GUIDA AL CALCOLO DEL FATTORE DI RISCHIO NELLA SICUREZZA AZIENDALE

Metodologie, Normative e Strumenti per la Valutazione del Rischio sul Lavoro (ex D.Lg. 81/0)

DONATO VITALE

L'IMPORTANZA DELLA SICUREZZA AZIENDALE

La sicurezza aziendale rappresenta un pilastro fondamentale per il buon funzionamento di qualsiasi organizzazione. Garantire ambienti di lavoro sicuri e salubri non è solo un obbligo normativo, ma anche un investimento strategico volto a tutelare la salute dei lavoratori, prevenire infortuni, ridurre l'assenteismo e migliorare la produttività.
Una corretta gestione della sicurezza contribuisce a creare una cultura aziendale positiva, nella quale ogni individuo si sente protetto e responsabilizzato. Inoltre, promuovere la sicurezza consente di ridurre i costi derivanti da incidenti, sanzioni amministrative o danni reputazionali.

In un contesto economico e normativo sempre più attento al benessere dei lavoratori, le imprese devono dotarsi di strumenti efficaci per identificare, valutare e gestire i rischi presenti nelle proprie attività. In questo scenario, il **calcolo del fattore di rischio** rappresenta un passaggio cruciale per pianificare interventi mirati e migliorare costantemente il livello di sicurezza.

OBIETTIVI DEL DOCUMENTO

Questo documento ha l'obiettivo di fornire una guida chiara, completa e operativa per il calcolo del **fattore di rischio** in ambito aziendale, con particolare riferimento alla sicurezza sul lavoro.

In particolare, il documento si propone di:

- Offrire una panoramica aggiornata delle normative vigenti in materia di valutazione dei rischi.
- Definire i concetti fondamentali legati al rischio, come pericolo, probabilità e danno.
- Presentare metodologie standard per il calcolo del rischio, utilizzate nei contesti industriali e professionali.
- Fornire esempi pratici, checklist e modelli utili per la compilazione della valutazione.
- Supportare i responsabili della sicurezza (RSPP, datori di lavoro, tecnici) nell'applicazione concreta delle misure preventive e protettive.

Il documento si rivolge a tutti coloro che sono coinvolti nella gestione della sicurezza aziendale, indipendentemente dal settore o dalla dimensione dell’impresa.

VALUTAZIONE DEI RISCHI E FORMAZIONE SULLA SICUREZZA

Corso per Responsabili e Addetti alla Sicurezza (D.Lgs. 81/2008)

Il Decreto Legislativo n. 81/2008, noto anche come "Testo Unico per la sicurezza sul lavoro", è entrato in vigore il 15 maggio 2008. Questo testo legislativo, recependo le direttive europee, riorganizza e aggiorna in modo sistematico tutte le precedenti normative sulla salute e sicurezza nei luoghi di lavoro, con l'obiettivo principale di migliorare costantemente le condizioni di sicurezza e di tutela della salute dei lavoratori.

Il D.Lgs. 81/2008 prevede in particolare:

- Specifiche misure per garantire la salute e la sicurezza dei lavoratori durante l'attività lavorativa.
- Applicabilità in ogni settore, pubblico e privato, e per ogni tipo di rischio professionale.
- Tutela estesa a tutte le categorie di lavoratori, inclusi lavoratori autonomi e categorie equiparate.
- Regolamentazione dell'organizzazione interna aziendale per la gestione della sicurezza, coinvolgendo attivamente sia i datori di lavoro sia i lavoratori stessi.

CONCETTI E DEFINIZIONI DI BASE

Per comprendere a fondo la valutazione dei rischi e le procedure di sicurezza, è fondamentale chiarire alcuni termini di base:

- **Rischio:** È la probabilità che si verifichi un evento dannoso o pericoloso, correlata alla gravità delle sue conseguenze. In altre parole, è la combinazione tra la probabilità che qualcosa di negativo accada e l'entità del danno che potrebbe derivarne.
- **Pericolo:** È la proprietà intrinseca o la capacità potenziale di un determinato fattore (come macchinari, sostanze chimiche, condizioni ambientali, ecc.) di causare un danno alla salute o alla sicurezza dei lavoratori.
- **Danno:** Consiste in una lesione fisica, psicologica o un deterioramento della salute delle persone, derivante direttamente o indirettamente dall'esposizione a un pericolo.
- **Incidente:** È un evento improvviso e non desiderato che ha causato o avrebbe potuto causare danni alle persone o ai beni.
- **Esposizione:** È il contatto diretto o indiretto con una fonte di pericolo (ad esempio agenti chimici, fisici o biologici) che potrebbe causare un danno alla salute o sicurezza di un lavoratore.

