Postel

Posteitaliane

POLITICA

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI E LA CONTINUITA' OPERATIVA

POSTEL

Firmato digitalmente da FANTASIA GIOVANNI
C=IT
O=POSTEL S.P.A.

NoidiPoste

Contesto e Scopo
Postel S.p.A. è la società del Gruppo Poste Italiane che offre servizi di Comunicazione e Gestione Documentale per le Imprese e la Pubblica Amministrazione.

La società opera con oltre 760 dipendenti distribuiti su una sede Direzionale (Roma), due sedi con funzione Commerciale (Milano e Padova), una sede con funzione di Staff e Operative (Genova), quattro Stabilimenti di Produzione (Melzo, Verona, Genova, Pomezia), nove magazzini di archiviazione (Avezzano, Scanzano, Gorgonzola, Bastia Umbra).

Tra i clienti di Postel vi sono le maggiori organizzazioni italiane appartenenti al settore bancario, alle utility, alle telecomunicazioni, alle assicurazioni e alla Pubblica Amministrazione.

Al fine di soddisfare le necessità e le aspettative dei clienti e dei propri partner, Postel ha adottato una strategia orientata a potenziare i propri servizi digitali. Essi devono essere facilmente accessibili dai clienti, sempre disponibili ma soprattutto sicuri. Considerando le molteplici minacce che potrebbero impattare la fruizione di tali servizi, anche in considerazione dell'attuale scenario di crisi internazionale, la sicurezza delle informazioni diventa un elemento imprescindibile per la qualità dei servizi erogati.

A tal fine Postel ha definito ed implementato un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) e un Sistema di Gestione della Continuità Operativa (SGCO), basati sui requisiti definiti dagli standard internazionali ISO/IEC 27001:2017 e ISO 22301:2019, integrati con i processi di business e coerenti con le risorse disponibili. I modelli di governo adottati, inoltre, rispondono alle logiche e alle strategie stabilite dalla Capogruppo Poste Italiane.

Vista l'importanza che i servizi e gli asset tecnologici rivestono nel conseguimento della mission, risulta di prioritaria importanza proteggere i processi tecnologici a supporto del business e del patrimonio informativo aziendale.

A tale scopo la Capogruppo Poste Italiane, ha avviato un processo di internalizzazione dei processi tecnologici che ha coinvolto tutte le Società del Gruppo, tra le quali Postel.

Ne consegue che nel ridefinire i Sistemi di Gestione, Postel tiene conto, nella determinazione dei propri obiettivi, del nuovo modello operativo delle strutture organizzative della Capogruppo deputate al presidio e all'erogazione dei servizi tecnologici che Postel deve assicurare ai propri clienti. Tali obiettivi vengono formalizzati all'interno della documentazione predisposta a supporto del Sistema di Gestione tenendo conto di elementi quali:

- Il Contratto che regolamenta l'erogazione dei servizi tecnologici tra Postel e Poste Italiane.
- Il modello di Gestione della Sicurezza delle Informazioni definito dalla Capogruppo.
- L'Analisi di impatto sui servizi (Business Impact Analisys) e l'Analisi del Rischio secondo le metodologie della Capogruppo.
- La definizione e formalizzazione puntuale di ruoli e responsabilità precise nell'ambito del SGSI e del SGCO
- Il modello operativo adottato dalle funzioni deputate all'erogazioni dei servizi nel perimetro esterno.

