Politica Aziendale

Sistema di Gestione della Continuità Operativa (BCMS)

Scopo della Politica

Zucchetti Healthcare riconosce la continuità operativa dei propri servizi come un elemento essenziale per garantire l'affidabilità delle soluzioni software e dei servizi digitali erogati nel settore sanitario e socioassistenziale, con particolare riferimento alla disponibilità delle piattaforme applicative, all'accesso ai dati e al supporto alle attività operative delle strutture clienti.

L'organizzazione si impegna a prevenire, gestire e superare eventi che possano compromettere la disponibilità dei servizi, l'integrità delle informazioni e la capacità operativa aziendale, inclusi eventi di natura cyber che possano impattare sui sistemi informativi e sui servizi digitali, assicurando il ripristino delle attività entro tempi coerenti con gli obblighi contrattuali, normativi e con le esigenze dei propri clienti.

In tale contesto, Zucchetti Healthcare adotta un approccio strutturato alla gestione della continuità operativa, orientato dai principi della norma ISO 22301 – *Security and Resilience – Business Continuity Management Systems*, che definisce i requisiti per l'istituzione, l'attuazione, il mantenimento e il miglioramento continuo di un *Sistema di Gestione della Business Continuity* (BCMS).

La presente Politica definisce i principi e gli indirizzi attraverso cui Zucchetti Healthcare governa il proprio sistema di Business Continuity e Disaster Recovery, assicurando la coerenza con il Sistema di Gestione Integrato dell'organizzazione, con le politiche aziendali in materia di sicurezza delle informazioni e con le normative e gli standard applicabili.

Ambito di applicazione

La presente Politica si applica all'insieme dei processi, delle risorse e delle infrastrutture che contribuiscono all'erogazione dei servizi dell'organizzazione e che risultano rilevanti ai fini della continuità operativa.

Il sistema di Business Continuity e Disaster Recovery di Zucchetti Healthcare comprende i processi aziendali identificati come critici per la continuità operativa, i servizi applicativi e infrastrutturali erogati ai clienti, i sistemi informativi e le infrastrutture tecnologiche utilizzate per l'erogazione dei servizi, nonché le risorse umane, organizzative e logistiche coinvolte nei processi aziendali e i servizi o le infrastrutture forniti da terze parti da cui dipende la continuità operativa dell'organizzazione.

Particolare attenzione è rivolta ai servizi digitali erogati in modalità cloud (SaaS) e ai servizi di hosting o infrastrutturali dedicati, che rappresentano componenti centrali dell'offerta aziendale e che, per la loro natura e per il contesto operativo del settore sanitario e socioassistenziale, richiedono specifiche misure di resilienza operativa, continuità del servizio e capacità di ripristino.

Principi generali

La continuità operativa è parte integrante della strategia aziendale e contribuisce alla tutela del valore erogato ai clienti, alla sicurezza delle informazioni e alla sostenibilità dei servizi. La capacità dell'organizzazione di garantire la continuità dei propri servizi digitali rappresenta un elemento

fondamentale di affidabilità e responsabilità nei confronti delle strutture sanitarie e socioassistenziali che utilizzano le soluzioni di Zucchetti Healthcare.

Valutazione dei rischi

Le decisioni in materia di continuità operativa sono basate su un approccio strutturato di analisi degli impatti e dei rischi. In particolare, l'organizzazione utilizza strumenti quali la Business Impact Analysis (BIA) e la Threat and Risk Analysis (TRA) per identificare i processi critici, valutare le potenziali interruzioni, incluse quelle derivanti da eventi cyber, e definire le priorità di intervento.

Misure di continuità e resilienza

Le misure di continuità e di ripristino sono progettate in modo proporzionato alla criticità dei processi e dei servizi, tenendo conto dei parametri di continuità definiti per ciascun processo, quali Maximum Tolerable Period of Disruption (MTP), Recovery Time Objective (RTO) e Recovery Point Objective (RPO), che costituiscono il riferimento operativo per la definizione delle strategie di continuità e di disaster recovery.