DISTINZIONE TRA RISCHIO GENERICO E RISCHIO SPECIFICO

- **Rischio generico:** È legato a situazioni lavorative comuni a molte attività e non strettamente connesso alla specifica mansione svolta dal lavoratore. Ad esempio, il rischio di scivolare su superfici bagnate o cadere mentre si percorre una scala può essere considerato un rischio generico.
- **Rischio specifico:** È associato direttamente a una particolare mansione, ambiente di lavoro o processo produttivo. Ad esempio, l'utilizzo di macchinari specifici, la manipolazione di sostanze chimiche pericolose, o l'esposizione prolungata a rumore elevato costituiscono rischi specifici.

Queste definizioni costituiscono la base su cui si sviluppa il processo di valutazione dei rischi, necessario per individuare e attuare le misure preventive e protettive più idonee.

FIGURE COINVOLTE NELLA SICUREZZA

Di seguito un’immagine riassuntiva delle figure coinvolte:

Il Datore di Lavoro, secondo la natura dell’attività aziendale o dell’unità produttiva, in collaborazione con il Responsabile del Servizio di Prevenzione e Protezione (RSPP) e il Medico Competente (nei casi previsti dalla sorveglianza sanitaria obbligatoria), previa consultazione del Rappresentante dei Lavoratori per la Sicurezza (RLS), ha l'obbligo di:

- Valutare tutti i rischi per la salute e sicurezza dei lavoratori, compresi quelli specifici per gruppi di lavoratori particolarmente esposti (anche riguardo alla scelta di attrezzature di lavoro, sostanze chimiche utilizzate e all’organizzazione degli ambienti di lavoro) ed elaborare il Documento di Valutazione dei Rischi (DVR).
- Designare il Responsabile del Servizio di Prevenzione e Protezione (RSPP).

Questi obblighi sono esplicitamente indicati come non delegabili (Art. 17 del D.Lgs. 81/2008).

Per gestire efficacemente la sicurezza, il Datore di Lavoro organizza e coordina specifiche figure professionali:

- **Servizio di prevenzione e protezione** (Art. 31, D.Lgs. 81/2008)
- **Medico competente** (Art. 38, D.Lgs. 81/2008)
- **Addetti all’emergenza**, comprendenti figure per antincendio, primo soccorso e gestione delle emergenze

ANALISI DEL RISCHIO

La valutazione qualitativa di un rischio si fonda principalmente su due fattori chiave:

- **La probabilità** che si verifichi un evento indesiderato;
- **La gravità delle conseguenze** che tale evento potrebbe comportare.

Questa analisi si basa anche sull'esperienza e sulla competenza di chi la conduce, tenendo conto di:

- **Il livello di conoscenza disponibile** sul rischio specifico;
- **L'affidabilità e completezza delle informazioni raccolte**.

Una volta stimato il livello di rischio, è necessario stabilire se esso possa essere considerato accettabile oppure no. Per fare ciò, è importante definire dei criteri chiari di accettabilità, i quali possono essere influenzati da diversi elementi:

- **Obblighi normativi**, laddove previsti dalla legge;
- **Standard tecnici o pratiche consolidate**, riconosciute nel settore;
- **Politiche interne dell'organizzazione**, in base agli obiettivi e alla tolleranza al rischio.

Questi criteri permettono di decidere se un rischio può essere mantenuto, se deve essere ridotto oppure eliminato attraverso opportune misure di prevenzione o mitigazione.

VALUTAZIONE DEI RISCHI: DEFINIZIONE E PRINCIPI NORMATIVI

1. **Definizione (Art. 2, comma 1, lett. q, D.Lgs. n. 81/2008)**
   La valutazione dei rischi consiste in un'analisi complessiva e documentata di tutti i pericoli che possono compromettere la salute e la sicurezza dei lavoratori in un'organizzazione.
   È finalizzata a individuare misure adeguate di prevenzione e protezione per garantire un progressivo miglioramento nel tempo delle condizioni lavorative.
2. **Ambito di applicazione (Art. 28, comma 1, D.Lgs. n. 81/2008)**
   La valutazione deve coprire **tutti i rischi** connessi all'attività lavorativa, incluse:
   - La scelta di attrezzature, sostanze e preparati chimici;
   - L'organizzazione e sistemazione degli ambienti di lavoro;
   - I rischi specifici di categorie particolari di lavoratori, come:
     - Lavoratori esposti a stress lavoro-correlato;
     - Lavoratrici in gravidanza;
     - Differenze di genere;
     - Età dei lavoratori;
     - Origine geografica (provenienza da altri Paesi);
     - Tipologia contrattuale (tempo determinato, part-time, somministrazione, ecc.).

