

Nell'ambito della sicurezza delle informazioni la Direzione attribuisce importanza strategica al trattamento delle informazioni e concretizza la volontà di difendere la confidenzialità, l'integrità e la disponibilità dei dati.

Gli obiettivi principali del SGSI si realizzano nell'assicurare:

1. La **riservatezza** del patrimonio informativo gestito: proprietà per cui l'informazione non è resa disponibile o comunicata a individui, entità o processi non autorizzati;
2. L'**integrità** del patrimonio informativo gestito: proprietà di tutelare l'accuratezza e la completezza degli asset, ossia di qualsiasi informazione o bene attinente a cui l'organizzazione attribuisce un valore;
3. La **disponibilità** del patrimonio gestito: proprietà per cui l'informazione deve essere accessibile ed utilizzabile previa richiesta di una entità autorizzata;
4. Il **rispetto dei requisiti cogenti**, normativi e contrattuali;
5. L'adeguata **formazione** in tema di sicurezza delle informazioni del personale;

Ulteriori approfondimenti degli obiettivi sono riportati nel piano strategico aziendale per l'annualità di riferimento.

L'implementazione del Sistema di Gestione per la sicurezza delle informazioni implica

- Identificare una metodologia di valutazione del rischio adeguata al SGSI, ai requisiti di business individuati, a quelli cogenti e normativi e gestire il rischio ad un livello accettabile e in modo allineato al più generale contesto di gestione del rischio strategico dell'organizzazione.
- Identificare, attraverso idonea analisi dei rischi, il valore del patrimonio informativo, all'interno del campo di applicazione del SGSI, al fine di comprendere le vulnerabilità e le possibili minacce che possano esporlo a rischi.
- Gestire la riservatezza, disponibilità e integrità delle informazioni nel rispetto anche dei principi di privacy by design e privacy by default e della normativa cogente.
- Proteggere i dati rispetto ad accessi non autorizzati in funzione della loro criticità, valore e sensibilità compresi i servizi di hosting e servizi SaaS erogati in modalità public cloud;
- Migliorare la consapevolezza interna dei rischi sulla sicurezza delle informazioni.
- Garantire la continuità operativa dei processi aziendali.
- Garantire ai Clienti canali efficaci ed efficienti di comunicazione per lo scambio di informazioni e per supportare gli stessi in qualsiasi evento che possa pregiudicare la sicurezza delle informazioni e in particolar modo dei dati personali, nel rispetto della normativa in vigore.
- Definire e rendere effettive le linee operative per un'architettura di sicurezza intesa come l'insieme di regole, funzioni, strumenti, oggetti e controlli, coerentemente disegnati e resi funzionanti, che garantiscano in ogni struttura organizzativa, ambiente informatico, singolo elaboratore, il rispetto degli standard definiti dalla ARC DATA.

Monitorare, cogliendo ogni spunto di miglioramento, il sistema SGSI attuato

La Direzione Generale dell'Organizzazione, sulla base delle premesse di cui sopra, provvede costantemente ad orientare i collaboratori alla qualità mediante le necessarie azioni organizzative.

La gestione delle attività in conformità alle norme di riferimento per il SGSI è obiettivo di tutti i collaboratori della ARC DATA e coinvolge ogni funzione aziendale nell'ambito dei compiti assegnati. La Direzione esaminerà in modo critico ed oggettivo l'adeguatezza e l'efficacia nel tempo del Sistema Gestione Aziendale attraverso riscontri diretti ed esami periodici dei risultati ottenuti. Il presente documento sarà sottoposto a riesame annuale in sede di Riesame di Direzione al fine di valutarne la continua adeguatezza ed idoneità alla nostra Organizzazione.

La Direzione