UNIVERSITÀ POLITECNICA DELLE MARCHE

DII
Dipartimento di Ingegneria dell'Informazione

unimc

Le sfide etiche dell'Intelligenza Artificiale nella Sicurezza sul Lavoro e la Mitigazione dei Rischi: Cybersecurity e DataProtection e Social Responsability.

FEDERICA MORICHETTI

Facoltà di Ingeneria

Università Politecnica delle Marche- Ancona

federicainforming@gmail.com- Mobile: 3398002495

Giovedì 02 Ottobre 2025- Venerdì 03 Ottobre 2025

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

INDICE

INTRODUZIONE

INTRODUZIONE

Finalità

Il presente elaborato è finalizzato all'analisi preventiva dei rischi degli infortuni sul lavoro derivanti dall'impiego dell'intelligenza artificiale nelle attrezzature utilizzate dai lavoratori; in particolare si tratta di un'azienda operante nel settore del commercio all'ingrosso e al dettaglio di prodotti per animali che ha acquistato nuovi carelli elevatori dotati di un sistema di Intelligenza Artificiale.

La relazione si fonda su un'esperienza professionale da me seguita e sviluppata in collaborazione con un team multidisciplinare composto da colleghi con competenze specifiche anche in ambito tecnico-informatico, al fine di garantire un approccio specialistico e integrato alla gestione del progetto.

L'analisi progettuale si concentra sulla valutazione dei rischi **in materia di cybersecurity, sulla conformità alla protezione dei dati personali, e affronta inoltre gli aspetti etici e giuridici dell'IA, con particolare attenzione al ruolo della Responsabilità Sociale d'Impresa (CSR).**

INTRODUZIONE

Descrizione del contesto

L'Azienda ha più sedi operative nelle quali le aree Magazzino e Logistica sono di notevoli dimensioni; la struttura informatica è caratterizzata sia da server fisici che da server in cloud a cui sono collegati i dispositivi hardware utilizzati dagli operatori.

L'azienda, dotata di un Modello di Organizzazione e Gestione 231, di un Codice Etico e della Certificazione della Parità di Genere (Uni PdR 125/2021) è molto attenta e sensibile al valore della Persona e agli aspetti sociali in ogni contesto operativo interno ed esterno.

Pertanto è fondamentale che tale valutazione del rischio prenda in considerazione anche gli impatti di natura psicologica che le tecnologie possono causare al lavoratore.

INTRODUZIONE

IA e Sicurezza sul Lavoro (Cenni)

La sicurezza sul lavoro si è evoluta in una disciplina complessa che integra aspetti tecnici, organizzativi e umani. La valutazione dei rischi, sancita dal D.Lgs. 81/08, ha spostato il focus dalla semplice reazione all'incidente alla sua prevenzione e oggi essa cresce e si evolve anche grazie all'impiego di sistemi di Intelligenza Artificiale.

L'Intelligenza Artificiale deve essere considerata un nuovo alleato per la salute e la sicurezza dei lavoratori: non una minaccia, ma uno «strumento>> a servizio dell'uomo.

Le principali applicazioni pratiche dell'Intelligenza Artificiale in ambito Safety possono riguardare a titolo esemplificativo, ma non esaustivo:

- **Analisi Predittiva dei Rischi**

L'AI può analizzare dataset massivi (registri di infortuni, turni di lavoro, report meteorologici, dati dei sensori) per identificare modelli nascosti e prevedere la probabilità di incidenti.

INTRODUZIONE

- **Monitoraggio Intelligente e Rilevamento di Pericoli**

Soluzioni in grado di monitorare l'ambiente di lavoro in tempo reale per rilevare automaticamente comportamenti o condizioni pericolose.

- **Robotica Collaborativa (Cobots)**

I robot collaborativi, o cobots, sono progettati per lavorare in sinergia con gli operatori umani adattando il proprio comportamento in tempo reale per evitare collisioni.

- **Formazione e Simulazione Immersiva**

L'AI, combinata con la **Realtà Virtuale (VR)** e la **Realtà Aumentata (AR)**, offre un nuovo approccio alla formazione implementando il percorso di apprendimento.

L'implementazione dell'AI in ambito di sicurezza non è priva di rischi; a tal proposito si citano come tematiche di criticità: Privacy – Trasparenza- Responsabilità- Discriminazione- Aspetti psicologici (Stress da lavoro correlato).

