CRITICALSERVICE
VALUE ADDED SERVICES

SGI

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

POLITICA AZIENDALE PER LA QUALITA', LA SICUREZZA DELLE INFORMAZIONI E LA PROTEZIONE DEI DATI PERSONALI

Cod. **PO-SGI-A5.1.01** Rev. **1** 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 SGI, 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	01/03/2023	RSI	Prima edizione del documento all'interno del SGI	AD
1	30/09/2024	RSI	Nuova impaginazione e integrazione strategia implementazione BCMS ISO 22301	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 coinvolte nell' ambito di applicazione (es. soci, clienti e potenziali, fornitori e potenziali, PA, ecc.)

1.3 Documenti collegati

Tipo	Codice	Titolo

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 Controlli ISO

ISO/IEC 27001	2022	A5.1										

1.6 Conformità Legale

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

2 ELENCO DEI CONTENUTI

3 PREMESSA

In Critical Service, comprendiamo l'importanza cruciale di adeguare costantemente i propri servizi ai più elevati standard di sicurezza delle informazioni nel contesto digitale in cui operiamo come azienda specializzata in cybersecurity. La protezione delle informazioni è fondamentale per preservare la fiducia dei clienti, garantire la continuità operativa e proteggere la reputazione nostra e dei nostri clienti. Ci impegniamo a implementare politiche e procedure di sicurezza robuste, adottando le migliori pratiche del settore e utilizzando tecnologie all'avanguardia.

Inoltre, riconosciamo che l'importanza della qualità dei servizi offerti è fondamentale per distinguerci nel mercato e soddisfare le esigenze dei nostri clienti. L'aumento delle richieste da parte di mercati sempre più esigenti e clienti consapevoli ci spinge ad adeguarci a standard organizzativi e di erogazione dei servizi che ci

consentano di distinguerci per qualità, affidabilità e sicurezza nella gestione delle informazioni. La qualità dei servizi che offriamo non riguarda solo la sicurezza delle informazioni, ma anche l'efficacia, l'efficienza e l'accuratezza con cui svolgiamo le attività legate alla cybersecurity.

Garantire una qualità elevata nei nostri servizi ci consente di soddisfare le aspettative dei clienti e superare le loro esigenze. Una gestione qualitativa dei servizi ci permette di ridurre gli errori, migliorare la produttività e fornire risultati affidabili e di valore per i nostri clienti. La qualità dei servizi è un elemento chiave per costruire e mantenere la fiducia dei nostri clienti, poiché dimostra la nostra capacità di fornire soluzioni sicure, efficaci e all'avanguardia.

4 SCOPO

Lo scopo di questa politica è quello di consentirci di fornire ai nostri clienti servizi di Network Operations Center (NOC), Monitoring Operations Center (MOC), Security Operations Center (SOC) di alta qualità e garantire la sicurezza delle informazioni aziendali e la protezione dei dati personali contro tutte le minacce, sia interne che esterne, sia intenzionali che accidentali. Questa politica integra gli aspetti di qualità, sicurezza delle informazioni e dati personali, per fornire un approccio olistico e coerente alla gestione dei nostri servizi e delle informazioni sensibili anche in cloud.

5 AMBITO DI APPLICAZIONE

Questa politica si applica a tutti i processi aziendali coinvolti nell' erogazione dei servizi NOC, MOC, SOC forniti dalla nostra azienda. La politica si estende inoltre alla gestione della qualità e della sicurezza delle informazioni nel contesto di un Sistema di Gestione Integrato conforme alle norme ISO 9001 e ISO 27001 con estensione alle norme ISO 27017 e 27018 per sicurezza delle informazioni e dei dati personali cloud.
La politica si applica a tutto il personale, sia interno che esterno, coinvolto nei processi di fornitura dei servizi sopra menzionati, nonché alle risorse tecniche, alle infrastrutture e ai processi utilizzati per erogare tali servizi. Inoltre, l'ambito di applicazione include le informazioni aziendali e quelle trattate per conto dei nostri clienti, indipendentemente dalla loro natura o forma (digitale, cartacea, verbale, etc.).
La politica si applica a tutti i luoghi, le attività e i processi in cui svolgiamo le attività di NOC, MOC, SOC o di supporto.
Tutti i dipendenti, collaboratori e fornitori sono tenuti a rispettare questa politica e a contribuire alla sua attuazione e al raggiungimento degli obiettivi di qualità e sicurezza delle informazioni.

