Politica del SGI - Sistema di Gestione Integrato

secondo le normative di riferimento ISO/IEC 27001:2013 e ISO/IEC 20000-1:2018

La Direzione Generale intende proteggere le informazioni da un ampio spettro di minacce allo scopo di assicurare la continuità dei servizi erogati, minimizzare i rischi, garantire il ritorno dagli investimenti, le opportunità di business, il rispetto delle leggi, la redditività. Tutti i dati e le relative elaborazioni per la gestione dei servizi devono essere protetti per garantire che giungano integre a chi deve utilizzarle, che non vadano disperse o peggio ancora che non finiscano nelle mani di concorrenti o di approfittatori.
L'Informazione è un Asset, e come altri Asset materiali o immateriali è essenziale per l'organizzazione Msd Systems; come tale ha anche bisogno di essere protetta. Le protezioni sono tanto più necessarie quanto più l'interconnessione è amplia, la qual cosa espone l'Informazione ad una più larga varietà di rischi e di vulnerabilità: frodi, spionaggio, vandalismi, incendi.
Tutti devono essere consapevoli del problema e garantire il proprio impegno nell'erogazione dei propri servizi, nella condivisione degli obiettivi ed i principi della sicurezza delle informazioni. Sulla struttura organizzativa e sui processi in essere in Msd Systems è stato integrato il SGI cioè un sistema di operazioni e di controlli per gestire il rischio relativo alle informazioni e per fornire ai propri clienti un ottimale servizio IT. In particolare con l'implementazione di questo sistema La Direzione si occupa di:

- Accrescere la consapevolezza sulla sicurezza informatica e sull'importanza della qualità dei servizi erogati;
- Garantire la sicurezza dei dati, delle informazioni aziendali e dei dati personali;
- Fornire fiducia all'interno dell'organizzazione;
- Sviluppare il proprio business attraverso i servizi erogati e la riduzione dei rischi informatici;
- Garantire un continuo aggiornamento delle proprie infrastrutture tecniche ed organizzative;
- Migliorare la gestione delle relazioni con i soggetti terzi;
- Essere compatibili dal punto di vista legale e con tutte le altre norme internazionali vigenti;
- Analizzare i rischi e trattarli sulla base di criteri di accettazione definiti, in ogni caso non compromettendo il rispetto delle leggi dello Stato ed i requisiti contrattuali.
- Rendere consapevoli tutti i dipendenti della necessità di operare responsabilmente mediante formazione a tutti i livelli;
- Introdurre specifiche attività di controllo e precauzioni contro gli incidenti relativi all'erogazione dei servizi e alla sicurezza delle informazioni;
- Prendere adeguati provvedimenti ogni qualvolta si verificheranno delle violazioni.

Il sistema di Gestione Integrato include una serie di aspetti che vengono presi in considerazione per garantire il miglioramento continuo dei processi interni aziendali tra cui:

  - Il monitoraggio di tutti gli eventi con la verifica dell'efficacia dei controlli prescritti ed il successivo riesame;
  - L'attivazione di azioni di miglioramento;
  - La gestione della documentazione e delle registrazioni di sistema;
  - L'addestramento di tutto il personale per conseguire competenza e consapevolezza sulle problematiche della sicurezza delle informazioni e dell'erogazione dei servizi;
  - Audit interni per verificare che i controlli sono efficaci, gli obiettivi dei controlli vengono raggiunti e che le procedure vengono applicate: in sintesi che il SGI sia conforme alla norma di riferimento UNI ISO IEC 27001:2017 ed alla ISO 20000-1:2018;
  - Il Riesame della Direzione;
  - Il miglioramento con Azioni Correttive e Preventive.

Infine, al fine di garantire le adeguate misure di controllo e gestione del sistema di sicurezza informatica, Msd System ha ritenuto opportuno assegnare le seguenti responsabilità:

- Alla Direzione stessa, per definire il Dominio degli Asset da proteggere e valutare le modalità di erogazione dei propri servizi, riesaminando periodicamente lo stato di avanzamento del SGI e l'efficacia della presente politica;
- Al Responsabile SGI, per valutare i rischi cui possono essere esposti i vari Asset e intraprendere azioni di miglioramento;
- Al Responsabile SGI ed AQ, per pianificare i controlli, implementarli e monitorarli, registrare tutte le minacce e altre NC verificatesi in relazione al SGI;
- Ad ogni Dipendente, perché si attenga alle autorizzazioni prescritte e segnali al Responsabile SGI eventuali minacce o eventuali NC riscontrate.

Milano, 19 Maggio 2021 La Direzione