Politica per la Sicurezza delle Informazioni

CENTRIC

Scopo

Lo scopo del presente documento è quello di descrivere i principi generali di sicurezza delle informazioni definiti da IT CENTRIC al fine di sviluppare un efficiente e sicuro Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), stabilire il quadro di riferimento per gli obiettivi da perseguire e l'impegno della Direzione al soddisfacimento dei requisiti applicabili e al miglioramento continuo delle prestazioni.

Ambito di applicazione

La politica per la sicurezza delle informazioni 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 ed erogazione di servizi di formazione in presenza e a distanza. La sede di riferimento è Corso Trieste, 291 81100 Caserta (CE).

Generalità

Per IT CENTRIC la gestione della sicurezza delle informazioni ha come obiettivo primario preservare la riservatezza, l'integrità e la disponibilità delle informazioni, al fine di salvaguardare il patrimonio rappresentato dagli asset e dalle conoscenze aziendali, soddisfare i requisiti delle parti interessate e tutelare le persone fisiche di cui si trattano i dati personali.
Per le caratteristiche dei servizi che la società offre ai propri clienti e per il valore che rappresentano le informazioni nel proprio business, la politica per la sicurezza delle informazioni rappresenta un indirizzo strategico fondamentale e prioritario.
Per perseguire l'obiettivo primario la Direzione pone grande attenzione alla progettazione, alla gestione e alla manutenzione della propria struttura tecnologica, fisica, logica e organizzativa.
La Direzione impegna, quindi, la propria organizzazione a sviluppare e manutenere un sistema di gestione per la sicurezza delle informazioni nell'ambito delle attività svolte e dei servizi erogati in accordo ai requisiti della norma ISO/IEC 27001, che rappresenta lo standard internazionale di riferimento per preservare la riservatezza, l'integrità e la disponibilità delle informazioni.

Principi generali di sicurezza delle informazioni

Tutte le persone che lavorano e/o collaborano con IT CENTRIC sono impegnate a rispettare i seguenti principi:

1. Riservatezza: 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: 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: assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati quando ne fanno richiesta;
4. Controllo: assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
5. Autenticità: garantire una provenienza affidabile dell'informazione;
6. Privacy: garantire la protezione e il controllo dei dati personali.

La Direzione è fortemente impegnata a una grande responsabilizzazione di tutte le persone che lavorano per e con IT CENTRIC nel garantire la rigorosità del proprio operato per adempiere, con la massima attenzione, ai compiti assegnati.
La responsabilità finale della sicurezza delle informazioni ricade sulla Direzione che ha delegato il Responsabile del sistema di gestione integrato, il Responsabile IT ed i referenti di ciascuna unità organizzativa coinvolta ad attuare quanto necessario.

Quadro generale di riferimento per gli obiettivi per la sicurezza delle informazioni
La Direzione definisce il seguente quadro di riferimento per determinare gli obiettivi per la sicurezza delle informazioni:

- le informazioni critiche per il business aziendale e i dati personali considerati particolari (art. 9 del Regolamento UE 2016/679) devono essere protetti da idonee misure di sicurezza da rivalutare periodicamente in base alla valutazione dei rischi;
- i dati personali, che IT CENTRIC custodisce a qualsiasi titolo (Titolare del trattamento o Responsabile del trattamento nominato da Titolari esterni) devono essere trattati nel pieno rispetto degli obblighi di legge (Regolamento UE 2016/679 sulla protezione dei dati personali; normative e provvedimenti nazionali in materia di protezione dei dati personali);
- i dati e le informazioni devono essere protetti, tramite la messa in opera di idonee contromisure logiche, fisiche e organizzative, da accessi non autorizzati;
- i dati e le informazioni devono conservare le caratteristiche di inalterabilità durante le operazioni di trattamento;
- i dati e le informazioni contenute nei sistemi informativi devono essere prontamente a disposizione degli utenti autorizzati nel momento in cui le richiedono;
- è necessario assicurare il rispetto di tutti i parametri di misurazione della qualità dei servizi erogati così come definiti nei contratti (SLA) e nella documentazione del SGSI;
- gli obiettivi di sicurezza devono essere misurabili e stabiliti in base a:
    - i risultati della valutazione dei rischi, periodicamente e sistematicamente aggiornata sulla base dei dati provenienti dal monitoraggio e dal funzionamento del SGSI;
    - i requisiti legali imposti dal legislatore nazionale e comunitario;
    - i requisiti contrattuali che IT CENTRIC ha accettato nei confronti dei propri committenti.
- il personale aziendale deve ricevere formazione e addestramento sulle modalità di trattamento dei dati e sulla sicurezza delle informazioni;
- IT CENTRIC deve operare nel pieno rispetto della legge sui diritti di proprietà intellettuale nell'utilizzo di pacchetti software commerciali e di altro materiale coperto dal diritto d'autore;
- IT CENTRIC deve aggiornare i propri programmi antivirus per prevenire gli attacchi di virus informatici, con una frequenza strettamente connessa ai rilasci del fornitore qualificato;
- IT CENTRIC adotta un insieme di contromisure per prevenire malicious software;
- IT CENTRIC adotta una politica di gestione degli incidenti di sicurezza e segnalazione a chi di dovere, a garanzia della continua operatività dei processi critici per il proprio il business.

Impegni della Direzione
La politica della sicurezza rappresenta in concreto l'impegno della Direzione 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.

La Direzione con la presente politica si impegna a garantire 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 e ai singoli locali aziendali avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti;
7. siano assicurati la conformità ai 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 siano gestiti al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni;
9. la business continuity aziendale e il disaster recovery siano attuati attraverso l'applicazione di procedure di sicurezza stabilite;
10. i trattamenti dei dati personali, sia nei casi in cui la società operi in qualità di Titolare che nei casi in cui operi per conto terzi in qualità di Responsabile del Trattamento, avvengano nel rispetto del Regolamento Europeo sulla Protezione dei Dati Personali GDPR 679/2016;

La Direzione della IT CENTRIC si impegna infine a:

- adottare un sistema di gestione sicura delle informazioni conforme ai requisiti specificati della norma ISO/IEC 27001;
- mantenere costantemente monitorato il grado di conformità del sistema alle norme e leggi applicabili di natura cogente e volontaria, e gli obblighi contrattuali pertinenti l'ambito di applicazione del SGSI;
- garantire mezzi e risorse idonee al suo mantenimento e miglioramento continuo, in particolare per quanto attiene la mitigazione/riduzione dei livelli di rischio sulla sicurezza delle informazioni e l'adozione di misure idonee a prevenire situazioni anomale e di emergenza;
- rendere consapevoli tutte le persone che dell'organizzazione degli obblighi e delle responsabilità di ciascuno nella gestione della sicurezza delle informazioni e delle conseguenze in caso di eventi, dolosi e colposi, relativi all'utilizzazione non autorizzata, modifica o distruzione di informazioni critiche.

La politica della sicurezza delle informazioni viene costantemente aggiornata e verificata, attraverso un riesame annuale, per assicurare la coerenza con le finalità strategiche dell'organizzazione. La politica è condivisa con l'organizzazione, le terze parti ed i clienti, attraverso la sua pubblicazione sul sito.