6 DEFINIZIONE DELLA SICUREZZA DELLE INFORMAZIONI

La sicurezza delle informazioni consiste nel proteggere le informazioni e i sistemi informativi da accessi non autorizzati, utilizzi impropri, divulgazioni indesiderate, interruzioni, modifiche o distruzioni. L'obiettivo principale è garantire su base permanente:

- **Confidenzialità:** assicurando che le informazioni siano accessibili solo a coloro che sono autorizzati ad accedervi.
- **Integrità*:*** preservando l'accuratezza e la completezza delle informazioni e dei processi di elaborazione.
- **Disponibilità*:*** garantendo che gli utenti autorizzati possano accedere alle informazioni e alle risorse pertinenti quando necessario.

7 OBIETTIVI

L'obiettivo generale è di assicurare la qualità dei servizi forniti e la sicurezza delle informazioni trattate, garantendo la riservatezza, l'integrità e la disponibilità delle informazioni gestite.

7.1 Obiettivi specifici per la qualità

a. erogare i servizi con particolare attenzione alla soddisfazione del cliente, fornendo un servizio di supporto ed assistenza continuativo di alta qualità;
b. analizzare le richieste di mercato e percepire gli orientamenti al fine di adattare costantemente il servizio offerto alle esigenze dei clienti;
c. offrire servizi con un elevato rapporto qualità/prezzo e mantenere un alto livello qualitativo nelle attività di implementazione e assistenza;
d. garantire la flessibilità e la personalizzazione dei servizi, impegnandoci a progettare e realizzare servizi standard o speciali in base alle specifiche esigenze del cliente;
e. mantenere un'organizzazione logistica efficiente per garantire livelli di alta disponibilità di servizio e tempi di risposta rapidi e affidabili;
f. assicurare l'impiego di personale altamente qualificato per il montaggio e l'assistenza tecnica dei servizi prodotti o commercializzati;
g. fornire una tempestiva assistenza al cliente finale, garantendo risposte rapide e soluzioni efficaci.
h. coinvolgere i fornitori nell'aderenza agli standard qualitativi, compresi la puntualità delle consegne dei prodotti e l'attivazione dei servizi, la qualità e l'affidabilità dei prodotti e dei servizi, al fine di garantire una catena di fornitura affidabile, efficiente e di alta qualità.

7.2 Obiettivi specifici per la sicurezza delle informazioni

a. preservare la riservatezza, l'integrità e la disponibilità delle informazioni e la sicurezza degli asset tecnologici che le supportano;
b. assicurare e garantire la conformità con le leggi, i regolamenti e gli obblighi contrattuali;
c. rafforzare il proprio impegno per la resilienza aziendale integrando i principi della gestione della continuità operativa, conformi alla norma ISO 22301, con le strategie per la sicurezza delle informazioni.
d. promuovere la consapevolezza sulla sicurezza delle informazioni tra i dipendenti e le parti interessate.
e. garantire affidabilità e sicurezza di tutte le componenti che supportano i servizi;
f. garantire la sicurezza dei canali attraverso cui vengono trasferite le informazioni;
g. gestire e tenere sotto controllo i rischi per la sicurezza delle informazioni contenendoli entro livelli accettabili;
h. comunicare ai propri clienti l'impegno costante per la protezione delle loro informazioni;
i. supportare i clienti nell'analisi e nella gestione dei rischi di sicurezza, sia nelle attività formali/documentali, sia in quelle sostanziali legate alla prevenzione dei rischi stessi;
j. sviluppare i processi per l'erogazione del servizio sulla base di standard riconosciuti, metodologie consolidate, obbligazioni contrattuali, Leggi e Regolamenti applicabili.

