POLITICA AZIENDALE - POLITICA DELLA QUALITÀ, DELLA SICUREZZA DELLE INFORMAZIONI E DELLA SICUREZZA INFORMATICA

La politica aziendale

Corley S.r.l. ha adottato un sistema di gestione per la Qualità e per la Sicurezza delle Informazioni conforme ai requisiti delle norme **UNI EN ISO 9001:2015** e **ISO/IEC 27001:2022**, con l'applicazione delle linee guida **ISO/IEC 27017:2015** e **ISO/IEC 27018:2019**. Il sistema comprende la sicurezza informatica dei sistemi informativi e di rete e integra gli obblighi derivanti dal D.Lgs. 138/2024 (recepimento della Direttiva UE 2022/2555 – NIS2), che si applica a Corley in quanto soggetto incluso nell'elenco dei soggetti NIS, e dal Regolamento UE 2016/679 (GDPR) in materia di protezione dei dati personali. Tale approccio evidenzia la consapevolezza dell'Organizzazione rispetto alla necessità di garantire la qualità dei servizi erogati e di tutelare i propri asset informativi e quelli dei clienti, assicurandone protezione, riservatezza, integrità, disponibilità e autenticità.

L'Organizzazione ha dimostrato di aver analizzato il proprio contesto operativo e di aver identificato le parti interessate, considerando le loro esigenze e aspettative. Ha inoltre effettuato una valutazione dei rischi e delle opportunità strategiche, elementi che risultano fondamentali per definire, implementare e migliorare il Sistema di Gestione Integrato (SGI).

La Direzione si è formalmente impegnata affinché la politica aziendale sia coerente con gli scopi dell'Organizzazione, supporti il miglioramento continuo dell'efficacia e dell'efficienza dei processi aziendali e garantisca il rispetto delle prescrizioni legali applicabili.

Questo approccio, basato su standard internazionalmente riconosciuti, rappresenta un fattore di garanzia e trasparenza, nonché un elemento chiave per il raggiungimento della soddisfazione delle parti interessate, dirette e indirette.

Scopi e obiettivi

La Direzione di Corley S.r.l. ha definito, divulgato e si impegna a mantenere attiva e operativa, a tutti i livelli dell'Organizzazione, la politica per la Gestione della Qualità, della Sicurezza delle Informazioni e della Sicurezza Informatica. Tale politica è stata concepita per garantire la massima soddisfazione del cliente e per tutelare le informazioni aziendali contro minacce interne ed esterne, intenzionali o accidentali, in conformità alla norma **ISO/IEC 27001:2022** e al D.Lgs. 138/2024 (NIS2).

Corley S.r.l. si impegna a perseguire obiettivi specifici, coerenti con la politica adottata, che includono:

1. **Conformità normativa:** rispetto rigoroso delle leggi e dei regolamenti applicabili, nazionali e dell'Unione europea, tra cui il Regolamento UE 2016/679 (GDPR), il D.Lgs. 196/2003, il D.Lgs. 138/2024 (NIS2) con le determinazioni dell'Agenzia per la Cybersicurezza Nazionale (ACN) e il Regolamento UE 2024/1689 sull'intelligenza artificiale.
2. **Protezione dei dati personali:** trattamento dei dati personali nel rispetto dei principi del GDPR e della protezione dei dati fin dalla progettazione e per impostazione predefinita, sia quando Corley agisce come titolare del trattamento sia quando tratta dati per conto dei clienti come responsabile, sulla base di contratti ex art. 28 GDPR e delle istruzioni documentate del titolare; garanzia dell'esercizio dei diritti degli interessati; designazione di un Responsabile della protezione dei dati (DPO).
3. **Comunicazione con le parti interessate:** attivazione di canali di comunicazione interni ed esterni per favorire uno scambio continuo e costruttivo.

