POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

a. GLI OBIETTIVI

La sempre più crescente importanza delle informazioni gestite in ambito commerciale e tecnico, visto il campo di attività in cui si trova ad operare, ha fatto rilevare a GPA la necessità di adottare un sistema di gestione per:

- garantire la sicurezza dei dati e delle informazioni interessate che viaggiano sui sistemi informatici, sia aziendale che quelli gestiti per conto del cliente o messi a disposizione dei clienti
- effettuare la gestione informatica dei dati in oggetto.

Lo standard normativo ISO/IEC 27001:2013 rappresenta la norma adatta per creare un sistema di gestione che permetta di assicurare, monitorare, mantenere, migliorare la gestione della sicurezza delle informazioni, evitare la manomissione delle stesse e la sottrazione da parte di terzi, nonché prevedere e ridurre al minimo i rischi cui i dati sono sottoposti.

La creazione di un sistema di gestione della sicurezza delle informazioni (SGSI) proposto dalla ISO 27001 rappresenta un valore aggiunto per GPA che vuole distinguersi nel proprio mercato di riferimento.

I vantaggi dell'adozione di un sistema così concepito possono riassumersi nei seguenti punti fondamentali:

- Accrescere la consapevolezza sulla sicurezza tra lavoratori, Direzione, responsabili, clienti e fornitori, fornendo un sistema di procedure definite sulla base della realtà aziendale che dia risalto alla formazione ed all'informazione nonché alla responsabilità da parte di tutti gli utenti
- Individuare i beni critici per il business dell'azienda, le informazioni e i dati sensibili, interni o meno, fondamentali per la gestione del sistema ed il suo mantenimento
- Garantire un sistema di norme e strutture che vada a perseguire per i punti specificati dalla norma, la sicurezza dei dati e delle informazioni aziendali e delle strutture adibite alla loro conservazione
- Fornire un sistema in cui riporre fiducia, sia all'interno che all'esterno dell'organizzazione
- Aggiornamento e monitoraggio: arricchire cioè la conoscenza, la dimestichezza e la capacità pratica della Direzione nella gestione e nel mantenimento di un sistema di sicurezza dell'informazione
- Sviluppare un corretto sistema di business, attraverso riduzione del rischio di diffusione all'esterno non controllata delle informazioni che si intendono gestire in modo sicuro
- Continuo aggiornamento delle proprie infrastrutture tecniche ed organizzative alla luce delle esigenze riscontrate cogenti e mutevoli (compliance e contract review)
- Migliorare la gestione delle relazioni con i soggetti terzi (comunicazioni, divulgazione delle informazioni, accesso alle informazioni aziendali, livelli di rischio)
- Compatibilità legale con le norme nazionali ed internazionali vigenti in tema di privacy e tutela dei dati personali, diritti di proprietà intellettuale, diritto d'autore, concorrenza. Nonché compatibilità con altri schemi normativi internazionali che regolano l'implementazione di altri sistemi di gestione (es.ISO 9001:2008 Sistema di Gestione per la Qualità)
- Tutela delle credenziali di accesso ai propri sistemi informatici e alle proprie attrezzature da parte dell'utenza aziendale e dei clienti.

L'Organizzazione, strutturando un sistema formato da politiche, manuali, procedure, istruzioni operative, documenti e registrazioni, persegue l'obiettivo di migliorare e mantenere il sistema, evidenziandone punti di forza e di debolezza.
Tutte le azioni che andranno a dare evidenza di un miglioramento o comunque di una gestione con particolari problematiche, saranno oggetto di registrazione e revisione annuale, per valutarne applicazione ed efficacia.

b. IL SISTEMA DI GESTIONE SICUREZZA DELLE INFORMAZIONI (SGSI)

Intendiamo proteggere le informazioni aziendali relative a:

- area commerciale
- area tecnica
- area amministrativa
- sistemi informativi dei clienti

dal più ampio spettro di minacce possibile, allo scopo di assicurare la continuità delle nostre attività, minimizzare i rischi, garantire il ritorno degli investimenti, le opportunità di business, il rispetto delle leggi, la redditività dell'attività aziendale.
Tutti i dati e le relative elaborazioni per la gestione delle nostre attività di business 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 in forma non autorizzata o controllata.
L'Informazione è considerata un asset, e come altri asset sono considerati le strutture materiali o immateriali che la gestiscono. Il controllo dell'informazione è essenziale per l'organizzazione di GPA e 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.

