Politica per la Sicurezza delle informazioni

La Direzione Aziendale di TECNIT SRL considera il proprio Sistema di Gestione per la sicurezza delle Informazioni uno strumento strategico per il conseguimento dell'eccellenza, un obiettivo da perseguire in tutte le attività svolte dalla azienda. TECNIT opera nel settore della **"Gestione della riservatezza, integrità e disponibilità dei dati nella progettazione, realizzazione, assistenza e gestione di sistemi elettronici in ambito sicurezza, telecomunicazioni e reti telematiche.."**

La Direzione Aziendale ha definito la propria politica SI attraverso il presente documento ed assicura che tale Politica sia comunicata e compresa all'interno ed all'esterno della Società attraverso le seguenti azioni:

- Riunioni annuali con il personale e i collaboratori coinvolti nei processi critici;
- Esposizione della Politica in punti visibili dell'azienda;
- Pubblicazione del documento sul proprio sito internet;
- Riferimento a documenti contrattuali con fornitori esterni (ove necessario).

In tale ambito l'azienda si impegna ad operare in sostanziale accordo con la Norma ISO/IEC 27001:2017. La strategia espressa dalla Direzione Aziendale per la Propria Politica, affinché questa sia compresa, attuata e sostenuta ad ogni Livello Aziendale, è riassunta nei seguenti punti:

- Assicurare il rispetto dei Livelli di Servizio (SLA) definiti in sede contrattuale con il cliente per quanto attiene il livello di Sicurezza delle Informazioni;
- Assicurare standard di sicurezza crescenti nel tempo tramite:
  - Valutazione, trattamento e controllo dei rischi
  - Effettuazione di periodici monitoraggi sulle performance di sicurezza
  - Verificare il rispetto di elevati standard di sicurezza da parte di fornitori di servizi IT
- Comunicazioni al personale in merito alla necessità di soddisfare gli obiettivi, le politiche e i requisiti cogenti applicabili (leggi, regolamenti);
- Garantire l'impegno aziendale al miglioramento continuo e al perseguimento degli obiettivi;
- Pianificazione e assicurazione della disponibilità delle risorse (materiali e umane, in termini di quantità e competenza);
- Elevare le capacità professionali e le competenze di tutto il Personale, e perseguire l'obiettivo di allocare sulle varie attività operative le risorse più adatte allo svolgimento delle stesse;
- Effettuare periodicamente il riesame della Analisi del Contesto, della Analisi dei Rischi, delle aspettative delle parti interessate del Sistema;
- Garantire un adeguato controllo al fine di permettere l'accesso solo a personale autorizzato;
- Impegnarsi a creare un'efficace classificazione e trattamento delle informazioni;
- Massimizzare la sicurezza del sito da minacce fisiche o ambientali;
- Implementare politiche di "Clean Desk" e "Clean Screen" volte a precludere l'accesso a informazioni riservate a persone non autorizzate;
- Effettuare periodicamente azioni di back up al fine di evitare perdite o distruzioni di dati;
- Garantire la sicurezza durante il trasferimento di informazioni;
- Implementare un sistema di controlli sulla crittografia per migliorare il grado di sicurezza delle informazioni;
- Gestire in modo mutuamente vantaggioso i rapporti con i fornitori aziendali per condividere l'obiettivo della salvaguardia della sicurezza delle informazioni;
- Perseguire la piena e rigorosa conformità alle norme nazionali e internazionali in materia di protezione dei dati personali, in particolare il GDPR.

Gli obiettivi specifici saranno definiti annualmente dalla Direzione e formalizzati mediante il piano annuale di miglioramento allegato al Verbale di Riesame e diffusi a tutto il personale dipendente.

Elmas, 15/02/2021

La Direzione