Campo di Applicazione
Postel ha definito ed implementato un Sistema di Gestione per la Sicurezza delle Informazioni sul perimetro dei seguenti processi:

- Servizi di mass printing, gestione documentale, conservazione a norma, servizi di firma grafometrica, servizi digitali per la pubblica amministrazione e per i privati, erogati anche in modalità cloud (SAAS) con l'applicazione dei controlli previsti dalle linee guida ISO/IEC 27017 e ISO/IEC 27018 con propria infrastruttura e/o di terzi.
- Servizi di custodia, gestione, indicizzazione, classificazione informatica, supporto logistico e organizzativo degli archivi di deposito.
- Servizi di progettazione e dematerializzazione massiva di documenti

Da punto di vista della Continuità Operativa, sulla base dei possibili scenari di crisi e degli impatti sul piano economico, legale e di immagine, Postel ha individuato nella Conservazione a Norma e Gestione Elettronica Documentale i servizi altamente critici da far rientrare nel perimetro del Sistema di Gestione della Continuità Operativa

Obiettivi
Nell'ambito dei sopra citati Sistemi di Gestione vengono definiti ruoli, responsabilità e attività da realizzare da parte del management aziendale con l'obiettivo di fornire la guida strategica necessaria, assicurare il raggiungimento degli obiettivi stabiliti, assicurare che i rischi siano gestiti nel modo appropriato e verificare che le risorse aziendali siano allocate in modo ottimale.

Allo scopo di tutelare gli interessi di Postel e aumentare la fiducia dei propri clienti e partner, i Sistemi di SI e CO sono parte integrante del processo di Governance dell'Azienda e si pongono i seguenti obiettivi:

- Garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati.
- Garantire all'organizzazione la piena disponibilità delle informazioni gestite e la consapevolezza della loro criticità al fine di implementare adeguati livelli di protezione;
- Garantire che l'organizzazione e il fornitore di servizi tecnologici adottino procedure finalizzate al pieno rispetto dei livelli di sicurezza necessari.
- Garantire un efficace sistema di monitoraggio e relativi indicatori con lo scopo di prevenire eventuali incidenti che possono ridurre i livelli di protezione delle informazioni
- Garantire un efficace e misurabile processo di gestione degli incidenti e gestire correttamente e tempestivamente le necessarie comunicazioni e ridurre il più possibile gli impatti sul business.
- Garantire l'accesso alle sedi aziendali alle sole persone autorizzate a garanzia degli asset presenti.
- Garantire il rispetto della normativa cogente e il rispetto dei requisiti di sicurezza stabiliti nei contratti con i clienti e terze parti.
- Garantire la disponibilità delle informazioni e la resilienza dei servizi di Postel attraverso l'implementazione di soluzioni di continuità del business definite in un apposito Piano di Continuità Operativa dotato di precisi obiettivi ed elementi di verifica tesi a minimizzare gli impatti sul business in caso di crisi, assicurando un rapido ripristino del normale stato di svolgimento delle attività di business e la verifica a posteriori sulle azioni intraprese.
- Assicurare il rispetto dei livelli di servizio attraverso lo sviluppo e l'implementazione di soluzioni di continuità operativa anche in caso di eventi di crisi.
- Garantire la salvaguardia e la tutela delle vite umane a fronte di un evento di crisi;

Responsabilità e Leadership
L'Alta Direzione definisce i ruoli e le responsabilità all'interno dell'organizzazione e si impegna ad assicurare il raggiungimento degli obiettivi della Politica per la Sicurezza delle Informazioni e della Continuità Operativa. Assicura inoltre le risorse necessarie all'implementazione e mantenimento dei due Sistemi di Gestione.

L'organizzazione definisce un processo nell'ambito del quale viene individuata ed erogata la formazione necessaria a garantire una sempre maggiore consapevolezza di tutto il personale sui temi della sicurezza delle informazioni e della continuità operativa.

La Politica integrata della Sicurezza delle Informazioni e per la Continuità Operativa viene comunicata a tutto il personale dipendente e alle parti interessate e aggiornata periodicamente in occasione delle variazioni organizzative rilevanti.

Miglioramento Continuo
L'Alta direzione si impegna al miglioramento continuo dei Sistemi di Gestione per la Sicurezza delle Informazioni e della Continuità Operativa attraverso il riesame e la revisione periodica degli stessi, l'aggiornamento della Policy e delle Procedure emesse allo scopo della piena aderenza alla norma di riferimento.

Firmato
Giovanni Fantasia
Amministratore Delegato

Postel

Posteitaliane