7.3 Obiettivi specifici per la sicurezza delle informazioni in Cloud

a. **Utilizzo di servizi cloud:** Nella progettazione dell'utilizzo di risorse gestite nell'ambiente di cloud computing, ad esempio programmi applicativi, Critical Service, tiene conto di quanto segue:

- le informazioni archiviate nell'ambiente di cloud computing possono essere soggette all'accesso e alla gestione da parte del fornitore di servizi cloud;
- i processi possono essere eseguiti su un servizio cloud virtualizzato multi-tenant;
- gli utenti del servizio cloud e il contesto in cui utilizzano il servizio cloud;
- gli amministratori del servizio cloud del servizio cloud che hanno accesso privilegiato;
- le posizioni geografiche dell'organizzazione del fornitore di servizi cloud e i paesi in cui il fornitore di servizi cloud può archiviare i dati di Critical Service (anche temporaneamente);

b. **Offerta di servizi cloud:** Nella progettazione e fornitura ai propri clienti di risorse gestite nell'ambiente di cloud computing, Critical Service si impegna a gestire e garantire quanto segue:
- i requisiti di sicurezza delle informazioni di base applicabili alla progettazione e all'implementazione del servizio cloud;
- rischi da addetti ai lavori autorizzati;
- multi-tenant e isolamento del servizio cloud (compresa la virtualizzazione);
- accesso alle risorse dei clienti del servizio cloud da parte del personale Critical Service;
- procedure di controllo dell'accesso, ad esempio un'autenticazione forte per l'accesso amministrativo ai servizi cloud;
- comunicazioni ai clienti del servizio cloud durante la gestione delle modifiche;
- sicurezza della virtualizzazione;
- accesso e protezione dei dati dei clienti del servizio cloud;
- gestione del ciclo di vita degli account dei clienti del servizio cloud;
- comunicazione di violazioni e linee guida per la condivisione delle informazioni a supporto di indagini e analisi forensi.

7.4 Obiettivi specifici per la protezione dei dati personali anche in Cloud

- **Liceità, correttezza e trasparenza dei trattamenti di dati personali:** L'azienda si impegna a garantire la liceità, la correttezza e la trasparenza in tutti i trattamenti dei dati personali, rispettando rigorosamente le leggi sulla protezione dei dati e informando in modo chiaro e completo gli interessati su come i loro dati personali vengono raccolti, utilizzati e protetti.
- **Consapevolezza e formazione:** L'azienda si impegna a garantire che tutti i dipendenti siano consapevoli dei requisiti del GDPR e siano adeguatamente formati per trattare correttamente i dati personali.
- **Design e privacy by default**: L'azienda si impegna a integrare la privacy fin dalle prime fasi di progettazione dei prodotti e dei servizi, adottando misure tecniche e organizzative adeguate a garantire la protezione dei dati personali.
- **Responsabile della protezione dei dati (DPO**): L'azienda designa un Responsabile della protezione dei dati (DPO) che si occupa di monitorare la conformità al GDPR, fornendo consulenza interna e fungendo da punto di contatto per le autorità di controllo e gli interessati.
- **Consenso informato:** L'azienda si impegna a ottenere, ove necessario allo svolgimento di uno o più trattamenti di dati, il consenso esplicito e informato degli interessati prima di raccogliere o trattare i loro dati personali, fornendo informazioni chiare e trasparenti sulle finalità e sulle modalità di trattamento.
- **Trasferimenti internazionali di dati**: L'azienda si impegna a garantire che i trasferimenti di dati personali al di fuori dello Spazio economico europeo (SEE) siano effettuati conformemente alle disposizioni del GDPR, ad esempio mediante l'utilizzo di clausole contrattuali tipo o di meccanismi di certificazione.

