POLITICA PER LA SICUREZZA DELLE INFORMAZIONI E LA CYBERSECURITY

La Direzione di Lawer S.p.A. ha predisposto una Politica per la sicurezza delle informazioni e la cybersecurity attraverso la quale erogare i propri servizi garantendo sicurezza delle informazioni e continuità operativa. La direzione strategica, i principi, le regole di base e gli obiettivi di tale Politica sono stati definiti al fine di raggiungere i seguenti obiettivi:

1. Garantire la **protezione del proprio patrimonio informativo** e di risorse umane, riducendo al minimo il rischio di danni provocati da incidenti di sicurezza deliberati o involontari dall'interno, dall'esterno o da potenziali minacce;
2. Garantire la resilienza e la **continuità operativa** dei servizi offerti così come la protezione delle infrastrutture di Lawer;
3. Perseguire obiettivi di **miglioramento continuo**.

Inoltre, attraverso l'applicazione della presente politica, Lawer intende conformarsi ai principi e ai controlli stabiliti dalle norme e regolamenti che disciplinano le attività di business in cui opera l'azienda, tra i quali, in particolare, le regolamentazioni inerenti alla Privacy e alla sicurezza dei dati personali (GDPR) e la cybersecurity (NIS2).

La responsabilità nell'applicazione della presente Politica riguarda l'intera organizzazione aziendale, dalla Direzione fino a ogni singolo dipendente. Tale applicazione avviene nel rispetto delle leggi e delle disposizioni vigenti, dei requisiti contrattuali, delle norme e delle procedure aziendali.

Protezione del patrimonio informativo

La protezione del patrimonio informativo di Lawer, dei propri clienti e dei propri fornitori è posta al centro delle strategie conservative, di tutela e di protezione ponendo riservatezza, integrità e disponibilità al centro di tali strategie. Predisponendo investimenti atti a garantire sicurezza e protezione del sistema informativo, Lawer vuole ridurre il rischio di incidenti, minimizzando il rischio di perdita e/o indisponibilità dei dati dei clienti, pianificando e gestendo le attività a garanzia della continuità di servizio. Tali obiettivi di sicurezza e protezione vengono perseguiti attraverso:

1. Identificazione dei rischi, attraverso una continua e adeguata analisi dei rischi che esamini costantemente le vulnerabilità e le minacce associate alle attività a cui si applica il sistema, al fine di comprendere le vulnerabilità e le possibili minacce presenti in azienda che possono esporre a rischi di mancato raggiungimento degli obiettivi.

2. Gestione del rischio ad un livello accettabile attraverso la progettazione, attuazione, e mantenimento di idonee contromisure per la sicurezza delle informazioni, per garantire la qualità dei prodotti e servizi forniti e per la salute e sicurezza dei luoghi di lavoro.
3. Tutela della confidenzialità delle informazioni assicurando che le informazioni siano:
    - accessibili solo a chi ne è autorizzato;
    - precise e complete;
    - disponibili a chi ne ha i diritti di accesso.
4. Azioni tempestive ed efficaci di fronte a necessità emergenti nel corso delle attività lavorative.
5. Identificazione dei pericoli e dei rischi presenti all'interno dell'organizzazione.

La Direzione ed i Responsabili di ogni dipartimento si impegnano affinché i principi sopra delineati vengano effettivamente ed efficacemente applicati ad ogni passaggio del processo produttivo e nei servizi che Lawer offre ai propri clienti, nonché nei riguardi dei propri fornitori e del proprio personale.

Continuità operativa

La continuità operativa e la resilienza dei servizi offerti e la protezione delle infrastrutture di Lawer sono garantite dall'attenta gestione e aggiornamento del Sistema informatico. Quest'ultimo si basa sui seguenti principi guida:

1. Proattività nella gestione del rischio;
2. Ripristino tempestivo e sicuro;
3. Test e miglioramento continuo;
4. Comunicazione trasparente.

Rispettare la presente politica per la continuità operativa significa:

1. **Proteggere le infrastrutture critiche:** grazie alle aggiornate pratiche di Disaster Recovery è possibile proteggere asset critici e garantire il ripristino rapido delle operazioni in caso di interruzioni;
2. **Mitigare i rischi:** affrontare eventi inattesi o interruzioni non pianificate, che possono derivare da attacchi informatici, disastri naturali o guasti tecnici, attraverso un processo continuo di valutazione e mitigazione del rischio.

Miglioramento continuo

Il miglioramento continuo del Sistema di Lawer si basa sul coinvolgimento, sulla cooperazione e la collaborazione tra le risorse aziendali. Tale obiettivo primario viene perseguito mediante:

1. Riesame periodico della Politica, degli obiettivi e della loro attuazione nel Sistema.
2. Una visione per processi che tiene in considerazione il contesto organizzativo e le strategie direzionali, la pianificazione degli obiettivi, la gestione delle risorse, degli asset, delle politiche e delle procedure, i criteri per l'autovalutazione e la verifica interna dell'organizzazione e gli stimoli verso tale miglioramento.
3. Attenzione all'ambiente circostante, affidandosi a un approccio di tipo preventivo di fronte ai problemi anziché sul controllo a posteriori e sulla relativa correzione, in modo da ridurre significativamente la probabilità di accadimento di incidenti, infortuni o altre non conformità.
4. Formazione e aggiornamento del personale, mantenendo alti livelli di performance, capacità di rispondere ai cambiamenti e individuare nuove opportunità di crescita.
5. Coinvolgimento del personale, accogliendone i contributi e le segnalazioni, in un ambiente lavorativo aperto a una comunicazione costruttiva e aperta al dialogo.
6. Promozione della collaborazione, comprensione e consapevolezza del Sistema da parte dei fornitori strategici.

La presente politica viene formulata e riesaminata dalla Direzione Aziendale. Tutto il personale, in base alle proprie conoscenze, ha la responsabilità di riferire al Responsabile del Sistema qualsiasi punto debole individuato nei sistemi aziendali. La presente politica viene riesaminata regolarmente per identificare eventuali modifiche che la influenzano e per accertarsi che permanga idonea alle finalità dell'organizzazione e alle aspettative degli stakeholders.

La Direzione