ALL. B - POLITICA DELLA DELLA SICUREZZA DELLE INFORMAZIONI

MISSION AZIENDALE

LA CAAEM S.R.L.S. si prefigge di diventare un'organizzazione riconosciuta dai clienti e dagli operatori della **Pubblica Amministrazione** e delle **Aziende Private di medio-grandi dimensioni** come un'azienda di riferimento per la tipologia di prodotto e servizio ad esse offerto tramite erogazione di servizi che soddisfino le nuove esigenze nate dall'evoluzione dell'organizzazione aziendale, si impegna nella **ricerca e nell'adozione delle migliori tecnologie.**

L'obiettivo primario della **CAAEM S.R.L.S.** è quello di migliorare costantemente l'efficacia e l'efficienza della propria struttura per rispondere al meglio alle necessità dei clienti in termini di qualità del prodotto e del servizio offerto.

E' in questa ottica che la Direzione Generale dell'azienda ha deciso di dotarsi e di mantenere attivo uno strumento di gestione manageriale dell'impresa quale il **Sistema di Gestione della Sicurezza delle Informazioni (RSGI)**, in conformità ai requisiti della norma UNI EN ISO 27001:2022, considerandolo come il modello di gestione che, correttamente inserito e coerentemente applicato nella struttura aziendale, conduce al miglioramento organizzativo e produttivo auspicato.

AGIRE NELL'AMBITO DEL SISTEMA DI GESTIONE PER LA SICUREZZA SIGNIFICA CHE:

- Il cliente è il riferimento principale e pertanto è necessario il massimo impegno di tutti per comprendere le sue aspettative, e per mantenere con questi un rapporto continuativo e di crescita;
- Ogni componente dell'organizzazione non deve limitarsi a svolgere bene il proprio compito ed a conseguire gli obiettivi prefissati, ma deve collaborare per la propria crescita professionale e quella dei propri colleghi di lavoro;
- Gli errori devono essere considerati il patrimonio delle conoscenze ed una opportunità di crescita;
- L'individuazione degli errori è finalizzata alla comprensione delle cause che hanno portato all'insuccesso e devono rappresentare la voglia di riscatto e di rilancio verso futuri nuovi miglioramenti;
- Ogni collaboratore è invitato a fornire suggerimenti per l'individuazione dei punti critici dell'organizzazione e per l'utilizzo più efficace ed efficiente delle risorse disponibili.

POLITICA PER LA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

CONTENUTO

Il SGSI si applica a tutte le attività di:

Progettazione ed erogazione di corsi di formazione professionale

Tutte le informazioni che vengono create o utilizzate dall'azienda devono essere salvaguardate e protette opportunamente, secondo la classificazione a loro attribuita dalla loro creazione, al loro utilizzo fino alla loro eventuale eliminazione. Le informazioni quindi devono essere gestite in modo sicuro, accurato e affidabile e devono essere prontamente disponibili per gli usi consentiti. E' utile sottolineare che per "utilizzo dell'informazione" si intende qualsiasi forma di trattamento che si avvalga di supporti elettronici, cartacei o consenta, in una qualsiasi forma, la comunicazione verbale. Relativamente all'ambito della progettazione e sviluppo, tale sistema deve prevedere, in ottemperanza alla norma ISO IEC 27001:2022 che il responsabile della sicurezza svolga periodicamente una "valutazione dei rischi tenendo chiaramente in considerazione gli obiettivi strategici espressi nella presente politica, degli incidenti occorsi nel periodo e dei cambiamenti strategici di business e tecnologici accaduti; tale analisi dei rischi ha lo scopo di valutare il rischio di ogni asset (o beni con valore utilizzati nella tecnologia dell'informazione o comunicazione) 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 metodologia della redazione inoltre la direzione partecipa alla definizione dei parametri ed alla scala dei valori da impiegare, considerando al termine della valutazione i risultati ottenuti accettando la "soglia di rischio accettabile", il "trattamento di mitigazione dei rischi" oltre tale soglia ed il rischio residuo a seguito del trattamento.

Tale analisi sarà ponderata anche rispetto al valore del business dei singoli beni da proteggere e dovrà identificare chiaramente le azioni da intraprendere da classificare 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 inoltre essere elaborata ogni qualvolta si verifichino cambiamenti tali da incidere sul profilo del rischio complessivo del sistema.

OBIETTIVI

L'obiettivo del sistema di gestione della sicurezza delle informazioni in **CAAEM S.R.L.S.** è di garantire un adeguato livello di sicurezza dei dati e delle informazioni nell'ambito della progettazione, sviluppo ed erogazione dei servizi aziendali tramite l'identificazione, la valutazione ed il trattamento dei rischi ai quali i servizi stessi sono soggetti. Il sistema di gestione della sicurezza delle informazioni di **CAAEM S.R.L.S.** definisce un insieme di misure organizzative, tecniche procedurali a garanzia del soddisfacimento dei sotto elencati requisiti di sicurezza di base:

- **Riservatezza:** ovvero la proprietà dell'informazione di essere nota solo a chi ne ha i privilegi;
- **Integrità:** ovvero la proprietà dell'informazione di essere modificata solo ed esclusivamente da chi ne possiede i privilegi;
- **Disponibilità:** ovvero la proprietà dell'informazione di essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti che ne godono i privilegi.

Inoltre con la presente politica, **la CAAEM S.R.L.S.** intende formalizzare i seguenti obiettivi nell'ambito della sicurezza delle informazioni :

- Preservare al meglio l'immagine dell'azienda quale fornitore affidabile e competente;
- Proteggere il proprio patrimonio informativo;
- 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 sui temi della sicurezza;

RESPONSABILITÀ

Tutto il personale che a qualsiasi titolo collabora con l'azienda è responsabile dell'osservanza della presente policy e a partecipare alla segnalazione delle anomalie, anche formalmente non codificate di cui dovesse venire a conoscenza.

