SIPLES Srl

Politica per la Sicurezza delle Informazioni

La SIPLES Srl si occupa di lavorazioni e servizi di in ambito navale e industriale, in particolare: TRATTAMENTI PROTETTIVI DI PONTI DI VOLO E PONTI COPERTI E SCOPERTI SU UNITA' NAVALI. SABBIATURE A RECUPERO E VERNICIATURE NAVALI ED INDUSTRIALI.

- Scopo. La SIPLES S.r.l. ha stabilito la politica di sicurezza delle informazioni con l'obiettivo di garantire una protezione adeguata dei dati, delle informazioni e dei sistemi informatici aziendali destinati al supporto ed all'elaborazione. La presente politica rappresenta un documento di riferimento di livello strategico, dal quale derivano e a cui si ispirano ulteriori politiche specifiche e procedure tecniche inerenti alla Sicurezza delle Informazioni.
- Obiettivi. L'azienda persegue come obiettivo prioritario l'armonizzazione delle misure di protezione delle informazioni, al fine di evitare frammentazioni non giustificate se non per motivi specifici, tra cui:

• Informazioni soggette a vincoli di riservatezza previsti da normative nazionali o regolamenti europei;
• Informazioni la cui riservatezza è richiesta da soggetti privati tramite specifiche clausole contrattuali;
• Informazioni strategiche aziendali;
• Dati la cui perdita o alterazione potrebbe comportare impatti economici rilevanti;
• L'approccio alla protezione delle informazioni si basa sui tre principi fondamentali della Sicurezza delle Informazioni:
• Riservatezza: garantire che l'accesso alle informazioni sia riservato ai soli soggetti autorizzati;
• Integrità: preservare l'accuratezza e la completezza delle informazioni;
• Disponibilità: assicurare che le informazioni siano fruibili dagli utenti autorizzati quando necessario.

La SIPLES S.r.l. considera essenziale proteggere le informazioni e i sistemi aziendali da minacce fisiche e danni ambientali. A tal fine, adotta misure volte a limitare l'accesso non autorizzato a immobili, server e infrastrutture critiche, attraverso strumenti quali il controllo degli accessi fisici, antintrusione, videosorveglianza e l'utilizzo di dispositivi di sicurezza. Inoltre, l'azienda tiene in considerazione i rischi ambientali, come incendi o altre calamità naturali, implementando adeguate misure di protezione, quali sistemi antincendio e soluzioni di backup energetico, al fine di garantire la continuità operativa.

Principi di gestione operativa delle comunicazioni. La SIPLES S.r.l. si impegna a garantire una gestione operativa efficace delle proprie infrastrutture informatiche, assicurando il rispetto dei requisiti di sicurezza. Questo implica una gestione ottimale delle risorse, la manutenzione periodica dei sistemi e una pianificazione operativa che riduca al minimo i rischi, mediante l'impiego di tecnologie idonee e l'adozione di procedure specifiche per la gestione e la trasmissione delle informazioni.

Controllo degli accessi. Il controllo degli accessi, sia logici che fisici, rappresenta un aspetto fondamentale per la SIPLES S.r.l., che si impegna a garantire che solo il personale autorizzato possa accedere a dati sensibili e sistemi critici. Il controllo degli accesi fisici alle aree aziendali, la gestione adeguata delle credenziali, l'adozione di autenticazioni e la restrizione dei permessi in base ai ruoli e alle responsabilità aziendali risultano determinanti per la protezione di progetti, dati tecnici e altre risorse strategiche.

Gestione della continuità operativa. L'azienda ritiene essenziale adottare strategie volte a garantire la continuità operativa anche in situazioni di emergenza o interruzioni impreviste. L'implementazione di un piano di continuità operativa consente di mantenere attive le funzioni aziendali critiche, grazie all'adozione di sistemi di backup regolari, piani di ripristino in caso di disastro e l'identificazione di fornitori o risorse alternative che possano supportare le operazioni in caso di guasto.

-Leadership. Attraverso la presente politica, la Direzione della SIPLES S.r.l. manifesta il proprio impegno a:

• Effettuare un monitoraggio costante dei processi per garantire la protezione delle informazioni nell'ambito del Sistema di Gestione della Sicurezza delle Informazioni;
• Favorire il miglioramento continuo del sistema stesso;
• Documentare, analizzare e gestire tempestivamente eventuali violazioni o incidenti di sicurezza, individuandone le cause principali e adottando misure correttive adeguate;
• Promuovere la formazione continua e la sensibilizzazione del personale in materia di sicurezza delle informazioni, sottolineando l'importanza del loro contributo per l'efficacia del sistema;
• Gestire i rischi connessi alla conservazione e al trattamento delle informazioni, mantenendoli entro livelli accettabili.

-Distribuzione e comunicazione. Il presente documento è di dominio pubblico ed è consultabile liberamente dalle parti interessate. Inoltre, viene reso accessibile a tutto il personale aziendale.

Taranto: 31/03/2025 La Direzione: