POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Per ARETHUSA la gestione della Sicurezza delle Informazioni ha come obiettivo primario la ***protezione dei dati*** *e delle* ***informazioni*** *al fine di* ***tutelare*** *il patrimonio rappresentato dalle* ***conoscenze aziendali****, quello dei propri* ***clienti*** *e di tutelare le* ***persone fisiche*** *di cui si trattano i* ***dati personali****. Per le caratteristiche dei servizi che ARETHUSA offre ai propri clienti e per il valore che rappresentano le informazioni nel proprio business la Politica della Sicurezza delle Informazioni rappresenta un* ***indirizzo strategico fondamentale e prioritario***

ARETHUSA pone particolare attenzione ai temi riguardanti la sicurezza durante il ciclo di vita di progettazione ed erogazione dei propri servizi, che devono essere ritenuti un bene primario dell'azienda.

Il SGSI (Sistema di Gestione per la Sicurezza delle Informazioni) si applica a tutti i servizi di

Progettazione di ingegneria civile, ambientale, impianti tecnologici e di ingegneria della manutenzione: Servizi di consulenza ambientale e sicurezza negli ambienti di lavoro

ed ai dati ad essi collegati che riguardano il Data Center di ARETHUSA, che raggruppa tutte le apparecchiature e tecnologie che sono necessarie al funzionamento del sistema informativo dell'azienda.

Consapevole del fatto che i propri servizi possono comportare l'affidamento di dati e informazioni critiche, Arethusa opera secondo normative di sicurezza internazionalmente riconosciute.

Per questo motivo si 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 ARETHUSA 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 27001:2017.

L'obiettivo del Sistema di Gestione per la Sicurezza delle Informazioni di ARETHUSA è di **garantire un adeguato livello di sicurezza dei dati e delle informazioni** nell'ambito delle proprie attività, 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 di ARETHUSA 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 ARETHUSA 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 e tra i propri collaboratori interni, il livello di sensibilità e la competenza su temi di sicurezza.

Il SGSI si applica a tutte le attività di Arethusa, ai servizi e ai dati ad esse collegati.

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.

È qui da intendersi con "utilizzo dell'informazione" qualsiasi forma di trattamento che si avvalga di supporti elettronici, cartacei o consenta, in una qualsiasi forma, la comunicazione verbale.

Relativamente all'ambito delle attività operative, tale sistema prevede – in conformità alla norma ISO/IEC 27001:2017 – che il **Responsabile per la Sicurezza delle Informazioni** svolga periodicamente una 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 per 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.

Responsabilità di osservanza ed attuazione
Tutto il personale che, a qualsiasi titolo, collabora con Arethusa è responsabile dell'osservanza di questa policy e della segnalazione di anomalie, anche non formalmente codificate, di cui dovesse venire a conoscenza.
Il Responsabile della sicurezza delle informazioni si occupa della progettazione del Sistema di Gestione della Sicurezza delle Informazioni ed in particolare di:

- 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.
- verificare gli incidenti di sicurezza e adottare le opportune contromisure;

Tutti i soggetti esterni che intrattengono rapporti con ARETHUSA 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.

Applicabilità

La presente politica si applica indistintamente a tutti gli organi aziendali. L'attuazione della presente politica è obbligatoria per tutto il personale ARETHUSA, così come per i Consulenti, 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.

ARETHUSA 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.

Riesame

ARETHUSA verificherà periodicamente l'efficacia e l'efficienza del Sistema di Governo per la Sicurezza delle Informazioni, garantendo l'adeguato supporto per l'adozione delle necessarie migliorie al fine di consentire l'attivazione di un processo continuo, che deve tenere sotto controllo il variare delle condizioni al contorno o degli obiettivi di business aziendali al fine di garantire il suo corretto adeguamento. **Il Responsabile per la Sicurezza delle Informazioni** si riunirà quindi con cadenza almeno annuale con l'Amministratore Unico e con l'ufficio IT, con il compito di fissare gli obiettivi, assicurare un indirizzamento chiaro e condiviso con le strategie aziendali e un supporto visibile alle iniziative di sicurezza. Promuove inoltre la sicurezza garantendo la congruità dei singoli budget destinati alla sicurezza, coerentemente con le politiche e le linee strategiche aziendali definite.

L'Amministratore ritiene che la strategia aziendale più idonea al conseguimento di tale Politica per la Sicurezza delle Informazioni consista nella piena implementazione del Sistema di gestione per la prevenzione della corruzione conforme alla norma **ISO 27001: 2017.**

Casoria 04/11/2021 L'Amministratore