L' intera organizzazione è consapevole del problema e si impegna a condividere gli obiettivi ed i principi della sicurezza delle informazioni.
Sulla struttura organizzativa e sui processi operativi aziendali è stato sovrapposto l'SGSI cioè un sistema di operazioni e di controlli per gestire il rischio. In particolare, con l'implementazione di questo sistema:
• Vengono analizzati i rischi;
• Vengono trattati i rischi sulla base di criteri di accettazione dei rischi stessi, in ogni caso non compromettendo il rispetto delle leggi dello Stato ed i requisiti contrattuali. Pertanto:
accettiamo consapevolmente i rischi se soddisfano quei criteri; alternativamente:

- evitiamo i rischi non permettendo azioni/attività che potrebbero essere causa dei rischi stessi;
- i rischi sono trasferiti a terze parti.

Rendiamo consapevoli tutte le nostre risorse e dipendenti che operano nel vivo del sistema che gestisce le informazioni che si intendono proteggere, della necessità di operare responsabilmente mediante formazione a tutti i livelli;
Introduciamo specifiche attività di controllo e precauzione contro i disastri;
Prenderemo adeguati provvedimenti ogni qualvolta si verificheranno delle violazioni.

Questo sistema include:

- monitoraggio di tutti gli eventi con la verifica periodica dell'efficacia dei controlli prescritti ed il successivo riesame annuale della Direzione;
- attivazione delle azioni di miglioramento;
- gestione della documentazione e delle registrazioni di sistema;
- addestramento del personale per conseguire competenza e consapevolezza sulle problematiche della sicurezza delle informazioni;
- audit interni per verificare che i controlli siano efficaci, gli obiettivi dei controlli vengono raggiunti e che le procedure vengano applicate: in sintesi che il SGSI sia conforme alla norma di riferimento ISO/IEC 27001: 2013;
- miglioramento attraverso le Azioni Correttive e Preventive.

Nell'ambito di questo sistema sono assegnate le seguenti responsabilità:

- Direzione aziendale - la definizione degli Assets da proteggere;
- Security Team - valutazione dei rischi cui possono essere esposti i vari Assets;
- Security Team ed Amministratore di Sistema - l'impostazione dei controlli, la loro implementazione e monitoraggio;
- Security Team ed Amministratore di Sistema - la registrazione di tutte le minacce verificatesi la pianificazione ed implementazione dei controlli necessari;
- Dipendenti che lavorano con i rispettivi assets materiali o immateriali - attenersi alle autorizzazioni prescritte e segnalazione al Security Team o Amministratore di Sistema di eventuali minacce riscontrate;
- Direzione aziendale - riesaminare periodicamente lo stato di sicurezza delle informazioni e l'efficacia della presente politica;
- Security Team e Qualità - proporre alla Direzione e intraprendere azioni di miglioramento.

c. LA GESTIONE

Con GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI (GSI) intendiamo la definizione dei requisiti di sicurezza delle informazioni (nostre e dei clienti), l'analisi dei rischi, la definizione di un piano per soddisfare quei requisiti, nonché l'implementazione del piano stesso.
Abbiamo definito l'elenco degli Assets che dobbiamo proteggere in termini di Hw, Sw, rete, tipologia di dati, località e attività i cui dati sono immagazzinati e/o elaborati nel nostro Sistema Informativo e i sistemi informativi dei clienti.
In particolare, gli assets protetti, inclusi quelli relativi ai requisiti legali e contrattuali, sono:

c.1.HW

Server
Apparati di rete
PC (Client aziendali e Notebook).