INTRODUZIONE

Etica e IA (Cenni)

L'Etica professionale è un insieme di principi e valori che regolano il comportamento dei professionisti/imprenditori nel loro ambiente lavorativo. Questi principi sono fondamentali per garantire un comportamento corretto, responsabile e rispettoso nei confronti dei colleghi, dei clienti e dell'organizzazione stessa. Ogni organizzazione oggi è chiamata a «riesaminare» i propri modelli di business conferendo valore anche agli elementi di natura morale, psicologica che seppur rappresentano principi di diritto della persona, nella sfera aziendale avevamo un ruolo non «centrale».

L'Etica riguarda il nostro agire sia come singoli che nelle relazioni sociali e nella vita comunitaria; è l'opportunità di agire bene in quanto essa richiede all'uomo di riflettere, di comprendere cosa è bene per l'individuo e per la società attraverso l'attuazione dei valori e dei principi corretti.

Oggi questa dimensione è diventata fondamentale nei processi di innovazione tecnologica ivi compresi quelli basati su sistemi di Intelligenza Artificiale in quanto permette di posizionare la Persona al centro di ogni interesse, di tutelare i suoi diritti, di orientarla e di supportarla per l'uso costruttivo dei nuovi sistemi tecnologici. A tal proposito è importante evidenziare che lo sviluppo tecnologico è il risultato di scelte ben precise e valoriali; è il frutto di decisioni su "cosa sviluppare", "come sviluppare" e "per quali scopi".

METODOLOGIA OPERATIVA

METODOLOGIA OPERATIVA

Descrizione della Soluzione Tecnologica adottata

La soluzione tecnologica adottata dall'azienda consiste in un sistema integrato con i carrelli elevatori, basato su Intelligenza Artificiale (AI), progettato per monitorare e proteggere sia i pedoni sia i veicoli all'interno degli ambienti industriali, con l'obiettivo di ridurre il rischio di collisioni e di investimento, migliorando così la sicurezza dei lavoratori.

Il sistema utilizza telecamere integrate nel carrello elevatore per la rilevazione di persone e/o oggetti in modalità tagless con AI adattandosi alle esigenze di ogni ambiente.

Il sistema rallenta dinamicamente il carrello elevatore in presenza di rischio attivando anche alert visivi ed acustici. È possibile configurare aree con limiti di velocità associati, che attivano la decelerazione del carrello quando vi entra; gli operatori e i pedoni vengono informati tramite segnali.

Oltre alle funzionalità di rilevamento, il sistema è in grado di localizzare in tempo reale la posizione dei veicoli e dei lavoratori all'interno delle aree operative. La soluzione è supportata da una piattaforma dedicata che consente anche la generazione di report finalizzati al monitoraggio e al miglioramento continuo della sicurezza sul lavoro.

METODOLOGIA OPERATIVA

Metodologia Operativa- Impostazione

L'analisi progettuale è basata sul principio della Privacy- By Design e X- By Design al fine di avere un approccio proattivo conforme sia alla Data Protection, alla Cybersecurity che al AI Act e all'Etica sull'IA, nell'ottica di sistemi trasparenti, robusti e responsabili.

Questo approccio metodologico e multidisciplinare permette di garantire dei risultati di mitigazione dei rischi reali, implementabili e monitorabili nel breve- medio periodo parallelamente alle evoluzioni organizzative e tecnologiche dell'azienda.

Nelle Tabelle seguenti sono descritte **le n. 5 Fasi** su cui si struttura la metodologia di analisi dei rischi.

METODOLOGIA OPERATIVA

Schema riassuntivo delle Fasi Metodologiche

Tipologia di Fase	Descrizione
Fase 1. **Mappatura dei Dati**	Vengono analizzate le tipologie di dati oggetto del trattamento. Essi sono rappresentati da: immagini di localizzazione; ID degli operatori.
Fase 2. **Threat Modeling**	Vengono identificate le potenziali minacce privacy e vulnerabilità. Ad esempio: ○ Rispetto dei principi di necessità e di minimizzazione dei dati. ○ Mancanza di Trasparenza. ○ Accessi non autorizzati al sistema. ○ Perdita della riservatezza. ○ Alterazione e/o Manomissione dei Dati. ○ Conservazione prolungata.

METODOLOGIA OPERATIVA

Tipologia di Fase	Descrizione
Fase 3. **Valutazione del Rischio (Formula)**	Valutazione del Rischio Calcolo del rischio in base alla formula $R = P \times G$ Impatto (G) Probabilità (P)
Fase 4. **Mitigazione del Rischio**	Definizione ed attuazione delle misure tecniche e procedurali per la prevenzione e mitigazione dei rischi**.**
Fase 5. **Monitoraggio**	Verifica nel tempo dell'efficacia delle misure, eventuale implementazione delle medesime. Coinvolgimento degli stakeholder, del DPO, OdV e Comitato Parità di Genere.

