SA LUCIANO FRANZOSINI • Via Simen 3 • **CH-6830 CHIASSO**
Tel. +41 (0)91 695 50 10 • Fax +41 (0)91 695 50 11
info@franzosini.ch • www.franzosini.com • CHE - 463.417.075 IVA

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

SISTEMA DI GESTIONE ISO/IEC 27001:2022

SA LUCIANO FRANZOSINI • Via Simen 3 • **CH-6830 CHIASSO**
Tel. +41 (0)91 695 50 10 • Fax +41 (0)91 695 50 11
info@franzosini.ch • www.franzosini.com • CHE - 463.417.075 IVA

Controllo delle revisioni

Versione	Redazione	Data	Approvazione	Data	Motivo
1.0	RSGSI	03/01/2025	Direzione	07/01/2025	Prima Emissione

Lista di distribuzione

Questo documento è accessibile a chiunque all'interno e all'esterno di ***SA Luciano Franzosini***.

SA LUCIANO FRANZOSINI • Via Simen 3 • **CH-6830 CHIASSO**
Tel. +41 (0)91 695 50 10 • Fax +41 (0)91 695 50 11
info@franzosini.ch • www.franzosini.com • CHE - 463.417.075 IVA

SOMMARIO

SA LUCIANO FRANZOSINI • Via Simen 3 • **CH-6830 CHIASSO**
Tel. +41 (0)91 695 50 10 • Fax +41 (0)91 695 50 11
info@franzosini.ch • www.franzosini.com • CHE - 463.417.075 IVA

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

La sicurezza e la salvaguardia del patrimonio informativo costituiscono condizione imprescindibile per il raggiungimento degli obiettivi di business di ***SA Luciano Franzosini***. I requisiti per la sicurezza delle informazioni sono coerenti con gli obiettivi aziendali e il Sistema di Gestione della Sicurezza delle Informazioni (SGSI) rappresenta lo strumento che consente la condivisione delle informazioni, lo svolgimento di operazioni corrette e la riduzione dei rischi connessi alle informazioni a livelli accettabili.

In considerazione di ciò, lo svolgimento delle attività aziendali deve sempre avvenire garantendo adeguati livelli di:

- Riservatezza: proprietà per cui l'informazione non è resa disponibile o rivelata a individui, entità o processi non autorizzati;
- Integrità: proprietà relativa alla salvaguardia dell'accuratezza e della completezza delle informazioni e dei beni ad esse collegati;
- Disponibilità: proprietà di essere accessibile e utilizzabile su richiesta di un'entità autorizzata;

delle informazioni attraverso l'adozione di un formale "Sistema di Gestione della Sicurezza delle Informazioni" (SGSI) in linea con i requisiti attesi dagli stakeholders dell'Organizzazione e nel rispetto delle normative vigenti.

In particolare, il Sistema di Gestione della Sicurezza delle Informazioni è applicato a tutte le attività e i servizi erogati da ***SA Luciano Franzosini*** a beneficio del mercato di riferimento e dei propri clienti.

Gli obiettivi generali del SGSI perseguiti con l'impegno della direzione, sono:

- dimostrare agli stakeholders la propria capacità di fornire con regolarità servizi sicuri, massimizzando gli obiettivi di sicurezza;
- minimizzare il rischio di perdita e/o indisponibilità dei dati gestiti, con particolare attenzione alla protezione delle informazioni inerenti ai brand dei clienti, pianificando e gestendo le attività a garanzia della continuità di servizio;
- svolgere una continua e adeguata analisi dei rischi che esamini costantemente le vulnerabilità e le minacce associate alle attività a cui si applica il sistema;
- rispettare le leggi e le disposizioni vigenti, i requisiti contrattuali e le procedure in essere;
- accentrare le best-practices messe in pratica per perseguire il costante miglioramento delle procedure riservate all'Organico e fornire ad esso chiare linee guida;
- promuovere la collaborazione, comprensione e consapevolezza del SGSI da parte dei fornitori strategici;
- conformarsi ai principi e ai controlli stabiliti dalla ISO/IEC 27001:2022 o altre norme/regolamenti che disciplinano le attività in cui opera l'azienda, tra i quali, in particolare le regolamentazioni inerenti ai trattamenti dei dati personali e la loro sicurezza.

Tutto il personale, nell'ambito delle relative responsabilità, è coinvolto nella segnalazione al Responsabile del Sistema di Gestione della Sicurezza delle Informazioni (RSGSI) di eventuali eventi negativi o incidenti riscontrati e di qualsiasi debolezza identificata nel SGSI.

Tutta l'organizzazione, a partire dai vertici, è impegnata a supportare l'implementazione, la messa in opera e il riesame periodico per il miglioramento continuo del SGSI.

