Politica Aziendale

Sistema Integrato per Qualità, Service Management, Sicurezza delle Informazioni, Continuità Operativa, Intelligenza Artificiale e Responsabilità d'Impresa (ESG)

Identità e finalità

Zucchetti Healthcare sviluppa ed eroga soluzioni software e servizi digitali per il settore sanitario, sociosanitario e assistenziale, supportando organizzazioni pubbliche e private nella gestione dei servizi alla persona.

In questo contesto l'affidabilità dei sistemi informativi, la protezione delle informazioni, la continuità dei servizi e l'utilizzo responsabile delle tecnologie digitali rappresentano elementi essenziali per garantire qualità dei servizi e fiducia da parte delle organizzazioni clienti e delle altre parti interessate.

Per questo motivo l'azienda adotta un *Sistema di Gestione Integrato* che governa in modo coordinato qualità dei servizi, sicurezza delle informazioni, continuità operativa e utilizzo responsabile delle tecnologie digitali, inclusi i sistemi basati su intelligenza artificiale.

La presente Politica definisce i principi e gli indirizzi generali che orientano lo sviluppo dei prodotti, la gestione dei processi e l'erogazione dei servizi.

Il Sistema di Gestione Integrato è articolato in specifici sistemi di gestione tematici, disciplinati da politiche dedicate che ne definiscono principi e modalità operative. Tali sistemi tematici operano in modo coordinato all'interno del Sistema di Gestione Integrato aziendale.

In tale contesto, l'organizzazione riconosce la cybersicurezza come elemento strutturale per l'affidabilità dei servizi digitali, assicurando la protezione delle reti e dei sistemi informativi, la resilienza operativa e la capacità di prevenzione, rilevazione e gestione degli eventi cyber, in coerenza con i requisiti normativi applicabili.

Scopo e campo di applicazione

La Politica definisce i principi attraverso cui Zucchetti Healthcare governa in modo integrato:

- qualità dei servizi;
- sicurezza delle informazioni e dei servizi;
- continuità operativa;
- gestione dei servizi digitali;
- utilizzo responsabile delle tecnologie basate su intelligenza artificiale.

Essa si applica a tutte le attività, ai processi organizzativi, alle infrastrutture tecnologiche e ai servizi attraverso cui l'organizzazione sviluppa ed eroga le proprie soluzioni.

La Politica riguarda l'intera organizzazione e tutte le persone che operano per conto di Zucchetti Healthcare, inclusi dipendenti, collaboratori e consulenti. I principi qui definiti si estendono inoltre ai fornitori, ai partner tecnologici e alle terze parti coinvolte nello sviluppo o nell'erogazione dei servizi.

Quadro di riferimento: standard, normative e sistemi di gestione

Il Sistema di Gestione Integrato di Zucchetti Healthcare si fonda sull'adozione di standard internazionali e sul rispetto delle normative applicabili al settore dei servizi digitali in ambito sanitario e sociosanitario. A tal fine l'organizzazione adotta:

- un Sistema di Gestione per la Qualità conforme alla UNI EN ISO 9001, che costituisce il riferimento per la gestione per processi e il miglioramento continuo delle attività aziendali;
- un Sistema di Gestione per la Sicurezza delle Informazioni conforme alla ISO/IEC 27001, integrato con le estensioni ISO/IEC 27017 e ISO/IEC 27018, esteso ai principi del Privacy Information Management System per il governo delle informazioni personali, della protezione dei dati personali e dell'accountability privacy[1];
- un modello di Business Continuity e Disaster Recovery (BCMS) orientato dai principi della norma ISO 22301, finalizzato a garantire la resilienza e la continuità dei servizi digitali, disciplinato nella Politica di Business Continuity e Disaster Recovery[2];
- un Sistema di Gestione dei Servizi IT (ITMS) orientato ai principi della norma ISO/IEC 20000 e alle buone pratiche IT Service Management (ITIL), finalizzato a garantire l'affidabilità, la qualità e la continuità dei servizi digitali erogati, come definito nella Politica di gestione dei servizi IT[3];
- un Sistema di Gestione per l'Intelligenza Artificiale (AIMS) orientato ai principi dello standard ISO/IEC 42001 e coerente con il Regolamento europeo sull'Intelligenza Artificiale (AI Act), finalizzato a garantire uno sviluppo e un utilizzo responsabile dei sistemi di AI, come disciplinato nella Politica aziendale per l'utilizzo dell'Intelligenza Artificiale[4];
- un Sistema di Gestione della Cybersicurezza (CSMS), che mette in atto principi, ruoli, responsabilità, misure organizzative e presidi tecnico-operativi finalizzati alla prevenzione, gestione e mitigazione dei rischi cyber, sviluppato in coerenza con il perimetro applicativo della Direttiva (UE) 2022/2555 (NIS2), con i requisiti di sicurezza già presidiati dal Sistema di Gestione per la Sicurezza delle Informazioni e con gli indirizzi definiti nella Politica per la Cybersicurezza[5].

L'organizzazione opera, inoltre, nel rispetto delle normative europee e nazionali applicabili in materia di protezione dei dati personali, sicurezza digitale e conformità dei prodotti e servizi erogati. In tale ambito rientrano, in particolare, il Regolamento (UE) 2016/679 (GDPR), per quanto riguarda il trattamento dei dati personali, e il Regolamento (UE) 2017/745 (MDR), nei casi in cui i software siano qualificati come dispositivi medici o siano utilizzati nell'ambito di processi e contesti clinici regolati.

Principi della Politica Integrata

La Politica Integrata di Zucchetti Healthcare si fonda su principi che orientano lo sviluppo dei prodotti, la gestione dei processi e l'erogazione dei servizi.

[1] Politica Aziendale PAC02 per il Sistema di Gestione della Sicurezza delle Informazioni.
[2] Politica Aziendale PAC03 per il Sistema di Gestione della Continuità Operativa.
[3] Politica Aziendale PAC05 per il Sistema di IT Service Management.
[4] Politica Aziendale PAC04 per il Sistema di Gestione della Intelligenza Artificiale.
[5] Politica Aziendale PAC06 per il Sistema di Gestione della Cybersicurezza.

L'organizzazione promuove un orientamento alla *qualità e al valore dei servizi*, adottando un approccio per processi e perseguendo il miglioramento continuo delle proprie attività.

La *protezione delle informazioni e dei sistemi digitali* rappresenta un principio essenziale. Le informazioni sono tutelate secondo i principi di riservatezza, integrità e disponibilità attraverso un approccio sistematico alla sicurezza basato sulla gestione del rischio.

L'organizzazione promuove la sicurezza e la resilienza dei servizi digitali quale elemento essenziale di affidabilità e continuità, adottando un approccio integrato alla *gestione dei rischi cyber* che considera sistemi, infrastrutture, processi e relazioni con terze parti.

L'organizzazione assicura la *continuità operativa dei servizi digitali*, adottando misure organizzative e tecnologiche finalizzate alla prevenzione delle interruzioni e al ripristino tempestivo delle funzionalità critiche.

L'utilizzo delle *tecnologie digitali e dei sistemi basati su intelligenza artificiale* avviene nel rispetto dei principi di trasparenza, tracciabilità e supervisione umana, assicurando che tali tecnologie supportino l'attività delle persone senza sostituirne la responsabilità.

Il Sistema di Gestione Integrato si fonda inoltre sulla *responsabilità organizzativa diffusa*, secondo cui tutte le persone che operano per conto dell'organizzazione contribuiscono alla qualità dei servizi, alla sicurezza delle informazioni e alla resilienza dei sistemi.