4. **Sicurezza delle informazioni e sicurezza informatica:** protezione dei dati, dei sistemi informativi e di rete e degli asset informativi di Corley e dei clienti, considerati beni di valore strategico, al fine di garantire la continuità del business e dei servizi erogati, e ottimizzare il ritorno sugli investimenti e le opportunità commerciali.
5. **Misure tecniche e organizzative:** implementazione di misure, proporzionate ai rischi e allo stato dell'arte e in linea con le misure di sicurezza definite dall'ACN, volte a garantire la riservatezza, l'integrità, la disponibilità e l'autenticità delle informazioni gestite.
6. **Miglioramento continuo:** definizione di obiettivi per il miglioramento delle prestazioni in termini di qualità e sicurezza delle informazioni.
7. **Coinvolgimento del personale:** promozione di attività di formazione, informazione e sensibilizzazione per rendere tutto il personale, compresi gli organi di amministrazione, consapevole delle proprie responsabilità e del contributo individuale al raggiungimento degli obiettivi aziendali.
8. **Sviluppo professionale:** mantenimento di un alto livello professionale tra dipendenti, collaboratori e professionisti, riconoscendo l'importanza del fattore umano come elemento differenziante.
9. **Gestione degli incidenti di sicurezza e delle violazioni di dati personali:** riduzione del rischio di incidenti e gestione degli eventi secondo la Procedura di gestione degli incidenti di sicurezza e dei data breach, che comprende rilevazione, contenimento, analisi, ripristino, notifica nei termini di legge al CSIRT Italia e al Garante per la protezione dei dati personali, comunicazione ai clienti e agli interessati e analisi post-incidente.
10. **Diffusione della cultura informatica:** promozione di conoscenze e competenze tecnologiche per creare consapevolezza e identità informatica nel territorio attraverso metodologie innovative e strumenti avanzati.
11. **Coinvolgimento dei fornitori e sicurezza della catena di approvvigionamento:** selezione e monitoraggio dei fornitori anche in base alla sicurezza dei loro prodotti, servizi e pratiche; definizione nei contratti di requisiti di sicurezza e obblighi di segnalazione degli incidenti e, quando trattano dati personali per conto di Corley, stipula di contratti ex art. 28 GDPR; invito ai fornitori a implementare un sistema di gestione qualità e sicurezza delle informazioni allineato agli standard aziendali.
12. **Protezione delle risorse aziendali:** adozione di misure precauzionali proporzionate, percepite come strumenti abilitanti e non come vincoli, per supportare la missione aziendale.
13. **Uso responsabile dell'intelligenza artificiale:** utilizzo dei sistemi di IA secondo la Policy sull'uso dei sistemi di intelligenza artificiale (Mod. 6-M), esclusivamente con strumenti autorizzati e senza inserire dati dei clienti o dati personali in strumenti non approvati, e formazione del personale sull'uso consapevole dell'IA.
14. **Salute e sicurezza sul lavoro:** sensibilizzazione del personale interno ed esterno al rispetto delle procedure aziendali per garantire sicurezza, salute e benessere nei luoghi di lavoro, in conformità alle normative vigenti.

La Direzione conferma il proprio impegno a mantenere, monitorare e migliorare continuamente il Sistema di Gestione Integrato, con l'obiettivo di rispondere alle aspettative delle parti interessate e garantire la piena conformità ai requisiti normativi e agli standard di riferimento.

Tutto quanto sopra descritto permette a Corley S.r.l. di continuare a distinguersi come Innovation Partner, progettando, integrando e sviluppando architetture e applicazioni innovative utilizzando i servizi AWS, restando sempre un passo avanti a livello di sicurezza e innovazione, con l'obiettivo di garantire ai propri clienti l'eccellenza in ambito cloud AWS.

"La nostra Visione: Diventare il punto di riferimento nel panorama della consulenza informatica inerente le tecnologie Cloud AWS, guidando la trasformazione digitale delle aziende attraverso soluzioni tecnologiche innovative, sicure e sostenibili."

"La nostra Missione: fornire soluzioni informatiche innovative, affidabili e personalizzate, garantendo la massima qualità dei servizi offerti, per supportare i nostri clienti nel raggiungimento dei loro obiettivi strategici e tecnologici. Ci impegniamo a sviluppare relazioni di fiducia con i nostri clienti e a promuovere una cultura aziendale orientata al miglioramento continuo."

"I nostri Valori: Corley è prima di tutto un'azienda fatta di persone, obiettivi e passione. Sostenibilità, Divulgazione, Formazione, Passione per il Cloud, Customer Obsession, Innovazione, Supporto allo studio, Crescita professionale,

Approccio ibrido e Ricerca, sono i nostri 10 punti fermi."

