POLITICA PER LA
SICUREZZA DI DATI E INFORMAZIONI

Contenuti

Premessa

ENGIM progetta e sviluppa sistemi hardware/software basati su tecnologia GNSS e a radiofrequenze per soluzioni "mobile" e per la sicurezza dei lavoratori che operano in solitario.

ENGIM considera la sicurezza delle informazioni come strategica per proteggere il patrimonio informativo proprio e dei clienti per i quali lavora, e per fornire servizi di qualità elevata verso i Clienti che mostrano un crescente interesse per la sicurezza. La sicurezza delle informazioni è diventata un fattore di valenza strategica trasformabile in vantaggio competitivo. L'informazione è ritenuta un asset essenziale per il business aziendale e, come tale, deve essere protetta. ENGIM ha deciso, pertanto, di realizzare e mantenere attivo un Sistema di Gestione per la Sicurezza delle Informazioni e di garantire un adeguato livello di sicurezza dei dati e delle informazioni nell'ambito delle proprie attività produttive anche attraverso l'identificazione, la valutazione ed il trattamento dei rischi ai quali esse stesse sono soggette.

Il Sistema di Gestione per la Sicurezza per le Informazioni di ENGIM definisce un insieme di misure organizzative, tecniche e procedurali a garanzia del soddisfacimento dei 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.

ENGIM, nell'implementazione del proprio sistema di gestione, ha considerato anche le indicazioni fornite dalle linee guida UNI CEI EN ISO/IEC 27017:2021 e UNI CEI EN ISO/IEC 27018:2020 al fine di elevare la sicurezza del proprio sistema ai servizi erogati in SAAS e all'attenzione rivolta alle PII memorizzate in cloud.

Indirizzo strategico e dichiarazione della Direzione

Al fine di fornire l'indirizzo generale e strategico di ENGIM nel breve, medio e lungo termine, per garantire la tutela e la protezione delle informazioni nell'ambito delle proprie attività in accordo con le indicazioni dello standard UNI CEI ISO/IEC 27001, ENGIM ha elaborato la politica in materia di protezione del patrimonio informativo aziendale descritta in questo documento. Per raggiungere gli obiettivi di sicurezza informatica individuati come necessari dalla Direzione, è stato implementato il Sistema di Gestione della Sicurezza delle Informazioni coerente con la politica che l'azienda intende attuare. Il mantenimento del sistema è garantito da un processo continuo di **miglioramento** che coinvolge tutte le funzioni aziendali:

- Il personale, che metterà in atto le politiche ed i requisiti di sicurezza per raggiungere gli obiettivi prefissati;
- I clienti, che avranno garanzie per le loro esigenze di sicurezza, in misura conforme agli impegni assunti da ENGIM;
- I fornitori, che contribuiranno, in quanto partner, al raggiungimento degli obiettivi dell'organizzazione, e accetteranno le politiche di sicurezza ed i rischi connessi alla fornitura.

La Direzione è consapevole che la realizzazione del Sistema di Gestione ha richiesto uno sforzo iniziale significativo e che il mantenimento e il miglioramento continuo devono essere garantiti da un supporto organizzativo adeguato.

A tale scopo l'organizzazione di ENGIM è stata pensata in modo tale che i ruoli e le responsabilità sulla Sicurezza delle Informazioni siano definiti e in grado di operare nella direzione indicata dalla presente politica.

La Direzione renderà disponibili gli investimenti idonei a soddisfare le politiche e gli obiettivi stabiliti e ritiene opportuno affrontare la fase di avvio del Sistema con l'inserimento di risorse esterne che siano in grado di dare il loro supporto qualitativo e quantitativo su tutti gli aspetti inerenti alla sicurezza delle informazioni.

Questa politica rappresenta gli obiettivi ed i requisiti generali emessi dalla Direzione di ENGIM che devono essere recepiti dalle strutture aziendali, ciascuna per lo specifico ambito di competenza, affinché l'attività lavorativa sia conforme a quanto specificato nella presente politica.

Valutazione dei rischi e quadro generale dei controlli

I requisiti di sicurezza sono identificati da una valutazione sistematica dei rischi per la sicurezza con metodologie riconosciute da standard internazionali. Tale valutazione terrà in considerazione anche gli aspetti relativi all'utilizzo di servizi in SAAS e dell'ulteriore criticità dovuta alla conservazione di PII.

I risultati della valutazione dei rischi contribuiranno a determinare le azioni appropriate per la gestione e per l'implementazione dei controlli a protezione contro tali rischi. Ne determinano anche le relative priorità.

La valutazione dei rischi sarà ripetuta periodicamente per affrontare eventuali cambiamenti che potrebbero influenzare il fattore di rischio.

Dalla valutazione dei rischi i costi dei controlli dovranno essere bilanciati dai benefici della protezione contro i danni che il business potrebbe riportare a seguito di difetti nella sicurezza delle informazioni.

Il Patrimonio Informativo aziendale

Qualunque tipo di aggregazione di dati che hanno un valore per l'azienda, indipendentemente dalla forma e dalla tecnologia utilizzata per il loro trattamento e conservazione, contribuisce alla formazione del patrimonio informativo. L'informazione deve essere protetta in tutti i possibili formati nei quali è resa disponibile:

- cartaceo (documenti, lettere, elenchi, etc.)
- elettronico (database, dischi, nastri, etc.)
- verbale (riunioni, conversazioni personali e telefoniche, seminari, interviste, etc.)

A seconda della tipologia e dell'origine, le informazioni che costituiscono il Patrimonio Informativo aziendale possono essere suddivise in.

