Politica di Sicurezza delle Informazioni

PREMESSA

Uno degli asset più importanti per FiberCop, sul quale basa il proprio business, è rappresentato dalle ***informazioni***, intese come qualsiasi aggregazione di dati che abbia valore ed interesse aziendale, indipendentemente dalla forma assunta e dalla tecnologia utilizzata per il suo trattamento. La protezione delle informazioni e di tutti gli asset correlati ad esse, costituisce, quindi, un elemento fondamentale per la tutela e la continuità dei processi di business e deve essere gestita attraverso un sistema organizzativo e normativo che indirizza ruoli, responsabilità, strategie e regole da adottare all'interno di FiberCop.

SCOPO E CAMPO DI APPLICAZIONE

Scopo del presente documento è:

- definire gli obiettivi di sicurezza delle informazioni;
- esprimere l'impegno di FiberCop, attraverso il proprio management, a soddisfare i requisiti di sicurezza delle informazioni secondo un processo di miglioramento continuo;
- indicare i requisiti di sicurezza delle informazioni che FiberCop intende adottare.

Il campo di applicazione del presente documento si estende a tutti gli asset aziendali (processi, persone, tecnologie) che trattano informazioni per conto di FiberCop. Le Funzioni di FiberCop dovranno declinare e specializzare, ognuna per l'ambito di competenza ed attraverso opportuni documenti, gli indirizzi espressi dalla presente politica, al fine di raggiungere obiettivi di sicurezza definiti.

DESCRIZIONE DEL PROCESSO E DELLE RESPONSABILITÀ

Obiettivi di sicurezza

Il patrimonio informativo di FiberCop è costituito dall'insieme delle informazioni gestite mediante l'utilizzo di asset aziendali, quali persone, processi, tecnologie, localizzate fisicamente in sedi specifiche o basate su servizi cloud od ancora in completa mobilità, di proprietà di FiberCop o di Terze Parti (es. Fornitori, Partner, collaboratori esterni, clienti).

Gli obiettivi definiti da FiberCop per la protezione delle informazioni sono commisurati:

- in funzione delle normative di riferimento;
- al loro valore rispetto al business;

pertanto, FiberCop si impegna a:

- stabilire regole, priorità, elaborare piani e rendere disponibili le risorse necessarie per la completa adozione del presente documento;
- definire processi, ruoli e responsabilità per la sicurezza delle informazioni;
- garantire un livello di riservatezza, integrità e disponibilità delle informazioni proporzionale al rispettivo valore di business, ovvero alle perdite dirette o indirette che un incidente di sicurezza può determinare sui servizi erogati ai propri clienti;
- garantire la sicurezza dei servizi erogati ai propri clienti previsti nei contratti;

- tutelare la riservatezza delle informazioni strategiche e dei piani industriali per lo sviluppo del proprio business;
- tutelare la propria immagine dai danni causati da un incidente di sicurezza delle informazioni;
- rispettare i requisiti normativi, legislativi e le regole interne in coerenza con il proprio codice etico e di condotta;
- garantire la sicurezza delle informazioni personali dei dipendenti, nel rispetto della normativa vigente ed a tutela del dipendente;
- sensibilizzare e formare il personale sulla sicurezza delle informazioni;
- tenere traccia, analizzare e gestire qualsiasi incidente reale o presunto che interessi la sicurezza delle informazioni;
- collaborare con Enti/Istituzioni nella gestione di incidenti di sicurezza ad impatto nazionale/internazionale;
- collaborare con Enti/Istituzioni per la gestione sicura delle informazioni strategiche trattate sui propri asset;
- collaborare con Enti/Istituzioni al fine di condividere metodologie e best practices da adottare per il continuo miglioramento delle proprie politiche di sicurezza;
- rispettare gli oneri contrattuali inerenti la sicurezza delle informazioni.

Strategia di conseguimento

Per raggiungere gli obiettivi di sicurezza precedentemente descritti, FiberCop ha stabilito di dotarsi di un Sistema di Gestione della Sicurezza delle Informazioni (di seguito SGSI) che abbia le seguenti caratteristiche:

- identifichi un modello adeguato al governo dei processi e delle attività specifiche per la sicurezza del patrimonio informativo, definendo ruoli e responsabilità all'interno di FiberCop;
- contenga un framework di riferimento che supporti l'organizzazione nell'identificare ambiti, priorità di intervento ed allocazione delle risorse necessarie per la piena ed efficace attuazione delle politiche di sicurezza;
- permetta di stabilire le politiche ed identificare le esigenze di sicurezza a partire dall'analisi dei rischi, acquisendo consapevolezza rispetto al livello di esposizione a minacce del patrimonio informativo ed all'impatto di eventuali incidenti di sicurezza sul business aziendale;
- consenta di formalizzare tutte le misure di sicurezza in conformità agli standard internazionali di settore ed alle normative vigenti;
- permetta di valutare i livelli di rischio residuo con l'obiettivo di assicurare un continuo miglioramento del livello di sicurezza del patrimonio informativo e delle risorse aziendali;
- assicuri la verifica dell'effettiva ed efficace implementazione delle misure di sicurezza individuate e ne controlli il mantenimento.

Il SGSI deve essere progettato ed implementato in modo da permette al management di valutare, periodicamente, anche mediante indicatori di performance, i risultati del processo di gestione del

rischio, per indirizzare azioni preventive, correttive o di miglioramento e le necessarie risorse per applicarle.

REQUISITI GENERALI PER LA REALIZZAZIONE DEL SGSI

Nell'ambito del SGSI, gli **Asset** di FiberCop sono stati ricondotti a due categorie:

- **Primari**: appartengono a tale categoria le informazioni di qualunque tipo, nonché i processi;
- **Secondari**: sono tutti gli asset dove vengono trattate le informazioni; appartengono a tale categoria l'hardware, le infrastrutture di supporto, il software, le reti, le postazioni di lavoro (PdL), i dispositivi mobili, i supporti cartacei o digitali, il personale, i fornitori, le sedi fisiche e l'organizzazione.

I requisiti di sicurezza generali, che FiberCop intende adottare, sono definiti sulla base di standard e best practices di sicurezza. Tali requisiti sono di seguito raggruppati per tematica.

- Politiche e procedure per la sicurezza delle informazioni
- Organizzazione della sicurezza delle informazioni
- Relazione con Terze Parti
- Gestione del rischio
- Analisi, Classificazione e modalità di gestione degli asset
- Gestione degli accessi, autorizzazione e tracciamento
- Gestione operativa della sicurezza e delle comunicazioni
- Acquisto, sviluppo e manutenzione degli asset
- Sicurezza dei locali, delle infrastrutture e degli strumenti a supporto delle elaborazioni di informazioni
- Gestione degli incidenti di sicurezza informatica
- Business Continuity
- Conformità a requisiti vigenti, contrattuali ed agli standard di sicurezza
- Sicurezza delle informazioni nella gestione del personale
- Verifiche di sicurezza

A conferma della strategicità attribuita alla sicurezza delle informazioni, FiberCop si è certificata ISO 27001 per il processo di ICT Risk Management