Policy aziendale integrata per le Qualità e la Sicurezza delle informazioni

ISO/IEC 27001 e ISO 9001

Wintech Spa – Padova 06/08/2021

Estratto della Politica Integrata per la Qualità e per la Sicurezza delle Informazioni

Politica

Stabilire la Politica

Il vertice aziendale di Wintech Spa, impegnandosi ad applicare il Sistema di Gestione Integrato all'interno dell'organizzazione, ha formalmente dichiarato la propria Mission e gli obiettivi strategici, che sono stati comunicati a tutti i livelli aziendali per assicurarsi che i contenuti siano chiaramente individuati, compresi e soddisfatti.

Le Politiche per la Qualità e la Sicurezza delle Informazioni sono state riscritte in un unico documento facente parte del Sistema di Gestione Integrato, che è rivolto sia all'interno che all'esterno dell'azienda – pubblicato nel sito aziendale. Tale documento può essere inviato, in versione ridotta, a chi ne faccia esplicita richiesta alla Direzione, previa approvazione di quest'ultima.

Il contenuto della Politica viene riesaminato annualmente dal vertice aziendale per verificarne la coerenza. Le modifiche vengono trasmesse alle parti interessate al fine di verificarne l'adeguatezza; per tale motivo si è ritenuto di considerare la Politica Integrata della Qualità e della Sicurezza delle Informazioni come documento in gestione controllata, estraneo al Manuale.

La politica integrata è stata valutata dalla direzione come appropriata alle finalità organizzative, è resa disponibile nel CRM in forma integra, ed un estratto della stessa si trova sul sito aziendale. Inoltre, è stata comunicata all'interno dell'organizzazione, sia per farne comprendere l'importanza, che per condividere gli standard che l'azienda vuole mantenere nel raggiungimento dei propri obiettivi.

Comunicare le Politiche della Sicurezza delle Informazioni e della Qualità

L'Organizzazione deve definire, comunicare e diffondere, a tutte le parti interessate, le politiche per la Qualità e per la Sicurezza delle Informazioni, che indichino il bisogno di soddisfare:

- requisiti di Sicurezza e di Qualità del cliente;
- requisiti contrattuali;
- regolamenti e requisiti cogenti.

Questa politica integrata di Wintech Spa rappresenta l'impegno dell'organizzazione, nei confronti di clienti e terze parti, a garantire la sicurezza delle informazioni e la qualità degli strumenti fisici, logici e organizzativi atti al trattamento delle informazioni in tutte le attività.

Wintech Spa considera il Sistema di Gestione Integrato, con le norme UNI EN ISO 9001 e UNI 27001 nella corrente versione, come un valido strumento per poter perseguire un miglioramento continuo, al fine di poter mantenere la propria credibilità sul mercato nell'ambito dell'Information Technology (IT).

Gli aspetti cardine dell'azienda sono:

- **Collaborazione**. Wintech ritiene indispensabile la collaborazione interna tra le persone, ed esterna verso partner, fornitori e società partecipate. Al fine di raggiungere gli obiettivi aziendali, si ritiene indispensabile considerare gli obiettivi dei terzi con cui si collabora nella realizzazione dei servizi verso i clienti.
- **Orientamento al Cliente**. Un fattore chiave, alla base della crescita e della redditività a lungo termine, è l'impegno a soddisfare pienamente i clienti in ogni loro contatto con Wintech. Il radicamento nel mercato è necessario per una politica di vicinanza al cliente e di attenzione alle sue necessità.

- **La qualità del servizio**. Wintech intende perseguire elevati livelli di qualità nel servizio offerto. I clienti devono riconoscere Wintech come una società che realizza servizi di livello qualitativo elevato, caratterizzati da un servizio eccellente a costi competitivi.

La Qualità secondo Wintech è l'espressione di:

- prevenzione degli errori, miglioramento continuo, razionalizzazione di tutti i processi, per migliorarne efficacia ed efficienza;
- delega di responsabilità in base alle rispettive professionalità, motivazione, riconoscimento e formazione di tutti i collaboratori;
- integrazione di fornitori e clienti come partner della qualità.

Wintech si impegna quindi formalmente affinché la propria Politica della Qualità venga compresa, attuata e sostenuta da tutti i livelli aziendali attraverso la continua verifica, l'assegnazione di chiare e precise responsabilità e la realizzazione di mirati programmi di addestramento e formazione per i collaboratori.

Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni gestite attraverso i servizi forniti, localizzate nella sede dell'azienda e nelle sedi dei Data Center.