ESECUZIONE DELLE FASI METODOLOGICHE

ESECUZIONE DELLE FASI METODOLOGICHE

Mappatura dei Dati

Il Team di lavoro ha eseguito la mappatura dei dati oggetto del progetto di IA nell'uso del carrello elevatore analizzando l'intero ciclo di "vita" dei dati ovvero: i dati generati, tracciati dal sistema IA e i dati successivamente elaborati e conservati nel sistema informatico aziendale.

Si precisa che l'analisi ha interessato sia il **"dato personale**" (**ex art. 4 GDPR 679/2016** <<*dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*>>) che **il concetto più ampio di dato presente nella Direttiva NIS 2** la quale si riferisce ai dati principalmente come informazioni elaborate, trasmesse o archiviate da sistemi di rete e informatici (*Es. Dati personali (secondo il GDPR) Dati aziendali e commerciali; Dati operativi dei servizi essenziali; Informazioni di sistema e di configurazione*.).

Inoltre l'analisi ha preso in esame anche i devices impiegati nell'uso del presente sistema di innovazione tecnologica.

ESECUZIONE DELLE FASI METODOLOGICHE

Nella Tabella sottostante **(Tab_01)** sono **riportate le tipologie di dati** oggetto della mappatura.

Tab_01

Piattaforma IA Tipologia di Dati	Sistema Informatico Aziendale Tipologia di Dati
Immagini (sagome di persone e/o autoveicolo o merce). Id operatori. Log di eventi di rischio (data, ora, posizione, allarme). Dati di telemetria del carrello (velocità, traiettoria, frenate).	Nome e cognome lavoratore Account email Dati dei lavoratori derivanti dalle procedure in materia di sicurezza sul lavoro.

ESECUZIONE DELLE FASI METODOLOGICHE

Threat Modeling

In questa fase vengono identificati i potenziali vettori di attacco e gli attori malevoli che potrebbero colpire il sistema andando a ledere l'integrità, la disponibilità e la riservatezza dei dati.

Nella presente analisi i potenziali fattori di rischio sono stati individuati per ogni "area di intervento" ovvero:

- **Cybersecurity**
- **Privacy**
- **IA**
- **Etica**

ESECUZIONE DELLE FASI METODOLOGICHE

Cybersecurity

Tipologia di minaccia	Descrizione	Rischio
Spoofing	- uso di account condivisi o credenziali deboli in piattaforma. -falsificazione delle coordinate di localizzazione del carrello o del lavoratore (attacco al segnale).	Uso fraudolento del carrello senza autorizzazione. Mancato rallentamento del carrello in presenza di persone/ostacoli; creazione di falsi report; perdita di integrità dei dati causata dalla manipolazione.
Denial of Service	Jamming Interruzione/disturbo delle comunicazioni Wi-Fi; Radar; GSM	Non funzionamento del sistema di rallentamento, di riconoscimento di persone e/o cose e mancato e/o non preciso funzionamento degli alert con aumento della probabilità di incidenti e infortuni.

ESECUZIONE DELLE FASI METODOLOGICHE

Cybersecurity

Tipologia di minaccia	Descrizione	Rischio
Information Disclosure	Accesso non autorizzato ai dati.	Dati che possono essere acquisiti da soggetti non legittimati; rischio di malware e compromissione della sicurezza e riservatezza dell'organizzazione aziendale.
Manomissione	Alterazione dei log. Perdita di protezione dei dati.	Il sistema non rileva più i pedoni generando il rischio di incidenti. Rischio di perdita di integrità dei firmware. Alterazione e/o cancellazione di file aziendali che, oltre alla violazione della riservatezza, possono determinare un danno reputazionale all'azienda.

ESECUZIONE DELLE FASI METODOLOGICHE

Cybersecurity

Tipologia di minaccia	Descrizione	Rischio
Data Poisoning	L'iniezione di dati errati o falsi durante l'addestramento del modello compromette le prestazioni dell'AI	Aggiungere foto di scaffali, manichini o cartoni etichettati come "pedone" → l'AI impara a confondere oggetti con persone, generando falsi positivi.
Automation Bias	Eccessivo affidamento al sistema	Riduzione della vigilanza con il rischio di compiere azioni pericolose e rischiose.

ESECUZIONE DELLE FASI METODOLOGICHE

Cybersecurity

Tipologia di minaccia	Descrizione	Rischio
Errore Umano	Gestione inadeguata delle credenziali. Errori di configurazione.	Rischio di compromissione dei dati. Aumento della vulnerabilità dell'intero sistema con rischio di creare situazioni di non-sicurezza. Rischio di interruzione dell'operatività.

ESECUZIONE DELLE FASI METODOLOGICHE

Privacy

Tipologia di minaccia	Descrizione	Rischio
Accessi non autorizzati	-Violazioni della rete aziendale. -Violazione del profilo di utente. -Abuso interno dei dati.	Estrapolazione dei dati con impatto sulla privacy della persona-lavoratore e sulla riservatezza dell'organizzazione aziendale. Manipolazione del corretto funzionamento del sistema.

ESECUZIONE DELLE FASI METODOLOGICHE

Privacy

Tipologia	Descrizione	Rischio
Perdita dell'integrità dei dati	**-**Virus e/o malware. - Assenza di Piano di Business Continuity. -Manomissione dei log di sicurezza.	Blocco del sistema informatico aziendale. - Perdita dei dati per assenza di corrette procedure di back up con potenziale esposizione a danni per la tutela dell'azienda e della sua reputazione. - Un attacco informatico altera i registri che tracciano i movimenti del carrello e le rilevazioni dei pedoni, impedendo la ricostruzione fedele di un incidente sul lavoro.

ESECUZIONE DELLE FASI METODOLOGICHE

Privacy

Tipologia	Descrizione	Rischio
Indisponibilità dei dati	Attacco ransware o cyber. Perdita di connettività.	I dati video e i log dei sensori vengono criptati, rendendo impossibile verificare la dinamica di un incidente sul lavoro. Sia il sistema IA che l'intero sistema informatico aziendale non funzionano e possono causare incidenti e/o infortuni nonché non corretto aggiornamento delle misure di sicurezza.

ESECUZIONE DELLE FASI METODOLOGICHE

Privacy

Tipologia	Descrizione	Rischio
Trasferimento in Paesi non compliant al GDPR	Aumento del rischio di perdita/diminuzione della sicurezza e della riservatezza.	I dati sono fonte di acquisizione e di divulgazione con conseguenze anche gravi per la tutela della riservatezza della Persona-Lavoratore e della Governance Aziendale. Responsabilità per eventuali danni nei confronti di Terze Parti.

ESECUZIONE DELLE FASI METODOLOGICHE

Privacy

Tipologia	Descrizione	Rischio
Data retention eccessiva	Conservazione dei dati in tempi non compliant con la finalità e la necessità di trattamento.	Aumento del rischio che i dati possano formare oggetto di Data Breach con conseguente rischio di diffusione illecita dei dati.

Tipologia	Descrizione	Rischio
Disclosure of information	Esposizione dei Log a soggetti non autorizzati. Esfiltrazione di dati.	Un tecnico esterno che effettua manutenzione accede ai log dei carrelli, dove sono registrati orari, percorsi, identità dell'operatore e situazioni di quasi-incidente. A seguito di un attacco malevolo vengono compromessi ed acquisiti dati aziendali sia quelli relativi alla soluzione tecnologica che quelli collegati e conservati nel sistema informatico aziendale. Questo scenario causa rischi sia per la sicurezza e la salute dei lavoratori che per la tutela dei diritti della persona-lavoratore.

ESECUZIONE DELLE FASI METODOLOGICHE

Privacy

Tipologia	Descrizione	Rischio
Unawareness	Mancanza di conoscenza e responsabilizzazione nelle operazioni di trattamento dei dati personali.	Report non veritieri Comunicazione dei dati sensibili a soggetti non autorizzati. Aumento dei pericoli e degli incidenti e degli infortuni. Divulgazione dei dati in canali pubblici (Esempio: pagine social, Whatsapp e altri strumenti di comunicazione digitale e mediatica).

Tipologia	Descrizione	Rischio
Trattamento eccessivo di dati	Trattamento e conservazione dei dati non limitato a quelli necessari e per scopi ulteriori rispetto a quelli dichiarati nel progetto di innovazione.	Lavoratore esposto a sorveglianza continua da parte del Datore di Lavoro con violazione dei suoi diritti.

ESECUZIONE DELLE FASI METODOLOGICHE

Privacy

Tipologia	Descrizione	Rischio
Errore Umano	Invio errato di dati. Mancata attuazione delle policies aziendali.	Comunicazione di dati sulla sicurezza e salute dei lavoratori e/o sui clienti aziendali a soggetti non legittimati. Rischio di creare scenari di pericolo per la salute dei lavoratori. Ipotesi di Data Breach . Aumento della probabilità per l'azienda di essere esposta a procedimenti giudiziari e a sanzioni.

ESECUZIONE DELLE FASI METODOLOGICHE

Intelligenza Artificiale

Tipologia	Descrizione	Rischio
Bias Algoritmico	Training Dataset diversificato e senza validazione periodica	Il sistema IA potrebbe riconoscere meglio alcune situazioni (es. pedoni in movimento) e peggio altre (pedoni fermi o con abbigliamento riflettente), aumentando i falsi negativi.