c.2 SW

Sistemi Operativi
Software gestionali ed Applicativi
Software di monitoraggio
RETE

c.3 TIPOLOGIA di DATI

Documentazione, dati e registrazioni di origine interna relativa ai processi Aziendali;
Documentazione, dati e registrazioni di origine esterna (di proprietà del cliente).

c.4 LOCALITA'

Datacenter Acantho Imola (BO), via Molino Rosso 8.
Datacenter Supernap, Siziano.
Datacenter Logos Technology Venezia/Mestre (IN FASE DI DISMISSIONE - IPOTESI OTTIMISTICA DI DISMISSIONE: ENTRO META' 2024).
Servizi di Continuità - via Molino Rosso 9/C - Imola (BO).

Le nostre attività sono fortemente dipendenti dal Sistema Informativo: l'assenza di sicurezza o anche la diminuzione del livello di sicurezza comprometterebbero la gestione di quanto sopra espresso in termini di dati.

Dalla GSI intendiamo conseguire i seguenti obiettivi:

- evitare l'accesso ai nostri Sistemi Informativi da parte dei non autorizzati,
- evitare che le informazioni che vengono trasmesse ed elaborate nei nostri Sistemi Informativi vengano modificate, rese non disponibili a chi deve utilizzarle o distrutte intenzionalmente o anche solo accidentalmente.

Dobbiamo anche proteggere l'informazione che attiene alle leggi dello Stato cogenti ed al nostro business.

c.5 REQUISITI PER GARANTIRE LA SICUREZZA DELLE INFORMAZIONI

I requisiti per garantire la sicurezza delle informazioni sono:

***CONFIDENZIALITÀ/RISERVATEZZA**:* attribuzione a ciascun dipendente implicato nel sistema informativo degli accessi fisici e logici al Sistema Informativo secondo responsabilità e mansioni;

***INTEGRITÀ**:* l'informazione deve essere resa disponibile integra a chi ne ha diritto;

***DISPONIBILITÀ**:* l'informazione deve essere disponibile quando richiesta dalle persone autorizzate.

Dobbiamo anche salvaguardare il capitale investito nel Sistema Informativo in termini di hardware, software, e mantenimento del sistema stesso.
Prendere coscienza dei costi che dobbiamo sopportare per sostituzioni e manutenzioni conseguenti a cedimenti della sicurezza. La gestione del rischio è eseguita per gli Asset di cui sopra con la seguente metodologia:

- Analisi alto livello del rischio di ogni Assets con le protezioni in atto;
- Individuazione degli Assets che dall'analisi alto livello presentano un valore dell'Asset non trascurabile "compromesso" dal rischio;
- Analisi di dettaglio del rischio su quegli Assets che dall'analisi alto livello presentano un valore dell'Asset compromesso non trascurabile;

Se dall'analisi di dettaglio il livello di rischio rimane non trascurabile: verificare l'efficacia delle protezioni di Baseline e/o introduzione di nuove protezioni dedicate agli specifici Assets.

Per garantire quanto sopra vengono messe in atto le seguenti contromisure:

- Impostazione ed attuazione dei necessari ed adeguati controlli per la difesa da attacchi o incidenti;
- Rendere edotti tutti i lavoratori e collaboratori di **GPA implicati** nel Sistema Informativo aziendale e quelli dei clienti, delle proprie specifiche responsabilità per evitare comportamenti e prassi operative non idonee;
- Impegno del management a perseguire gli obiettivi per la sicurezza;
- Meccanismi per la distribuzione delle autorizzazioni agli accessi fisici e logici e contromisure in caso di violazione;
- Adozione di un sistema di controllo degli accessi;
- Ogni lavoratore/collaboratore deve essere consapevole della necessità di operare per salvaguardare le informazioni. A tale scopo tutti saranno addestrati a seguire le regole, le procedure che sono state stabilite.
- Introduzione di processi di monitoraggio per valutare l'applicazione e l'efficacia.
- Le politiche adottate sono comunicate a lavoratori e i KPI attraverso la comunicazione a mezzo web;
- Le politiche adottate sono riesaminate annualmente.