

Politica del Sistema di Gestione Integrato

SOMMARIO.....	Errore. Il segnalibro non è definito.
0.1 Introduzione e scopo	3
0.1.1 Obiettivi strategici.....	3
0.1.2 Sicurezza delle informazioni.....	4
0.1.3 Impegno della direzione	5
0.1.4 Comunicazione e diffusione.....	5

Introduzione e scopo

Xifram S.r.l. ha stabilito la seguente Politica del proprio Sistema di Gestione Integrato, che integra e completa il Codice Etico pubblicato anche sul sito dell'organizzazione.

Tale Politica impone che, in coerenza con la *mission* dell'Organizzazione, la gestione di tutti i processi aziendali sia impostata secondo le regole proprie dell'applicazione del Sistema di Gestione Integrato (SGSI) rispondente alle norme UNI EN ISO 9001 e UNI CEI ISO/IEC 27001.

Il Sistema di Gestione adottato, basato sull'analisi del rischio e del contesto aziendale (*risk based thinking*), consente di abbracciare un modello di miglioramento continuo dei processi dell'Organizzazione, il quale si esplica attraverso la pianificazione, l'attuazione, il monitoraggio, il riesame e l'aggiornamento costante dei processi e del sistema stesso.

Obiettivi strategici

La Direzione di Xifram S.r.l. ha analizzato il contesto interno ed esterno e identificato le esigenze e le aspettative delle parti interessate rilevanti, in modo da garantire che il Sistema di Gestione Integrato sia coerente con la strategia aziendale e contribuisca al raggiungimento degli obiettivi di medio-lungo periodo. A tal proposito, si stabilisce che gli obiettivi strategici di Xifram S.r.l. sono:

- **soddisfazione del cliente interno ed esterno**, adottando un approccio strategico per garantire che i prodotti e/o servizi soddisfino le loro aspettative in termini di qualità del prodotto/servizio offerto, velocità e flessibilità nel soddisfacimento delle richieste, professionalità e disponibilità delle risorse impiegate;
- **coinvolgimento delle persone**, infatti la forza che consente all'Organizzazione di raggiungere gli obiettivi prefissati è il proprio personale. Responsabilizzazione, impegno ed ottenimento degli obiettivi sono fortemente richiesti e incentivati attraverso la creazione di una sistematica consapevolezza del concetto di qualità e di sicurezza delle informazioni. Per raggiungere tale obiettivo è necessaria la promozione dello sviluppo delle competenze del personale ad ogni ruolo, attraverso programmi di formazione mirati, strategie di apprendimento continuo e iniziative di sensibilizzazione, garantendo un ambiente di lavoro informato, responsabile e orientato alla qualità e alla sicurezza delle informazioni;
- **selezione di fornitori qualificati**, non a caso la realizzazione e il mantenimento di rapporti collaborativi stretti è essenziale per il raggiungimento degli obiettivi dell'organizzazione. È essenziale che gli obiettivi siano diffusi, capiti ed accettati da tutti i collaboratori opportunamente selezionati e qualificati sulla base di un'attenta analisi del rischio di fornitura;
- **salvaguardare la sicurezza e la privacy dei dati**: è di fondamentale importanza per L'Organizzazione salvaguardare la riservatezza, l'integrità e la disponibilità dei dati propri e dei propri stakeholders;
- **definizione e rispetto dei livelli di servizio**, garantendo che gli SLA (Service Level Agreement) concordati con gli stakeholders vengano opportunamente definiti e rispettati. Tale obiettivo può essere raggiunto solo mantenendo attivo un sistema organizzato in cui obiettivi, compiti e flussi informativi siano chiari e condivisi all'interno dell'Organizzazione;
- **contrasto delle minacce cyber** proteggendo le infrastrutture e i dati dell'Organizzazione e dei propri stakeholders attraverso l'adozione di strategie di prevenzione, di rilevamento e di risposta alle minacce informatiche; garantendo la resilienza operativa e la sicurezza delle informazioni;
- **approccio per processi**, ottimizzati attraverso l'identificazione, la comprensione e il controllo

dei processi interconnessi, migliorandone l'efficienza operativa, riducendo i costi e garantendo risultati coerenti e prevedibili. Tale obiettivo è raggiunto attraverso lo stanziamento, da parte della direzione, di risorse necessarie al conseguimento degli obiettivi prefissati e al mantenimento del Sistema di Gestione Integrato;

- **orientamento al miglioramento continuo**, favorendo l'evoluzione costante dei processi, prodotti e servizi attraverso l'analisi dei dati, l'innovazione e l'ottimizzazione delle risorse, garantendo efficienza, qualità e competitività nel lungo periodo. La revisione periodica del Sistema è garantita attraverso azioni di controllo (audit) interne ed esterne. La revisione periodica dei rischi aziendali consente di analizzare accuratamente possibili nuove minacce ed eventi per poter reagire adeguatamente ai cambiamenti interni ed esterni all'Organizzazione;
- **infine il rispetto dei requisiti normativi e legislativi** attraverso un monitoraggio costante, l'implementazione di procedure adeguate e la formazione del personale, assicurando trasparenza, sicurezza e affidabilità operativa, con il fine di ridurre al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

