CRITICALSERVICE
VALUE ADDED SERVICES

SGI

Sistema **G**estione **I**ntegrato
ISO/IEC 27001- ISO/IEC 9001 – ISO/IEC 22301

POLITICA AZIENDALE PER LA CONTINUITA' OPERATIVA

Cod. **PO-SGI-A5.1.04** Rev. **0** del **30/09/2024**

Tipo documento: **Politica Generale**

PUBBLICO

Attenzione! *Le informazioni contenute in questo documento e nei suoi allegati sono destinate ai soggetti contenuti nella lista di distribuzione riportata al paragrafo 1.2. La loro divulgazione a soggetti terzi rispetto ai destinatari è consentita unicamente per ragioni legate all'attuazione e allo sviluppo del SGSI, previa autorizzazione esplicita della direzione aziendale.*

PI e CF 11242420013 - REA TO – 1198652 - Corso Benedetto Croce, 5 – 10135 Torino (TO)
Cap. Soc. i.v. 50.000 Euro

1 Scheda del documento

1.1 Tabella delle revisioni

Rev.	Data	Modificato	Descrizione della modifica	Approvato
0	30/09/2023	RSI	Prima edizione del documento all'interno del SGI	AD

1.2 Lista di distribuzione

Tutto il personale di Critical Service s.r.l. (es. dipendenti e potenziali, collaboratori e potenziali, tirocinanti, ecc.)
Parti interessate esterne interessate

1.3 Documenti collegati

Tipo	Codice	Titolo
POLITICA GENERALE	PO-SGI-05.1.01	POLITICA PER LA QUALITA', LA SICUREZZA DELLE INFORMAZIONI E LA PROTEZIONE DEI DATI PERSONALI

1.4 Riferimenti normativi

Titolo	Note
UNI EN ISO 9001:2015	Sistemi di gestione per la qualità- Requisiti
ISO/IEC 27001:2022	Information security, cybersecurity and privacy protection — Information security management systems — Requirements
UNI EN ISO/IEC 27002:2023	Sicurezza delle informazioni, cybersecurity e protezione della privacy - Controlli di sicurezza delle Informazioni.
UNI EN ISO/IEC 27017:2021	Tecnologie Informatiche - Tecniche di sicurezza - Raccolta di prassi sui controlli per la sicurezza delle informazioni per i servizi in cloud basata sulla ISO/IEC 27002
UNI EN ISO/IEC 27018:2020	Tecnologie informatiche - Tecniche di sicurezza - Raccolta di prassi per la protezione dei dati personali trattati in cloud pubblici da responsabili del trattamento
UNI EN ISO/IEC 22301:2019	Sicurezza e resilienza - Sistemi di gestione per la continuità operativa - Requisiti
Regolamento EU 2016/679	General Data Protection Regulation (GDPR)

1.5 Controllo ISO

ISO/IEC 27001	2023	A5.1	A.529	A5.30								
ISO/IEC 22301	2019	5.2										

1.6 Conformità Legale

Reg. EU 2016/679 GDPR	Articoli	5.2	24	25	32							

2 PREMESSA

Critical Service opera in settori critici e strategici, dove l'affidabilità dei servizi e la resilienza operativa rappresentano fattori chiave per il successo e la fiducia dei nostri clienti e partner. Consapevoli dell'importanza di garantire la continuità delle nostre attività anche in situazioni di emergenza o interruzione, questa politica stabilisce l'impegno dell'azienda a implementare un sistema di gestione della continuità operativa (BCMS) conforme alla norma ISO 22301:2019. L'obiettivo è proteggere le nostre operazioni, ridurre i rischi e garantire la ripresa rapida e sicura dei servizi essenziali, preservando al contempo la sicurezza delle informazioni come previsto dalla ISO/IEC 27001:2022.

3 SCOPO

Questa politica definisce l'approccio strategico di Critical Service per garantire la continuità delle operazioni aziendali, minimizzare l'impatto delle interruzioni e migliorare la resilienza organizzativa.

4 AMBITO DI APPLICAZIONE

Questa politica si applica a tutte le sedi operative, i processi, le risorse, i sistemi ICT, il personale e le infrastrutture di Critical Service coinvolti nella fornitura di servizi essenziali ai clienti.

