Allegato 2

Politica per la Sicurezza delle Informazioni

1. Introduzione

La politica di sicurezza delle informazioni Castagna Giorgio s.r.l. uninominale è adottata al fine di proteggere il sistema di gestione delle informazioni da eventi quali minacce o incidenti, esterni e/o interni, oggettivi e/o soggettivi, che possono compromettere l'erogazione dei servizi.

Lo scopo di questo documento è indicare le esigenze, gli obiettivi, le finalità, ed i modelli organizzativi della strategia di sicurezza che Castagna Giorgio s.r.l. uninominale persegue, al fine di orientare lo sviluppo, la gestione, il controllo e la verifica dell'efficacia della sua attuazione.

2. Ambito di applicazione

La politica per la sicurezza delle informazioni di Castagna Giorgio s.r.l. uninominale si applica a tutte le informazioni trattate dall'Azienda, qualsiasi natura e forma esse abbiano o prendano, a tutti i sistemi di gestione e a tutti i supporti di memorizzazione utilizzati per il loro trattamento e la loro conservazione.

I destinatari della politica sono tutti i dipendenti, i collaboratori o i consulenti, a tempo pieno e a tempo determinato. Sono tenuti al rispetto della politica tutti i soggetti che a vario titolo fruiscono dei servizi informativi di Castagna Giorgio s.r.l. uninominale, nonché i Clienti. In particolare, sono tenuti al rispetto della politica di sicurezza, i fornitori di servizi informatici per la loro tipica condizione di operare direttamente sui sistemi di gestione delle informazioni.

3. Scopo

In relazione a quanto definito nel documento **"Manuale Operativo per la Sicurezza ISO 27001"**, lo scopo del presente documento è quello di descrivere i principi generali oltre a fornire una direttiva gestionale ed un sostegno per la corretta gestione della sicurezza delle informazioni definiti da Castagna Giorgio s.r.l. uninominale

Castagna Giorgio s.r.l. uninominale considera il sistema di gestione e le informazioni gestite parte integrante del proprio patrimonio. È obiettivo di assoluta priorità, salvaguardare la sicurezza del proprio sistema informativo e tutelare la riservatezza, l'integrità e la disponibilità delle informazioni prodotte, raccolte o comunque trattate, da ogni minaccia intenzionale o accidentale, interna o esterna.

4. Descrizione

Per Castagna Giorgio s.r.l. uninominale la sicurezza delle informazioni ha come obiettivo primario la protezione dei dati e delle informazioni, della struttura tecnologica, fisica, logica ed 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:

a. **Riservatezza:** a la garanzia che una determinata informazione sia preservata da accessi impropri e sia utilizzata esclusivamente dai soggetti autorizzati;

b. **Integrità:** la garanzia che ogni informazione sia realmente quella originariamente inserita nel sistema informatico, che sia stata modificata in modo legittimo da soggetti autorizzati e che ne rimanga traccia;

c. **Disponibilità:** la garanzia di reperibilità dell'informazione in relazione alle esigenze di continuità di erogazione del servizio e di rispetto delle norme che ne impongono la conservazione sicura;

d. **Controllo:** l'assicurazione che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;

e. **Autenticità:** la garanzia che l'informazione ricevuta corrisponda a quella generata dal soggetto o entità che la ha trasmessa;

f. **Privacy:** la garanzia che la protezione ed il controllo dei dati personali, soprattutto quelli ritenuti particolari, siano vigilati e gestiti conformemente alla normativa.

g. **Cyber security** si occupa della protezione dei dati da accessi non autorizzati, nella Cyber Security sono presenti elementi giuridici, umani, tecnici e organizzativi in grado di analizzare i punti vulnerabili di un sistema, le minacce e i rischi associati.

Castagna Giorgio s.r.l. uninominale pone a base della politica di tutela delle informazioni, un idoneo Risk Assessment di tutte le risorse (Asset) che costituiscono il sistema di gestione delle informazioni, al fine di comprendere le vulnerabilità, di valutare le possibili minacce e di predisporre le necessarie contromisure.

La consapevolezza che non è possibile ottenere, in ambito informatico come del resto in natura, una condizione di sicurezza assoluta, comporta che lo scopo della politica di sicurezza delle informazioni è quello di gestire il rischio ad un livello accettabile attraverso la progettazione, l'attuazione ed il mantenimento di un "Sistema di Gestione della Sicurezza delle Informazioni" (c.d. **"SGSI"**) in linea con la propensione al rischio informatico definito a livello aziendale.