Le misure tecniche e organizzative adottate sono orientate alla resilienza dei servizi, anche rispetto a eventi di sicurezza informatica, garantendo capacità di ripristino in caso di indisponibilità, compromissione o perdita di dati, per consentire il recupero tempestivo delle funzionalità critiche e la continuità dell'erogazione dei servizi

Gestione degli eventi critici

La gestione degli eventi critici è coordinata attraverso un sistema di governance formalizzato, che definisce ruoli, responsabilità e modalità di comunicazione interna ed esterna. In caso di eventi che possano compromettere la continuità operativa, l'organizzazione attiva le strutture decisionali e operative previste dal sistema di gestione della continuità operativa e dalle procedure di gestione degli incidenti e delle crisi.

Ruoli, responsabilità e consapevolezza

La Direzione garantisce l'impegno e le risorse necessarie per l'attuazione della presente Politica e per il mantenimento del sistema di Business Continuity.

Il Business Continuity Manager (Process Owner o Service Manager) coordina le attività di analisi, pianificazione, test e miglioramento dei piani di continuità operativa e di disaster recovery, assicurando il monitoraggio delle misure adottate e il loro aggiornamento nel tempo.

Il Comitato di crisi gestisce le situazioni di emergenza e coordina le decisioni operative in caso di attivazione dei piani di continuità operativa o di disaster recovery, garantendo la gestione coordinata degli eventi critici e delle comunicazioni interne ed esterne.

I responsabili di processo e le funzioni tecniche collaborano alla definizione delle misure di continuità operativa e partecipano alle attività di ripristino in caso di evento critico, contribuendo all'attuazione delle strategie e delle procedure previste dal sistema di gestione della continuità operativa.

Tutto il personale è tenuto a contribuire alla resilienza organizzativa adottando comportamenti coerenti con le procedure aziendali e partecipando alle attività di formazione e sensibilizzazione previste nell'ambito del sistema di Business Continuity.

Miglioramento continuo

Il miglioramento continuo del sistema di Business Continuity e Disaster Recovery è perseguito attraverso l'analisi degli incidenti e delle interruzioni operative, al fine di identificare le cause degli eventi e individuare eventuali opportunità di miglioramento delle misure di prevenzione e risposta.

L'organizzazione assicura inoltre la verifica periodica dei piani di continuità operativa e disaster recovery mediante attività di test, simulazioni ed esercitazioni, nonché l'aggiornamento delle misure tecniche e organizzative adottate per la continuità dei servizi, in funzione dell'evoluzione dei rischi, delle infrastrutture tecnologiche e del contesto operativo.

Le evidenze emerse dalle attività di verifica, dagli audit interni e dalle analisi degli eventi sono integrate nei processi di riesame e miglioramento del sistema di gestione, anche attraverso il Riesame della Direzione, al fine di garantire l'adeguatezza, l'efficacia e l'allineamento del sistema di Business Continuity con gli obiettivi strategici dell'organizzazione.

Diffusione della Politica

La Politica è comunicata a tutto il personale ed è resa disponibile alle parti interessate rilevanti, secondo modalità idonee a garantirne la comprensione e l'applicazione.

La Direzione promuove la conoscenza della Politica e ne sostiene l'attuazione nell'ambito delle attività aziendali, assicurando che i principi di continuità operativa siano integrati nei processi organizzativi e nelle decisioni operative.

Integrazione nel Sistema di Gestione

Il Sistema di Gestione della Continuità Operativa opera in coordinamento con gli altri sistemi di gestione adottati dall'organizzazione, assicurando coerenza tra gli obiettivi di sicurezza, gli indirizzi strategici aziendali e i processi operativi[1].

Le politiche, le procedure e le misure di sicurezza sono pertanto applicate in modo trasversale ai processi aziendali, contribuendo al miglioramento continuo dell'organizzazione e alla qualità dei servizi erogati.

Rovereto, 29/06/2026

Paolo Galfione

(Amministratore Unico)

Nome: PAOLO GALFIONE
Emesso da: InfoCamere Qualified Electronic Signature CA
Località: Cles, Italia
Data: 29/06/2026

[1] Si rimanda in generale alla Politica Aziendale integrata PAC01, alla Politica Aziendale PAC02 per il Sistema di Gestione della Sicurezza delle Informazioni, alla Politica Aziendale PAC04 per il Sistema di Gestione della Intelligenza Artificiale, alla Politica Aziendale PAC05 per il Sistema di IT Service Management e alla Politica Aziendale per la Cybersicurezza PAC06.