RISK ASSESSMENT

LA CHIAVE PER UNA GESTIONE AZIENDALE SICURA ED EFFICIENTE

"SPERARE DI NON INCORRERE IN UN ATTACCO INFORMATICO, AL GIORNO D'OGGI, È UN PO' COME TUFFARSI IN MARE SPERANDO DI NON BAGNARSI"

LOKKY.IT

LUCA TRICARICO

L-31 | UNIPEGASO | 2025

Introduzione

In un mondo sempre più interconnesso e incerto, le imprese si trovano quotidianamente a dover affrontare un panorama di rischi variegato ed in continua evoluzione. Minacce digitali, crisi economiche, nuove normative e cambiamenti ambientali sono solo alcune delle sfide che le aziende devono imparare a gestire e per quanto possibile prevenire.

La gestione del rischio oggi rappresenta un vero e proprio vantaggio competitivo: non solo difende l'azienda, ma la aiuta a crescere con consapevolezza. Trasformare l'incertezza in opportunità è ciò che distingue un'organizzazione resiliente da una vulnerabile.

Negli ultimi anni, sempre più aziende stanno adottando strumenti avanzati per la valutazione dei rischi. L'aumento degli attacchi informatici, solo in Italia nel 2024 è aumentato del 15% (*Cybersecurity360*), l'evoluzione del quadro normativo e la digitalizzazione spinta hanno reso il **Risk Assessment** un elemento imprescindibile nella pianificazione aziendale.

Secondo il rapporto di *Allied-Market-Research*, il mercato globale dei sistemi di gestione del rischio dovrebbe raggiungere quasi 19 miliardi di dollari entro il 2026. Una cifra che testimonia quanto sia urgente e diffusa la necessità di proteggere il proprio business.

Che cos'è il Risk Assessment?

Il ***Risk Assessment*** è il processo di identificazione, analisi e valutazione dei rischi che possono influenzare un'azienda. Il Risk Assessment aiuta le aziende a individuare in anticipo quei fattori che potrebbero mettere a rischio il loro funzionamento, analizzando sia la probabilità che un dato evento si verifichi sia l'impatto di eventi dannosi. Attraverso questo processo, è possibile prendere decisioni adatte ad ogni tipo di problematica o situazione studiata e introdurre misure mirate per limitare o prevenire conseguenze negative su persone, beni e attività.

Le aziende spesso si affidano a modelli organizzati per valutare i rischi e stabilire quali affrontare per primi. Questo tipo di analisi può riguardare anche aspetti delicati come la sicurezza informatica. Nelle realtà più grandi, a gestire questo processo è solitamente una figura dedicata, come il Chief Risk Officer, che si occupa di coordinare tutte le attività legate alla prevenzione e al controllo dei rischi.

Le Fasi del Risk Assessment

Definizione di contesto
Prima di parlare di rischio, è fondamentale capire dove opera l'azienda, quali sono i suoi obiettivi e quali fattori (interni o esterni) possono influenzarli.

Identificazione dei rischi
Ogni settore ha le sue criticità. Possono essere economiche, operative, informatiche o ambientali. Identificarle è il primo passo per controllarle.

Valutazione
Si analizzano probabilità e impatti, per stabilire un ordine di priorità.

Pianificazione della risposta
Per ogni rischio, si decide cosa fare: evitarlo, ridurlo trasferirlo o accettarlo.

Monitoraggio e Aggiornamento
I rischi non sono statici; servono controlli periodici per aggiornare strategie e misure.

Template per Risk Management Plan
*link template tipo, a cura di Leonardo S.p.a.

Definizione del Contesto Aziendale

Il primo passo nella gestione del rischio consiste nel definire con chiarezza il contesto aziendale e stabilire i criteri con cui valutare le diverse minacce. Per farlo, è necessario partire dagli obiettivi che l'azienda intende raggiungere: senza una visione chiara delle sue priorità e strategie, è difficile capire quali rischi possono realmente compromettere il percorso. Analizzare l'ambiente interno ed esterno fin dall'inizio permette di mettere a fuoco le aree più esposte e di concentrare la valutazione dove serve davvero, aumentando così l'efficacia delle azioni di prevenzione.

I rischi che un'azienda deve affrontare possono nascere sia da fattori interni che esterni. I primi riguardano scelte organizzative, modalità operative o l'uso delle risorse a disposizione. I secondi, invece, derivano da dinamiche esterne come i cambiamenti nelle leggi, l'andamento del mercato o altri elementi che l'impresa non può controllare direttamente.