MOTIVAZIONI E CONCETTI CHIAVE DELLA VALUTAZIONE DEI RISCHI

3. **Motivazione principale**
   Una delle principali ragioni per cui si effettua la valutazione dei rischi è **prevenire infortuni e malattie legate al lavoro**, riducendo la probabilità di eventi dannosi per il personale.
4. **Infortunio sul lavoro**
   Evento imprevisto e non voluto, causato da un'azione **violenta**, che può generare:
   - Lesioni fisiche o psicologiche;
   - Malattia o danni permanenti;
   - Inabilità temporanea o permanente;
   - Nei casi più gravi, il decesso.

   La causa può essere:
   - **Traumatica** (cadute, urti, ecc.);
   - **Termica** (colpo di calore, ustioni);
   - **Elettrica** (folgorazione);
   - **Psichica** (shock, reazioni estreme);
   - **Da sforzo eccessivo** (movimenti o carichi fuori dalla norma);
   - **Biologica** (virus, batteri, agenti patogeni).
5. **Incidente e quasi incidente**
   - **Incidente**: evento che genera o può generare un infortunio.
   - **Quasi incidente**: situazione pericolosa che **non ha causato danni**, ma **avrebbe potuto farlo** se le circostanze fossero state diverse.
6. **Malattia professionale (Art. 139 e seguenti del T.U. INAIL)**
   Patologia che si sviluppa nel tempo per **esposizione prolungata** a fattori di rischio legati all'attività lavorativa, come:
   - Sostanze chimiche;
   - Agenti fisici o biologici;
   - Agenti cancerogeni o tecnici.

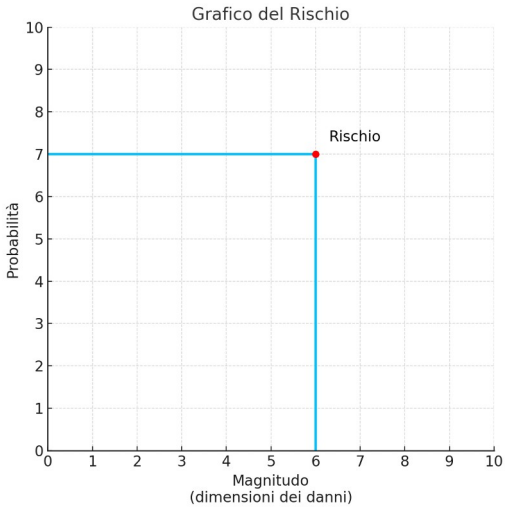
   A differenza dell'infortunio, **non è necessaria una causa immediata o violenta**, ma serve stabilire un **nesso causale** tra attività lavorativa ed esposizione al rischio.

La valutazione dei rischi viene effettuata in base alla tipologia dei pericoli individuati, attraverso metodologie di analisi che permettono di stimare sia la probabilità di accadimento (P), sia la gravità (magnitudo) delle conseguenze (M) associate. Sulla base di tali stime, si determina la necessità e l'urgenza di adottare misure correttive per eliminare o ridurre il rischio.

Il rischio è quindi definito come una funzione che dipende dalla probabilità del verificarsi di un evento pericoloso e dalla gravità delle sue conseguenze.

$$R = \frac{M \times P}{K_i}$$

- **R è il rischio,**
- **M** è la magnitudo (entità del danno),
- **P** è la probabilità di accadimento,
- **K_i** è un coefficiente di riduzione del rischio (es. legato a misure di sicurezza adottate).



L'asse orizzontale rappresenta la **Magnitudo** (dimensioni dei danni).

- L'asse verticale rappresenta la **Probabilità**.
- Il punto rosso rappresenta il **Rischio**, come combinazione tra magnitudo e probabilità.
- Le linee azzurre aiutano a visualizzare le coordinate.