- **Protezione dei dati particolari e giudiziari:** L'azienda si impegna a trattare le categorie particolati e giudiziarie di dati personali in conformità alle restrizioni previste dal GDPR, adottando misure di sicurezza adeguate a prevenire l'accesso, la divulgazione o l'uso non autorizzato di tali dati.
- **Diritti degli interessati:** L'azienda si impegna a rispettare e facilitare l'esercizio dei diritti degli interessati, come il diritto di accesso, il diritto alla rettifica, il diritto all'oblio, il diritto alla portabilità dei dati e il diritto all'opposizione al trattamento.
- **Sicurezza dei dati:** L'azienda si impegna a implementare misure di sicurezza adeguate a proteggere i dati personali da perdite, accessi non autorizzati, alterazioni o divulgazioni illecite, tenendo conto dello stato dell'arte, dei costi di attuazione e della natura, della portata, del contesto e delle finalità del trattamento.
- **Valutazione dell'impatto sulla protezione dei dati (DPIA):** L'azienda si impegna a condurre le valutazioni dell'impatto sulla protezione dei dati (DPIA) per valutare e mitigare i rischi associati alle attività di trattamento dei dati personali, specialmente quando il trattamento potrebbe comportare rischi elevati per i diritti e le libertà degli interessati.
- **Notifica delle violazioni dei dati:** L'azienda si impegna a notificare tempestivamente le violazioni dei dati personali alle autorità di controllo competenti e, se del caso, agli interessati, conformemente agli obblighi di notifica previsti dal GDPR.
- **Conservazione dei dati:** L'azienda si impegna a conservare i dati personali solo per il tempo necessario per raggiungere le finalità per le quali sono stati raccolti, rispettando i limiti di conservazione previsti dalla legge e assicurandosi che i dati vengano eliminati in modo sicuro una volta scaduto il periodo di conservazione.
- **Privacy nelle comunicazioni di marketing**: L'azienda si impegna a rispettare le norme del GDPR per le attività di marketing, ad esempio ottenendo il consenso degli interessati per l'invio di comunicazioni di marketing e fornendo loro la possibilità di revocare il consenso in qualsiasi momento.
- **Responsabilità dei fornitori di servizi**: L'azienda si impegna a garantire che i fornitori di servizi che trattano dati personali per conto dell'azienda siano adeguatamente selezionati, valutati e sottoposti a contratti vincolanti che stabiliscano gli obblighi di conformità al GDPR.
- **Monitoraggio e audit**: L'azienda si impegna a implementare meccanismi di monitoraggio e audit interni per verificare la conformità al GDPR, identificare potenziali violazioni e adottare le misure correttive appropriate.
- **Consapevolezza della privacy degli interessati**: L'azienda si impegna a informare gli interessati sui loro diritti in materia di privacy, a fornire loro informazioni chiare sulla gestione dei loro dati personali e a rispondere alle loro richieste e preoccupazioni in modo tempestivo ed efficace.
- **Trattamento di dati personali per conto di altro titolare mediante servizi cloud.** L'azienda, in qualità di Responsabile del trattamento si impegna a garantire la conformità dei trattamenti svolti mediante i propri servizi cloud ai requisiti contrattuali (es. contratti di servizio e data processing agreement) e a tutte le legge applicabili derivanti dal contesto di utilizzo e fornitura del servizio cloud come, ad esempio, l' area geografica di archiviazione dei dati da parte del fornitore del servizio cloud.

8 STRATEGIE

Per garantire la qualità dei servizi e la sicurezza delle informazioni trattate, sono adottate le seguenti strategie operative:

- operare sempre nel rispetto degli accordi contrattuali e normativi;
- promuovere lo sviluppo professionale e la professionalità dei nostri collaboratori attraverso attività di formazione e aggiornamento continuo.
- garantire che tutte le attività siano svolte con serietà, competenza e professionalità.

- Implementare strumenti e processi di controllo per valutare il livello di qualità dei nostri servizi, al fine di migliorarne costantemente i metodi e i risultati.
- Implementare un Business Continuity Management System (BCMS) certificato con la norma ISO 22301

Tutto il personale è informato, coinvolto e sollecitato a operare in conformità con la presente politica e sensibilizzato ad agire in conformità con i requisiti del sistema di gestione integrato e a segnalare eventuali violazioni di sicurezza di cui venga a conoscenza.

Inoltre, il mantenimento di un sistema di gestione certificato per la qualità e sicurezza delle informazioni garantisce quanto segue:

- monitoraggio costante dei processi e delle misure di sicurezza delle informazioni.
- registrazione, analisi e investigazione tempestive di eventuali non conformità. violazioni e incidenti di sicurezza, identificando le cause e definendo le adeguate azioni di mitigazione.
- condotta di audit interni e audit da parte di organismi indipendenti per verificare l'efficacia dei controlli per la qualità e delle contromisure di sicurezza.
- indirizzamento ottimale degli investimenti in base alla tipologia di informazioni trattate e alle esigenze di qualità del servizio espresse dagli stakeholder.
- fornitura di adeguata formazione al personale.

A tal fine, la Direzione si impegna a diffondere la cultura della qualità e della sicurezza delle informazioni, formando e informando il proprio personale, riconoscendo che il contributo delle risorse umane è uno degli aspetti più determinanti per garantire l'efficacia del sistema di gestione integrato.