L'Identificazione dei Rischi

La seconda fase del processo di gestione del rischio consiste nel riconoscere in modo sistematico tutte le minacce che potrebbero mettere a rischio il buon funzionamento dell'azienda. In generale, queste minacce si possono suddividere in quattro categorie principali:

1. Rischi finanziari:

Riguardano eventuali perdite economiche causate da situazioni come clienti che non riescono a pagare, oscillazioni dei cambi nelle operazioni internazionali o costi imprevisti che sfuggono alla pianificazione iniziale.

2. Rischi operativi:

Sono problemi che nascono all'interno dell'azienda e che compromettono le attività quotidiane. Può trattarsi, ad esempio, di ritardi nelle consegne, difficoltà nel reperire materiali o guasti alle attrezzature che bloccano la produzione.

3. Rischi informatici:

In un'epoca digitale, i sistemi informativi sono spesso nel mirino. I pericoli vanno dagli attacchi hacker a virus informatici, fino a semplici errori umani che possono compromettere dati sensibili o processi aziendali.

4. Rischi ambientali:

Questi si collegano alle conseguenze che l'attività aziendale ha sull'ambiente. Emissioni nocive, gestione inadeguata dei rifiuti o un utilizzo non sostenibile delle risorse naturali possono esporre l'impresa a danni economici e di reputazione.

La Valutazione del Rischio

Una volta individuati i rischi, è necessario capire quanto siano pericolosi. La terza fase consiste proprio nella loro valutazione: si cerca di stimare sia la probabilità che questi eventi si verifichino, sia l'impatto che potrebbero avere sull'azienda. Questo passaggio è essenziale per capire su quali minacce intervenire per prime e con quali priorità.

In generale ogni rischio viene analizzato sulla base di due aspetti fondamentali:

- **Probabilità** che l'evento si verifichi
- **Impatto** quanto potrebbe danneggiare l'organizzazione se un evento accadesse

Per effettuare questa analisi, le imprese possono scegliere tra approcci qualitativi e quantitativi. **L'analisi qualitativa** è spesso il punto di partenza: classifica i rischi in base alla gravità potenziale, ad esempio in basso, medio o alto. Questo tipo di valutazione è utile per ottenere una panoramica rapida e orientare le decisioni iniziali.

Tra gli strumenti più utilizzati ci sono:

- **La matrice del rischio**, che incrocia impatto e probabilità per definire la criticità di ogni scenario.
- **Sessioni di brainstorming**, che sfruttano il confronto tra diversi punti di vista per far emergere rischi non immediatamente evidenti.
- **La tecnica Delphi**, utile per raccogliere pareri esperti in modo strutturato e arrivare a un consenso.
- **L'approccio EASW**, che aiuta a immaginare scenari futuri e a prepararsi in modo proattivo a possibili sviluppi.

Tutti questi strumenti permettono alle aziende di valutare meglio i pericoli e prepararsi con maggiore consapevolezza.

L’analisi quantitativa del rischio entra maggiormente nel dettaglio, cercando di stimare con precisione quali potrebbero essere le conseguenze economiche di un evento negativo. Qui non si parla più solo di livelli generici, ma si utilizzano numeri e modelli per capire quanto potrebbe costare, in termini concreti, un determinato rischio.

Il calcolo di base si fonda su una formula semplice ma efficace:

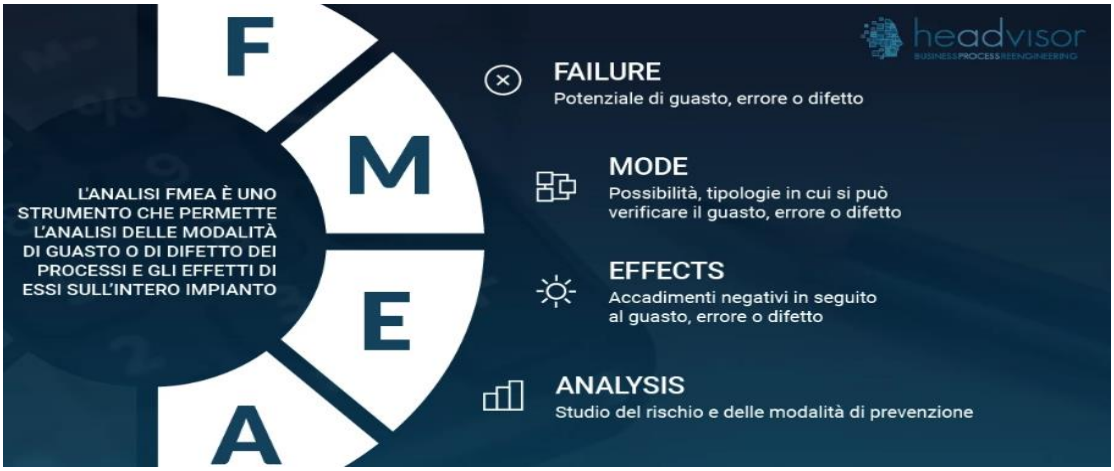
Rischio = Probabilità × Impatto

In alcune situazioni si tiene conto anche del tempo, ad esempio la frequenza con cui un evento può verificarsi:

Rischio = (Probabilità × Impatto) × Frequenza

Per ottenere queste stime, le aziende possono servirsi di vari strumenti statistici e decisionali, tra cui:

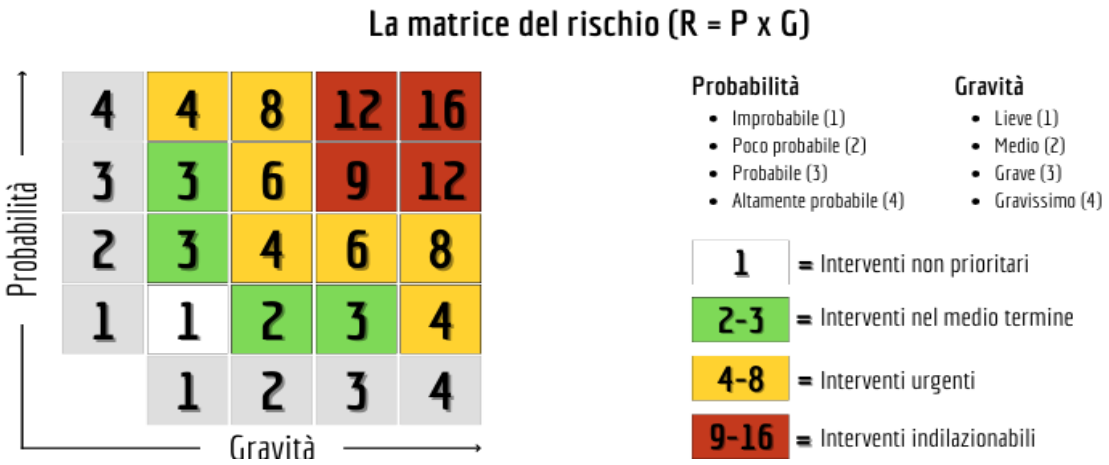
- **Simulazioni Monte Carlo**
- **Alberi decisionali**
- **Distribuzioni di probabilità**
- **Valore monetario atteso (EMV)**
- **FMEA (Failure Mode and Effects Analysis)**, un metodo strutturato per identificare punti deboli e valutare il loro impatto.



https://www.headvisor.it/sites/default/files/images/analisi-fmea-per-il-risk-management-headvisor.webp

Questi approcci aiutano le imprese a prendere decisioni più razionali e informate, specialmente quando sono in gioco investimenti o processi complessi.

Uno degli strumenti più utilizzati per valutare la gravità dei rischi è la *Matrice di Rischio.* Si tratta di un semplice schema che mette in relazione due fattori fondamentali: la probabilità che un evento si verifichi e il suo impatto sull'organizzazione. Incrociando questi elementi, è possibile attribuire un livello di priorità a ciascun rischio e decidere come affrontarlo.



Facciamo un esempio legato alla sicurezza informatica:
immaginiamo un'azienda i cui sistemi informatici non sono aggiornati e senza firewall.

In questo caso:

- **Probabilità (P)**: il rischio di subire un attacco è alto → valore 4
- **Impatto (G)**: una violazione dei dati può causare danni economici, reputazioni e sanzioni legali → valore 4
- **Tempo o frequenza (T)**: i sistemi online senza monitoraggio → valore 3

Risultato della valutazione:
Rischio = 4 × 4 × 3 = **48** → un rischio considerato **elevato** → interventi urgenti

Azioni preventive immediate:

- Installare un firewall e antivirus aggiornati
- Formare il personale sui comportamenti sicuri
- Eseguire backup frequenti
- Stabilire policy chiare per la gestione delle credenziali

Misure di mitigazione più avanzate:

- Aggiornare regolarmente tutti i sistemi con le patch di sicurezza
- Attivare l'autenticazione a due fattori (2FA)
- Crittografare i dati sensibili

Questo esempio mostra come una valutazione numerica ben fatta possa aiutare le aziende a capire dove intervenire e con quale urgenza.