IL MODELLO A MATRICE PER LA VALUTAZIONE DEI RISCHI

Uno degli strumenti più utilizzati per stimare il rischio residuo e definire le priorità di intervento è il modello a matrice, basato sulla formula **R = P x D**, dove *R* rappresenta il rischio, *P* la probabilità e *D* il danno.

La sua ampia adozione è dovuta alla facilità d'uso: una volta comprese le regole di applicazione e utilizzato con coerenza, consente di ottenere rapidamente una stima del rischio residuo. In base al valore ottenuto, si può stabilire con maggiore chiarezza quali azioni correttive siano più urgenti. Questo tipo di valutazione costituisce un elemento essenziale nella stesura del **Documento di Valutazione dei Rischi (DVR)**.

Il funzionamento del metodo si basa sull'interazione tra due fattori principali: la **probabilità** che un evento accada e la **gravità del danno** che potrebbe derivarne. Analizzando questi aspetti congiuntamente, è possibile ottenere una valutazione oggettiva e strutturata del livello di rischio presente.

QUALI SONO I POSSIBILI VALORI DEL RISCHIO?

Poiché il livello di rischio deriva dal prodotto tra le due variabili descritte in precedenza (probabilità e danno), i valori che può assumere si ricavano direttamente da questa combinazione e sono i seguenti:

P/D	1	2	3	4
1	1	2	3	4
2	2	4	6	8
3	3	6	9	12
4	4	8	12	16

Tabella Matriciale Rischio

Di seguito viene riportato il significato di tali valori:

- 🟩 **Verde – Intervallo di sicurezza**
  Il livello di rischio è trascurabile o assente. Non sono necessarie misure correttive.
- 🟨 **Giallo – Intervallo di rischio accettabile**
  Il rischio è presente ma ritenuto tollerabile. È consigliabile monitorare la situazione.
- 🟥 **Rosso – Intervallo di rischio significativo**
  Il rischio è rilevante e può comportare conseguenze gravi. Sono richiesti interventi di mitigazione.
- ⬛ **Nero – Intervallo di grave rischio**
  Il livello di rischio è molto alto. È necessario intervenire immediatamente per ridurre il pericolo.

È evidente che l'obiettivo principale del Servizio di Prevenzione e Protezione consiste nel ricondurre tutti i rischi presenti nell'ambiente di lavoro all'interno della fascia verde, cioè quella corrispondente agli intervalli di sicurezza.

Situazioni di rischio potenziali e azioni correttive :
Durante la valutazione del rischio possono presentarsi due scenari distinti:

1. **Il rischio stimato rientra direttamente in un intervallo di sicurezza**
   In questo caso – che rappresenta la situazione ideale – è comunque necessario pianificare interventi a **medio-lungo termine** per mantenere elevati gli standard di sicurezza.
2. **Il rischio risulta elevato**, con un valore superiore alla soglia accettabile ($R = P \times D > 4$),
   In tale situazione ci si trova di fronte a un rischio **significativo e/o grave**, e occorre attuare **misure correttive immediate** per migliorare le condizioni di sicurezza nei luoghi di lavoro.

RIASSUMENDO QUANTO SOPRA, SI PUÒ RAPPRESENTARE LO SCENARIO NEL SEGUENTE SCHEMA:

Valore del Rischio (R)	Priorità	Misure migliorative da intraprendere
R > 8	Alta	Applicare con estrema urgenza tutte le misure di prevenzione e protezione disponibili per ridurre il rischio.
4 < R ≤ 8	Medio-Alta	Attuare con urgenza le misure di prevenzione e protezione non ancora considerate, al fine di abbassare il livello di rischio.
R ≤ 4	Medio-Bassa	Pianificare interventi migliorativi nel medio-lungo termine per mantenere adeguati standard di sicurezza.

L'introduzione del tema delle misure migliorative ci conduce al concetto di rischio residuo, un elemento chiave nell'ambito della valutazione dei rischi aziendali.

GESTIONE DEI RISCHI

- **Analisi e definizione degli interventi di adeguamento e miglioramento**
  Studio approfondito delle soluzioni da adottare per adeguare e migliorare le condizioni attuali.
- **Valutazione della fattibilità degli interventi**
  Verifica concreta della possibilità di realizzare le azioni individuate.
- **Pianificazione degli interventi**
  Definizione dei tempi e delle risorse economiche necessarie per attuare gli interventi previsti.
- **Gestione e controllo delle misure attuate**
  Organizzazione delle procedure di esecuzione, verifica costante e controlli periodici per assicurare l'efficacia e l'efficienza degli interventi messi in atto.