Campo di applicazione

La presente politica è applicabile in modo uniforme a tutti gli organi e livelli dell'Azienda, senza alcuna distinzione. La sua attuazione è considerata obbligatoria per tutto il personale aziendale ed è integrata negli accordi stipulati con soggetti esterni che, in qualsiasi forma, risultino coinvolti nel trattamento di informazioni rientranti nel campo di applicazione del Sistema di Gestione Integrato.

Tutte le figure professionali presenti all'interno della struttura organizzativa, indipendentemente dalle responsabilità specifiche loro assegnate, svolgono un ruolo cruciale nel raggiungimento degli obiettivi legati alla qualità e alla sicurezza delle informazioni. Di conseguenza, l'effettiva applicazione dei Sistemi di Gestione richiede il coinvolgimento attivo, l'impegno e l'interazione efficace di tutte le funzioni aziendali.

L'impegno collettivo del personale, a ogni livello, è considerato essenziale per garantire il rispetto della politica e il conseguimento dei risultati attesi, in linea con gli standard ISO di riferimento.

Politica specifica qualità

Per Corley S.r.l., la Qualità rappresenta sia un obiettivo strategico che uno strumento fondamentale per:

- Promuovere, rispettare e tutelare la Sicurezza e la Privacy.
- Raggiungere l'eccellenza nei risultati aziendali.
- Garantire il soddisfacimento delle esigenze del Cliente, sia interno che esterno.
- Valutare in modo corretto e sistematico i rischi e le opportunità.
- Effettuare un'analisi puntuale e accurata del contesto in cui opera l'Organizzazione.
- Ridurre al minimo gli sprechi in termini di tempo, costi e risorse.

Corley S.r.l. si impegna a perseguire questi obiettivi attraverso:

- **Un'Organizzazione efficace**, orientata alla prevenzione delle non conformità.
- **Un impegno costante nel miglioramento continuo**, con particolare attenzione all'efficacia del Sistema di Gestione della Qualità e della Sicurezza delle Informazioni.
- **Un servizio di qualità**, che garantisca una risposta rapida e professionale alle richieste dei Clienti, bilanciando Qualità ed efficienza.

Gli obiettivi specifici in ambito qualità includono:

1. **Rispetto dei livelli di servizio**: monitorare costantemente il rispetto dei livelli di servizio definiti nei contratti e perseguire il miglioramento continuo attraverso l'adozione di best practices aziendali.

   In linea con l'obiettivo di garantire la massima soddisfazione del Cliente e rafforzare il proprio ruolo di Innovation Partner specializzato in tecnologie AWS, Corley S.r.l. offre un approccio flessibile alla gestione dei Livelli di Servizio (SLA). L'Organizzazione mette a disposizione dei clienti la propria competenza avanzata in due modalità principali:

   A. *Consulenza Strategica sugli SLA*: In qualità di partner ufficiale AWS, Corley S.r.l. fornisce consulenza specialistica per supportare il cliente nell'identificazione, definizione e gestione ottimale dei Livelli di Servizio relativi alle proprie architetture e applicazioni basate sui servizi Cloud AWS.

B. *Delega della Gestione SLA:* Per i clienti che attivano specifici contratti di supporto, Corley S.r.l. offre la possibilità di delegare la gestione operativa dell'infrastruttura AWS. In tale configurazione, Corley S.r.l. assume la responsabilità del monitoraggio e dell'intervento proattivo e reattivo, implementando le azioni necessarie per il raggiungimento degli obiettivi di performance e disponibilità (SLA) definiti con il cliente. Gli specifici SLA contrattualizzati con il cliente rappresenteranno un SLA composito, che si fonda su due pilastri:

- Gli SLA nativi forniti da Amazon Web Services per i singoli servizi utilizzati (SLA del fornitore cloud).
- I tempi di presa in carico e intervento garantiti da Corley S.r.l. (SLA di supporto).

Corley S.r.l. si impegna inoltre a gestire l'ambiente AWS del cliente seguendo le best practice atte a massimizzare la resilienza e a supportare il cliente nelle eventuali procedure di richiesta di credito di servizio (Service Credit) verso AWS, qualora lo SLA del fornitore non fosse rispettato.