5 OBIETTIVI

Critical Service si impegna a:

- Garantire la disponibilità e la sicurezza dei servizi critici durante e dopo un'interruzione.
- Proteggere la riservatezza, l'integrità e la disponibilità delle informazioni aziendali anche in condizioni avverse.
- Ridurre al minimo i tempi di ripristino delle attività e i costi associati alle interruzioni.
- Stabilire una collaborazione efficace con clienti, fornitori e partner per mitigare le interdipendenze.

6 PRINCIPI GUIDA PER LA CONTINUITA' OPERATIVA

- Conformità normativa: Assicurare il rispetto dei requisiti delle norme ISO 22301:2019 e ISO/IEC 27001:2022, nonché di tutte le leggi e regolamenti applicabili.
- Gestione dei rischi: Identificare e gestire i rischi operativi e le vulnerabilità, garantendo la sicurezza delle informazioni anche durante le emergenze.
- Pianificazione e test: Mantenere e testare regolarmente piani di continuità operativa per verificarne l'efficacia.
- Miglioramento continuo: Monitorare le prestazioni del BCMS e implementare azioni correttive per affrontare eventuali carenze.
- Comunicazione e formazione: Garantire che tutto il personale sia consapevole del proprio ruolo in caso di emergenza e che riceva formazione adeguata.

7 INTEGRAZIONE CON LA SICUREZZA DELLE INFORMAZIONI

Critical Service garantisce che la continuità operativa sia integrata con il sistema di gestione della sicurezza delle informazioni (SGSI), conforme alla ISO/IEC 27001:2022, per proteggere i dati sensibili e ridurre i rischi di compromissione durante le interruzioni.

8 RESPONSABILITÀ

Per garantire un'efficace gestione della continuità operativa, è fondamentale che ogni livello dell'organizzazione comprenda il proprio ruolo e le proprie responsabilità. Critical Service promuove una cultura aziendale basata sull'impegno condiviso verso la resilienza operativa, con una chiara definizione dei compiti e delle responsabilità. La collaborazione tra i diversi livelli e funzioni aziendali è essenziale per prevenire, gestire e superare le interruzioni, assicurando il mantenimento dei servizi critici.

8.1 Responsabilità specifiche

Alta Direzione

- Stabilire la visione strategica per la continuità operativa.
- Allocare le risorse necessarie per implementare e mantenere il BCMS.
- Monitorare l'efficacia delle misure implementate e approvare le azioni di miglioramento.

Responsabile della Continuità Operativa:

- Coordinare lo sviluppo e la manutenzione del BCMS.
- Pianificare e condurre test periodici per verificare l'efficacia dei piani di continuità.
- Redigere report per la Direzione sulle prestazioni e sull'aderenza ai requisiti normativi.

Personale:

- Conoscere e rispettare le procedure di continuità operativa applicabili al proprio ruolo.
- Partecipare attivamente alle attività di formazione e simulazione.
- Segnalare tempestivamente eventuali vulnerabilità o situazioni critiche.

9 DIVULGAZIONE DELLA POLITICA

La politica per la continuità operativa è comunicata:

- **Internamente:** A tutto il personale attraverso intranet aziendale, sessioni di formazione e manuali operativi.
- **Esternamente:** A clienti, partner e fornitori rilevanti, su richiesta o in base a requisiti contrattuali.

10 SANZIONI

La mancata osservanza della politica per la qualità e la sicurezza delle informazioni può comportare sanzioni disciplinari, fino alla cessazione del rapporto lavorativo o contrattuale.
L'organizzazione si riserva il diritto di monitorare e controllare l'operato dei propri dipendenti per garantire la conformità con questa politica e altre politiche e procedure ad essa correlate.

11 VALIDITA' APPROVAZIONE E MODIFICHE

La presente politica per la continuità operativa è approvata dall'Alta Direzione nella persona del Legale rappresentante aziendale o suo Delegato. Tutte le modifiche a questa politica sono approvate dall'Alta Direzione prima dell'implementazione.
La politica è valida dalla data di approvazione da parte dell'alta direzione

Torino, 30/09/2024

Amministratore Delegato
Clizia GIANNI'

CRITICAL SERVICE S.R.L.
C.so Benedetto Croce 5
10135 TORINO
C.F./P. IVA 11242420013