# POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

## 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 CATA la necessità di adottare un sistema di gestione per:

- Garantire la sicurezza dei dati e delle informazioni disponibili sui sistemi informatici e presenti in formato cartaceo, sia propri dell'organizzazione che del cliente, o messi a disposizione dei clienti;
- effettuare un'adeguata gestione informatica e fisica dei dati in oggetto.

Lo Standard ISO/IEC 27001:2022 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) in linea con quanto proposto dalla ISO 27001 rappresenta un valore aggiunto per CATA che vuole distinguersi nel rapporto con i propri clienti.

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

- Accrescere la consapevolezza sulla sicurezza tra lavoratori, Direzione, clienti e fornitori, fornendo un sistema di prassi e procedure definite sulla base della realtà dell'organizzazione che dia risalto alla formazione ed all'informazione, nonché alla responsabilità da parte di tutti gli utenti;
- individuare gli asset critici per i servizi dell'organizzazione, le informazioni e i dati particolari, interni o meno, fondamentali per la gestione del sistema ed il suo mantenimento;
- garantire un sistema di norme e strutture che vada a perseguire, secondo 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;
- aggiornare e monitorare: 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 erogazione dei servizi, 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 presenti nell'organizzazione, 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 9001:2015 - 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, prassi, 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.

## Il Sistema di Gestione della Sicurezza delle Informazioni (SGSI)

Intendiamo proteggere le informazioni aziendali relative a:

- personale interno di CATA,
- risultati economici/finanziari e progetti strategici di CATA,
- clienti che accedono ai servizi erogati da CATA,

dal più ampio spettro di minacce possibile, allo scopo di assicurare la continuità delle nostre attività, minimizzare i rischi, garantire il ritorno degli investimenti, il rispetto delle leggi, il controllo e contenimento delle spese sostenute per la gestione dei servizi erogati.
Tutti i dati e le relative elaborazioni per la gestione dei nostri servizi devono essere protetti per garantire che giungano integri a chi deve utilizzarli, che non vadano dispersi o peggio ancora che non finiscano nelle mani di persone fisiche o giuridiche in forma non autorizzata o non controllata.

L'Informazione è considerata un asset, e come altri assets sono considerati le strutture materiali o immateriali che la gestiscono. Il controllo dell'informazione è essenziale per l'organizzazione di CATA 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'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:

- Sono analizzati i rischi;
- sono 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:
  - si accettano consapevolmente i rischi se soddisfano quei criteri; alternativamente:
    - si evitano i rischi non permettendo azioni/attività che potrebbero essere causa dei rischi stessi;
    - i rischi sono trasferiti a terze parti.
  - si rendono 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;
  - si introducono specifiche attività di controllo e precauzione contro i disastri;
  - si valuteranno adeguati provvedimenti ogni qualvolta si verifichino delle violazioni.

Tale Sistema di include inoltre:

- il monitoraggio di tutti gli eventi con la verifica periodica dell'efficacia dei controlli prescritti ed il successivo riesame annuale della Direzione;
- l'attivazione delle azioni di miglioramento;
- la gestione della documentazione e delle registrazioni di sistema;
- l'addestramento del personale per conseguire competenza e consapevolezza sulle problematiche della sicurezza delle informazioni;
- l'attività di audit interno 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: 2022;
- il miglioramento attraverso le azioni correttive e di prevenzione.

Nell'ambito di questo sistema sono assegnate le seguenti responsabilità alle terze parti coinvolte nella gestione della sicurezza dell'informazione:

- Fornitori esterni – La definizione degli assets da proteggere;
- SGSI / Direzione – La valutazione dei rischi cui possono essere esposti i vari assets;

- Fornitori esterni – L'impostazione dei controlli, la loro implementazione e monitoraggio;
- Fornitori esterni – La registrazione di tutte le minacce verificatesi la pianificazione ed implementazione dei controlli necessari;
- Dipendenti che lavorano con i rispettivi assets materiali o immateriali – Il rispetto delle autorizzazioni prescritte e segnalazione al Fornitore esterno e alla Direzione di eventuali minacce riscontrate;
- Direzione – Il riesame periodico dello stato di sicurezza delle informazioni e l'efficacia della presente politica;
- Fornitore esterno – La proposta alla Direzione e l'attuazione azioni di miglioramento.

## La gestione

Con GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI (GSI) intendiamo la definizione dei requisiti di sicurezza delle informazioni (di CATA 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.
In particolare, gli assets protetti, inclusi quelli relativi ai requisiti legali e contrattuali, sono:

- HW
- Server
- Apparati di rete
- PC (Client aziendali e Notebook)
- SW
- Sistemi Operativi
- Software gestionali ed Applicativi
- Software di monitoraggio
- RETE

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).

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 Regionali e Statali in relazione ai servizi offerti.

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 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 Asset con le protezioni in atto definite dal Fornitore esterno;
- 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 non trascurabile (asset potenzialmente compromesso);
- se dall'analisi di dettaglio il livello di rischio rimane non trascurabile: verificare l'efficacia delle protezioni messe a disposizione dal Fornitore esterno 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, collaboratori, clienti e fornitori di CATA**,** implicati nel Sistema Informativo, 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 bacheca aziendale ed a mezzo web;
- le politiche adottate sono riesaminate annualmente.

Trieste, 13/12/2024

La Direzione Generale
Alessandro Quaglio