SCHEMA RIASSUNTIVO:

P	Livello di probabilità	Criterio di Valutazione
1	Improbabile	- La mancanza rilevata può provocare un danno per la concomitanza di più eventi poco probabili indipendenti. - Non sono noti episodi già verificatisi. - Il verificarsi del danno susciterebbe incredulità
2	Poco probabile	- La mancanza rilevata può provocare un danno solo in circostanze sfortunate di eventi. - Sono noti solo rarissimi episodi già verificatisi. - Il verificarsi del danno ipotizzato susciterebbe grande sorpresa.
3	Probabile	- La mancanza rilevata può provocare un danno, anche se in modo automatico o diretto - E' noto qualche episodio di cui alla mancanza ha fatto seguire il danno - Il verificarsi del danno ipotizzato susciterebbe una moderata sorpresa in azienda
4	Altamente probabile	- Sono noti episodi in cui il pericolo ha causato danno. - Il pericolo può trasformarsi in danno con una correlazione diretta. - Il verificarsi del danno non susciterebbe sorpresa.

ESEMPIO DI LIVELLI DI DANNO

VALORE	SIGNIFICATO DEL VALORE	CRITERIO DI SCELTA
1	LIEVE	Incidente che dà luogo a disturbi rapidamente reversibili (pochi giorni); Esposizione cronica che dà luogo a disturbi rapidamente reversibili (pochi giorni).
2	DI MODESTA ENTITÀ	Incidente che dà luogo a disturbi reversibili (mesi); Esposizione cronica che dà luogo a disturbi reversibili (mesi).
3	GRAVE	Incidente con effetti di invalidità permanente parziale o comunque irreversibili; Esposizione cronica con effetti di invalidità permanente parziale o comunque irreversibili.
4	MOLTO GRAVE	Incidente con effetti di invalidità totale o mortale; Esposizione cronica con effetti mortali o totalmente invalidanti.

CONTENUTI ESSENZIALI DEL DOCUMENTO DI VALUTAZIONE DEI RISCHI (DVR)

1. **Descrizione generale dell’azienda**
    - Informazioni anagrafiche e descrizione dell’attività svolta.
    - Illustrazione del ciclo produttivo e dei principali processi lavorativi.
2. **Organigramma della sicurezza**
    - Elenco dei soggetti con incarichi specifici in materia di sicurezza: Datore di lavoro, RSPP, RLS, Medico competente, Preposti, Addetti al primo soccorso, Addetti antincendio e gestione emergenze.
3. **Analisi delle mansioni e dei rischi connessi**
    - Descrizione delle mansioni lavorative.
    - Attività svolte, attrezzature e macchinari utilizzati.
    - Esposizione ad agenti fisici, chimici, biologici, con dettaglio su quantità, durata e livello di esposizione.
    - Indicazione delle mansioni che comportano rischi specifici e necessitano di formazione, esperienza e capacità professionali particolari.
4. **Partecipazione e consultazione**
    - Coinvolgimento del RLS, del Medico competente e di altre figure interne o consulenti esterni nella valutazione dei rischi.
    - Commenti, osservazioni e contributi raccolti durante il processo.
5. **Valutazione dei rischi**
    - Risultati dettagliati della valutazione dei rischi per ogni mansione.
    - Identificazione dei rischi residui.
    - Criteri adottati nella scelta delle attrezzature, sostanze e nell’organizzazione degli ambienti di lavoro.
6. **Misure di prevenzione e protezione**
    - Misure già attuate per la tutela della salute e sicurezza.
    - Programma degli interventi migliorativi, con indicazione delle scadenze e dei responsabili attuatori.
    - Procedure operative per l’attuazione delle misure di sicurezza.
    - Ruoli e responsabilità nell’organizzazione aziendale.
7. **Dispositivi di protezione individuale (DPI)**
    - Elenco dei DPI adottati.
    - Criteri di scelta e caratteristiche tecniche.

8. **Formazione, informazione e addestramento**
    - Fabbisogni formativi rilevati.
    - Programmi di formazione rivolti a lavoratori, preposti, RLS, addetti all'emergenza, ecc.
9. **Procedure di emergenza**
    - Piani antincendio, pronto soccorso, evacuazione.
    - Comportamenti da adottare in caso di pericolo grave e immediato.
10. **Rispondenza alle normative specifiche**

- Riferimenti alle valutazioni richieste dai singoli Titoli del D.Lgs. 81/2008 (es. rischio chimico, biologico, rumore, ecc.).