Sicurezza delle informazioni

Xifram S.r.l. ha come obiettivo primario la protezione dei dati, delle informazioni, delle strutture tecnologiche, sia fisiche che logiche, proprie e dei propri stakeholders. Tale obiettivo è raggiungibile attraverso l'assicurazione di:

- **riservatezza delle informazioni** - le informazioni devono essere accessibili solo da chi è autorizzato;
- **integrità delle informazioni** - le informazioni devono essere puntualmente protette e dev'essere garantita la completezza delle stesse oltre che dei metodi utilizzati per la loro elaborazione;
- **disponibilità delle informazioni** - solo gli utenti autorizzati possono effettivamente accedere alle informazioni e ai beni collegati nel momento in cui lo richiedono.

La mancanza di adeguati livelli di sicurezza può comportare il danneggiamento dell'immagine dell'Organizzazione, la mancata soddisfazione del cliente, il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti nonché danni di natura economica e finanziaria.

Un adeguato livello di sicurezza è altresì basilare per la condivisione delle informazioni.

L'azienda identifica tutte le esigenze di sicurezza tramite l'analisi dei rischi che incombono sui propri asset aziendali che consente di acquisire idonea consapevolezza sul livello di esposizione a minacce. La valutazione del rischio permette di valutare le potenziali conseguenze e gli impatti che possono derivare dalla mancata applicazione di misure di sicurezza al sistema informativo e quale sia la realistica probabilità di attuazione delle minacce identificate. I risultati di questa valutazione determinano le azioni necessarie per gestire i rischi individuati e le misure di sicurezza più idonee.

I principi di Xifram S.r.l. per la gestione della sicurezza delle informazioni abbracciano i seguenti aspetti:

- garantire un catalogo costantemente aggiornato degli asset rilevanti ai fini della gestione delle informazioni;
- classificare le informazioni in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza ed integrità coerenti ed appropriati;
- garantire che l'accesso ai sistemi sia sottoposto a procedure d'identificazione e autenticazione differenziate in base al ruolo ed agli incarichi ricoperti;
- definire procedure per l'utilizzo sicuro degli asset dell'Organizzazione in special modo di quelli mobili;

- garantire la piena consapevolezza relativamente alla sicurezza delle informazioni in tutti gli stakeholders, per tutta la durata del rapporto di lavoro;
- segnalare e gestire tempestivamente gli incidenti di sicurezza o possibili tali;
- prevenire l'accesso non autorizzato alle sedi e ai singoli locali dell'Organizzazione per garantire la sicurezza di dati ed infrastruttura;
- predisporre, mantenere e regolarmente testare un piano di continuità che permetta all'Organizzazione di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative;
- includere in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici il concetto di sicurezza *by design*;
- eseguire *penetration test* periodici nelle infrastrutture e negli applicativi per valutare la resilienza dei sistemi ad attacchi esterni ed evincere eventuali vulnerabilità.

Impegno della direzione

La direzione di Xifram S.r.l. sostiene attivamente il rispetto degli obiettivi prefissati e il loro allineamento al Sistema di Gestione Integrato e alla strategia dell'Organizzazione anche in riferimento ai cambiamenti previsti dall'evoluzione del mercato, da nuove minacce, significativi eventi di sicurezza nonché dall'evoluzione del contesto normativo e legislativo.

Essa svolge un ruolo attivo costante e di sostegno nella promozione e guida di tutte le attività influenti sull'applicazione della presente Politica, tramite una struttura i cui compiti sono:

- garantire che siano identificati tutti gli obiettivi;
- stabilire i ruoli aziendali e le responsabilità per lo sviluppo e il mantenimento del Sistema di Gestione Integrato;
- fornire risorse sufficienti alla pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo del Sistema di Gestione Integrato;
- monitorare sul continuo e corretto utilizzo delle procedure individuate;
- approvare e sostenere tutte le iniziative volte al miglioramento del Sistema di Gestione Integrato.

La Direzione mette in atto tutte quelle azioni utili perché gli obiettivi e la presente Politica siano compresi e applicati da tutto il personale nonché da tutti gli stakeholder che abbiano un coinvolgimento diretto ed indiretto con le attività dell'Organizzazione.

Comunicazione e diffusione

La presente Politica è comunicata a tutto il personale, resa disponibile alle parti interessate rilevanti e pubblicata nei canali interni ed esterni dell'Organizzazione, affinché sia compresa, applicata e sostenuta in modo coerente a tutti i livelli.

Padova, 20/10/2025
Xifram S.r.l.