**ML INFORMATICA** è un'azienda specializzata nella fornitura di servizi informatici e nella consulenza a supporto della compliance aziendale, impegnata nell'offrire soluzioni innovative e affidabili per soddisfare le esigenze tecnologiche della propria Clientela. La Direzione dell'azienda riconosce l'importanza della Sicurezza delle Informazioni in questo contesto, poiché costituisce un elemento cruciale per assicurare il rispetto e la massima soddisfazione dei Clienti, nonché di tutte le altre parti interessate.

A tal fine, ML INFORMATICA ha formulato la propria "Politica del Sistema di Gestione per la Sicurezza delle Informazioni", sottolineando che la sicurezza delle informazioni rappresenta una responsabilità prioritaria nei confronti di tutti gli Stakeholder. Questo impegno è integrato in ogni aspetto delle attività dell'organizzazione, parallelamente alla costante ricerca di nuove tecnologie. L'obiettivo è garantire la qualità dei servizi offerti e la Sicurezza delle Informazioni relative a Clienti, fornitori e tutte le altre parti interessate. Il Sistema di Gestione per la Sicurezza delle Informazioni è attualmente esteso a tutte le fasi coinvolte nella fornitura dei nostri servizi. Queste attività abbracciano la progettazione, lo sviluppo, l'installazione, l'esercizio e la manutenzione di applicativi Software on premise e as a Service. Copre anche l'analisi, la consulenza, la progettazione, l'implementazione, l'integrazione, la manutenzione e l'assistenza di infrastrutture informatiche e sistemi ICT, l'erogazione di servizi gestiti in ambito Network & Security e la consulenza in materia di Trattamento dei Dati e Sicurezza informatica.

**Obiettivi di Sicurezza delle Informazioni**

Garantire la protezione delle informazioni è essenziale per gestire correttamente i rapporti con i Clienti, innovare prodotti e servizi e garantire un servizio di qualità. Per questo motivo le Informazioni devono essere adeguatamente protette equilibrando il livello di rischio accettato con il grado di protezione richiesto. In questo modo, si tutela il valore delle Informazioni e si assicura l'efficienza, l'efficacia e la continuità dei processi aziendali. Le informazioni sono sempre più gestite digitalmente e accessibili ad un pubblico sempre più ampio. Questo aumento di accessibilità, se da un lato offre vantaggi, dall'altro accresce i rischi per la sicurezza. Affrontare questa sfida richiede l'implementazione di misure e strumenti adeguati, rispondendo alla crescente domanda di sicurezza da parte dei clienti, al fine di garantire la protezione delle informazioni. Gli obiettivi di sicurezza includono:

**Stabilire e mantenere un solido quadro di governance della sicurezza**: Il primo passo per creare una strategia completa di sicurezza informatica è stabilire un robusto quadro di governance specifico per l'azienda. Ciò implica l'identificazione e la documentazione dei ruoli e delle responsabilità delle principali parti interessate. È essenziale definire chiare linee di autorità e canali di comunicazione per garantire che tutte le parti coinvolte conoscano le proprie responsabilità e siano allineate con gli obiettivi specifici di sicurezza dell'organizzazione.

**Condurre valutazioni periodiche del rischio**: ML INFORMATICA effettua valutazioni regolari dei rischi per identificare potenziali vulnerabilità nell'infrastruttura digitale aziendale. Queste valutazioni vengono condotte regolarmente per individuare nuove minacce o punti deboli nelle difese di sicurezza e per valutare la sicurezza complessiva della catena di approvvigionamento digitale.

**Stabilire un piano completo di risposta agli incident:** ML INFORMATICA ha adottato un piano di risposta agli incident specificamente progettato con l'obiettivo di consentire una rapida reazione a qualsiasi evento indesiderato, garantendo la sicurezza dei dati e dei servizi offerti.

**Implementare una formazione regolare di sensibilizzazione dei dipendenti**: ML INFORMATICA forma regolarmente tutti i dipendenti e promuove la cultura della sicurezza in azienda. Questo processo trasforma il personale in un elemento difensivo forte attraverso una formazione regolare che si concentra sulla consapevolezza della sicurezza, sulle ultime minacce e sulle migliori pratiche per salvaguardare le risorse digitali dell'organizzazione. La formazione comprende anche aspetti come la gestione delle password, la prevenzione delle truffe di phishing e l'importanza di segnalare immediatamente attività sospette.

**Mantenere la sicurezza della catena di approvvigionamento**: Oltre a valutare regolarmente il rischio della catena di approvvigionamento, ML INFORMATICA sceglie partner che rispettino i requisiti di sicurezza per ridurre il rischio di

attacchi informatici di terze parti. Ciò include l'implementazione di misure di sicurezza nella catena di approvvigionamento, come valutazioni e audit dei rischi dei fornitori, accordi contrattuali specifici sulla sicurezza e monitoraggio continuo.

**Aggiornare e applicare regolarmente patch all'infrastruttura e alle applicazioni** per risolvere le vulnerabilità note e garantire la sicurezza delle risorse digitali, ML INFORMATICA assicura che l'infrastruttura digitale e le applicazioni siano costantemente aggiornate e che le patch vengano applicate regolarmente.

**Implementare il monitoraggio delle minacce e svolgere attività di intelligence** ML INFORMATICA monitora costantemente i feed delle minacce per rimanere aggiornata sulle ultime minacce informatiche. I feed di threat intelligence forniscono informazioni in tempo reale su potenziali attacchi informatici, vulnerabilità e attività dannose, contribuendo proattivamente alla prevenzione degli attacchi informatici e alla sicurezza dell'infrastruttura digitale.