11. **Schede sintetiche per mansione**

- Riepilogo per ciascuna mansione: attività, rischi, livelli di esposizione, DPI e misure adottate.

12. **Programmazione e aggiornamento del DVR**

- Frequenza della riunione periodica sulla sicurezza.
- Periodicità prevista per la revisione del DVR e criteri per il suo aggiornamento.

13. **Allegati tecnici**

- Relazioni di misurazioni strumentali (rumore, polveri, agenti chimici, microclima, illuminazione, ecc.).
- Documentazione specifica (es. Documento Protezione da Esplosioni, planimetrie con uscite di emergenza, vie di fuga, estintori, ecc.).

AGGIORNAMENTO DELLA VALUTAZIONE DEI RISCHI E REVISIONE DEL DVR

La valutazione dei rischi deve essere **aggiornata** e il Documento di Valutazione dei Rischi (DVR) **revisionato entro 30 giorni** in caso di:

- **Modifiche aziendali** che possano rendere obsoleta la valutazione (es. cambiamenti nell'organizzazione, nei processi produttivi, nei luoghi di lavoro);
- **Variazioni delle mansioni o delle lavorazioni**, che comportino nuovi rischi o modifiche nei livelli di esposizione dei lavoratori;
- **Esiti della sorveglianza sanitaria** che evidenzino la necessità di rivedere la valutazione dei rischi;
- **Indicazioni degli organi di vigilanza**, espresse tramite provvedimento motivato;
- **Conclusioni delle riunioni periodiche** sulla sicurezza;
- **Nuove disposizioni legislative o normative** in materia di salute e sicurezza sul lavoro;

- **Scadenze programmate** per il riesame del documento.

CADENZE DI AGGIORNAMENTO SPECIFICHE

- **Agenti fisici** (rumore, vibrazioni, campi elettromagnetici, radiazioni ottiche artificiali, microclima, ecc.):
  La valutazione dei rischi deve essere **programmata con cadenza almeno quadriennale** e condotta da personale qualificato del Servizio di Prevenzione e Protezione, in possesso di competenze specifiche.
- **Agenti cancerogeni o mutageni**:
  La valutazione dei rischi deve essere **ripetuta almeno ogni tre anni**, salvo necessità di aggiornamenti anticipati secondo quanto previsto dalla normativa vigente.

PROCEDURE DI MITIGAZIONE DEL RISCHIO

Una volta identificati e classificati i rischi, è necessario attuare **misure di prevenzione e protezione** volte a ridurre sia la **probabilità** che il **danno** associato a ciascun pericolo. Questo processo prende il nome di **mitigazione del rischio** e rappresenta uno dei passaggi più importanti nella gestione della sicurezza aziendale.

Strategie di mitigazione

Le azioni per la riduzione del rischio si classificano in due grandi categorie:

🔒 **Misure di prevenzione**

Interventi che **agiscono sulla probabilità** che si verifichi l'evento dannoso. Ad esempio:

- Formazione e addestramento del personale.
- Definizione di procedure operative sicure (POS).
- Manutenzione ordinaria di impianti e macchinari.
- Segnaletica di sicurezza.
- Sorveglianza sanitaria periodica.

🛡️ **Misure di protezione**

Interventi che **agiscono sulla riduzione del danno** nel caso in cui l'evento si verifichi. Ad esempio:

- Utilizzo di **Dispositivi di Protezione Individuale (DPI)**: caschi, guanti, occhiali, scarpe antinfortunistiche.
- Sistemi di contenimento (barriere, carter, protezioni mobili).
- Piani di evacuazione e gestione delle emergenze.
- Presenza di estintori, rilevatori di gas, dispositivi di arresto di emergenza.

GERARCHIA DEGLI INTERVENTI DI SICUREZZA

Le norme internazionali, come la ISO 45001 e la ISO 12100, suggeriscono una **gerarchia di interventi**, da preferire in ordine decrescente di efficacia:

1. **Eliminazione del pericolo**
   Es.: sostituire una sostanza tossica con una meno pericolosa.
2. **Sostituzione con alternativa meno rischiosa**
   Es.: utilizzare una macchina con protezioni integrate.
3. **Controlli tecnici/ingegneristici**
   Es.: installare barriere fisiche o protezioni automatizzate.
4. **Segnaletica, avvisi, procedure organizzative**
   Es.: cartelli di pericolo, percorsi tracciati, turni ridotti.
5. **Formazione e consapevolezza**
   Es.: corsi obbligatori per l’uso sicuro delle attrezzature.
6. **DPI (ultima risorsa)**
   Da usare solo quando non è possibile eliminare o ridurre il rischio in altri modi.

