Tecnodata Trentina srl

Sistema di gestione della sicurezza delle informazioni

Indice generale

1. Introduzione

Il presente documento riporta una sintesi, resa pubblica sul sito istituzionale della società, degli indirizzi in termini di sicurezza che Tecnodata Trentina srl (Tecnodata nel seguito) attua nell'ambito del sistema di gestione della sicurezza delle informazioni proprie e dei soggetti che a vario titolo interagiscono con essa.

Il documento, **nell'ambito di un processo teso al miglioramento continuo della sicurezza dei servizi erogati e dei dati trattati,** viene aggiornato e rivisto in funzione dell'evoluzione della società e dei fattori esogeni che possano influenzare attività e relativi risvolti in materia di sicurezza.

Tecnodata assume per se stessa e per i servizi erogati ai clienti comportamenti e prassi di sicurezza orientate al rigoroso rispetto degli accordi contrattuali, comportamenti etici, prescrizioni normative applicabili al contesto proprio e dei propri clienti.

2. Obiettivi di fondo perseguiti dalla politica sicurezza Tecnodata

L'obiettivo di fondo perseguito dalle politiche di sicurezza adottate da Tecnodata è quello di limitare e contenere i fattori di rischio che potrebbero compromettere riservatezza, accuratezza e disponibilità delle informazioni e dei servizi erogati da Tecnodata sul mercato o utilizzati per gestione interna.

Scopo delle politiche di sicurezza, come accennato negli impegni assunti da Tecnodata sul mercato, è anche quello di governare e limitare i fattori di rischio che possano determinate mancanze negli impegni presi da Tecnodata nel rispetto su accordi contrattuali, comportamenti etici, prescrizioni normative applicabili al contesto proprio e dei propri clienti.

3. Principali ruoli e riferimenti interni

Al perseguimento degli obiettivi di fondo sopraccennati concorre in misura diversa tutto il personale Tecnodata:

- la direzione stabilisce i parametri di riferimento per il conseguimento degli obiettivi di fondo avendo cura di esaminarli e rivederli periodicamente alla luce delle evoluzioni negli scenari di minaccia, nell'ambito del proprio mandato istituzione di governo generale della società;
- le funzioni operative svolgono, applicando i concetti etici e di diligenza parte integrante del sistema Tecnodata, i controlli operativi di primo livello, eseguiti nel corso delle attività lavorative di erogazione dei servizi;
- le funzioni apicali preposte alla sicurezza e controllo svolgono i controlli di secondo e terzo livello miranti con attività specifiche di manutenzione e controllo su dispositivi, applicazioni, dati a mantenere il livello di rischio residuo contenuti su livelli connaturati alla natura merceologica della società

4. Principali riferimenti normativi e gestione rischi di compliance

Il contesto operativo in cui Tecnodata svolge la sua attività è assoggettato a numerose norme di governance che regolamento vari aspetti. Nello specifico sono presenti due grandi raggruppamenti:

- norme direttamente applicabili a Tecnodata in relazione alle attività svolte sul mercato. Rientrano in tale raggruppamento le norme attinenti le comunicazioni elettroniche (riconducibili principalmente al Dlgs 259/2003 e alle direttive europee sui servizi di comunicazione elettronica), il commercio elettronico (principalmente riconducibile ai Dlgs 70/2003, Dlgs 206/2005, Dlgs 21/2014 e alle delibere AGCOM), la cybersecurity (principalmente riconducibile alle regolamentazioni NIS2, DORA e ai correlati provvedimenti attuativi emessi dai legislatori europei e nazionali nonché dalle authority di riferimento ACN/AGID). Si aggiungo inoltre le norme attinenti la privacy, la sicurezza del lavoro, i reati informatici indicati dal codice civile, le normative volontarie di qualità secondo gli standard ISO.
- norme indirettamente applicabili a Tecnodata in relazione alle norme applicabili ai clienti e che indirettamente ricadono anche su Tecnodata. Esse variano in funzione della tipologia del cliente e hanno un perimetro di applicazione limitato dai servizi erogati.

Con riferimento ai rischi di compliance applicabili al contesto TECNODATA derivanti dalle sopracitate norme, la politica di fondo adottata da Tecnodata è di non ammettere deroghe su tematiche di inadempienza normativa. Pertanto il rischio di compliance viene gestito e monitorato al più alto livello aziendale.

5. Indirizzi di sicurezza adottati nei vari ambiti di riferimento

Il perseguimento degli obiettivi di fondo di cui sopra viene declinato in una serie di iniziative su dati, applicazioni, infrastrutture nel seguito sinteticamente illustrate.