2. **Riduzione delle non conformità**: mantenere elevati gli standard qualitativi nell'erogazione dei servizi, assicurando il rispetto rigoroso delle specifiche contrattuali sottoscritte con i clienti.
3. **Formazione continua del personale**: garantire che tutto il personale sia adeguatamente formato rispetto alle attività operative, alle normative vigenti (sicurezza, privacy, ecc.) e ai sistemi di gestione aziendale. L'Organizzazione promuove una piena consapevolezza delle problematiche relative alla sicurezza delle informazioni, coinvolgendo dipendenti e collaboratori fin dal momento della selezione e per tutta la durata del rapporto di lavoro.
4. **Manutenzione di luoghi di lavoro, attrezzature, mezzi e infrastrutture**: assicurare che gli asset aziendali siano catalogati correttamente, che le manutenzioni periodiche siano programmate e puntualmente eseguite.

Corley S.r.l. dimostra così un impegno tangibile verso il miglioramento continuo della qualità, garantendo la soddisfazione del Cliente e la conformità agli standard di riferimento.

Politica specifica sicurezza delle informazioni e sicurezza informatica

Il patrimonio informativo di Corley S.r.l., composto dall'insieme delle informazioni gestite e dai sistemi informativi e di rete che le trattano, compresi quelli gestiti per conto dei clienti, è oggetto di tutela attraverso un approccio sistematico alla sicurezza delle informazioni e alla sicurezza informatica.

Principi fondamentali per la sicurezza delle informazioni

1. **Riservatezza:** le informazioni sono accessibili esclusivamente al personale autorizzato.
2. **Integrità:** la precisione e la completezza delle informazioni e dei metodi utilizzati per la loro elaborazione sono protetti.
3. **Disponibilità:** gli utenti autorizzati accedono alle informazioni e agli asset correlati ogniqualvolta necessario.
4. **Autenticità:** è garantita l'affidabilità dell'origine delle informazioni e dell'identità degli utenti e dei sistemi che vi accedono.

La mancanza di adeguati livelli di sicurezza può causare gravi conseguenze, tra cui danni alla reputazione aziendale, insoddisfazione dei clienti, rischio di sanzioni legali e perdite economiche. Un livello appropriato di sicurezza è essenziale anche per una condivisione sicura e affidabile delle informazioni.

Gestione del rischio e azioni di mitigazione

L'azienda identifica e valuta i rischi associati ai propri asset aziendali attraverso un'analisi sistematica, che consente di comprendere il livello di esposizione a minacce potenziali. La valutazione del rischio, aggiornata periodicamente, permette di definire le misure di sicurezza necessarie e le azioni più idonee per mitigare i rischi identificati.

