POLITICA della SICUREZZA delle INFORMAZIONI

SCOPO

Le informazioni devono essere sempre protette, qualsiasi sia la loro forma e comunque condivise, comunicate o memorizzate.
La Sicurezza delle Informazioni è la protezione di informazioni da una vasta gamma di minacce, al fine di garantire la business continuità, ridurre al minimo i rischi e massimizzare il guadagno di investimenti e opportunità.

CAMPO DI APPLICAZIONE

- Questa politica sostiene l'organizzazione generale delle politiche per la sicurezza delle informazioni
- Questa politica si applica a tutta l'organizzazione.

OBIETTIVI

⇒ Rischi strategici e operativi per la sicurezza delle informazioni sono compresi e trattati per raggiungere un livello accettabile per l'organizzazione.

⇒ La riservatezza delle informazioni degli interessati, dello sviluppo dei piani annuali e degli eventuali piani di marketing è protetta.

⇒ L'integrità dei documenti contabili è conservata.

⇒ Pubblici servizi web e reti interne soddisfano determinati livelli di disponibilità.

PRINCIPI

- ✓ Questa organizzazione incoraggia l'analisi dei rischi e quindi può tollerare i rischi che potrebbero non essere tollerati in organizzazioni gestite in modo conservativo, a condizione che rischi concernenti le informazioni siano capiti, monitorati e trattati, se necessario, come previsto dal Sistema di Gestione conforme alla norma 27001.
- ✓ Tutto il personale è reso consapevole e responsabile per quanto riguarda la sicurezza delle informazioni rilevanti connesse al proprio ruolo.
- ✓ Sono state assegnate risorse per il finanziamento dei controlli di sicurezza delle informazioni .
- ✓ Nella gestione complessiva del sistema di informazione viene analizzata la possibilità di frode associata all'abuso dei sistemi di informazione.
- ✓ Sono disponibili evidenze oggettive sullo stato della Sicurezza delle Informazioni.
- ✓ I rischi per la Sicurezza delle Informazioni sono monitorati e sono intraprese idonee azioni qualora eventuali cambiamenti generino rischi che non sono accettabili dall'organizzazione.
- ✓ Nel Sistema di Gestione conforme alla norma 27001 sono descritti i criteri per la classificazione del rischio e il livello di accettabilità.
- ✓ Non saranno tollerate situazioni che pongono l'organizzazione in violazione di leggi e norme di legge.

RESPONSABILITÀ

- Il Responsabile della Sicurezza delle informazioni
  i) fornisce supporto per l'organizzazione del personale
  ii) garantisce che i verbali sullo stato della Sicurezza delle Informazioni siano disponibili
  iii) agisce in caso di incidente delle informazioni

- Ogni membro del personale ha responsabilità in materia di Sicurezza delle Informazioni come parte del proprio lavoro.

RISULTATI CHIAVE

1) Gli Incidenti di Sicurezza delle Informazioni non comporteranno costi gravi e imprevisti o un'interruzione di servizi e delle attività commerciali.
2) Le perdite dovute a frodi saranno conosciute e confinate entro limiti accettabili.
3) L'accettazione da parte degli interessati di prodotti o servizi contestualizzati nell'organizzazione non sarà influenzata negativamente dalle preoccupazioni legate alla Sicurezza delle Informazioni.

RELATIVE POLITICHE

Per la corretta implementazione del sistema sono state definite, dall'organizzazione, delle politiche specifiche, raccolte in allegato.