

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

La Direzione ha individuato le seguenti informazioni, parte del proprio patrimonio immateriale, giudicate strategiche per la propria attività e quindi da difendere con l'implementazione di un sistema di gestione "ad hoc":

1. Le informazioni di progettazione e produzione di sistemi integrati di acquisizione e controllo dati;
2. I software (SW) applicativi per tali sistemi;
3. La documentazione fornita dalle parti interessate e per la quale si richiede esplicitamente una protezione sicura;
4. Le informazioni relative alla gestione del personale con particolare attenzione alla protezione dei dati personali;
5. Le informazioni relative alla gestione delle attività commerciali.

La Direzione persegue impegni e obiettivi di cui alla seguente politica:

1. attuare, mantenere e migliorare con continuità il proprio Sistema di Gestione per la Sicurezza delle Informazioni e i processi aziendali;
2. mantenere la conformità a leggi, norme, regolamenti e requisiti vigenti ed applicabili;
3. valutare (cioè individuare, analizzare, ponderare) e poi trattare sistematicamente i rischi per la sicurezza delle informazioni (risk assesment);
4. garantire la sicurezza delle informazioni ritenute strategiche per l'attività aziendale proteggendo la loro:
 - a. riservatezza: una informazione riservata non è disponibile ad individui non autorizzati;
 - b. integrità: una informazione integra è conservata in modo da impedirne la modifica e/o la cancellazione se non da parte di persone autorizzate;
 - c. disponibilità: una informazione disponibile è accessibile solo a individui autorizzati garantendo loro l'utilizzo in modi e tempi previsti;
 - d. autenticità: garanzia della provenienza delle informazioni;
5. garantire le seguenti caratteristiche al sistema per la sicurezza delle informazioni:
 - a. efficienza (accettabilità): il sistema di gestione deve essere mantenuto ed operare con un utilizzo adeguato di risorse materiali, commisurato e proporzionato alla realtà aziendale;
 - b. efficacia: il sistema di gestione deve essere realizzato in modo da raggiungere ragionevolmente gli obiettivi prefissati di anno in anno;
 - c. correttezza: il sistema di gestione è realizzato tenendo conto anche delle necessarie misure per minimizzare il numero di possibili errori o non conformità;
 - d. gestibilità: il sistema di gestione è documentato per essere mantenuto o modificato senza difficoltà.
6. coinvolgere e accrescere la consapevolezza dei dipendenti e delle parti interessate sull'importanza del proprio sistema di gestione per la sicurezza delle informazioni;



Manuale del Sistema di Gestione per la Sicurezza delle informazioni
(Allegato 6 – Politica per la sicurezza delle informazioni - Rev. 00 del 10-04-2025)

7. garantire il perseguimento degli obiettivi per la sicurezza delle informazioni, formalizzati in piani dedicati;
8. garantire sempre la massima preparazione e coinvolgimento del personale nell'ambito delle attività di competenza;
9. garantire sempre l'uso di strumenti e attrezzature all'avanguardia;
10. garantire l'impegno costante per la prevenzione degli incidenti relativi alla sicurezza delle informazioni e per la pronta ed efficace risposta ai medesimi;
11. predisporre e provare periodicamente adeguati piani di continuità operativa ("business continuity management plan") e piani di recupero dati ("disaster recovery plan").
12. individuare e perseguire nel tempo ulteriori obiettivi come indicato nel manuale del SGSI e come previsto dai piani di miglioramento.

SARZANA (La Spezia), 10-04-2025

LA DIREZIONE

Mauro Spampani