L'azienda pone particolare attenzione ai temi riguardanti la sicurezza durante il ciclo di vita di progettazione e sviluppo dei propri servizi e prodotti, che devono essere ritenuti un bene primario dell'azienda.
Il SGSI (Sistema di Gestione per la Sicurezza delle Informazioni) si applica a tutte le attività di analisi, progettazione, sviluppo e manutenzione dei prodotti e servizi.
Consapevole del fatto che i propri servizi per soggetti esterni possono comportare l'affidamento di dati e informazioni critiche, l'unità organizzativa tecnica opera secondo normative di sicurezza riconosciute.
Per questo motivo intende adottare le misure, sia tecniche che organizzative, necessarie a garantire al meglio l'integrità, la riservatezza e la disponibilità sia del patrimonio informativo interno che di quello affidato dai propri Clienti.
Su tali basi l'azienda ha deciso di porre in essere un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) definito secondo regole e criteri previsti dalle best practice e dagli standard internazionali di riferimento in conformità alle indicazioni della norma internazionale ISO/IEC 27001:2022.

L'obiettivo del Sistema di Gestione per la Sicurezza delle Informazioni dell'azienda è di garantire un adeguato livello di sicurezza dei dati e delle informazioni nell'ambito della progettazione, sviluppo ed erogazione dei servizi, attraverso l'identificazione, la valutazione e il trattamento dei rischi ai quali i servizi stessi sono soggetti.
Il Sistema di Gestione per la Sicurezza per le Informazioni dell'azienda definisce un insieme di misure organizzative, tecniche e procedurali a garanzia del soddisfacimento dei sotto elencati requisiti di sicurezza di base:

- RISERVATEZZA: l'informazione deve essere nota solo a chi dispone di opportuni privilegi;
- INTEGRITÀ: l'informazione deve essere modificabile solo ed esclusivamente da chi ne possiede i privilegi;
- DISPONIBILITÀ: l'informazione deve essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti che dispongono dei relativi privilegi.

Inoltre con la presente politica l'azienda intende formalizzare i seguenti obiettivi nell'ambito della sicurezza delle informazioni:

- Preservare al meglio l'immagine dell'azienda quale fornitore affidabile e competente;
- Proteggere al meglio il patrimonio informativo proprio e dei propri clienti;
- Adottare le misure atte a garantire la fidelizzazione del personale e la sua professionalità;
- Rispondere pienamente alle indicazioni della normativa vigente e cogente;
- Aumentare, nel proprio personale, il livello di sensibilità e la competenza su temi di sicurezza.

Tutte le informazioni, che vengono create o utilizzate dall'azienda sono da salvaguardare e debbono essere protette, secondo la classificazione attribuita, dalla loro creazione, durante il loro utilizzo, fino alla loro eliminazione. Le informazioni debbono essere gestite in modo sicuro, accurato e affidabile, e debbono essere prontamente disponibili per gli usi consentiti.
Relativamente all'ambito della progettazione e sviluppo, tale sistema prevede – in conformità alla norma ISO/IEC 27001:2022 – che il Responsabile per la Sicurezza delle Informazioni svolga periodicamente un'analisi dei rischi che tenga in considerazione gli obiettivi strategici espressi nella presente politica, degli incidenti occorsi durante tale periodo e dei cambiamenti strategici, di business e tecnologici avvenuti; l'analisi dei rischi ha lo scopo di valutare il rischio associato ad ogni asset da proteggere rispetto alle minacce individuate.
La Direzione condivide con il Responsabile della Sicurezza delle Informazioni la metodologia da impiegare per la valutazione del rischio, approvando il relativo documento; nella redazione della

metodologia la Direzione partecipa anche alla definizione delle scale di valore da impiegare per valorizzare i parametri che concorrono alla valutazione del rischio.
In seguito dell'elaborazione dell'analisi dei rischi da parte del Responsabile per la Sicurezza delle Informazioni ed in base alla metodologia condivisa con la Direzione, la Direzione stessa valuta i risultati ottenuti accogliendo la soglia di rischio accettabile, il trattamento di mitigazione dei rischi oltre tale soglia e il rischio residuo in seguito al trattamento.
Tale analisi sarà ponderata anche rispetto al valore di business dei singoli beni da proteggere e dovrà identificare chiaramente le azioni da intraprendere che saranno classificate secondo una scala di priorità che rispetti gli obiettivi aziendali, il budget a disposizione e la necessità di mantenere la conformità alle norme e leggi vigenti.
Detta analisi dovrà essere effettuata anche a fronte di eventi che possano modificare il profilo di rischio complessivo del sistema.

Sono assegnate le seguenti responsabilità
Tutti i membri facenti parte dell'organico aziendale che, a qualsiasi titolo, collabora con l'azienda sono responsabili dell'osservanza di questa policy e della segnalazione di anomalie, anche non formalmente codificate, di cui dovessero venire a conoscenza.
La direzione ha il compito di fissare gli obiettivi, assicurare un indirizzamento chiaro e condiviso con le strategie aziendali e un supporto alle iniziative di sicurezza. Promuove la sicurezza garantendo la congruità dei singoli budget destinati alla sicurezza, coerentemente con le politiche e le linee strategiche aziendali definite.
Il responsabile della sicurezza delle informazioni si occupa della progettazione del Sistema di Gestione della Sicurezza delle Informazioni ed in particolare di:

- emanare tutte le norme necessarie ivi inclusa la tipologia di classificazione dei documenti affinché l'organizzazione aziendale possa condurre, in modo sicuro, le proprie attività;
- adottare criteri e metodologie per l'analisi e la gestione del rischio;
- suggerire le misure di sicurezza organizzative, procedurali e tecnologiche a tutela della sicurezza e continuità delle attività dell'azienda;
- pianificare un percorso formativo, specifico e periodico in materia di sicurezza per il personale;
- controllare periodicamente l'esposizione dei servizi aziendali alle principali minacce;
- verificare gli incidenti di sicurezza e adottare le opportune contromisure;
- promuovere la cultura relativa alla sicurezza delle informazioni.

Tutti i soggetti esterni che intrattengono rapporti con l'azienda devono garantire il rispetto dei requisiti di sicurezza esplicitati dalla presente politica di sicurezza anche attraverso la sottoscrizione di un "patto di riservatezza" all'atto del conferimento dell'incarico, allorquando questo tipo di vincolo non sia espressamente citato nel contratto.
La presente politica si applica indistintamente a tutti gli organi dell'Azienda. L'attuazione della presente politica è obbligatoria per tutto il personale L'azienda, così come per i Consulenti e i collaboratori esterni di cui ID & A srl si avvale per la prestazione del servizio, e va inserita nell'ambito della regolamentazione degli accordi nei confronti di qualsiasi soggetto esterno che, a qualsiasi titolo, possa venire a conoscenza delle informazioni gestite in azienda.
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.

Brescia, 10/07/2023