Il vertice aziendale si impegna a perseguire, con i mezzi e le risorse adeguate, gli obiettivi di questa politica.

CYBER THREAT INTELLIGENCE

L'Organizzazione per far fronte alle minacce nell'ambito della sicurezza delle informazioni si impegna nel raccogliere informazioni sulle minacce, analizzarle ed intraprendere, poi, le azioni di mitigazione adeguate, utilizzando un approccio multirischio.

Lo scopo della Cyber Threat Intelligence è:

- valutare anzitempo la presenza di potenziali minacce;
- ridurre i rischi, attraverso rappresentazioni predittive;
- offrire maggiore visibilità e profondità di comprensione rispetto ai punti critici, le probabilità di accadimento e l'ampiezza dell'impatto su un'organizzazione.

Le informazioni sulle minacce esistenti o emergenti devono essere raccolte ed analizzate al fine di facilitare azioni informate per ridurne l'impatto ed evitare che le stesse possano causare danni all'organizzazione.

Si possono considerare tre livelli di threat intelligence:

1. Informazioni strategiche sulle minacce: scambio di informazioni di alto livello sul panorama delle minacce (es. tipi di attacchi, tipi di attaccanti)
2. Informazioni tattiche sulle minacce: informazioni sulla metodologia, strumenti e tecniche di attacco;
3. Informazioni operative sulle minacce: dettagli sugli attacchi specifici.

La CTI trasforma l'informazione su una vulnerabilità, in un'informazione di "intelligence" su una minaccia. Questo permette alle aziende di:

- contestualizzare i rischi nel concreto;
- fornire preventivamente risposte in materia di sicurezza;
- guidare le azioni di contenimento;
- ottimizzare l'allocazione delle risorse e dei budget in maniera più efficiente.

L'obiettivo è quello di scegliere le misure di sicurezza più appropriate al contesto, basando tale scelta sul rischio, la probabilità e il livello di impatto di una violazione a cui può essere soggetta un'organizzazione, attraverso un processo predittivo. La CTI rappresenta quindi non solo un valido aiuto per comprendere come l'organizzazione potrebbe essere attaccata, ma anche come definire le migliori strategie per prevenire, difendere e mitigare eventuali incidenti.

In questi termini la Cyber Threat Intelligence deve essere considerata un vero e proprio processo aziendale che miri alla difesa preventiva, predittiva e di contesto delle minacce informatiche inedite ed emergenti.

Per garantire un'efficace CTI, l'Organizzazione segue una serie di buone pratiche che si realizzano tramite:

- Monitoraggio continuativo: rilevando periodicamente e costantemente le vulnerabilità delle infrastrutture informatiche internamente ed esternamente al perimetro dell'organizzazione.

Ciò aiuta a identificare qualsiasi altra presenza di minacce in rete come ad es. furto di credenziali, violazione dei dati personali, attacchi di phishing, compromissione degli asset critici dovuti a malware, botnet, etc.;

- Formazione costante dell'Organico mediante bollettini informativi riguardanti minacce potenziali debitamente intercettate e, di base, sensibilizzazione al tema del "security-first" mediante invito a letture o visione di brevi video-corsi;
- Vulnerability Assessment periodici;
- Verifiche della Cyber Reputation: monitoraggio periodico degli host e dei domini DNS dell'organizzazione esposti su internet, verificando il livello reputazionale e/o di compromissione, come ad es. la presenza in black-list per attività di spam, phishing, frode;
- Report periodici sulle minacce.

REVISIONE E COMUNICAZIONE DELLA POLITICA

La presente politica è approvata dalla direzione, pubblicata, comunicata e accettate dal personale pertinente e dalle parti interessate pertinenti.

La presente politica è riesaminata regolarmente dalla Direzione. Il riesame include la valutazione delle opportunità di miglioramento della politica per la sicurezza delle informazioni dell'organizzazione e delle politiche specifiche e la gestione della sicurezza delle informazioni in risposta ai cambiamenti.

L'approvazione e/o l'aggiornamento della presente Politica richiedono un atto formale deliberato dal Consiglio di Amministrazione. Qualora il Consiglio di Amministrazione abbia delegato tale potere all'Amministratore delegato, l'approvazione e l'aggiornamento è rimessa a quest'ultimo.

Il riesame della politica per la sicurezza delle informazioni tiene conto dei risultati dei riesami della direzione e degli audit.

La presente Politica è affissa presso la sede principale e le sedi periferiche dell'Organizzazione, nonché disponibile presso il sito web aziendale.

Chiasso, 07/01/2025

Direzione

Marco Olivier Tepoorten