- Informazioni derivanti dal **Patrimonio Informativo del Cliente,** rappresentate dall'insieme delle informazioni gestite da ENGIM attraverso i processi produttivi e attualmente localizzate nei Data Center gestiti direttamente o indirettamente dall'Azienda. La sicurezza di queste informazioni deve essere garantita per contratto con i Clienti e qualsiasi incidente di sicurezza avrebbe conseguenze dirette sull'immagine e sullo sviluppo del business aziendale.

- Informazioni derivanti dal **Patrimonio informativo interno**, rappresentate da tutte le informazioni interne all'Azienda ed in parte gestite attraverso i Sistemi Informativi. Queste informazioni hanno influenza sulle altre e condizionano direttamente o indirettamente tutte le attività di business.

Le informazioni devono essere valutate per attribuire loro la relativa importanza a livello del business aziendale al fine di implementare contromisure di sicurezza adeguate e proporzionali alle diverse forme ed alle differenti modalità di interazione utilizzate. Particolare attenzione è rivolta alle 'PII' che possono rappresentare una criticità importante per i sistemi in cloud.

Obiettivi e implementazione del sistema

La presente politica di sicurezza delle informazioni individua gli aspetti di sicurezza implementati all'interno dell'organizzazione al fine di supportare la missione di ENGIM e di perseguire gli obiettivi primari di seguito riportati.
Le funzioni aziendali preposte alla gestione e sicurezza delle informazioni hanno il compito di tradurre gli obiettivi individuati e i requisiti generali di sicurezza delle informazioni in contromisure e policy di sicurezza più specifiche, nell'ottica di ottenere un congruo Sistema di Gestione della Sicurezza delle Informazioni.

Gli **obiettivi primari** da perseguire secondo la politica di sicurezza adottata sono i seguenti:

- Ridurre a 0 gli eventi gravi (Ransomware, dirottamento di pagamenti, violazioni gravi)
- Strutturare un reparto IT in grado di avere il controllo sulla sicurezza delle informazioni logiche: mappatura degli asset, valutazione dei rischi e riduzione del livello complessivo di rischio;
- Monitorare le prestazioni del Sistema per la Sicurezza dei Dati: implementare logiche e strumenti per il monitoraggio delle prestazioni di sicurezza (inventario, network monitoring, vulnerability assessment, penetration test, analisi del codice sorgente, stato di protezione dalle minacce, incidenti, monitoraggio di apparati, sistemi e log);
- conformità alle normative vigenti volontarie (ISO 27001 in primis), linee guida relative alla conservazione delle informazioni in SAAS (ISO 27017), attenzione particolare alle PII conservate in SAAS (ISO 27018) e obbligatorie (Reg. Eu GDPR in primis).

Raggiungendo questi obiettivi, la Direzione si aspetta di salvaguardare la reputazione aziendale, il patrimonio fisico e intangibile dell'azienda, la continuità delle operazioni a beneficio di tutti gli stakeholders (clienti, proprietà, lavoratori, fornitori e collettività).
Essi sono ottenuti e mantenuti attraverso la collaborazione dei lavoratori a tutti i livelli, che sono tenuti a:

- garantire la riservatezza, l'integrità e la disponibilità delle informazioni;
- valutare i livelli di rischio;
- monitorare i livelli di sicurezza;
- formalizzare requisiti di sicurezza nelle relazioni con clienti e fornitori;
- garantire una cultura aziendale per la sicurezza delle informazioni e un relativo adeguato livello di competenza;
- pianificare e gestire la continuità del business.

I contenuti delle indicazioni e delle prescrizioni del sistema si applicano a tutto il personale interno ed esterno, alle aziende partner, ai fornitori ed outsourcers ed a chiunque entra in contatto con le informazioni di proprietà di ENGIM o gestite da questa per conto dei clienti.
Tutto il personale che, a titolo di dipendente, consulente o collaboratore, collabora con l'azienda nei processi di progettazione, sviluppo, gestione e controllo dei servizi erogati è responsabile dell'osservanza delle prescrizioni e delle

indicazioni del sistema ed è tenuto a proteggere tutte le informazioni trattate durante le proprie attività lavorative. Il personale, consapevole dell'importanza delle informazioni trattate deve agire per garantire la protezione e provvedere alla segnalazione di anomalie, anche non formalmente codificate, di cui dovesse venire a conoscenza.
Nel caso in cui le regole di sicurezza stabilite siano disattese da dipendenti, consulenti e/o collaboratori dell'azienda, la Direzione di ENGIM si riserva di adottare, nel pieno rispetto dei vincoli di legge e contrattuali, le misure più opportune nei confronti dei soggetti trasgressori.
I soggetti esterni che, intrattengono rapporti con ENGIM 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 nel caso in cui questo tipo di vincolo non sia espressamente citato nel contratto.

Conclusioni

La Politica per la Sicurezza delle Informazioni deve essere sempre coerente con gli obiettivi di business aziendali e pertanto la Direzione si riserva di apportare eventuali modifiche al presente documento in base al conseguimento dei risultati di ENGIM, alle aspettative di tutte le parti interessate, all'andamento del mercato di riferimento.
In accordo alla Politica della Sicurezza delle Informazioni e con cadenza almeno annuale, la Direzione fisserà gli obiettivi per la Sicurezza utilizzando anche i risultati raggiunti nel corso dell'anno precedente. Questa politica è stata approvata dalla Direzione di ENGIM.

Alberto Artioli - 11 Settembre 2024