Risk Treatment

Dopo aver valutato i rischi, il passo successivo è decidere come affrontarli. La quarta fase del processo consiste proprio nella gestione del rischio, cioè nell'attivare tutte quelle strategie e azioni che aiutano a contenere le minacce e a proteggere gli obiettivi dell'azienda

A questo scopo, si definisce un **piano di trattamento del rischio**, che stabilisce in modo chiaro quali misure devono essere adottate per ogni rischio significativo. Questo piano è un elemento fondamentale, soprattutto nei contesti legati alla sicurezza informatica, dove le vulnerabilità possono avere conseguenze molto serie. In genere, più un rischio è grave, più sarà necessario un piano dettagliato per gestirlo. Nei casi meno critici, invece, le azioni possono essere più semplici o addirittura opzionali. Un piano efficace non può limitarsi alla teoria: deve prevedere **obiettivi concreti**, scadenze precise e strumenti pratici per assicurarsi che tutto venga effettivamente messo in atto.

Per ogni rischio identificato, ci sono quattro elementi chiave da definire:

1. **Quale strategia seguire?**
   Si può scegliere di evitare il rischio, ridurlo, trasferirlo a terzi (come con un'assicurazione), oppure accettarlo se è considerato tollerabile.

2. **Come verrà gestito?**
   Bisogna descrivere le azioni da intraprendere e segnalare se ci sono legami con altri rischi o progetti.

3. **Chi è responsabile?**
   È importante indicare chiaramente la persona (o il team) che si occuperà di monitorare e guidare l'implementazione del piano.

4. **Qual è la scadenza?**
   Ogni intervento dovrebbe avere un obiettivo temporale.
   Se la soluzione richiede tempo, si possono prevedere misure temporanee per proteggere l'azienda nel frattempo.

In un contesto dove i sistemi aziendali sono sempre più interconnessi e complessi, è fondamentale unire le linee guida delle norme ISO con i requisiti del GDPR, ciò permette di costruire un sistema di gestione del rischio solido, flessibile e orientato alla prevenzione. Tecniche come la crittografia o la pseudonimizzazione dei dati sono strumenti chiave in questo processo.

Per affrontare in modo efficace i rischi, le aziende devono anche confrontarsi con le **normative in vigore**, che stabiliscono regole ben precise in materia di sicurezza, protezione dei dati e continuità operativa.

Tra i riferimenti più importanti ci sono il **GDPR**, la **direttiva NIS2** e gli standard **ISO**, che rappresentano veri e propri pilastri nel costruire un sistema aziendale sicuro e conforme alle norme vigenti.

GDPR General Data Protection Regulation

NIS2 Network and Information Systems Directive 2

ISO Organizzazione Internazionale per la Normazione

GDPR – General Data Protection Regulation
Il Regolamento europeo sulla protezione dei dati *(GDPR)* è entrato in vigore nel 2018 e riguarda tutte le aziende che trattano informazioni personali di cittadini europei. L'obiettivo principale è tutelare la privacy delle persone, garantendo trasparenza, sicurezza e controllo sui dati raccolti.

Tra i principi chiave:

- Il trattamento dei dati deve avvenire solo con il consenso informato.
- Gli utenti devono poter accedere, modificare o cancellare i propri dati.
- In caso di violazioni, le aziende devono avvisare le autorità entro 72 ore.

Non rispettare il GDPR può portare a sanzioni molto elevate.

Direttiva NIS2

La *Direttiva NIS2* (Direttiva UE 2022/2555), entrata in vigore il 17 gennaio 2023, punta a rafforzare la sicurezza informatica nei settori considerati essenziali, come energia, trasporti, finanza, sanità e infrastrutture digitali dell'UE. Ma non solo: l'ambito di applicazione si è allargato anche a fornitori di servizi cloud, e-commerce e piattaforme online.

Le aziende interessate devono:

- Avere piani di risposta agli incidenti informatici.
- Adottare misure di gestione dei rischi e delle vulnerabilità.
- Cooperare con le autorità nazionali in caso di attacchi o violazioni.

NIS2 impone anche un rafforzamento delle attività di vigilanza da parte degli Stati membri, con sanzioni per le organizzazioni non conformi.