Principi guida per la gestione della sicurezza delle informazioni

1. **Accesso sicuro ai sistemi:** tutti gli accessi sono regolati da procedure di identificazione e autenticazione, con autorizzazioni differenziate per ruolo e compiti e con autenticazione a più fattori per gli accessi privilegiati e da remoto, secondo quanto definito nelle procedure. Le autorizzazioni sono periodicamente riesaminate.
2. **Utilizzo sicuro dei beni aziendali:** sono definite procedure specifiche per l'uso sicuro degli asset aziendali, inclusi sistemi e informazioni.
3. **Asset inventory aggiornato:** è mantenuto un catalogo sempre aggiornato degli asset aziendali, identificando per ciascuno un responsabile e classificandoli in base al livello di criticità per garantire la loro gestione con criteri di riservatezza e integrità adeguati.
4. **Valutazione periodica dei rischi:** l'analisi dei rischi è rivista almeno una volta all'anno, durante il riesame della Direzione, o in seguito a eventi avversi o aggiornamenti degli asset.
5. **Gestione tempestiva di eventi avversi:** ogni evento o incidente di sicurezza, anche solo sospetto, è segnalato immediatamente e gestito secondo la Procedura di gestione degli incidenti di sicurezza e dei data breach, per minimizzare i danni, ripristinare la normalità operativa nel minor tempo possibile e adempiere agli obblighi di notifica.
6. **Protezione fisica delle sedi:** è necessario prevenire accessi non autorizzati alle strutture aziendali e garantire la sicurezza delle apparecchiature.
7. **Formazione continua del personale:** tutti i dipendenti e collaboratori ricevono formazione continua sulle normative (sicurezza, privacy, ecc.) e sui sistemi di gestione, acquisendo piena consapevolezza delle problematiche legate alla sicurezza delle informazioni.
8. **Compliance contrattuale con terze parti:** tutti i contratti con terze parti rispettano i requisiti legali e i principi di sicurezza delle informazioni; Corley si impegna a regolare con contratti ex art. 28 GDPR tutti i rapporti nei quali tratta dati personali per conto dei clienti.
9. **Continuità operativa e disaster recovery:** è predisposto un piano di continuità operativa e di disaster recovery, con backup periodicamente verificati, per affrontare eventi imprevisti e garantire il ripristino dei servizi critici in tempi ragionevoli; il piano è sottoposto a test periodici.
10. **Sicurezza informatica by design:** la sicurezza è integrata in ogni fase del ciclo di vita dei sistemi e dei servizi, dalla progettazione alla dismissione.
11. **Gestione delle vulnerabilità e monitoraggio:** i sistemi sono mantenuti aggiornati, le vulnerabilità sono individuate e corrette in base alla loro criticità, gli eventi di sicurezza sono monitorati e i log sono conservati per il tempo necessario ad accertare eventuali incidenti e, per gli accessi degli amministratori di sistema, per almeno sei mesi.
12. **Aggiornamento legislativo continuo:** l'azienda garantisce il rispetto di tutte le normative applicabili, minimizzando il rischio di sanzioni legali o danni reputazionali.
13. **Conformità NIS2** – Adottare le misure di sicurezza di base previste dalla Determinazione ACN n. 379907/2025 secondo il piano di adeguamento (Mod. 6-N) e garantire la notifica degli incidenti significativi al CSIRT Italia nei termini di legge.
14. **Gestione delle crisi** – Garantire una risposta coordinata agli eventi più gravi tramite il Comitato di crisi e la Procedura di gestione delle crisi aziendali, verificata con esercitazioni documentate.
15. **Sicurezza della catena di approvvigionamento** – Qualificare e monitorare i fornitori anche sotto il profilo della sicurezza (Mod. 8-F, Mod. 8-V), con priorità ai fornitori critici.
16. **Uso responsabile dell'Intelligenza Artificiale** – Utilizzare solo gli strumenti di IA autorizzati e alfabetizzare il personale, secondo la Policy sull'uso dei sistemi di IA (Mod. 6-M) e l'AI Act.

Con l'applicazione di questi principi e misure, Corley S.r.l. dimostra il proprio impegno nel mantenere i più alti standard di sicurezza delle informazioni, contribuendo a proteggere i dati aziendali e soddisfare le aspettative di clienti e stakeholder.

Responsabilità di osservanza e attuazione

L'attuazione delle policy aziendali e il rispetto dei requisiti del Sistema di Gestione Integrato sono responsabilità condivise tra diverse categorie di soggetti, secondo i seguenti principi:

1. **Personale interno**
    - Tutti i dipendenti e collaboratori che, a qualsiasi titolo, operano per l'Azienda e sono coinvolti nel trattamento di dati e informazioni all'interno del campo di applicazione del Sistema di Gestione Integrato, sono tenuti a rispettare le policy stabilite.
    - Il personale è altresì responsabile della tempestiva segnalazione di qualsiasi anomalia, incidente o violazione, anche solo sospetti, di cui venga a conoscenza, contribuendo così al miglioramento continuo del sistema.

2. **Soggetti esterni**
    - Tutte le parti esterne che intrattengono rapporti di collaborazione con l'Azienda devono garantire il rispetto delle disposizioni contenute nella presente policy e conformarsi alle norme aziendali applicabili.

Ruoli chiave e responsabilità specifiche

- **Organi di amministrazione (Consiglio di Amministrazione):**
    - Approvano le misure di gestione dei rischi per la sicurezza informatica, ne sovrintendono l'attuazione e ne rispondono ai sensi dell'art. 23 del D.Lgs. 138/2024; seguono una formazione specifica in materia di sicurezza informatica.

- **Il Responsabile del Sistema di Gestione per la Qualità (RGQ):**
    - Garantisce la corretta implementazione e manutenzione del Sistema di Gestione per la Qualità, in linea con le policy e gli obiettivi aziendali.
    - Pianifica e coordina gli audit interni del Sistema di Gestione Integrato; gli audit sulla sicurezza delle informazioni sono svolti da soggetti diversi dall'RSI e quelli sui processi di cui la RGQ è responsabile da un auditor indipendente.