Argomento	Orientamento
Sicurezza delle informazioni	Rientrano in tale ambito gli indirizzi che Tecnodata adotta per limitare i rischi di sicurezza legati alla possibilità che le informazioni proprie o dei clienti possano subire perdite in termini di riservatezza, integrità e disponibilità delle stesse. Gli orientamenti adottati da Tecnodata in tal senso sono. • al fine di garantire la **riservatezza** delle informazioni sono attive prassi di classificazione delle stesse associate a pratiche di vincolo sugli accessi alla rete e ai dati da parte degli account mediante l'utilizzo di firewall, sistemi di composizione delle password articolati e controlli sulla coerenza degli account tra la mansione svolta e i dati che devono essere acceduti per lo svolgimento della medesima. I criteri di riservatezza vengono inoltre estesi anche alle informazioni cartacee per le quali Tecnodata adotta regole di conservazione in locali ad accesso ristretto e regole di utilizzo improntate al concetto di "scrivania pulita" a cui tutti lavoratori facenti parte dell'organico si attengono al termine della giornata lavorativa; • al fine di garantire **l'integrità** delle informazioni sono attive prassi tendenti ad impedire l'utilizzo delle informazioni con sistemi di accesso a reti e dati vincolati da firewall e sistemi di composizione delle password nonché a svolgere controlli rivolti a tracciare gli accessi alle stesse. L'integrità delle informazioni può inoltre dipendere anche dal corretto funzionamento degli applicativi che pertanto sono oggetto di tutele nel loro uso e manutenzione. Si rimanda per questi aspetti l'apposito riquadro dedicato alla sicurezza degli applicativi nel seguito esposto; • al fine di garantire la **disponibilità** delle informazioni sono attive prassi tendenti a duplicare con sistematicità informazioni e applicazioni residenti sui server nonché garantire la continuità operativa delle infrastrutture e risorse dedicate all'erogazione dei servizi applicando sulle stesse il principio della duplicazione e ridondanza. Si veda per questi aspetti l'apposito riquadro dedicato alla sicurezza delle infrastrutture nel seguito esposto.
Sicurezza delle applicazioni	Rientrano in tale ambito gli indirizzi che Tecnodata adotta al fine di proteggere gli applicativi in uso sui server, per uso proprio o per i clienti, da utilizzi impropri oppure per evitare l'utilizzo di applicativi contenenti elementi di disturbo alla sicurezza dati. In sintesi essi sono riconducibili ai seguenti punti: • accesso vincolato agli ambienti ove risiedono gli applicativi. Il vincolo viene stabilito, per i dati interni, da una procedura autorizzativa che prevedere l'utilizzo in base alla mansione. Sugli applicativi in uso ai clienti, viene garantito un sistema di protezione ex-ante per impedire l'utilizzo dell'applicativo se non da strutture autorizzate dallo stesso cliente; • utilizzo, per suo interno, di applicativi di comprovata affidabilità e reputazione appurata con ricerche e analisi ante-utilizzo; • sistematica attività di scansione, con adeguati strumenti di sicurezza informatica, sugli eseguibili scaricati da internet o di non comprovata affidabilità e reputazione; • conservazione ridondata tramite sistematiche azioni di back up delle versioni delle applicazioni uso; • costante attività manutentiva sulla base delle indicazioni fornite dai fornitori degli applicativi, sentite anche ove possibili, opinioni "rumors" da fonti e contatti specialistici.
Sicurezza della infrastruttura tecnica e organizzativa	Rientrano in tale ambito gli indirizzi che Tecnodata adotta sull'infrastruttura tecnico/organizzativa di supporto al funzionamento dei servizi affinché la stessa possa operare in sicurezza e garantire la continuità nell'erogazione dei medesimi. In sintesi essi sono riconducibili ai seguenti punti: • accesso fisico vincolato alle infrastrutture dei centri elaborazione dati • duplicazione dei centri di elaborazione con veloci criteri di ripartenza • adozione di dispositivi hardware di provata affidabilità con costante attività manutentiva sugli stessi • adozione di adeguate misure di sicurezza sui rischi catastrofali legati agli edifici ove sono residenti i macchinari con annessi controlli periodici svolti da soggetti specializzati • adozione, con adeguati strumenti di monitoraggio remoto, di metodiche di osservazione del funzionamento dei dispositivi distribuiti sul territorio, con veloci tempi di reazione in caso di malfunzionamento degli stessi • ridondanza nelle competenze delle strutture organizzative in grado di sopperire a eventuali assenze