## SCOPO E CAMPO DI APPLICAZIONE

***CODEBASE SRL*** 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) ed il SGQ (Sistema di Gestione per la Qualità) a tutte le attività e ai servizi offerti.
Per questo motivo la società CODEBASE SRL adotta le misure, sia tecniche che organizzative, necessarie a garantire al meglio l'integrità, la riservatezza, la disponibilità e la qualità sia del patrimonio informativo interno che di quello affidatogli dai propri clienti. Su tali basi è implementato il Sistema integrato (SGSI e SGQ) definito secondo in conformità alle prescrizioni della norma internazionale UNI CEI ISO/IEC 27001:2022 estesa ai controlli UNI CEI ISO/IEC 27017:2015 e UNI CEI ISO/IEC 27018:2019 e alla norma UNI EN ISO 9001:2015.

## OBIETTIVI E PRINCIPI

L'obiettivo del SGSI di ***CODEBASE SRL*** 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 SRL*** intende raggiungere con l'implementazione del SGSI sono:

- Il soddisfacimento di tutti gli stakeholder interni ed esterni all'organizzazione.
- Monitorare il raggiungimento degli obiettivi per la qualità fissati.
- Monitorare il grado di raggiungimento di soddisfazione dei clienti in relazione ai servizi erogati.
- Di applicare e garantire la conformità ad un sistema di gestione per la qualità conforme ai requisiti della norma UNI EN ISO 9001:2015.
- Il soddisfacimento dei requisiti di riservatezza, integrità e disponibilità delle informazioni relative 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.

- Di applicare e garantire la conformità ad un sistema di gestione per la sicurezza delle informazioni conforme ai requisiti della norma UNI CEI EN ISO/IEC 27001:2022, integrando i controlli previsti dalla stessa norma con le linee guida definite:

    - ISO/IEC 27017:2015 – Prassi per i controlli di sicurezza delle informazioni per i servizi in Cloud

    - ISO/IEC 27018:2019 – Prassi per la protezione dei dati personali trattati nei servizi Cloud pubblici

- Di ottemperare ai requisiti richiesti dall'Agenzia per l'Italia Digitale (AgID) per la qualificazione come fornitori CSP e di servizi SaaS per il Cloud della PA, secondo le circolari AgID n. 2 e 3 del 9/04/2018, e per l'inserimento dei servizi SaaS di Codebase nel Marketplace Cloud previsto nelle circolari stesse.

- Assicurare il rispetto di tutte le normative Italiane cogenti, legali applicabili.

## SERVIZI EROGATI IN MODALITÀ CLOUD

L'organizzazione eroga servizi di cloud computing in modalità SaaS (Cloud Service Provider), Software-as-a-Service) in quanto i servizi all'utente finale sono erogati tramite applicazioni basate sul Web.

Codebase nell'utilizzare la infrastruttura IAAS a supporto dei propri processi acquisisce il ruolo di Cloud Service Customer.

Codebase utilizza un provider certificato CSP(Cloud Service Provider) qualificato Tipo C da AGID.

In relazione alla erogazione di applicazioni informatiche in modalità SaaS tramite piattaforme CLOUD, la Direzione si impegna ad adottare tutti gli opportuni requisiti di sicurezza ed obiettivi di

controllo previsti dalla ISO/IEC 27018 per garantire la protezione dei dati personali degli interessati che gestisce, con particolare riferimento a quelli dei propri clienti.

Rispetto a questi ultimi l'azienda, ai sensi della ISO 27018 e in accordo con la legislazione privacy vigente (GDPR), agisce come "Data Processor" ovvero come Responsabile del Trattamento, dichiarando questo status e i relativi obblighi che ne discendono nei contratti con i clienti.

Tali obblighi sono riportati nelle nomine a responsabile dei fornitori utilizzati da Codebase per svolgere il trattamento.

Codebase crede fermamente che i suddetti principi guida costituiscano l'essenza di una gestione accurata e consapevole della protezione dei dati personali e considera tutto ciò come un fattore imprescindibile non soltanto per assicurare il rispetto dei requisiti cogenti e regolamentati, ma anche per favorire una misura di competitività che fa della protezione dei dati personali una linea strategica di sviluppo del business e crea i presupposti fondamentali per ottenere la fiducia degli stakeholder.

La protezione dei dati personali viene inquadrata nella più ampia sicurezza delle informazioni e pertanto è oggetto di cura e gestione del sistema integrato adottato ed è pertanto intesa come inscindibile dalla politica generale di sistema. La Direzione dedica il medesimo impegno al rispetto della presente politica, nell'assegnare risorse, nel sostenere il personale coinvolto e nell'effettuare riesami di adeguatezza.

**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, 08 Gennaio 2024 La Direzione