Politica per la sicurezza delle informazioni

Rev. 4 del 9.10.2025

INDICE

SCOPO 2

DESCRIZIONE 2

AMBITO DI APPLICAZIONE 3

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI 4

RESPONSABILITÀ DELLA POLITICA DI SICUREZZA DELLE INFORMAZIONI 5

SCOPO

Lo scopo del presente documento è quello di descrivere i principi generali di sicurezza delle informazioni definiti da Vedetta 2 Mondialpol S.p.A. al fine di sviluppare un efficiente e sicuro Sistema di Gestione della Sicurezza delle Informazioni (SGSI).

DESCRIZIONE

Per Vedetta 2 Mondialpol S.p.A. la sicurezza delle informazioni ha come obiettivo primario la protezione dei dati e delle informazioni, della struttura tecnologica, fisica, logica e organizzativa, responsabile della loro gestione. Questo significa ottenere e mantenere un sistema di gestione sicura delle informazioni, nell'ambito del campo di applicazione definito per il SGSI, attraverso il rispetto delle seguenti proprietà:

1. **Riservatezza**: assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati;
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 e il controllo dei dati personali.

Nell'ambito della gestione dei servizi offerti dalla Centrale Operativa di Vedetta 2 Mondialpol S.p.A., attraverso la propria infrastruttura tecnologica, l'osservanza dei livelli di sicurezza stabiliti attraverso l'implementazione del SGSI, assicura:

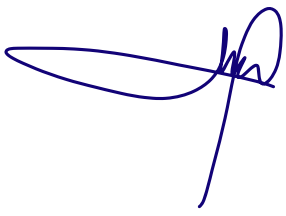
- la garanzia di aver implementato procedure e policy che possano garantire un'alta resilienza dei servizi e di disponibilità, riservatezza e integrità delle informazioni;
- la selezione, quando necessario, di partner affidabili al trattamento del proprio patrimonio informativo;
- un'elevata immagine aziendale volta alla sicurezza dei Clienti;
- la completa osservanza degli accordi stabiliti con i Clienti;
- la soddisfazione del Cliente;
- il rispetto delle normative vigenti e degli standard internazionali di sicurezza, privacy e cybersecurity.

Per questo motivo Vedetta 2 Mondialpol S.p.A. ha sviluppato un sistema di gestione sicura delle informazioni seguendo i requisiti specificati nella norma ISO IEC 27001:2022 e delle Leggi cogenti come mezzo per gestire la sicurezza delle informazioni nell'ambito della propria attività di Centrale Operativa con particolare riferimento alla gestione degli allarmi.

AMBITO DI APPLICAZIONE

La politica per la sicurezza delle informazioni di Vedetta 2 Mondialpol S.p.A. si applica a tutto il personale interno e alle terze parti che collaborano alla gestione delle informazioni, nonchè a tutti i processi e risorse coinvolte nel campo di applicazione del sistema di gestione che risulta definito nel seguente campo di applicazione:

Gestione del sistema informativo a supporto dell'infrastruttura tecnologica per la ricezione, visualizzazione, gestione, trattamento e storicizzazione degli allarmi di Centrale Operativa e relativi servizi digitali erogati in datacenter locale e remoto.

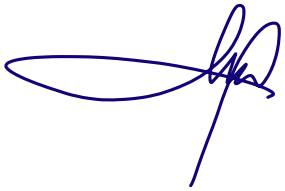


POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

La politica della sicurezza delle informazioni di Vedetta 2 Mondialpol S.p.A. rappresenta l'impegno dell'organizzazione nei confronti di Clienti e terze parti al fine di garantire la sicurezza delle informazioni, degli strumenti fisici, logici e organizzativi atti al trattamento delle informazioni in tutte le attività.

La politica della sicurezza delle informazioni di Vedetta 2 Mondialpol S.p.A. si ispira ai seguenti principi:

a. Garantire all'organizzazione la piena conoscenza delle informazioni gestite e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione.
b. Garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati o realizzati senza i diritti necessari.
c. Garantire che l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza.
d. Garantire che l'organizzazione e le terze parti che collaborano al trattamento delle informazioni, abbiano piena consapevolezza delle problematiche relative alla sicurezza.
e. Garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business.
f. Garantire che l'accesso alle sedi e ai singoli locali aziendali avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti.
g. Garantire la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti.
h. Garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni, anche in ottemperanza ai nuovi regolamenti cogenti per i servizi critici e importanti.



i. Garantire la business continuity aziendale e il disaster recovery, attraverso l'applicazione di procedure di sicurezza stabilite anche con strutture che vedono un'ampia ridondanza geografica dei servizi.

j. Garantire un corretto trattamento dei dati personali dei clienti in ottemperanza alle Leggi e ai regolamenti nazionali ed europei.

La politica della sicurezza delle informazioni è formalizzata nel SGSI; viene costantemente aggiornata per assicurare il continuo miglioramento ed è condivisa con l'organizzazione, le terze parti e i Clienti, attraverso un sistema intranet e specifici canali di comunicazione.

RESPONSABILITÀ DELLA POLITICA DI SICUREZZA DELLE INFORMAZIONI

La Direzione è responsabile del sistema di gestione sicura delle informazioni, in coerenza con l'evoluzione del contesto aziendale e di mercato, valutando eventuali azioni da intraprendere a fronte di eventi come:

- evoluzioni significative del business;
- nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio;
- significativi incidenti di sicurezza;
- evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni.

