Autoguidovie

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

PREMESSA

AUTOGUIDOVIE S.P.A. ha stabilito di dotare l'Organizzazione di un Sistema per la tenuta della sicurezza delle informazioni, in conformità alla Normativa **ISO/IEC 27001**.

Il Sistema Informativo (inclusivo delle risorse tecnologiche - hardware, software, dati, documenti elettronici, reti telematiche - e delle risorse umane dedicate alla loro amministrazione, gestione e utilizzo) rappresenta uno strumento di primaria importanza per il conseguimento degli obiettivi strategici e operativi della Società, in considerazione della criticità dei processi aziendali che dipendono da esso.

Il presente documento ha l'obiettivo di definire le politiche sui sistemi informativi, è approvato dalla direzione di **AUTOGUIDOVIE S.P.A.** e sarà revisionato periodicamente sia in caso di eventi esogeni, quali ad esempio modifiche della normativa esterna ovvero indicazioni delle Autorità, sia di modifiche organizzative ed operative che abbiano impatto sui Sistemi Informativi e sulla sicurezza informatica. Le revisioni vengono approvate dalla direzione.

POLITICHE AZIENDALI SUI SISTEMI INFORMATIVI

La Direzione si impegna a preservare la riservatezza, l'integrità e la disponibilità di tutte le informazioni (in formato elettronico e non) in tutta l'organizzazione al fine di mantenere il proprio vantaggio competitivo, solidità economica, redditività, conformità legale e contrattuale e immagine commerciale. Le informazioni ed i requisiti di sicurezza delle informazioni continueranno ad essere allineati con gli obiettivi aziendali ed il Sistema di Gestione per la Sicurezza delle Informazioni è destinato a essere un meccanismo di abilitazione della condivisione delle informazioni per l'operatività della Società e per ridurre i rischi relativi alle informazioni a livelli accettabili. Tutti i dipendenti dell'organizzazione, così come alcune terze parti, sono tenuti a rispettare le presenti politiche e l'intero Sistema di Gestione per la Sicurezza delle Informazioni.

La presente politica riguarda la gestione e l'utilizzo del sistema informativo in tutti i suoi aspetti e sarà riesaminata ogniqualvolta sarà necessario e comunque almeno una volta all'anno.

Per perseguire gli obiettivi aziendali, le informazioni devono soddisfare determinati requisiti:

1. **Riservatezza**: assicurare che l'informazione sia accessibile solamente ai soggetti ed ai processi debitamente autorizzati ed analizzati tramite una attenta analisi dei rischi;
2. **Integrità**: salvaguardare la consistenza dell'informazione da modifiche non autorizzate;
3. **Disponibilità**: assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati quando ne fanno richiesta;
4. **Controllo**: assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
5. **Autenticità**: garantire una provenienza affidabile dell'informazione;

6. **Privacy**: garantire la protezione ed il controllo dei dati personali fin dalle fasi progettuali (Privacy by Design) con soluzioni volte alla minimizzazione nell'uso di tali dati (Privacy by default con anonimizzazione e mascheramento dei dati, ove possibile).
7. **Cybersecurity**: garantire, all'interno dei processi, un'attenta analisi, conoscenza e mitigazione delle vulnerabilità dei sistemi e degli applicativi al fine di implementare processi sicuri e resilienti in termini di sicurezza delle informazioni.

La gestione del Sistema Informativo aziendale è svolta da personale qualificato che per esperienza, capacità e affidabilità fornisce garanzia del pieno rispetto delle disposizioni interne e delle normative esterne in materia.

Per poter gestire in modo adeguato il Sistema Informativo è essenziale un efficace processo di monitoraggio che faciliti la pronta individuazione e correzione di eventuali carenze relative a politiche, processi e procedure. Ciò può ridurre considerevolmente la frequenza e/o gravità degli eventi dannosi.