- **Responsabile della Sicurezza delle Informazioni e della Sicurezza Informatica (RSI):**
    - Conduce l'analisi dei rischi utilizzando metodologie appropriate e definisce misure di gestione per mitigare tali rischi.
    - Stabilisce norme e procedure per la gestione sicura delle attività aziendali.
    - Supervisiona la gestione delle violazioni di sicurezza, adottando le contromisure necessarie per minimizzare l'impatto e verificando periodicamente l'esposizione dell'Azienda a minacce e rischi.
    - Coordina il Team di gestione degli incidenti e dei data breach e sovrintende all'attuazione delle misure di sicurezza informatica previste dalla normativa NIS2, riferendo agli organi di amministrazione.

- **Amministratori del Sistema (AdS):**
    - Implementano e monitorano i controlli tecnici per garantire la sicurezza delle informazioni aziendali.
    - Collaborano nell'analisi delle vulnerabilità e nell'adozione di misure preventive e correttive.

- **Punto di Contatto NIS e Referente CSIRT:**
  - Curano i rapporti con l'Agenzia per la Cybersicurezza Nazionale e le notifiche degli incidenti significativi al CSIRT Italia.

- **Responsabile della protezione dei dati (DPO):**
  - Sorveglia l'osservanza della normativa in materia di protezione dei dati personali, fornisce consulenza e funge da punto di contatto per gli interessati e per il Garante (dpo@corley.it). Il ruolo è distinto e indipendente da quello dell'RSI.

- **Responsabile del Compliance Office (CO):**
  - Presidia la conformità normativa (GDPR, NIS2, AI Act), tiene i registri previsti e coordina con il DPO e con l'RSI gli adempimenti verso il Garante, i clienti e l'Agenzia per la Cybersicurezza Nazionale (Mod. 5-H).

- **Comitato di crisi:**
  - Gestisce le crisi aziendali di qualunque natura secondo la Procedura di gestione delle crisi aziendali, assumendo le decisioni necessarie a tutelare le persone, i clienti e la continuità dei servizi (Mod. 5-M).

Altri obblighi specifici includono:

- **Formazione e sensibilizzazione del personale:**
  - Organizzare programmi di formazione e promuovere la consapevolezza sulla sicurezza delle informazioni a tutti i livelli aziendali, garantendo che il personale sia adeguatamente preparato e aggiornato sulle normative e best practices di settore.

- **Monitoraggio e verifica:**
  - Eseguire verifiche periodiche per valutare l'efficacia e l'efficienza del Sistema di Gestione Integrato, individuando aree di miglioramento e garantendo la conformità normativa.

Conseguenze della mancata osservanza delle policy

Qualsiasi individuo (dipendente, consulente o collaboratore esterno) che, intenzionalmente o per negligenza, non rispetti le regole di sicurezza stabilite, causando danni all'Azienda, sarà soggetto a provvedimenti appropriati. Tali provvedimenti saranno adottati in conformità con la normativa vigente e con i vincoli contrattuali, al fine di tutelare gli interessi aziendali e prevenire il verificarsi di ulteriori violazioni.

Monitoraggio e riesame del sistema integrato

La Direzione si impegna a verificare periodicamente e regolarmente l'efficacia e l'efficienza del Sistema di Gestione Integrato, almeno una volta all'anno in sede di riesame della Direzione e in concomitanza di cambiamenti significativi. Tale attività mira a garantire un adeguato supporto all'introduzione delle necessarie migliorie e a promuovere un processo di miglioramento continuo. Questo processo assicura il mantenimento del controllo e l'adeguamento della policy aziendale, in risposta ai mutamenti dell'ambiente aziendale, del business e delle condizioni legali o regolamentari.

Responsabilità del riesame della politica

Il Responsabile del Sistema di Gestione (RGQ), con il supporto dell'RSI, è incaricato di condurre il riesame della politica aziendale. Tale riesame deve includere:

- **Verifica dello stato delle azioni correttive e di miglioramento** : accertare l'efficacia delle misure adottate e la loro conformità alla policy aziendale.