PIANIFICAZIONE DELLE AZIONI CORRETTIVE

Una volta individuate le misure da adottare, è fondamentale pianificarle in modo **organizzato e documentato**. Questo processo include:

- **Definizione delle priorità** (in base al livello di rischio).
- **Assegnazione delle responsabilità** (chi fa cosa).
- **Tempi di attuazione** chiari e realistici.
- **Monitoraggio dei risultati** e verifica dell'efficacia.
- **Aggiornamento periodico** della valutazione dei rischi.

SICUREZZA IN AMBITO INFORMATICO

In un contesto aziendale moderno, la sicurezza informatica è parte integrante della gestione complessiva del rischio. La crescente digitalizzazione dei processi aziendali comporta l'esposizione a **minacce informatiche** che possono compromettere dati sensibili, fermare la produzione o causare danni economici e reputazionali gravi.

COS'È LA SICUREZZA INFORMATICA AZIENDALE

La **sicurezza informatica (cybersecurity)** si riferisce all'insieme di misure tecniche, organizzative e procedurali volte a proteggere:

- **Riservatezza**: i dati devono essere accessibili solo a chi è autorizzato.
- **Integrità**: i dati devono essere corretti e non alterati.
- **Disponibilità**: i sistemi e i dati devono essere sempre accessibili agli utenti legittimi.

PRINCIPALI MINACCE INFORMATICHE PER LE AZIENDE

Minaccia	Descrizione breve
Malware	Software dannosi (es. virus, trojan, ransomware).
Phishing	Email ingannevoli che mirano a rubare credenziali.
Accessi non autorizzati	Intrusioni nei sistemi da parte di utenti esterni o interni.
Perdita di dati	Cancellazione accidentale o furto di dati sensibili.
Attacchi DDoS	Sovraccarico dei server che porta all'interruzione dei servizi.
Errore umano	Comportamenti non sicuri da parte degli utenti.

BUONE PRATICHE DI SICUREZZA INFORMATICA

Per mitigare i rischi in ambito informatico, è necessario adottare una combinazione di **tecnologie**, **procedure** e **formazione**. Le principali azioni consigliate includono:

🔐 **Protezione tecnica**

- Installazione di **antivirus e firewall**.
- Aggiornamento costante dei software e dei sistemi operativi.
- Crittografia dei dati sensibili.
- Backup periodici dei dati (on-site e off-site).

🕵️‍♀️ **Gestione degli accessi**

- Creazione di credenziali sicure (password complesse, autenticazione a 2 fattori).
- Assegnazione dei privilegi minimi necessari agli utenti.
- Monitoraggio degli accessi ai sistemi e dei log di sistema.

🧠 **Formazione e consapevolezza**

- Programmi di **awareness** per il personale.
- Simulazioni di attacchi (es. test di phishing).
- Politiche aziendali chiare sull'uso sicuro degli strumenti informatici.

VALUTAZIONE DEL RISCHIO INFORMATICO

Come per la sicurezza fisica, anche per l'**ICT** è possibile applicare il metodo di **valutazione del rischio**:

Esempio di rischio	Probabilità (P)	Danno (D)	R = P × D	Livello	Azione
Mancato backup settimanale	3	4	12	Elevato	Implementare backup automatici
PC con software obsoleto	4	3	12	Elevato	Aggiornare e monitorare le versioni
Uso di password deboli	5	3	15	Molto elevato	Formare il personale + MFA

Riferimenti normativi per la cybersecurity

- **Regolamento UE 2016/679 (GDPR)**: impone misure di sicurezza per proteggere i dati personali.
- **Direttiva NIS 2** (in vigore dal 2023): obblighi per la cybersicurezza nelle infrastrutture critiche.
- **ISO/IEC 27001**: standard internazionale per i sistemi di gestione della sicurezza delle informazioni (SGSI).
- **Linee guida AgID** per la sicurezza informatica nella Pubblica Amministrazione (valide anche per le aziende in appalto).