POLITICA AZIENDALE PER LA SICUREZZA DELLE INFORMAZIONI

La Politica Aziendale di SIAP+MICROS impone che, in coerenza con la missione aziendale, la gestione di tutti i processi aziendali sia impostata con le regole dell'applicazione del Sistema di gestione per la protezione delle informazioni secondo la norma ISO/IEC 27001:2017.

SCOPO E OBIETTIVI

La direzione ha definito, ha divulgato e si impegna a mantenere attiva a tutti i livelli della propria organizzazione la presente politica per la Gestione della Sicurezza delle Informazioni.

Lo scopo della presente policy è:

garantire la tutela e la protezione da tutte le minacce, interne o esterne, intenzionali o accidentali, delle informazioni nell'ambito delle proprie attività in accordo con le indicazioni fornite dallo standard ISO/IEC 27001 e dalle linee guida contenute nello standard ISO/IEC 27002 nelle loro ultime versioni.

CAMPO DI APPLICAZIONE

La presente politica si applica indistintamente a tutti gli organi e i livelli di SIAP+MICROS ed a quanti siano incaricati dalla stessa di qualsiasi trattamento dei dati.

L'attuazione della presente politica è obbligatoria per tutto il personale ed è inserita nella regolamentazione degli accordi con qualsiasi soggetto esterno che, a qualsiasi titolo, possa essere coinvolto con il trattamento di informazioni che rientrano nel campo di applicazione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI).

L'azienda consente la comunicazione e la diffusione delle informazioni verso l'esterno solo per il corretto svolgimento delle attività aziendali che devono avvenire nel rispetto delle regole e delle norme cogenti.

POLICY SICUREZZA DELLE INFORMAZIONI

Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni gestite attraverso i servizi forniti e localizzate in tutte le sedi dell'azienda.

È necessario assicurare:

- la **confidenzialità delle informazioni**: ovvero le informazioni devono essere accessibili solo da chi è autorizzato.
- **l'integrità delle informazioni**: ovvero proteggere la precisione e la completezza delle informazioni e dei metodi per la loro elaborazione.
- la **disponibilità delle informazioni**: ovvero che gli utenti autorizzati possano 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 aziendale, 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 consente di acquisire consapevolezza sul livello di esposizione a minacce del proprio sistema informativo. La valutazione del rischio permette di valutare le potenziali conseguenze e i danni 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.

RESPONSABILITA' DI OSSERVANZA E ATTUAZIONE

L'osservanza e l'attuazione delle policy sono responsabilità di:
1- Tutto il personale che, a qualsiasi titolo, collabora con l'azienda ed è in qualche modo coinvolto con il trattamento di dati ed informazioni che rientrano nel campo di applicazione del Sistema di Gestione.
Tutto il personale è altresì responsabile della segnalazione di tutte le anomalie e violazioni di cui dovesse venire a conoscenza.

2-Tutti i soggetti esterni che intrattengono rapporti e collaborano con l'azienda. Devono garantire il rispetto dei requisiti contenuti nella presente policy.

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

- condurre l'analisi dei rischi con le opportune metodologie e adottare tutte le misure per la gestione del rischio
- stabilire tutte le norme necessarie alla conduzione sicura di tutte le attività aziendali
- verificare le violazioni alla sicurezza e adottare le contromisure necessarie e controllare l'esposizione dell'azienda alle principali minacce e rischi
- organizzare la formazione e promuovere la consapevolezza del personale per tutto ciò che concerne la sicurezza delle informazioni.
- verificare periodicamente l'efficacia e l'efficienza del Sistema di Gestione.

Chiunque, dipendenti, consulenti e/o collaboratori esterni a SIAP+MICROS, che in modo intenzionale o riconducibile a negligenza, disattenda le regole di sicurezza stabilite e in tal modo provochi un danno all'organizzazione, potrà essere perseguito nelle opportune sedi e nel pieno rispetto dei vincoli di legge e contrattuali.

IMPEGNO DELLA DIREZIONE

La direzione sostiene attivamente la sicurezza delle informazioni in azienda tramite un chiaro indirizzo, un impegno evidente, degli incarichi espliciti e il riconoscimento delle responsabilità relative alla sicurezza delle informazioni.
L'impegno della direzione si attua tramite una struttura i cui compiti sono:

- garantire che siano identificati tutti gli obiettivi relativi alla sicurezza delle informazioni e che questi incontrino i requisiti aziendali;
- stabilire i ruoli aziendali e le responsabilità per lo sviluppo e il mantenimento del SGSI;
- fornire risorse sufficienti alla pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo del SGSI;
- controllare che il SGSI sia integrato in tutti i processi aziendali e che procedure e controlli siano sviluppati efficacemente;
- approvare e sostenere tutte le iniziative volte al miglioramento della sicurezza delle informazioni;
- attivare programmi per la diffusione della consapevolezza e della cultura della sicurezza delle informazioni.

San Fior, 25 novembre 2020

A.D.