Politica di Sicurezza delle Informazioni

MOTIVAZIONE

La mancanza di controllo da parte delle aziende su come i dati e le informazioni vengono generati, dove vengono archiviati e a chi vengono trasmessi comporta il rischio di incidenti di sicurezza e di conformità normativa che possono avere un impatto negativo sull'attività stessa. La sicurezza delle informazioni è, infatti, un asset primario dell'azienda, e l'implementazione di misure efficaci può costituire una strategia che, nel tempo, si trasforma in un vantaggio competitivo.

Per questo motivo, Artificialy SA, specializzata in soluzioni di intelligenza artificiale, è sempre stata all'avanguardia nella protezione e sicurezza delle informazioni. Una misura fondamentale in tal senso è stata l'implementazione di un Sistema di Gestione della Sicurezza delle Informazioni, un insieme di processi organizzativi, tecnici e procedurali basati su best practice e standard di riferimento, anche in conformità con le direttive e lo standard internazionale ISO/IEC 27001:2022.

OBIETTIVI

L'obiettivo del Sistema di Gestione della Sicurezza delle Informazioni di Artificialy SA è garantire un livello di protezione e sicurezza adeguato per la circolazione delle informazioni all'interno dell'organizzazione, al fine di svolgere nel modo migliore la progettazione, lo sviluppo e l'erogazione dei servizi aziendali.

Senza procedure per identificare, valutare e analizzare i rischi, le minacce alla sicurezza a cui sono esposti quotidianamente i servizi e le procedure aziendali potrebbero comprometterne il corretto funzionamento, con possibili conseguenze economiche.

L'insieme delle misure organizzative, tecniche e procedurali stabilite dal Sistema di Gestione della Sicurezza delle Informazioni di Artificialy SA soddisfa i seguenti requisiti di sicurezza fondamentali:

- **Riservatezza**: l'accesso alle informazioni è consentito solo a chi possiede i privilegi appropriati.
- **Integrità**: la gestione delle informazioni (incluse le relative modifiche) è soggetta a vincoli precisi stabiliti dalla governance aziendale.
- **Disponibilità**: gli utenti autorizzati possono accedere liberamente alle informazioni ogniqualvolta ne abbiano bisogno nell'ambito dei processi operativi, e il recupero avviene in modo rapido e intuitivo.

Artificialy SA si propone di posizionarsi nel campo della sicurezza delle informazioni come:

- Un fornitore affidabile e competente nella salvaguardia dell'immagine aziendale.

- Un punto di riferimento in cui gli asset informativi dell'azienda vengono archiviati, custoditi e protetti.
- Un facilitatore della continuità operativa dei processi aziendali.
- Uno strumento pienamente conforme alla normativa applicabile e obbligatoria, che si traduce nella crescita delle competenze aziendali in materia di sicurezza delle informazioni.

CONTENUTO DELLA POLITICA

Qualsiasi informazione necessaria per lo svolgimento delle attività interne, dai dati di prodotto/servizio alla loro configurazione, deve essere protetta durante tutto il suo ciclo di vita, dalla creazione all'utilizzo fino alla dismissione. Il Sistema di Gestione della Sicurezza delle Informazioni fa parte di questo processo, consentendo una gestione delle informazioni sicura, accurata e affidabile, nonché un recupero tempestivo delle stesse.

In conformità con l'attuale standard ISO/IEC 27001:2022, tra le misure preventive richieste dal Sistema di Gestione della Sicurezza delle Informazioni figura la valutazione obbligatoria dei rischi per la sicurezza e del loro potenziale impatto sull'azienda, che deve essere effettuata periodicamente dal Responsabile della Sicurezza delle Informazioni. Il Responsabile della Sicurezza delle Informazioni deve verificare se i requisiti di sicurezza sopra menzionati vengono soddisfatti, analizzare i fattori critici che hanno determinato incidenti di sicurezza e collocarli nel contesto più ampio dei cambiamenti strategici, aziendali e tecnologici già attuati o da attuare.

Lo scopo di questa analisi è valutare il rischio associato a ciascun asset da proteggere rispetto alle minacce identificate. La procedura adottata dal Responsabile della Sicurezza delle Informazioni per effettuare questa valutazione è condivisa con la Direzione, che deve approvare il documento che descrive la metodologia da applicare. Inoltre, la Direzione contribuisce anche a definire i parametri utilizzati per determinare il livello di rischio. Una volta completata la valutazione da parte del Responsabile della Sicurezza delle Informazioni, i risultati vengono riesaminati congiuntamente con la Direzione, che stabilisce se il livello di rischio è accettabile in base alle metriche precedentemente definite. Infine, laddove ritenuto necessario, vengono definite misure di mitigazione del rischio e azioni per migliorare la sicurezza del sistema, sulla base delle priorità, del budget aziendale e della necessità di conformità alla normativa applicabile. Tutte le decisioni vengono prese tenendo conto del valore delle informazioni da proteggere e del verificarsi di eventi che possono incidere significativamente sulla sicurezza del sistema.

RESPONSABILITÀ

Le responsabilità sono distribuite come segue:

IL PERSONALE, che è responsabile del rispetto della politica di sicurezza delle informazioni concordata e deve segnalare al responsabile competente qualsiasi anomalia identificata.

IL COMITATO PER LA SICUREZZA DELLE INFORMAZIONI, che si riunisce almeno ogni sei mesi. È composto dalla Direzione e dal Responsabile della Sicurezza delle Informazioni, sebbene possano essere coinvolti anche dipendenti con le competenze tecniche necessarie per la valutazione di questioni specifiche. La Direzione è responsabile della definizione delle priorità e della promozione delle iniziative in materia di sicurezza delle informazioni, garantendo al contempo l'allineamento con le strategie aziendali e il budget assegnato al progetto.

IL RESPONSABILE DELLA SICUREZZA DELLE INFORMAZIONI, che è responsabile della redazione e della progettazione del Sistema di Gestione della Sicurezza delle Informazioni. In particolare, il Responsabile della Sicurezza delle Informazioni effettua l'analisi e la gestione dei rischi, identificando i criteri e le metodologie più appropriati, ed è responsabile del mantenimento della documentazione necessaria, incluse le procedure di classificazione dei documenti. Il ruolo comprende anche la proposta di misure di sicurezza adeguate e il riesame degli incidenti di sicurezza, insieme alle relative azioni correttive. Inoltre, il Responsabile della Sicurezza delle Informazioni si impegna a promuovere una cultura della sicurezza delle informazioni e a proporre programmi di formazione per il personale.

LE PARTI ESTERNE che interagiscono con Artificialy SA devono rispettare i principi di sicurezza specificati e, laddove ciò non sia espressamente previsto dal contratto, firmare un accordo di riservatezza per l'incarico assegnato.

APPLICABILITÀ

La presente Politica di Sicurezza delle Informazioni si applica a tutti gli organi interni ed esterni dell'azienda ed è vincolante per tutto il personale di Artificialy SA. Si applica inoltre a qualsiasi parte esterna che venga a conoscenza di informazioni gestite dall'azienda. Ciò richiede una previa regolamentazione degli accordi, al fine di garantire che la comunicazione con le parti esterne avvenga nel rispetto delle norme e dei regolamenti applicabili.

RIESAME

Artificialy SA garantisce la verifica periodica dell'efficacia e dell'efficienza del Sistema di Gestione della Sicurezza delle Informazioni. Laddove necessario, e in conformità con il contesto e gli obiettivi aziendali, adotta le misure necessarie per migliorare le politiche di sicurezza e garantirne la corretta implementazione, così da assicurare l'esecuzione continua e sicura di tutti i processi aziendali.