POLITICA PER LA SICUREZZA DELLE INFORMAZIONI, PROTEZIONE DEI DATI E BUSINESS CONTINUITY

La gestione della sicurezza delle informazioni può essere definita come l'insieme delle misure tecnologiche, organizzative, procedurali e legali che consentono a un'organizzazione di gestire i rischi a cui un sistema informativo è sottoposto.

Nell'era della digitalizzazione la creazione e l'utilizzo di tecnologie sempre più innovative richiede l'elaborazione di strategie che consentano di coniugare gli obiettivi di sviluppo sostenibile con l'accrescimento della sicurezza informatica, garantendo un'adeguata continuità operativa.

La centralità del progresso e la necessità della sua sicurezza, gestite nel rispetto della sostenibilità, oggi rivestono un ruolo cruciale per promuoverne un pieno sviluppo e richiedono un impegno da parte degli operatori del settore per mantenere in equilibrio tutti questi elementi.

Telebit comprende l'importanza di valutare le esigenze e le aspettative delle parti coinvolte riguardo al cambiamento climatico. Pertanto, ha esplicitamente incluso questo aspetto nella regolare analisi dei fattori interni ed esterni e delle parti interessate.

La Politica Integrata di Telebit è una dichiarazione d'intenti chiara e concisa che fa parte del Sistema di Gestione Integrato, di cui la Sicurezza delle Informazioni e Business Continuity è parte integrante, sottoscritta e firmata dalla Direzione. Essa dà indicazioni sullo sviluppo delle regole per la protezione delle informazioni, la continuità operativa e il rispetto delle leggi vigenti; risponde ai requisiti di riservatezza, integrità e disponibilità:

- la riservatezza: ovvero le informazioni devono essere accessibili solo da chi è autorizzato;
- l'integrità: ovvero proteggere la precisione e la completezza delle informazioni e dei metodi per la loro elaborazione;
- la disponibilità: ovvero che gli utenti autorizzati possano effettivamente accedere alle informazioni e ai beni collegati nel momento in cui lo richiedono.

La mancanza di adeguati livelli di sicurezza può comportare il danneggiamento dell'immagine aziendale, la mancata soddisfazione del cliente, il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti nonché ai danni di natura economica e finanziaria. Un adeguato livello di sicurezza è altresì basilare per la condivisione delle informazioni.

Ciascun asset aziendale materiale (edifici/impianti, tecnologie, persone} o immateriale (informazioni, organizzazione, business) dispone di adeguate strategie di protezione definite sulla base di specifiche politiche di sicurezza tra loro omogenee[1], finalizzate ad assicurare il costante equilibrio tra valore, rischio e costo necessario per la protezione/tutela.

Per il completo raggiungimento degli obiettivi di sicurezza aziendali, è fondamentale l'integrazione tra tutte le risorse che a vario titolo si occupano di sicurezza delle infrastrutture tecnologiche e le risorse di una specifica funzione aziendale, che deve definire le policy di sicurezza ed armonizzare le tecnologie e le metodologie adottate. La sicurezza aziendale, infatti, per essere un processo efficace, deve essere continua e permeare l'intera struttura aziendale.

La Politica aziendale sulla Sicurezza delle informazioni è declinata in documenti e procedure e policy operative.

Le policy operative costituiscono l'insieme delle regole da applicare a determinate persone e risorse di Telebit coinvolte nella gestione della Sicurezza delle Informazioni. Esse sono state aggregate secondo l'argomento trattato e raccolte in appositi documenti[2]. Le policy operative sono fortemente vincolate all'architettura di sicurezza che

[1] PRI03 Gestione dell'infrastruttura e la Guida all'uso
[2] PRI 03 Gestione dell'infrastruttura e la Guida all'uso

si intende realizzare e per questo motivo sono definite al termine delle fasi di analisi e gestione del rischio. ·
All'interno di Telebit la sicurezza delle informazioni e la protezione dei dati è garantita attraverso le seguenti indicazioni:

- Il personale conosce e applica le policy e le procedure aziendali relative alla sicurezza delle informazioni e alla protezione dei dati.
- Il personale archivia tutte le informazioni e le registrazioni di interesse per Telebit, comprese quelle riguardanti i clienti, in modo da renderle facilmente rintracciabili.
- Tutto il Software presente in Telebit dispone di regolari licenze e le informazioni sulle licenze associate ai singoli sistemi e sono archiviate su data base.
- Meccanismi fisici antintrusione impediscono l'accesso alle sale dove sono ubicati i Data Center di persone non dotate delle necessarie autorizzazioni.
- i Data Center sono predisposti per fronteggiare le emergenze e gli incidenti, sia naturali sia informatici, e garantire sempre la continuità del servizio. Sono in grado di funzionare anche in caso di possibili mancanze di tensione e/o temperature di esercizio non corrette.
- L'accesso logico ai sistemi e alla rete di Telebit è garantito da adeguati livelli di protezione.
- I software sono inoltre costantemente aggiornati per minimizzare il rischio di attacchi esterni.
- L'accesso avviene sempre attraverso login, password e opportuni algoritmi di crittografia possono essere configurati.
- Le più avanzate applicazioni anti-virus permettono di rilevare e rimuovere eventuali virus informatici senza pregiudicare la continuità del servizio.
- L'integrità dei dati è garantita da back-up giornalieri (i dati di back-up sono conservati in luoghi sicuri) e da specifiche procedure di restore.
- Le procedure di Business Continuity e Disaster Recovery assicurano la corretta gestione degli incidenti e delle emergenze da parte del personale.
- Telebit registra ciò che viene intercettato dai firewall perimetrali e dai sistemi di intrusion detection al fine di consentire azioni tempestive per prevenire eventuali attacchi esterni. Specifici meccanismi sono inoltre in grado di fornire la completa tracciabilità delle attività svolte (es.: log, nel rispetto della normativa Privacy).
- Le informazioni e i dati di Telebit, a seconda della classificazione e dei supporti, sono archiviate e protetti da accessi non autorizzati.
- I messaggi di posta elettronica indirizzati all'esterno sono tutelati mediante canali di trasmissioni crittografati e opportunamente classificati ai fini della sicurezza delle informazioni.
- Le connessioni remote a Telebit attivate dall'esterno sono sottoposte a un processo di autenticazione; l'utilizzo di protocolli adeguati garantisce la sicurezza degli accessi remoti.
- Meccanismi di time-out impediscono la presenza di sessioni di lavoro e/o di connessione troppo lunghe.
- Ogni cambiamento dell'infrastruttura in Telebit viene effettuato attraverso un processo strutturato per impedire eventuali perdite di informazioni o introdurre possibili vulnerabilità.

- Eventuali incidenti sono inoltre registrati, gestiti e analizzati onde evitarne il ripetersi e impedire azioni legali di terzi.
- Gli impianti ausiliari dei Data Center (gruppi di continuità, condizionatori, ecc.), al pari delle infrastrutture informatiche e degli applicativi di supporto, sono sottoposti a manutenzione preventiva e correttiva al fine di evitare possibili disservizi sui Data Center stessi.
- Telebit ha investito non solo nelle infrastrutture e nelle procedure operative, ma anche in risorse dedicate alla sicurezza delle informazioni e alla business continuity, costituendo un ufficio ICT preposto e nominando un responsabile dei dati.

Per quanto attiene le informazioni aziendali e del cliente di cui viene a conoscenza nel corso delle proprie attività, il personale di Telebit è soggetto ai vincoli di riservatezza imposti dal CCNL e dalla lettera di assunzione.

Allo stesso modo, eventuali fornitori che dovessero venire a conoscenza di tali tipologie di informazioni sono soggetti ai vincoli di riservatezza imposti dal contratto stipulato con Telebit.

Dosson di Casier, 13/05/2024

Il Legale Rappresentante

telebit S.p.A.
Legale Rappresentante
QUARTA GIACOMO