**Implementare una solida sicurezza della rete e degli endpoint**: per ridurre significativamente il rischio di accesso non autorizzato ai dati sensibili ML INFORMATICA ha implementato firewall robusti, sistemi di rilevamento delle intrusioni e software antivirus. Inoltre, vengono adottate misure di sicurezza degli endpoint, come la crittografia dei dati e i controlli degli accessi.

**Condurre controlli di sicurezza regolari**: per garantire che la strategia di sicurezza sia efficace e allineata con gli obiettivi generali dell'organizzazione ML INFORMATICA sottopone la propria sicurezza a controlli regolari attraverso audit di sicurezza. Tali audit includono una revisione completa del quadro di governance della sicurezza, valutazione dei rischi, piani di risposta agli incident e controlli di sicurezza.

**Conformità al Regolamento GDPR e Codice Privacy**

ML INFORMATICA considera cruciale garantire il rispetto dei principi di legge sulla protezione dei dati personali, come stabilito dal Regolamento GDPR e dal Codice Privacy per fornire alla propria clientela servizi basati sulla privacy by design, affrontando le principali questioni giuridiche, sia di natura legale che contrattuale, legate alla gestione dei Dati Personali.

Nelle attività di consulenza in ambito Privacy e GDPR, ML INFORMATICA mira a offrire servizi del più alto livello, sia in termini di qualità che di sicurezza con l'obiettivo di aiutare il Cliente a proteggere i Dati Personali della propria organizzazione da tutte le minacce, che possano essere interne o esterne, intenzionali o accidentali. In questo contesto, perseguire la conformità con le leggi sulla protezione dei dati è una parte integrante della nostra missione, contribuendo alla sicurezza e all'affidabilità delle operazioni del Cliente.

**Standard di Riferimento**

Basandosi sui propri obiettivi aziendali, ML INFORMATICA ha scelto di proteggere le proprie Informazioni e quelle affidatele dai clienti seguendo standard riconosciuti, metodologie consolidate, leggi e regolamenti. La protezione delle Informazioni si può ottenere applicando misure tecniche ed impostando con costanza ed efficacia politiche, processi e procedure aziendali.

Partendo da queste convinzioni, ML INFORMATICA ha deciso l'implementazione di un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) in conformità ai seguenti standard volontari:

- **Norma ISO 27001**, la norma internazionale che stabilisce i requisiti per un Sistema di Gestione della Sicurezza delle Informazioni (ISMS)**.** Un ISMS è un insieme di politiche, procedure e controlli che un'organizzazione utilizza per proteggere le proprie Informazioni da una vasta gamma di minacce, tra cui furti, violazioni dei dati e attacchi informatici

- **Linee guida ISO 27002** che forniscono una raccolta di "best practices" che possono essere adottate per soddisfare i requisiti della norma ISO 27001 al fine di proteggere le risorse informative

- **Norma ISO 9001** che stabilisce i requisiti per un sistema di gestione per la qualità. Un sistema di gestione per la qualità è un insieme di processi, procedure e risorse che un'organizzazione utilizza per garantire che i propri prodotti e servizi soddisfino i requisiti dei Clienti e le normative applicabili

**Impegno della Direzione**

L'impegno della Direzione è una responsabilità fondamentale che sottolinea il ruolo essenziale della leadership nell'implementazione ed efficacia del proprio Sistema di Gestione.

In particolare la Direzione si impegna attivamente integrando il Sistema di Gestione nella cultura aziendale, stabilendo obiettivi e politiche, assegnando responsabilità e assicurando la disponibilità di risorse necessarie. Si impegna a fornire le risorse necessarie per l'implementazione e il mantenimento del sistema di gestione, inclusa la formazione del personale e l'infrastruttura; comunica l'importanza della sicurezza delle informazioni e consulta i vari livelli dell'organizzazione per assicurare una partecipazione efficace. La Direzione infine è responsabile del monitoraggio costante delle performance del sistema di gestione, prendendo decisioni basate sui dati e impegnandosi nel miglioramento continuo.

**Miglioramento Continuo**

La Direzione sottopone periodicamente a riesame i risultati raggiunti in relazione agli obiettivi e alle politiche stabilite. Queste revisioni comprendono analisi dei dati, audit interni, feedback dei clienti e altre valutazioni. Nel caso emergessero opportunità di miglioramento durante il monitoraggio, l'organizzazione si impegna ad attuare misure correttive e preventive per garantire un costante ed efficace miglioramento del proprio Sistema di Gestione. La leadership dell'organizzazione gioca un ruolo chiave nel promuovere l'impegno per il miglioramento continuo. Questo coinvolgimento può tradursi nella definizione di obiettivi chiari, nell'allocazione di risorse e nel sostegno attivo alle iniziative di miglioramento.

**Diffusione della Politica**

La Direzione diffonde, si impegna a far comprendere e attua la politica non solo tra il personale interno, ma anche tra stagisti, collaboratori, consulenti e fornitori, con particolare attenzione a chiunque sia in qualsiasi modo coinvolto con le Informazioni che rientrano nel campo di applicazione del Sistema di Gestione della Sicurezza delle Informazioni.

Attraverso l'attuazione di questa politica ML INFORMATICA intende ottemperare all'impegno di conformità a ISO/IEC 27001:2022 nonché a conseguire e mantenere tale certificazione.

La politica sarà soggetta a riesame periodico per garantire la sua idoneità alle attività e alle capacità dell'azienda di soddisfare Clienti e parti interessate.

Lecco, 04 Gennaio 2024

La Direzione