Nell'ambito della gestione dei servizi offerti da Castagna Giorgio s.r.l. uninominale, attraverso la propria infrastruttura tecnologica, l'osservanza dei livelli di sicurezza stabiliti attraverso l'implementazione dell'SGSI, assicura:

- la garanzia di aver incaricato un partner affidabile al trattamento del proprio patrimonio informativo;
- un'elevata immagine aziendale;
- la completa osservanza delle Service Level Agreement stabilite con i clienti;
- la soddisfazione del cliente;
- il rispetto delle normative vigenti e degli standard internazionali di sicurezza.

Per questo motivo Castagna Giorgio s.r.l. uninominale ha sviluppato un sistema di gestione sicura delle informazioni seguendo i requisiti specificati della Norma ISO 27001 e delle leggi cogenti come mezzo per gestire la sicurezza delle informazioni nell'ambito della propria attività.

5. Obiettivi

La politica della sicurezza di Castagna Giorgio s.r.l. uninominale rappresenta l'impegno dell'organizzazione nei confronti di clienti e terze parti a garantire la sicurezza delle informazioni, degli strumenti fisici, logici e organizzativi atti al trattamento delle informazioni nelle attività oggetto di certificazione.

La politica della sicurezza delle informazioni di Castagna Giorgio s.r.l. uninominale si ispira ai seguenti principi:

- 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;
- garantire al personale e ai collaboratori un'adeguata conoscenza e un adeguato grado di consapevolezza dei problemi connessi con la sicurezza delle informazioni, al fine di consentire a detti soggetti di acquisire sufficiente coscienza della propria responsabilità in merito al trattamento delle stesse;
- garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati o realizzati senza i diritti/autorizzazioni necessarie;
- garantire che l'organizzazione e le terze parti collaborino al trattamento delle informazioni abbiano piena consapevolezza delle problematiche relative alla sicurezza ed adottino procedure volte al rispetto di adeguati livelli di sicurezza;
- 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;
- garantire che l'accesso alle sedi ed ai singoli locali aziendali avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti;
- garantire la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti;
- 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;
- garantire la Business Continuity aziendale e il Disaster Recovery, attraverso l'applicazione di procedure adeguate definite nel SGSI;
- garantire che il processo di gestione del rischio informatico adottato dall'Azienda sia adeguatamente presidiato e periodicamente aggiornato alla luce dei parametri contemplati all'interno della normativa costituente il SGSI.

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

6. Revisione e controllo

La Direzione, coadiuvata dal Responsabile della Sicurezza Gestione Sicurezza Informazioni (c.d. **"RSGSI"**), è responsabile della revisione periodica della politica affinché sia allineata agli eventuali e significativi cambiamenti intervenuti nell'organizzazione e/o nelle tecnologie utilizzate per la protezione delle informazioni.

La revisione sarà fatta periodicamente o in occasione di significative modifiche organizzative e/o tecnologiche rilevanti per la gestione delle informazioni.

7. Riferimenti normativi

Fare riferimento al " **Manuale Operativo per la Sicurezza informazioni**".

8. Termini e definizioni

Fare riferimento al " **Manuale Operativo per la Sicurezza**".

9. Responsabilità

La Direzione è il responsabile dei contenuti della politica di sicurezza delle informazioni, della sua emanazione, della sua attuazione e del suo aggiornamento, 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.

Le principali attività in carico al Responsabile della Sicurezza sono quelle di vigilare sulla corretta implementazione e sul corretto mantenimento nel tempo del Sistema di Gestione della Sicurezza delle Informazioni, di promuovere e di coordinare l'attività di analisi dei rischi, di gestire i rapporti con i fornitori di servizi rilevanti.

10. Comunicazione, formazione e sensibilizzazione degli utenti

La Politica della Sicurezza è divulgata a tutto il personale, ai collaboratori, ai Clienti e ai fornitori attraverso cartella aziendale interna e sul sito internet. Il Responsabile della Sicurezza Gestione Sicurezza Informazioni attraverso opportune sessioni informative e formative sensibilizza gli utenti interni ad una corretta applicazione delle procedure della sicurezza delle informazioni, stimolando gli stessi a collaborare fattivamente per una gestione sempre più coordinata ed esaustiva di tale tematica.

Rev. 0 del 03/09/2026

Direzione

CASTAGNA GIORGIO s.r.l.
Uninominale