La Società attiva unità organizzative interne che assicurano l'esecuzione di processi atti a:

a) diffondere il contenuto dei servizi, conoscere i punti di forza e di eventuale debolezza;
b) assicurare agli utenti formazione e accesso alle funzioni secondo criteri di sicurezza aderenti a principi di sana e prudente gestione o comunque alle politiche di gestione del rischio informatico;
c) attivare processi volti alla valorizzazione delle risorse informatiche, intese come leva per il raggiungimento degli obiettivi della Società;
d) realizzare un sistema di comunicazione dei fabbisogni o delle criticità del Sistema Informativo con l'obiettivo di attivare un processo di miglioramento continuo;
e) attuare controlli finalizzati a valutare la capacità dell'azienda di attenersi alle politiche interne;
f) individuare tempestivamente deviazioni (anomalie, malfunzionamenti, differenze rispetto a quanto conosciuto/approvato/autorizzato);
g) favorire azioni correttive.

AUTOGUIDOVIE S.P.A. predispone ed implementa il proprio Piano di Continuità Operativa ed il Piano di Disaster Recovery. Deve essere sempre assicurata la protezione dei dati e dei sistemi contro le possibili conseguenze dell'attività di software dannoso (c.d. Malware).

Inoltre, la Società, tenuto conto della particolare criticità dei ruoli connessi alla gestione del Sistema Informativo, in particolare del ruolo di "Amministratore di Sistema", adotta delle cautele volte a prevenire e ad accertare eventuali utilizzi non in linea con gli obiettivi aziendali del Sistema Informativo, inefficienze dello stesso, accessi non consentiti ai dati, in specie quelli realizzati con abuso della qualità di Amministratore di Sistema.

La Società, valuta con particolare cura l'attribuzione di funzioni tecniche inerenti la gestione del Sistema Informativo, tenendo in considerazione l'opportunità o meno di tale attribuzione e le concrete modalità sulla base delle quali si svolge l'incarico, unitamente alle qualità tecniche, professionali e di condotta del soggetto individuato, da vagliare anche in considerazione delle responsabilità, specie di ordine penale e civile, che possono derivare in caso di incauta o inidonea designazione.

Autoguidovie

L'attribuzione delle funzioni relative alla gestione del Sistema Informativo o alla gestione delle sue componenti si svolge previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni interne ed esterne anche quelle in materia di trattamento dei dati ivi compreso il profilo relativo alla sicurezza.

Nel ricorso ai servizi dei fornitori esterni, la Società utilizza analoghi criteri di valutazione di esperienza, capacità ed affidabilità del fornitore nello svolgimento dell'incarico affidato e della garanzia fornita del pieno rispetto delle vigenti disposizioni di legge, anche quelle in materia di trattamento dei dati ivi compreso il profilo relativo alla sicurezza.

Le attività che comportano rischi significativi per la Società, ove le soluzioni tecniche lo consentono, devono essere organizzate in modo da prevedere il concorso di più soggetti, con responsabilità formalmente ripartite, al fine di evitare l'accentramento delle stesse su una singola risorsa, garantendo un adeguato sistema di controlli incrociati.

La Società implementa apposite misure atte a garantire una pronta, efficace e corretta risposta al concretizzarsi degli incidenti di sicurezza. In tal senso, la Società attua, ove possibile, misure atte a mitigare i potenziali impatti degli incidenti e il ripristino della situazione iniziale in tempi brevi. La gestione degli incidenti prevede opportune procedure di escalation e di reporting in relazione alla gravità degli eventi occorsi.

Al fine di garantire lo svolgimento dell'operatività in situazioni di crisi, **AUTOGUIDOVIE S.P.A.** ha definito ed implementato il Piano di Continuità Operativa basato su un'appropriata identificazione dei processi critici, delle potenziali minacce che possono realizzarsi su di essi e delle contromisure da adottare. Il Piano di Continuità Operativa è testato e aggiornato regolarmente al fine di garantirne l'efficacia nel tempo.

Milano, 30/10/2024

Il Presidente di *Autoguidovie S.p.A.*
Camillo Ranza