Politica per la sicurezza delle informazioni

1. Motivazione

Quid Informatica Spa è una società che opera dal 1987 nel campo dell'Information and Communication Technology. Nel corso degli anni Quid Informatica ha sviluppato una crescente presenza nel settore dei Financial Services, sino a divenire protagonista di riferimento nel segmento Consumer Finance.
Data la natura delle proprie attività, Quid Informatica considera la sicurezza delle informazioni un fattore irrinunciabile per la protezione del proprio patrimonio informativo ed un fattore di valenza strategica facilmente trasformabile in vantaggio competitivo.
Quid Informatica pone particolare attenzione ai temi riguardanti la sicurezza informatica durante il ciclo di vita di progettazione e sviluppo dei propri progetti, servizi e prodotti, che devono essere ritenuti un bene primario dell'azienda.
Consapevole del fatto che i propri servizi per soggetti esterni possono comportare l'affidamento di dati e informazioni critiche, Quid Informatica opera secondo normative di sicurezza riconosciute a livello internazionale.
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 Quid Informatica ha deciso di attuare 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 27001:2022.
Il SGSI si applica a tutte le attività di analisi, progettazione, sviluppo e manutenzione dei prodotti e servizi ed ai dati ad esse collegati.

2. Obiettivi

L'obiettivo del Sistema di Gestione per la Sicurezza delle Informazioni di Quid Informatica è quello di garantire un **adeguato livello di sicurezza dei dati e delle informazioni** relativamente alla ricerca, sviluppo, analisi e progettazione, consulenza tecnica ed organizzativa, vendita ed assistenza di soluzioni software realizzate su specifiche del cliente e di soluzioni software proprietarie.

Tale obiettivo viene perseguito attraverso l'identificazione, la valutazione e il trattamento dei rischi ai quali i servizi stessi sono soggetti, comprendendo i processi trasversali dell'azienda che concorrono alla determinazione della sicurezza informatica nel suo complesso.

Il Sistema di Gestione per la Sicurezza per le Informazioni di Quid Informatica Spa definisce un insieme di misure organizzative, tecniche e procedurali a garanzia del soddisfacimento dei sottoelencati requisiti di sicurezza di base:

1. **Riservatezza**: per assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati e che le informazioni non siano rese disponibili o divulgate a persone o entità non autorizzate;

2. **Integrità**: per salvaguardare la consistenza dell'informazione da modifiche non autorizzate e garantire che l'informazione non subisca modifiche o cancellazioni a seguito di errori o di azioni volontarie, ma anche a seguito di malfunzionamenti o danni dei sistemi tecnologici;

3. **Disponibilità**: per assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati quando ne fanno richiesta e salvaguardia quindi il patrimonio informativo nella garanzia di accesso, usabilità e confidenzialità dei dati, riducendo i rischi connessi all'accesso alle informazioni (intrusioni, furto di dati, ecc.);

Inoltre, con la presente politica Quid Informatica Spa intende formalizzare i seguenti obiettivi nell'ambito della sicurezza delle informazioni:

- il rispetto delle leggi e normative vigenti;
- preservare l'immagine dell'azienda quale fornitore affidabile e competente;
- proteggere il patrimonio informativo proprio e dei propri Clienti;
- garantire l'efficienza operativa e affidabilità dei processi di sviluppo prodotti e servizi correlati;
- aumentare nel proprio personale il livello di sensibilità e la competenza su temi di sicurezza informatica;
- la continuità e l'efficienza dei processi organizzativi e operativi al fine di prevenire e ridurre al minimo l'impatto degli incidenti informatici volontari o casuali sulla sicurezza dei dati/informazioni gestite;
- la protezione dei mezzi resi disponibili, ed il loro corretto utilizzo;
- la salvaguardia della proprietà intellettuale;
- il recepimento delle esigenze e delle necessità delle parti interessate determinate dal cambiamento climatico.

3. Contenuto della politica

La politica per la sicurezza delle informazioni di Quid Informatica si applica a tutto il personale interno e quello delle terze parti che collaborano alla gestione delle informazioni ed a tutti i processi e risorse coinvolte nella progettazione, realizzazione, avviamento ed erogazione continuativa nell'ambito dei servizi.

La politica della sicurezza di Quid Informatica rappresenta l'impegno dell'organizzazione nei confronti di clienti e delle terze parti a garantire la sicurezza delle informazioni, degli strumenti fisici, logici e organizzativi atti al trattamento delle informazioni in tutte le attività.

In sintesi, la politica della sicurezza delle informazioni di Quid Informatica garantisce che:

1. l'organizzazione abbia piena conoscenza delle informazioni gestite e valuti di volta in volta la loro criticità, al fine di agevolare l'implementazione di adeguati livelli di protezione;
2. l'accesso alle informazioni avvenga in modo sicuro e adatto a prevenire i trattamenti non autorizzati o realizzati senza i diritti necessari;
3. l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza;
4. l'organizzazione e le terze parti che collaborano al trattamento delle informazioni siano adeguatamente formate e abbiano piena consapevolezza delle problematiche relative alla sicurezza;
5. le anomalie e gli incidenti aventi ripercussioni sul sistema informativo, sui servizi 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;

6. l'accesso alla sede ed ai singoli locali aziendali avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti;
7. la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti;
8. 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;
9. la Business Continuity aziendale e il Disaster Recovery, attraverso l'applicazione di procedure di sicurezza stabilite;
10. i trattamenti dei dati personali, sia nei casi in cui Quid Informatica operi in qualità di Titolare che nei casi in cui operi per conto terzi in qualità di Responsabile del Trattamento, avvenga nel rispetto del Regolamento Europeo sulla Protezione dei Dati Personali GDPR 679/2016.

4. Responsabilità

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

La **Direzione** ha 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 la sicurezza garantendo la congruità dei singoli budget destinati alla sicurezza, coerentemente con le politiche e le linee strategiche aziendali definite.

Il **Responsabile della Sicurezza delle Informazioni** si occupa della progettazione del **Sistema di Gestione della Sicurezza delle Informazioni** ed in particolare di:

- emanare tutte le norme necessarie ivi inclusa la tipologia di classificazione dei documenti affinché l'organizzazione aziendale possa condurre, in modo sicuro, le proprie attività;
- adottare criteri e metodologie per l'analisi e la gestione del rischio;
- suggerire le misure di sicurezza organizzative, procedurali e tecnologiche a tutela della sicurezza e continuità delle attività di Quid Informatica Spa;
- pianificare un percorso formativo, specifico e periodico in materia di sicurezza informatica per il personale;
- controllare periodicamente l'esposizione dei servizi aziendali alle principali minacce;
- verificare gli incidenti di sicurezza e adottare le opportune contromisure;
- promuovere la cultura relativa alla sicurezza delle informazioni.

5. Riesame

La presente politica viene riesaminata dalla Direzione regolarmente in occasione annuale del riesame della Direzione ed in caso di cambiamenti significativi che influenzano la sicurezza delle informazioni, al fine di garantirne l'idoneità, l'adeguatezza e l'efficacia.

Firenze, 26 settembre 2024

LA DIREZIONE