Tipologia	Descrizione	Rischio
Overfitting del modello	Addestramento limitato solo a set di dati già visti.	L'AI è addestrata su scenari limitati e non riconosce correttamente situazioni reali (scaffali stretti, luci basse, nebbia).

ESECUZIONE DELLE FASI METODOLOGICHE

Intelligenza Artificiale

Tipologia	Descrizione	Rischio
Manipolazione	Manipolazione sugli indumenti. Manipolazione ambientale.	Adesivi con colori particolari che possono non far riconoscere il pedone come "persona". Adesivi posizionati in punti strategici (a livello pavimento o scaffali) possono generare falsi positivi/negativi, facendo confondere il sistema tra oggetti e persone.

ESECUZIONE DELLE FASI METODOLOGICHE

Intelligenza Artificiale

Tipologia	Descrizione	Rischio
Errore Umano	Interpretazione errata degli output dell'IA da parte degli operatori, con conseguenti decisioni sbagliate. Data poisoning involontario: introduzione di dati incompleti, errati o non rappresentativi durante il training del modello. Errata configurazione dei sensori.	Rischio di non funzionamento corretto dei sistemi di sicurezza e di alert. Perdita dell'accountability.

ESECUZIONE DELLE FASI METODOLOGICHE

Etica

Tipologia	Descrizione	Rischio
Discriminazione e bias	Sistema addestrato con informazioni contenenti principi discriminatori.	Mancato rilevamento di alcuni operatori (ad esempio donne; ragazzi ecc). Aumento del rischio di non conformità e creazione di uno scenario di pericolo per la salute dei lavoratori. Generazione di scenari palesemente lesivi della persona in quanto discriminatori.

ESECUZIONE DELLE FASI METODOLOGICHE

Etica

Tipologia	Descrizione	Rischio
Automation Bias	Eccessivo affidamento ai sensori del sistema di Intelligenza Artificiale.	Operatore diminuisce la sua responsabilità di controllo e di attenzione con conseguente pericolo di generare incidenti e/o infortuni.

Tipologia	Descrizione	Rischio
Mancanza di Trasparenza (Principio etico dell'Esplicabilità)	Funzionamento e raccolta dei dati da parte del sistema in maniera poco chiara e comprensibile.	Il lavoratore inizia a percepire sfiducia e impossibilità di difesa dei suoi diritti generando un'ipotesi di Stress da Lavoro Correlato (Es Burnout).

ESECUZIONE DELLE FASI METODOLOGICHE

Etica

Tipologia	Descrizione	Rischio
Accountability opaca	Mancanza di chiarezza delle responsabilità in caso di incidente, di infortunio e/o di eventuale criticità.	Gestione delle responsabilità non corretta rispetto al ruolo e in contrasto con il Codice Etico e MOG231 con conseguente esposizione all'applicazione di non corretti provvedimenti disciplinari o contestazioni contrattuali.

Tipologia	Descrizione	Rischio
Bias Inclusivo	Il sistema non considera specifiche esigenze del lavoratore (disabilità, barriere linguistiche).	Aumento dei rischi per la salute dei lavoratori sia sotto il profilo dell'integrità fisica che sotto il profilo psico-sociale.

VALUTAZIONE DEL RISCHIO (Formula)

VALUTAZIONE DEL RISCHIO (Formula)

Formula

R=P×G

- **P (Probabilità)** = la possibilità che un evento/minaccia si verifichi.
- **G (Gravità/Impatto)** = l'entità delle conseguenze che l'evento comporta, se si realizza.
- **R (Rischio)** = livello di rischio risultante dall'interazione tra probabilità e gravità.

- **SCALA DEI VALORI PER LA MISURAZIONE**

Valori di Probabilità (P) –scala 1-5

1 = Evento improbabile / remoto
2 = Poco probabile
3 = Possibile
4 = Probabile
5 = Molto probabile / frequente.

VALUTAZIONE DEL RISCHIO (Formula)

Formula

- **Valori di Gravità (G) – scala 1-5**

1 = Impatto trascurabile (dati non sensibili, nessun danno)
2 = Impatto lieve (ritardi, piccoli disservizi)
3 = Impatto medio (violazione di dati non critici, infortunio lieve)
4 = Impatto grave (violazione di dati sensibili, infortunio serio)
5 = Impatto molto grave/catastrofico (violazione massiva, morte o invalidità, sanzioni rilevanti)

- **RANGE DI RISCHIO**

· **1–5** → **Rischio Basso**: accettabile, monitoraggio semplice.
· **6–10** → **Rischio Medio**: richiede misure di mitigazione.
· **11–15** → **Rischio Alto**: intervento urgente, azioni correttive forti.
· **16–25** → **Rischio Critico**: non accettabile, sospensione attività finché mitigato.