9 PRINCIPI GUIDA PER LA SICUREZZA DELLE INFORMAZIONI E DEI DATI PERSONALI

I principi guida per tutte le attività relative alla sicurezza delle informazioni sono i seguenti:

- **Classificazione e protezione:** Tutte le informazioni sono asset di valore e devono essere classificate in base alla loro sensibilità e adeguatamente protette in funzione della loro criticità;
- **Accesso alle Informazioni:** L'accesso alle informazioni deve essere basato sul principio del bisogno di conoscenza (c.d. "*need-to-know*") e controllato sulla base di una specifica politica di controllo degli accessi.
- **Misure di sicurezza:** Le misure di sicurezza devono essere proporzionali al rischio.
- **Crittografia:** Le informazioni più sensibili devono essere sottoposte a cifratura durante la trasmissione e quando sono memorizzate su dispositivi portatili o sistemi esterni.
- **Integrità delle Informazioni:** Devono essere prese misure per garantire l'integrità delle informazioni.
- **Conservazione delle Informazioni:** Le informazioni devono essere conservate per il periodo richiesto dalla legge o dalla politica interna dell'azienda.
- **Distruzione delle Informazioni:** Le informazioni devono essere distrutte in modo sicuro quando non sono più necessarie.

10 IMPEGNO A SODDISFARE I REQUISITI APPLICABILI

Critical Service si impegna a rispettare tutte le leggi, i regolamenti e gli altri requisiti applicabili alla sicurezza delle informazioni. Questo include, ma non è limitato a, la protezione dei dati personali, la proprietà intellettuale, le leggi sulla diffamazione, il diritto penale e i contratti con clienti e fornitori e le altre parti interessate.

11 MIGLIORAMENTO CONTINUO

La direzione si impegna a migliorare continuamente il sistema di gestione integrato per la qualità e la sicurezza delle informazioni attraverso la revisione regolare delle politiche, dei controlli, dell'efficacia delle misure di sicurezza e del rispetto delle leggi e dei regolamenti applicabili.

12 RESPONSABILITÀ

Il raggiungimento degli obiettivi per la qualità e la sicurezza delle informazioni richiede l'impegno e la collaborazione di tutto il personale. In particolare, ogni individuo coinvolto direttamente o indirettamente nell' erogazione dei servizi NOC -SOC e MOC è responsabile di comprendere e aderire a questa politica, nonché di segnalare eventuali violazioni o potenziali rischi per la sicurezza delle informazioni.

Le responsabilità per la gestione della qualità e della sicurezza delle informazioni sono assegnate a ruoli definiti all'interno dell'organizzazione, tra cui la direzione e i dipendenti.

- La direzione è responsabile della definizione e del mantenimento delle politiche e delle procedure per la qualità e per la sicurezza delle informazioni e del recepimento dei requisiti normativi e contrattuali. Inoltre, la direzione è responsabile della supervisione e dell'attuazione delle politiche e delle procedure per la gestione della qualità e la sicurezza delle informazioni.
- I dipendenti, in qualità di proprietari delle attività e degli asset informativi a loro assegnati, sono responsabili del rispetto delle politiche e delle procedure per la qualità e la sicurezza delle informazioni e del segnalare eventuali incidenti di sicurezza al Responsabile per la sicurezza delle informazioni.

Critical Service integra e mantiene aggiornato l'organigramma aziendale con i ruoli e responsabilità per la qualità e per la sicurezza delle informazioni derivanti dalla presente politica.

13 CONFORMITÀ

La politica per la qualità e la sicurezza delle informazioni viene mantenuta costantemente in linea con i requisiti legislativi, normativi e contrattuali applicabili.

14 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, mediante pubblicazione sul sito web www.criticalservice.it

15 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.

16 GESTIONE DELLE ESENZIONI ED ECCEZIONI

Le esenzioni e le eccezioni alla presente politica devono essere richieste da un responsabile di dipartimento o servizio e devono essere approvate dal Responsabile della Qualità e dal Responsabile per la Sicurezza delle Informazioni. Questo processo sarà sottoposto a controlli regolari per garantire che le esenzioni non compromettano la sicurezza generale delle informazioni e la qualità dei servizi erogati.

Tutte le eccezioni alla politica devono essere adeguatamente documentate, comprese le motivazioni per l'eccezione e i potenziali rischi associati. Le eccezioni devono essere riviste regolarmente per garantire che siano ancora necessarie.

17 VALIDITA' APPROVAZIONE E MODIFICHE

La presente politica per la qualità e per la sicurezza delle informazioni è approvata dall'Alta Direzione nella persona del Legale rappresentante aziendale o suo Delegato. Tutte le modifiche a questa politica devono essere 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