Acs.it/blog/sicurezza-informatica

lSO/IEC 27001 – Gestione della Sicurezza delle Informazioni

Lo *standard ISO/IEC 27001* è una certificazione riconosciuta a livello internazionale per chi vuole gestire in modo strutturato la sicurezza delle informazioni. Aiuta a proteggere dati sensibili, ridurre i rischi informatici e garantire la continuità aziendale.

I principali elementi includono:

- Definizione di politiche e procedure di sicurezza.
- Valutazione continua dei rischi informatici.
- Applicazione di controlli come accessi limitati, crittografia e backup.
- Audit periodici per il miglioramento continuo.

ISO 31700 – Privacy by Design

Collegata al GDPR, la ISO 31700 è una linea guida che promuove il concetto di "privacy fin dalla progettazione". In altre parole, le aziende devono pensare alla protezione dei dati già nella fase iniziale di sviluppo dei sistemi o dei servizi.

Lo standard fornisce strumenti per:

- Analizzare i rischi legati al trattamento dei dati personali.
- Stabilire misure preventive e correttive.
- Monitorare nel tempo l'efficacia delle azioni intraprese.

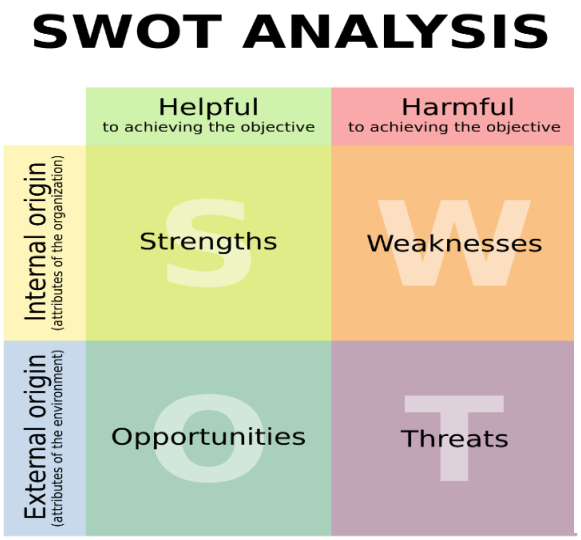
standard-iso-31700/dirittoaldigitale.com.

Per le imprese che operano nel mondo digitale, queste normative rappresentano un punto di riferimento essenziale. In un contesto dove tutto è connesso e i rischi si moltiplicano, avere regole chiare e condivise aiuta a proteggere le informazioni, a mantenere stabile l'operatività e a costruire un sistema aziendale più sicuro e affidabile

Metodologie per l'identificazione dei rischi:

La quinta fase è la metodologia per individuare il rischio; per individuare efficacemente le minacce potenziali, le aziende possono adottare diverse tecniche, tra cui:

- **Analisi dei processi aziendali:** esaminare le attività operative per identificare punti critici.
- **Brainstorming con i dipendenti:** coinvolgere il personale per raccogliere percezioni e intuizioni sui rischi.
- **Revisione delle normative e dei requisiti legali:** assicurarsi che l'azienda sia conforme alle leggi vigenti per evitare sanzioni.
- **Utilizzo di check-list e strumenti di valutazione standardizzati:** applicare strumenti riconosciuti per una valutazione sistematica dei rischi.
- **La Matrice Swot:** con la quale individuare punti di forza, punti di debolezza, nonché le opportunità o le minacce.



Un approccio strutturato nell'identificazione dei rischi consente alle aziende di sviluppare strategie di mitigazione efficaci, migliorando la resilienza e garantendo maggiore sicurezza operativa. Quindi Sarà importante aggiungere delle policy e/o delle procedure aziendali che aiutino a definire le linee guida per la gestione dei rischi. In questa fase sarà fondamentale la scelta delle risorse coinvolte (ruoli e responsabilità delle persone nei confronti dei rischi), gli strumenti e software da utilizzare per l'analisi dei rischi, le scale per misurarli, le tempistiche di monitoraggio con eventualmente le azioni di mitigazione da attuare.

L'importanza di una Consulenza nella Strategia Aziendale

E' un elemento cruciale nella gestione strategica di un'azienda, affidarsi a una **consulenza specializzata,** può fare la differenza tra una gestione del rischio efficace e una gestione del rischio **debole** o **incompleta**.

link per aziende di consulenza: Dogma.it - KPMG - Data Guard

Perché una consulenza è fondamentale nel Risk Assessment?