Comitato di sicurezza delle informazioni istituito per incontri pianificati semestralmente.

Fanno parte di tale comitato il **Comitato di direzione tecnica**, il **Responsabile della sicurezza dei dati**, ed il **Responsabile dei sistemi di gestione.** Il compito di tale comitato è quello di fissare gli obiettivi, assicurare un indirizzamento chiaro con le strategie aziendali e promuovere un supporto evidente alle iniziative di sicurezza garantendo la congruità dei singoli budget destinati alla sicurezza.

Responsabile della Sicurezza delle Informazioni che si occupa della progettazione del sistema della Sicurezza delle Informazioni ed in particolare**:**

- Suggerire le misure di sicurezza organizzative, procedurali, tecnologiche a tutela della sicurezza e per la continuità delle attività in e di CAAEM S.R.L.S.;
- Controllare periodicamente l'esposizione dei servizi aziendali alle principali minacce;
- Verificare gli incidenti di sicurezza ed adottare le opportune contromisure;

Responsabile dei Sistemi di Gestione della Sicurezza delle Informazioni (RSGI) che si occupa di**:**

- Emanare tutte le norme necessarie ivi inclusa la classificazione e divulgazione dei documenti affinché l'organizzazione aziendale possa condurre in modo sicuro le proprie attività;
- Pianificare per il personale un percorso formativo specifico e periodico in materia di sicurezza;
- Promuovere la cultura relativa alla sicurezza delle informazioni;
- Contribuire alla definizione delle contromisure da adottare a seguito di eventuali incidenti.

ALL. B - POLITICA DELLA DELLA SICUREZZA DELLE INFORMAZIONI

Tutti i soggetti esterni che intrattengono rapporti con **la CAAEM S.R.L.S.,** devono garantire il rispetto dei requisiti della sicurezza esplicitati dalla presente politica di sicurezza anche tramite la sottoscrizione di un "patto di riservatezza" all'atto del conferimento dell'incarico allorquando questo tipo di vincolo non è espressamente previsto nel contratto.

APPLICABILITA'

La presente politica si applica indistintamente a tutti gli organi dell'azienda. L'attuazione della presente politica è obbligatoria per tutte le risorse della **CAAEM S.R.L.S.,** 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. **LA CAAEM S.R.L.S.** consente la comunicazione e diffusione delle informazioni verso l'esterno solo per il corretto svolgimento delle attività aziendali che avvengono sempre nel rispetto delle regole nonché delle norme e leggi cogenti.

La Direzione Generale della **CAAEM S.R.L.S.,** vuole circondarsi di personale fortemente motivato consapevole che la crescita e prosperità di ognuno è direttamente collegata a quella dell'azienda.

La Direzione Generale della **CAAEM S.R.L.S.** definisce nel **Piano della Direzione** gli obiettivi e gli impegni misurabili per accertare il perseguimento della **Politica della Sicurezza delle Informazioni** e si impegna a fornire alle funzioni aziendali gli strumenti e le risorse necessarie al loro raggiungimento; inoltre si impegna a monitorare periodicamente il Sistema di Gestione per la Qualità e quello della Sicurezza delle informazioni per verificarne la conformità e l'efficacia al fine di consentire l'attivazione di un processo continuo, che deve tenere sotto controllo il variare delle condizioni o degli obiettivi di business aziendali garantendo il corretto adeguamento dei sistemi stessi.

Gli indirizzi generali dell'azienda per il periodo sono:

- ✓ Progettazione, sviluppo, applicazione di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI o ISMS dall'inglese Information Security Management System), secondo lo Standard ISO/IEC 27001:2022.
- ✓ Revisione complessiva dell'immagine aziendale coordinata per prodotti e servizi
- ✓ Incremento delle competenze di ogni risorsa dell'area assistenza
- ✓ Incremento del numero delle offerte accettate
- ✓ Riduzione del numero delle segnalazioni legate a malfunzionamenti dell'applicativo installato
- ✓ Aggiornamento del CRM per gestire i collegamenti fra clienti, moduli applicativi e contratti di manutenzione.
- ✓ Proseguimento dell'azione di definizione del Service Level Management introducendo opportune classificazioni delle segnalazioni di malfunzionamento dei programmi.
- ✓ Formalizzazione delle Policy sui back-up dei dati gestionali interni e dei test e di ripristino degli stessi (Server, PC utente) sia se effettuati da personale interno che da parte del fornitore SW.
- ✓ Gestione dei portatili e dei supporti in dotazione del personale che possono contenere temporaneamente informazioni di utilizzo aziendale in quanto oggetto di informazioni trasferite dal cliente.
- ✓ Miglioramento del livello di sicurezza dell'accesso all'ambiente di lavoro per intrusioni non autorizzate sia durante l'orario di lavoro che extra.
- ✓ Adeguamento degli standard di sicurezza del server con definizione dell'autorizzazione all'accesso della stessa solamente a personale addetto alla manutenzione della struttura informativa.
- ✓ Adeguamento della protezione degli apparati attivi, garantendo ad essi una efficace protezione da urti o danneggiamenti involontari.
- ✓ Mantenimento costante dell'obiettivo incidenti/interruzione di servizio uguale a zero come applicazione coerente ed efficace del Sistema di Gestione per la Sicurezza delle Informazioni

CASORIA (NA), Rev. 02 09/01/2023

La Direzione

CAAEM s.r.l.s.
L'Amministratore Unico
Ing. Cinzia Enza Federico