Politica Sicurezza delle Informazioni

Connessioni Sicure

Mission: El.Com S.r.l, conformemente a quanto stabilito dallo Standard Internazionale UNI CEI EN ISO/IEC 27001:2024, ritiene strategica l'elaborazione del Sistema di Gestione di Sicurezzadelle Informazioni (SGSI) con lo scopo di ottimizzare i processi aziendali e rendere prioritaria la protezione delle informazioni con la consapevolezza che queste rappresentano risorse essenziali per garantire la business continuity e assicurare fiducia di clienti, dipendenti e, in generale,degli stakeholder.

Questo rappresenta un ulteriore impulso per il costante miglioramento volto alla realizzazione dei seguenti obiettivi:

Obiettivi primari:

- ***Riservatezza***: per garantire che le informazioni siano accessibili solo a persone autorizzate;
- ***Integrità:*** per proteggere l'accuratezza e la completezza delle informazioni;
- ***Disponibilità:*** per garantire che gli utenti autorizzati possano accedere alle informazioni quando necessario.

Altri obiettivi:

- ***Autenticità:*** promuovendo la garanzia delle fonti e una provenienza affidabile delle informazioni;
- ***Completezza:*** considerandola quale sottospecie del principio di integrità, in quanto una manchevolezza equivarrebbe ad una cancellazione non autorizzata;
- ***Non ripudio:*** garantendo che le informazioni, qualora anche complete ed autentiche, siano protette da falsa negazione di ricezione, trasmissione, creazione, sottomissione, trasporto, consegna e ricevuta;
- ***Tracciabilità:*** conoscendo chi ha o avuto accesso a un'informazione e chi l'ha modificata. I dati necessari per tracciare l'informazione devono far parte della informazione stessa.

Per la realizzazione degli obiettivi strategici individuati sopra, El.com si impegna a:

1. Strutturarsi per la definizione di ruoli e responsabilità per una corretta gestione non solo delle informazioni, ma anche di eventuali attacchi, minacce e/o incidenti che impattino la Sicurezza delle informazioni;
2. Analizzare i rischi connessi al trattamento/conservazione/elaborazione delle informazioni;
3. Classificare le informazioni in base al loro valore, rischio e sensibilità ed elaborare/mantenere/implementare politiche aziendali in tema di Sicurezza delle informazioni differenziate e adeguate alla loro protezione;
4. Garantire la gestione dell'accesso alle informazioni, limitandolo al personale autorizzato in relazione al ruolo e alla responsabilità aziendali;
5. Garantire la disponibilità e l'accesso alle informazioni necessarie a tutti i dipendenti che, per ruolo e responsabilità rivestiti, sono autorizzati alla consultazione e/o alla modifica/cancellazione delle informazioni;
6. Adottare misure di sicurezza di tipo tecnico e organizzativo con l'obiettivo di proteggere le informazioni e i dati trattati/conservati/elaborati da accessi non autorizzati, manipolazioni, divulgazioni non autorizzate;
7. Monitorare e tenere traccia di eventuali attacchi/incidenti (violazioni della sicurezza, malware, perdita fisica del dato) garantendo, grazie alle segnalazioni, indagini e risposte appropriate e tempestive che promuovano, inter alia, il miglioramento continuo del Sistema di Gestione di Sicurezza delle informazioni;
8. Mettere in atto strategie e procedure che permettano di prevenire e mitigare gli effetti di eventuali attacchi/incidenti;
9. Elaborare/mantenere/implementare strategie per controllare l'accesso fisico agli ambienti;
10. Formare e informare i dipendenti sulla Sicurezza delle informazioni rispetto alle best practice per una corretta gestione delle password, la sensibilizzazione sulle minacce informatiche e le politiche aziendali relative alla Sicurezza delle informazioni;
11. Sottoporre specifici test agli stakeholder per monitorare il livello di consapevolezza raggiunto e, eventualmente, porre in essere azioni correttive e/o migliorative;
12. Comunicare in modo chiaro e trasparente con gli stakeholder rispetto alle politiche e pratiche adottate per la Sicurezza delle informazioni, anche tramite la pubblicazione sul sito aziendale della Politica sulla Sicurezza delle informazioni;
13. Mantenere un flusso di comunicazione continuo ed efficace con gli stakeholder con l'obiettivo di individuare strategie comuni in relazione alla protezione delle informazioni e accogliere le preoccupazioni/esigenze che potrebbero emergere;
14. L'organizzazione adotta il principio di security by design, garantendo che i requisiti di sicurezza delle informazioni siano integrati sin dalle fasi di progettazione, sviluppo e modifica di processi, sistemi e servizi.