- **Adattamento alla policy**: garantire che la politica aziendale rimanga coerente con gli obiettivi e le esigenze operative.

Fattori da considerare nel riesame

Il riesame deve tenere conto di:

- Risultati dei precedenti riesami e delle attività di monitoraggio e verifica.
- Evoluzioni nell'ambiente tecnico e tecnologico.
- Cambiamenti organizzativi interni.
- Disponibilità e adeguatezza delle risorse aziendali.
- Modifiche alle condizioni legali, regolamentari o contrattuali.
- Incidenti di sicurezza, violazioni di dati personali e relative notifiche.
- Esiti degli audit interni, delle verifiche del DPO e di eventuali controlli delle autorità.
- Evoluzione delle minacce informatiche e delle determinazioni dell'Agenzia per la Cybersicurezza Nazionale.

Esiti del riesame

Il risultato del riesame dovrà includere:

- Decisioni e azioni mirate al miglioramento dell'approccio aziendale alla gestione della qualità e della sicurezza delle informazioni.
- Raccomandazioni per il rafforzamento dell'efficacia del Sistema di Gestione e per l'allineamento della politica alle evoluzioni del contesto aziendale e normativo.

Attraverso queste attività, la Direzione garantisce che il Sistema di Gestione rimanga un elemento strategico per il successo aziendale, in linea con le best practices e gli standard internazionali di riferimento.

Impegno della direzione

La Direzione dimostra il proprio impegno attivo verso la sicurezza delle informazioni attraverso una leadership chiara, un supporto evidente e la definizione esplicita di incarichi e responsabilità. Questo impegno si concretizza tramite una struttura organizzativa dedicata, i cui compiti principali includono:

- **Definizione degli obiettivi di sicurezza delle informazioni**: garantire che gli obiettivi relativi alla sicurezza delle informazioni siano chiaramente identificati e allineati con i requisiti aziendali e normativi.
- **Assegnazione di ruoli e responsabilità**: stabilire ruoli aziendali specifici e responsabilità chiare per lo sviluppo, l'implementazione e il mantenimento del Sistema di Gestione Integrato.
- **Allocazione delle risorse**: fornire risorse adeguate e sufficienti per pianificare, implementare, organizzare, controllare, rivedere e migliorare continuamente il SGI.
- **Integrazione nei processi aziendali**: controllare che il SGI sia correttamente integrato in tutti i processi aziendali e che le procedure e i controlli siano sviluppati e applicati in modo efficace.
- **Supporto alle iniziative di miglioramento**: approvare e promuovere tutte le iniziative finalizzate al miglioramento continuo della qualità e della sicurezza delle informazioni.
- **Diffusione della consapevolezza**: attivare programmi e iniziative per la promozione della consapevolezza e della cultura della qualità e della sicurezza delle informazioni a tutti i livelli dell'Organizzazione.
- **Responsabilità degli organi di amministrazione**: approvare le misure di gestione dei rischi per la sicurezza informatica, sovrintenderne all'attuazione e partecipare alla formazione prevista, in conformità all'art. 23 del D.Lgs. 138/2024.

La Direzione garantisce che l'approccio alla gestione della sicurezza delle informazioni e della sicurezza informatica sia proattivo, strutturato e in linea con i principi della norma **ISO/IEC 27001:2022** e con gli obblighi del D.Lgs. 138/2024 (NIS2), favorendo il raggiungimento degli obiettivi aziendali e la protezione delle informazioni critiche per il business.

Torino, lì 30/10/2026

La Direzione

Gabriele Mittica

Stato delle revisioni

Rev.	Data	Descrizione della modifica	Redatto	Approvato
0	03.03.2025	Prima emissione	RGQ	DIR
1	04.11.2025	Correzione riferimento UNI CEI EN ISO/IEC 27001:2022	RGQ	DIR
2	30.10.2026	Estensione alla sicurezza informatica (NIS2); riferimenti a GDPR, D.Lgs. 196/2003, D.Lgs. 138/2024, determinazioni ACN; nuovi principi (autenticità, protezione dei dati personali, uso responsabile dell'IA); ruoli degli organi di amministrazione, Punto di Contatto NIS e Referente CSIRT, CO, Comitato di crisi e DPO; nuovo template documentale, riferimento alla ISO/IEC 27001 allineato al certificato.	RGQ	DIR