MITIGAZIONE DEL RISCHIO

MITIGAZIONE DEL RISCHIO

Mitigazione del Rischio Cybersecurity

La seguente analisi descrive le misure di mitigazione essenziali per affrontare i rischi legati alla cyber-sicurezza, al GDPR, all'affidabilità dell'IA e alle implicazioni etiche che sono stati descritti nelle slide precedenti.

A) Mitigazione Rischio Cybersecurity

Crittografia End-to-End: Tutti i dati raccolti dal sistema, sia quelli in transito (trasmessi alla rete aziendale) che quelli a riposo (memorizzati su un server o sul dispositivo stesso), devono essere crittografati con protocolli robusti. Questo impedisce l'accesso non autorizzato ai dati sensibili e ai log operativi.

Segmentazione della Rete: La rete a cui è collegato il sistema del carrello elevatore deve essere isolata (segmentata) dalla rete principale dell'azienda. In questo modo, un'eventuale compromissione non si estende ad altri sistemi aziendali critici.

Autenticazione Forte: L'accesso ai pannelli di controllo del sistema e ai dati raccolti deve essere protetto con sistemi di autenticazione a più fattori, limitato solo al personale autorizzato. Per quanto attiene ai dati salvati nel sistema informatico aziendale, definizione delle permission dei soli soggetti designati e impiego di credenziali forte.

MITIGAZIONE DEL RISCHIO

Mitigazione del Rischio Cybersecurity

Gestione degli Aggiornamenti: Le vulnerabilità del software devono essere corrette con aggiornamenti regolari (patch). La gestione degli aggiornamenti deve essere automatizzata e monitorata per garantire che tutti i dispositivi siano protetti contro le minacce più recenti.

Piano Business Continuity: Predisposizione del documento specifico per l'individuazione delle minacce e per la loro "gestione" al fine di minimizzare gli impatti e garantire una costante attività di monitoraggio e conseguente attuazione di interventi migliorativi. Inoltre il Piano di Business Continuity permette all'azienda di avere la sua continuità lavorativa nel rispetto della normativa e per garantire la tutela della salute dei lavoratori.

Penetration Testing: per monitorare eventuali vulnerabilità e programmare azioni di contrasto.

Protocolli di comunicazione: Utilizzo di protocolli cifrati e impiego di certificati digitali come quelli HTTPS/TLS, per garantire l'autenticità di un server o di un utente.

Whistleblowing: Presenza di una piattaforma per le segnalazioni in conformità a quanto disposto dal D.Lgs. 24/2023.

MITIGAZIONE DEL RISCHIO

Mitigazione del Rischio Privacy

Modello di Organizzazione Privacy: Predisposizione del piano di definizione della data governance con ruoli e responsabilità, modalità e procedure operative per garantire la tutela dell'integrità, della sicurezza e disponibilità dei dati e il loro monitoraggio nel tempo.

Definizione delle permission per ogni utente: L'accesso al sistema informatico aziendale e alla piattaforma di Intelligenza Artificiale è impostato con regole distinte per i vari utenti in base alle funzioni svolte nell'esercizio della mansione e con User e Pwd individuali e di tipo forte e con policy di cambio in base alla periodicità definita dall'azienda.

Crittografia e Back up sicuri : Impostazione di Back Up conformi alle disposizioni di legge e al GDPR con dati che devono essere criptati sul server e ridondati.

Sistemi di protezione della rete e degli accessi: Adozione di un Firewall Perimetrale per proteggere il traffico da e verso IP e IDS/IPS integrati per rilevare intrusioni; inoltre adozione di un Firewall interno al fine di impedire che un potenziale attacco possa diventare una minaccia anche per altre aree aziendali.

Penetration Testing: per monitorare eventuali vulnerabilità e programmare azioni di contrasto.

MITIGAZIONE DEL RISCHIO

Mitigazione del Rischio Privacy

Antivirus e Antimalware: Presenza di Antivirus e Antimalware in costante aggiornamento sia nel server che nei client per garantire una protezione ai dati elaborati, organizzati, conservati nel sistema informatico aziendale.

Definizione dei ruoli privacy: Predisposizione dell'Organigramma Privacy e delle nomine sia per i soggetti autorizzati alle attività di trattamento dei dati in maniera da stabilire gli ambiti di azione e di responsabilità dei medesimi che per le Terze Parti esterne identificate quali Responsabili del Trattamento ai sensi dell'art. 28 GDPR.