È necessario assicurare:

- **la confidenzialità delle informazioni**: ovvero le informazioni devono essere accessibili solo da chi è autorizzato;
- **l'integrità delle informazioni**: ovvero proteggere le informazioni da modifiche non autorizzate o non previste;
- **la disponibilità delle informazioni**: ovvero che gli utenti autorizzati possano effettivamente accedere alle informazioni collegate nel momento in cui lo richiedano.

La mancanza di adeguati livelli di sicurezza può influire sulla reputazione aziendale, oltre che causare la violazione di impegni contrattuali con il cliente e la violazione delle normative vigenti, che a loro volta possono generare ingenti danni di natura economica e finanziaria.

L'azienda identifica le esigenze di sicurezza tramite l'analisi dei rischi, che consente di acquisire consapevolezza sul livello di esposizione a minacce del proprio sistema informativo. L'analisi del rischio permette di valutare le potenziali conseguenze e i danni che possono derivare da un incidente dovuto alla mancata applicazione di misure di sicurezza, quantificando la realistica eventualità del verificarsi dei rischi identificati.

I risultati di questa valutazione determinano le azioni necessarie per mitigare i rischi individuati e le misure di sicurezza più idonee.

I principi generali della gestione della sicurezza delle informazioni abbracciano vari aspetti:

- deve esistere un catalogo costantemente aggiornato degli asset aziendali, rilevanti ai fini della gestione delle informazioni e per ciascuno deve essere individuato un responsabile. Le informazioni devono essere classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza, disponibilità ed integrità coerenti ed appropriati.
- Per garantire la sicurezza delle informazioni, ogni accesso ai sistemi deve essere sottoposto a una procedura di identificazione e autenticazione. Le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo e agli incarichi ricoperti dai singoli individui, in modo che ogni utente possa accedere alle sole informazioni di cui necessita; devono inoltre essere periodicamente sottoposte a revisione.
- Devono essere definite delle procedure per l'utilizzo sicuro dei beni aziendali, delle informazioni e dei loro sistemi di gestione.

- Deve essere incoraggiata la piena consapevolezza delle problematiche relative alla sicurezza delle informazioni verso tutto il personale – dipendenti, collaboratori e altri aventi titolo – a partire dal momento della selezione e per tutta la durata del rapporto di lavoro.
- Per poter gestire in modo tempestivo gli incidenti, tutti devono notificare qualsiasi problema relativo alla sicurezza. Ogni incidente deve essere gestito come indicato nelle procedure.
- È necessario prevenire l'accesso non autorizzato alle sedi e ai singoli locali aziendali dove sono gestite le informazioni e deve essere garantita la sicurezza delle apparecchiature. Devono essere predisposte adeguate misure di conservazione anche per i documenti in formato non elettronico.
- Deve essere assicurata la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni negli accordi con le terze parti.
- Deve essere predisposto un piano di continuità che permetta all'azienda di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulla missione aziendale.
- Gli aspetti di sicurezza devono essere inclusi in tutte le fasi di analisi, implementazione, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.
- Devono essere garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

L'osservanza e l'attuazione di questa policy sono responsabilità di:

Tutte le persone che, a qualsiasi titolo, collaborano con l'azienda e sono in qualche modo coinvolte con il trattamento di informazioni che rientrano nel campo di applicazione del Sistema di Gestione della Sicurezza delle Informazioni. Tutto il personale è altresì responsabile della segnalazione di tutte le anomalie e violazioni di cui dovesse venire a conoscenza.

Tutti i soggetti esterni che intrattengono rapporti e collaborano con l'azienda. Devono garantire un livello di sicurezza compatibile ai requisiti di sicurezza contenuti nella presente policy.

Il Responsabile della Sicurezza delle Informazioni che, nell'ambito del Sistema di Gestione della Sicurezza delle Informazioni e attraverso norme e procedure appropriate, deve:

- condurre l'analisi dei rischi con le opportune metodologie e adottare tutte le misure per l'identificazione del rischio;
- stabilire tutti gli standard necessari alla conduzione sicura di tutte le attività aziendali;
- raccogliere le notifiche di incident di sicurezza e dare le indicazioni al team tecnico per minimizzarne l'impatto;
- proporre la formazione e promuovere la consapevolezza del personale per tutto ciò che concerne la sicurezza delle informazioni;
- predisporre un piano periodico di ricerca delle vulnerabilità secondo metodologie comunemente utilizzate;
- verificare periodicamente l'efficacia e l'efficienza del Sistema di Gestione della Sicurezza delle Informazioni.

Chiunque – dipendenti, consulenti e/o collaboratori esterni dell'Azienda – che, in modo intenzionale o riconducibile a negligenza, disattenda le regole di sicurezza stabilite, potrà essere perseguito nelle opportune sedi, nel pieno rispetto dei vincoli di legge e contrattuali.