Competenze ed esperienza nel settore
Una società di consulenza porta **esperienza e metodologie consolidate**, aiutando l'azienda a individuare rischi nascosti e valutare scenari complessi.

Approccio oggettivo e analisi dettagliata
Un consulente esterno offre un **punto di vista neutrale** e basato su dati concreti, evitando distorsioni interne con un'analisi approfondita dei pericoli.

Personalizzazione della strategia di gestione del rischio
Ogni azienda ha esigenze uniche: una consulenza esperta permette di **adattare il Risk Assessment** al settore specifico e alle dimensioni dell'impresa, ottimizzando le risorse.

Conformità normativa e riduzione delle sanzioni
Il mancato rispetto delle normative può comportare **gravi sanzioni e danni alla reputazione**. I consulenti aiutano a garantire che l'azienda sia sempre in linea con leggi e regolamenti in materia di sicurezza, ambiente e governance.

Miglioramento della continuità operativa
Una corretta valutazione dei rischi, supportata da consulenti esperti, consente di **prevenire interruzioni e crisi**, garantendo la resilienza aziendale e la competitività nel mercato.

Ottimizzazione delle risorse finanziarie
Identificare e mitigare i rischi in anticipo permette di **evitare perdite economiche**, costi imprevisti e investire in modo più efficiente nella sicurezza e nello sviluppo aziendali**.**

Uno Sguardo al Cyber Risk

Secondo **l'Istitute of Risk Management**, "il *Cyber Risk* è qualsiasi minaccia che possa causare perdite economiche, danni alla reputazione o interruzioni operative a causa di malfunzionamenti nei sistemi informatici". Si tratta del rischio, ormai molto diffuso, di subire danni, diretti o indiretti, a causa di eventi accidentali e/o attacchi informatici malevoli che compromettono hardware, software, dati o infrastrutture digitali.

Perché il Cyber Risk è un pericolo che non interessa solo le grandi aziende?
Ogni giorno i media riportano casi di attacchi informatici, che colpiscono indistintamente colossi aziendali, piccole imprese e singoli utenti. Che si tratti di un Malware o di un hacker, gli effetti possono essere devastanti. Secondo il World Economic Forum," il *cyber crime* è tra i principali rischi globali per gravità. Non bisogna dirigere una multinazionale per diventare bersaglio: anche un semplice account personale può essere violato. "

Che cos'è un Rischio IT?
Una prima manifestazione del Cyber Risk può avvenire sotto forma di *Rischio IT*. Questo tipo di rischio è legato a problematiche tecniche o incidenti non intenzionali che impattano sui sistemi informatici. Esempi comuni includono cortocircuiti, blackout, errori umani (come un aggiornamento errato), oppure danni fisici come incendi. Sebbene gravi, questi eventi non sono crimini: si tratta piuttosto di problematiche gestionali o tecniche.

Che cos'è un Cyber Crime?
Quando l'origine del danno è intenzionale e criminale, si parla di *Cyber Crime*. Attacchi deliberati da parte di terzi spesso hacker o gruppi organizzati volti a rubare, danneggiare o manipolare informazioni. Le tecniche possono variare: furto di dati, accessi non autorizzati, Ransomware, phishing, sabotaggi, spionaggio informatico. È un crimine che può colpire chiunque: dall'impresa all'utente comune.

L'importanza della Cyber Insurance
una polizza assicurativa specifica per i rischi informatici. Questo tipo di copertura è utile sia per mitigare i danni economici e operativi derivanti da incidenti cyber, per l'assistenza e supporto nel gestire la crisi, il ripristino dei dati e la comunicazione post-attacco.

Agenzia per la Cybersicurezza Nazionale: acn.gov.it
ENISA – European Union Agency for Cybersecurity: enisa.europa.eu

Conclusione

In conclusione, implementare una valutazione strutturata dei rischi a 360° non è solo una questione tecnica, ma una leva strategica per rafforzare l'impresa.

Se gestito con continuità e competenza, un programma di valutazione del rischio permette alle aziende di*:*

- Ridurre drasticamente la probabilità di incidenti informatici e minimizzare le perdite finanziarie.
- Mantenere l'allineamento con normative nazionali e internazionali in materia di cybersecurity e data protection.
- Rafforzare la resilienza operativa e la capacità di risposta in caso di crisi.
- Migliorare l'efficienza nell'allocazione delle risorse digitali e nella pianificazione strategica.

La sicurezza assoluta non esiste, l'unica vera difesa è la **prevenzione!**