Definizione di Policy: Al fine di garantire la riservatezza dei dati dei lavoratori si procede con la predisposizione di policy interne che stabiliscono il divieto di utilizzare e raccogliere dati eccessivi e non conformi alle finalità del trattamento.

Limitazione della Conservazione: Impostazione dei tempi di conservazione dei log non superiore ai 30 giorni; impostazione dei tempi di conservazione delle altre tipologie di dati in conformità alle disposizioni normative; in particolare si cita la normativa lavoro e la normativa in materia di sicurezza sul lavoro.

MITIGAZIONE DEL RISCHIO

Mitigazione del Rischio Privacy

Gestione dei Fornitori: Al fine di ridurre i rischi che possono essere causati da Terze Parti è necessario procedere alla nomina quale Responsabile del Trattamento; verificare l'eventuale possesso di Certificazioni (ad esempio ISO 27001); inserimento nell'accordo tra le parti, le clausole di conformità al GDPR ivi compresa le Clausole Contrattuali Standard (SCC).

Nomina di un Responsabile della Protezione dei Dati (DPO): Per garantire maggiormente l'efficacia del sistema privacy, si rende opportuna la nomina di un DPO seppur non rientrante nelle fattispecie di obbligo ai sensi del GDPR.

Protocolli di comunicazione: Utilizzo di protocolli cifrati e impiego di certificati digitali come quelli HTTPS/TLS, per garantire l'autenticità di un server o di un utente. Inoltre lo scambio di comunicazione sia interna che verso l'esterno, è basato sull'uso degli account di posta elettronica aziendale.

Whistleblowing: Presenza di una piattaforma per le segnalazioni in conformità a quanto disposto dal D.Lgs. 24/2023.

MITIGAZIONE DEL RISCHIO

Mitigazione del Rischio Intelligenza Artificiale

Analisi preliminare della piattaforma: Verifica della documentazione tecnica rilasciata dal fornitore relativa alle caratteristiche del sistema e verifica dell'effettuazione di un test di robustezza & adversarial.

Qualità dei dati: Eliminazione di dati distorti o incompleti e controllo costante sui dati di addestramento al fine di prevenire il rischio di "*data poisoning".*

Human-in-the-loop Supervisione e sorveglianza costante da parte dei lavoratori.

Aggiornamento e manutenzione continua: Aggiornamenti firmware e modelli AI con patch di sicurezza; Revisione periodica degli algoritmi in base a nuove condizioni operative.

Sicurezza logica e cyber: Controllo accessi al modello e ai dati di addestramento. Crittografia dei dataset e dei parametri del modello.

MITIGAZIONE DEL RISCHIO

Mitigazione del Rischio Etica

Dataset Auditing: acquisizione e conservazione della documentazione del fornitore in cui vengono illustrate le caratteristiche della piattaforma IA al fine di prevenire sia il rischio di discriminazione ed accessibilità sia per documentare ogni intervento migliorativo.

Trasparenza e Spiegabilità (Explainable AI): il sistema deve essere progettato in maniera da fornire le informazioni agli operatori sulle modalità di funzionamento, sulla tipologia di raccolta dei dati, per quanto tempo e chi sono i soggetti autorizzati all'accesso.

Tracciabilità: il sistema deve tenere traccia della storicità degli input e dei prompt utilizzati al fine di poter effettuare eventuali verifiche.

Politica di intervento umano: il sistema prevede la possibilità che l'operatore possa intervenire.

Soglie di azione progressive: il sistema è impostato con logiche calibrate per evitare reazioni automatiche eccessive.

MITIGAZIONE DEL RISCHIO

Mitigazione del Rischio Etica

Coinvolgimento dei lavoratori: Pianificazione di riunioni con i lavoratori coinvolti nel progetto insieme ai soggetti responsabili per la sicurezza sul lavoro (RSPP, Preposti).

Policy e Codice Etico: Predisposizione di Policy specifiche relative al rispetto dei principi etici e dei diritti della persona nell'uso di tale nuovo processo tecnologico e contestuale aggiornamento del Codice Etico attuato in azienda.

Whistleblowing: Presenza di una piattaforma per le segnalazioni in conformità a quanto disposto dal D.Lgs. 24/2023.

MITIGAZIONE DEL RISCHIO

L’importanza della Formazione

La formazione rappresenta **l’elemento comune a tutte le “aree di intervento**” nonché un obbligo di conformità alle disposizioni normative. Il concetto di formazione deve essere inteso nella sua accezione più ampia che comprende non soltanto **l’apprendimento di concetti e di modalità operative (alfabetizzazione del sistema), ma anche il valore critico e consapevole dell’uso delle tecnologie**.

