

## Politica Sicurezza delle informazioni

Lo scopo del presente documento è quello di descrivere i principi generali di sicurezza delle informazioni definiti dalla Citigas Coop S.p.A. al fine di sviluppare un efficiente e sicuro Sistema di Gestione della Sicurezza delle Informazioni.

Per la Citigas Coop S.p.A. 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, 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 ed il controllo dei dati personali.

***Per questo motivo la Citigas Coop S.p.A. ha sviluppato un sistema di gestione sicura delle informazioni seguendo i requisiti specificati della Norma UNI CEI ISO/IEC 27001 e delle leggi cogenti come mezzo per gestire la sicurezza delle informazioni nell'ambito della propria attività.***

La presente politica per la sicurezza delle informazioni si applica a tutto il personale interno ed alle terze parti che collaborano alla gestione delle informazioni.

La politica della sicurezza 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 in tutte le attività.

### **Obiettivo qualitativo:**

- 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 ed 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.
- i. Garantire la business continuity aziendale e il disaster recovery, attraverso l'applicazione di procedure di sicurezza stabilite.

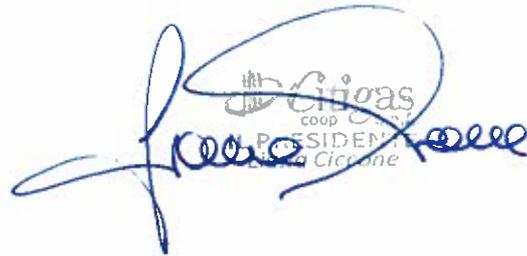
**Target quantitativo:**

- Numero di dipendenti che ricevono formazione su temi della protezione dei dati al 100% entro il 2030
- 0 data breach
- 0 disaster recovery

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.

Giulianova (TE), 02/09/2024

A handwritten signature in blue ink is written over a circular stamp. The stamp contains the Citigas logo and the text 'PRESIDENTE' and 'Luca Ciccone'.