

SCOPO E CAMPO DI APPLICAZIONE

CODEBASE società cooperativa è un'azienda che opera nel campo della progettazione e assistenza di programmi informatici. Data la natura delle proprie attività, considera la sicurezza delle informazioni un fattore cruciale per la protezione del proprio patrimonio informativo ed un fattore di valenza strategica sul mercato.

Consapevole del fatto che i servizi offerti possono comportare l'affidamento di dati e informazioni critiche, applica il SGSI (Sistema di Gestione per la Sicurezza delle Informazioni) a tutte le attività e ai servizi offerti.

Per questo motivo **CODEBASE società cooperativa** adotta 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 affidatogli dai propri clienti. Su tali basi è implementato il SGSI definito secondo in conformità alle prescrizioni della norma internazionale UNI CEI ISO/IEC 27001:2014.

OBIETTIVI E PRINCIPI

L'obiettivo del SGSI di **CODEBASE società cooperativa** è di garantire un adeguato livello di sicurezza dei dati e delle informazioni attraverso l'identificazione, la valutazione e il trattamento dei rischi ai quali i servizi/prodotti stessi sono soggetti. Inoltre, definisce un insieme di misure organizzative, tecniche e procedurali atte a garantire tale obiettivo.

I macro-obiettivi che **CODEBASE società cooperativa** intende raggiungere con l'implementazione del SGSI sono:

- Il soddisfacimento dei requisiti di riservatezza, integrità e disponibilità delle informazioni relativa al business, ai clienti, ai fornitori e al personale interno.
- Garantire all'organizzazione la piena conoscenza delle informazioni gestite e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione.
- Garantire una chiara allocazione delle autorità e responsabilità per la sicurezza delle informazioni.
- Garantire che il Personale interno abbia un elevato grado di consapevolezza e competenza sul tema della sicurezza delle informazioni;
- Garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati o realizzati senza i diritti necessari;
- Garantire che l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza;
- Garantire che l'organizzazione e le terze parti che collaborano al trattamento delle informazioni, abbiano piena consapevolezza delle problematiche relative alla sicurezza.
- Garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare

l'impatto sul business.

- Garantire che l'accesso alle sedi ed ai singoli locali aziendali avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti.
- Garantire la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti.
- Garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni.
- Garantire la continuità del business aziendale attraverso l'applicazione di procedure di sicurezza stabilite.
- Garantire la conformità alla Norma ISO/IEC 27001:2014, e il suo miglioramento continuo.
- Assicurare il rispetto di tutte le normative Italiane cogenti, legali applicabili.

RESPONSABILITÀ E RIESAME DELLA POLITICA DI SICUREZZA DELLE INFORMAZIONI

La Direzione coordina ed è responsabile del rispetto dei principi e della corretta implementazione del SGSI, in coerenza con l'evoluzione del contesto aziendale e di mercato, valutando eventuali azioni da intraprendere a fronte di eventi come:

- evoluzioni significative del business.
- Cambiamenti significativi del contesto in cui opera l'azienda.
- Cambiamenti significativi rispetto alle aspettative ed esigenze delle parti interessate alle attività dell'azienda.
- Nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio.
- Significativi incidenti di sicurezza.
- Evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni.

La Politica della Sicurezza delle Informazioni è formalizzata come documento del SGSI, e viene periodicamente riesaminata e aggiornata per assicurare il suo continuo miglioramento ed è condivisa con il personale interno, i clienti, i fornitori e terze parti rilevanti.

Caltanissetta, 06 Novembre 2020

La Direzione