Politica del SGI - Sistema di Gestione Integrato

secondo le normative di riferimento ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 e ISO/IEC 20000-1

La nostra realtà aziendale ha deciso di conformare i propri processi per la gestione ottimale del servizio IT secondo lo standard ISO 20000-1 e per la sicurezza delle informazioni allo standard ISO 27001 con estensione alla ISO/IEC 27017 e ISO/IEC 27018 per quanto concerne la protezione delle informazioni inerenti all'erogazione servizi di sicurezza informatica e servizi cloud computing. L'esigenza nasce dalla necessità di rispondere alle molteplici richieste provenienti dall'esterno, principalmente dai principali Partner di Canale, e dall'interno dell'organizzazione, inclusa la necessità di rispondere a quanto definito dal GDPR in materia di protezione dei dati personali di clienti e dipendenti.

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.
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 la qualità dei servizi erogati e adottare un sistema di gestione del rischio, al fine di garantire la riservatezza, l'integrità e la disponibilità dei dati e di far sì che rispondano ai requisiti di sicurezza delle informazioni;
- garantire un continuo aggiornamento delle proprie infrastrutture tecniche ed organizzative;
- migliorare la gestione delle relazioni con i soggetti terzi;
- rispettare le leggi e direttive in materia di protezione dei dati e di sicurezza delle informazioni nonché delle prescrizioni legislative applicabili ai propri servizi;
- 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 contattando le autorità competenti qualora fosse necessario.

In ambito "cloud services", MSD Systems estende i principi enunciati nella politica anche verso la sicurezza delle informazioni per affrontare la fornitura e l'utilizzo dei propri servizi cloud, assicurando che:

- i requisiti di sicurezza delle informazioni vengano adottati come base alla progettazione e all'implementazione del servizio cloud;

- vengano definiti i rischi derivanti dagli addetti ai lavori autorizzati;

- venga stabilita una multi-tenancy e isolamento del cliente del servizio cloud (compresa la virtualizzazione);

- venga garantito accesso alle risorse del cliente del servizio cloud da parte del personale MSD Systems;

- vengano garantite procedure di controllo degli accessi, tra cui l'autenticazione forte per l'accesso amministrativo ai servizi cloud;

- venga comunicata qualsiasi modifica ai clienti dei servizi cloud durante la loro gestione;

- sia adottata la sicurezza della virtualizzazione;

- venga garantito l'accesso e la protezione dei dati dei clienti dei servizi cloud;

- sia gestito il ciclo di vita degli account dei clienti dei servizi cloud;

- vengano comunicate eventuali violazioni e linee guida per la condivisione delle informazioni a supporto delle indagini.

MSD Systems inoltre si impegna a raggiungere la conformità con la legislazione applicabile in materia di protezione delle PII e con i termini contrattuali concordati tra il responsabile del trattamento delle PII nel cloud pubblico e i suoi clienti (clienti del servizio cloud).

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;
- 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 alle normative di riferimento sopra citate;
- il Riesame della Direzione;
- il miglioramento continuo con Azioni Correttive e di miglioramento.

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, 6 Maggio 2022

La Direzione