologie di valutazione e ai modelli matematici applicabili in ambito aziendale, con particolare focus sulla sicurezza informatica.

L'intero contenuto è stato concepito con l'obiettivo di fornire una guida accessibile ma rigorosa, utile sia in fase di analisi che di implementazione di strumenti software di supporto.

L'analisi condotta ha messo in luce come l'adozione di un approccio strutturato alla

valutazione del rischio, supportato da formule standardizzate, scale di classificazione e rappresentazioni visive come la matrice del rischio, consenta una gestione più oggettiva, tracciabile e replicabile del rischio stesso. Le variabili aggiuntive, come esposizione e mitigazione, permettono inoltre di affinare il modello e ottenere valutazioni sempre più vicine alla realtà operativa.

In un momento storico in cui le minacce informatiche evolvono rapidamente e assumono forme sempre più sofisticate, la capacità di **prevedere e contenere** eventi dannosi diventa un fattore competitivo determinante. Non si tratta più soltanto di prevenire gli incidenti, ma di sviluppare una resilienza dinamica e adattiva.

Focus AI e gestione del rischio: nuove prospettive operative

Un elemento sempre più centrale in questo scenario è rappresentato dall'**intelligenza artificiale**, la quale sta trasformando il modo in cui le aziende valutano, interpretano e rispondono ai rischi.

L'AI permette di superare i limiti delle valutazioni tradizionali grazie alla capacità di analizzare grandi quantità di dati, individuare correlazioni complesse e generare **modelli predittivi** ad alta affidabilità.

Oggi nelle aziende, l'intelligenza artificiale viene impiegata per:

- Automatizzare la raccolta e l'analisi dei dati provenienti da sistemi e reti
- Riconoscere pattern anomali che possono indicare minacce in corso
- Fornire **valutazioni dinamiche** del rischio residuo sulla base di eventi in tempo reale
- Suggerire o attuare automaticamente misure correttive proporzionate

Queste funzionalità rendono l'AI un alleato fondamentale per rafforzare la prevenzione, migliorare la risposta agli incidenti e ottimizzare la governance della sicurezza a tutti i livelli dell'organizzazione.