Questa dimensione, che è contenuta anche nel IA ACT, rappresenta un grande valore aggiunto in quanto permette all’azienda di garantire la tutela dei diritti dei lavoratori e la tutela della loro sicurezza conferendo agli stessi una crescita delle competenze; inoltre la formazione che è sinonimo di consapevolezza e responsabilizzazione (awarness), svolge una funzione di prevenzione dei rischi, di aumento della fiducia del lavoratore nonché è esempio di compliance ai principi di responsabilità sociale di impresa.

Infatti senza un’adeguata formazione, anche le migliori soluzioni tecniche rischiano di perdere efficacia, di essere mal utilizzate o addirittura di trasformarsi in nuove fonti di vulnerabilità.

L’efficacia di un sistema di innovazione tecnologica deve basarsi anche sulla formazione di tutti gli “attori” del processo e deve essere strutturata in maniera trasversale ovvero prevedere i contenuti di natura tecnica, di natura organizzativa e socio-culturale.

MONITORAGGIO

MONITORAGGIO

Monitoraggio

La pianificazione di un'attività continuativa di monitoraggio costituisce il focus point su cui si garantisce nel tempo l'efficacia, la resilienza e il rispetto dei diritti e dei doveri dell'intero progetto di innovazione tecnologica introdotto in azienda.

Si prevede l'attuazione di distinti livelli di monitoraggio rappresentati da:

a) **Verifiche interne sia di natura tecnica che organizzativa svolte dai soggetti responsabili**
b) **Audit esterni verso la società fornitrice della piattaforma IA.**
c) **Verifiche svolte dall'Organismo di Vigilanza.**

Il monitoraggio deve servire a proteggere, non a controllare.

CONCLUSIONE

CONCLUSIONE

Conclusione

Questo progetto rappresenta la nuova "sfida" metodologica di gestione ed organizzazione che oggi e sempre di più l'azienda è chiamata a svolgere di fronte all'implementazione delle tecnologie nel modus operandi aziendale.

Gli scenari del business hanno tracciato le direttive da seguire dove l'elemento digitale è uno dei fattori principali; pertanto è fondamentale iniziare a recepire il cambiamento e a comprenderne i valori positivi e i valori negativi per strutturare le idonee politiche di tutela e di crescita.

Si parla di era della "*datificazione*", si parla altresì di "*Nuova Rivoluzione Industriale*", sicuramente si può affermare che siamo di fronte ad un **cambio di paradigma organizzativo**, dove la tecnologia diventa parte integrante del sistema di governance e deve essere accompagnata da regole, procedure, ruoli e responsabilità adeguati unitamente ad un approccio proattivo e resiliente.

Ci sono molte sfide aperte da affrontare e risolvere:

- quelle relative alla definizione delle "responsabilità" nell'impiego dell'Intelligenza Artificiale;
- quelle derivanti dal crescere dei cyber risk che costituiscono fattori di crisi di impresa;
- quelle sociali che impattano sul comportamento dell'uomo e sulla sua sfera psicologica.

CONCLUSIONE

Il nuovo Modello Organizzativo deve fondarsi su una **cultura aziendale digitale** dove la formazione continua, la sensibilizzazione etica, la condivisione delle buone pratiche e il coinvolgimento di tutti i livelli gerarchici sono strumenti indispensabili per trasformare la tecnologia da potenziale rischio a leva di crescita sostenibile.

Inoltre è importante creare dei Team di lavoro formati da figure professionali dotate di competenze specifiche in quanto ogni sistema è caratterizzato da elementi diversi, ma trasversali e integrati tra loro.

A tal proposito il presente Case Study mette in evidenza l'inscindibile binomio **tra "Sicurezza" e "Safety"** contenuto anche nella Direttiva NIS2 (UE 2022/2555); infatti la convergenza di sistemi fisici e digitali (OT/IT integration, IoT, AI applicata alla logistica o alla manifattura) fa sì che i confini tra security e safety si sovrappongano. Pertanto, l'approccio moderno alla cybersecurity deve considerare la protezione integrata: non solo difesa dei dati, ma anche salvaguardia delle vite umane e dell'ambiente.

In conclusione, l'impatto delle nuove tecnologie sulle procedure lavorative non si esaurisce nell'ambito tecnico, ma investe dimensioni **giuridiche, sociali ed etiche**, richiedendo un ripensamento complessivo della responsabilità d'impresa. Solo attraverso un approccio integrato, che bilanci innovazione, sicurezza e rispetto dei diritti fondamentali, sarà possibile trasformare le nuove tecnologie da potenziale fonte di rischio a reale motore di progresso per la salute e la sicurezza dei lavoratori.