- aumentare il livello di sensibilità e la competenza sui temi della sicurezza da parte del personale.

Nello specifico, per garantire la sicurezza delle informazioni

- ogni accesso ai sistemi è sottoposto a una procedura d'identificazione e autenticazione. Le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui, in modo che ogni utente possa accedere alle sole informazioni di cui necessita, e devono essere periodicamente sottoposte a revisione.
- Sono definite delle procedure per l'utilizzo sicuro dei beni aziendali e delle informazioni e dei loro sistemi di gestione.
- E' incoraggiata la piena consapevolezza delle problematiche relative alla sicurezza delle informazioni in tutto il personale (dipendenti e collaboratori) a partire dal momento della selezione e per tutta la durata del rapporto di lavoro.
- Per poter gestire in modo tempestivo gli incidenti, tutti devono notificare qualsiasi problema relativo alla sicurezza. Ogni incidente deve essere gestito come indicato nelle procedure.
- È necessario prevenire l'accesso non autorizzato alle sedi e ai singoli locali aziendali dove sono gestite le informazioni e deve essere garantita la sicurezza delle apparecchiature.
- E' assicurata la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti.
- E' predisposto un piano di continuità che permetta all'azienda di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulla missione aziendale.
- Sono garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

Il sistema di gestione della sicurezza delle informazioni è creato per rispondere alle esigenze di cui sopra è attuato tramite la definizione e suddivisione dei compiti, la promulgazione di policy e procedure, la verifica della loro attuazione, un processo di analisi e gestione del rischio, la definizione e verifica di obiettivi periodici per il raggiungimento e il mantenimento della sicurezza delle informazioni, la formazione e la sensibilizzazione di tutte le risorse coinvolte, la revisione periodica del sistema stesso per garantirne sempre l'adeguatezza alla situazione aziendale e alla normativa.

La presente politica per la sicurezza si applica a tutti i dipendenti, fornitori, consulenti e terze parti che accedono alle informazioni gestite a qualsiasi titolo da "Datakey Software Engineering S.r.l.".
A loro è richiesto il rispetto delle procedure aziendali che regolano il SGSI nelle proprie attività quotidiane e la collaborazione per la sua buona attuazione. La politica si estende inoltre a tutti i sistemi, processi, strutture e attività che coinvolgono la gestione delle informazioni.

La Direzione della "Datakey Software Engineering S.r.l." ha definito, divulgato e si impegna a mantenere attiva a tutti i livelli della propria organizzazione la presente politica per la Gestione della Sicurezza delle Informazioni.

"Datakey Software Engineering S.r.l." si è sempre adoperata per garantire la protezione dei dati e delle informazioni coinvolte nel processo di "Progettazione ed erogazione di servizi per la gestione dei processi di legal procurement e supporto legale mediante soluzioni tecnologiche software web-based", e dell'infrastruttura fisica, tecnologica ed organizzativa utilizzata nel corso della loro gestione al fine di garantirne:

- 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
- la riservatezza, cioè ad assicurare che l'informazione sia accessibile unicamente ai soggetti e/o ai processi debitamente definiti ed autorizzati;
- l'integrità, cioè a salvaguardare la consistenza dell'informazione da modifiche non autorizzate;
- la disponibilità, cioè ad assicurare che gli utenti autorizzati abbiano accesso alle informazioni quando ne abbiano necessità.

Nella piena consapevolezza che 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.

Già da tempo l'azienda ha deciso di formalizzare il proprio impegno definendo, adottando e sottoponendo a certificazione un Sistema di Gestione della Sicurezza delle Informazioni (SGSI o anche Information Security Management System, ISMS) secondo lo standard ISO 27001, oggi aggiornato alla versione ISO/IEC 27001:2022 ed esteso a UNI CEI EN ISO/IEC 27017:2021 e UNI CEI EN ISO/IEC 27018:2020 per garantire la sicurezza delle informazioni nel contesto della gestione dei dati e delle informazioni acquisite da fornitori terzi e destinate al trattamento di informazioni personali identificabili (PII) dei suoi clienti al fine di:

- dimostrare in modo concreto il proprio impegno nel mantenimento della sicurezza delle informazioni;
- aumentare il livello di soddisfazione e di fidelizzazione della clientela già acquisita;
- suggerire alla clientela potenziale di scegliere la nostra organizzazione, quale partner affidabile e sicuro, che opera in conformità alle leggi e alle normative applicabili in materia di sicurezza delle informazioni;
- rispondere in modo ottimale alle esigenze dei clienti rispetto al panorama normativo che regola la protezione di dati;
- garantire la massima protezione dei dati e delle informazioni;
- assicurare la continuità operativa, minimizzare eventuali danni e massimizzare il ritorno degli investimenti e delle opportunità commerciali, valutando i rischi relativi al trattamento delle informazioni ed attuando le necessarie contromisure;

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.

Il Responsabile del Sistema di Gestione, nell'ambito del Sistema di Gestione provvede a:

- 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.

La Direzione verifica periodicamente e regolarmente o in concomitanza di cambiamenti significativi l'efficacia e l'efficienza del Sistema di Gestione, in modo da assicurare un supporto adeguato all'introduzione di tutte le migliorie necessarie e in modo da favorire l'attivazione di un processo continuo, con cui viene mantenuto il controllo e l'adeguamento della policy in risposta ai cambiamenti dell'ambiente aziendale, del business, delle condizioni legali.
Il riesame dovrà tenere conto di tutti i cambiamenti che possono influenzare l'approccio della azienda alla gestione della sicurezza delle informazioni, includendo i cambiamenti organizzativi, l'ambiente tecnico, la disponibilità di risorse, le condizioni legali, regolamentari o contrattuali e dei risultati dei precedenti riesami.

Roma, lì 01.12.2023

La Direzione _____