Zucchetti Healthcare riconosce infine l'importanza della *responsabilità d'impresa e della sostenibilità*, assumendo i principi ESG (Environmental, Social and Governance) come riferimento per orientare lo sviluppo delle proprie attività verso modelli affidabili, trasparenti e sostenibili nel tempo[6].

Impegni dell'organizzazione

Attraverso la presente Politica Zucchetti Healthcare si impegna a:

- garantire elevati standard di qualità nello sviluppo e nell'erogazione delle proprie soluzioni software e dei servizi digitali, adottando un approccio per processi e perseguendo il miglioramento continuo delle attività;
- proteggere le informazioni e i sistemi digitali, assicurandone riservatezza, integrità e disponibilità mediante l'applicazione del Sistema di Gestione per la Sicurezza delle Informazioni;
- assicurare la resilienza e la continuità dei servizi digitali, attraverso adeguate misure di prevenzione, gestione delle emergenze e ripristino delle funzionalità critiche, secondo i principi del sistema di Business Continuity e Disaster Recovery;
- gestire e sviluppare i servizi digitali secondo pratiche strutturate di gestione dei servizi IT, al fine di garantire affidabilità, stabilità e qualità operativa dei servizi erogati;
- sviluppare ed utilizzare le tecnologie digitali, inclusi i sistemi basati su intelligenza artificiale, in modo responsabile, trasparente e soggetto a supervisione umana, nel rispetto dei principi definiti nel sistema aziendale di gestione dell'intelligenza artificiale;

[6] In tale ambito, l'organizzazione considera rilevante valutare gli effetti dell'utilizzo delle proprie soluzioni e dei propri servizi nei contesti operativi degli enti clienti, con particolare attenzione agli impatti sui processi assistenziali, organizzativi e sull'utenza finale. Tali elementi costituiscono un riferimento significativo anche ai fini della valutazione del valore sociale generato e della rendicontazione nell'ambito del bilancio sociale.

- presidiare i rischi cyber associati ai servizi digitali, alle infrastrutture tecnologiche e alle relazioni con fornitori e partner, adottando misure tecniche e organizzative adeguate alla criticità dei servizi e garantendo la capacità di risposta e ripristino in caso di eventi avversi;
- operare nel rispetto delle normative applicabili e promuovere lo sviluppo sostenibile dei servizi digitali, contribuendo alla creazione di valore per clienti, istituzioni e comunità nel rispetto dei principi di responsabilità d'impresa e sostenibilità.

Governance e responsabilità

L'attuazione della presente Politica è assicurata attraverso un modello di governance che integra qualità, sicurezza delle informazioni, continuità operativa, gestione dei servizi digitali e utilizzo responsabile delle tecnologie.

La Direzione definisce gli indirizzi strategici del Sistema di Gestione Integrato e assicura le risorse necessarie al suo funzionamento.

Gli obiettivi relativi ai diversi ambiti del sistema sono monitorati attraverso processi di controllo, audit e riesame del sistema di gestione.

Le responsabilità operative sono attribuite alle funzioni organizzative competenti, che operano in coordinamento con la Direzione e con le strutture tecniche e operative dell'organizzazione.

I principi della Politica si applicano inoltre ai fornitori, ai partner tecnologici e alle terze parti coinvolte nello sviluppo o nell'erogazione dei servizi.

Gestione del rischio

Zucchetti Healthcare adotta un approccio sistematico alla gestione dei rischi quale elemento fondante del proprio Sistema di Gestione Integrato.

La gestione del rischio è applicata ai processi aziendali, alle infrastrutture tecnologiche, alle informazioni trattate e alle relazioni con fornitori e partner, con l'obiettivo di individuare e trattare i fattori che possono influire sulla qualità e sull'affidabilità dei servizi.

Questo approccio guida la definizione delle misure di sicurezza delle informazioni, delle strategie di continuità operativa e delle modalità di sviluppo e utilizzo delle tecnologie digitali, inclusi i sistemi basati su intelligenza artificiale.

Comunicazione, formazione e consapevolezza

L'efficacia della Politica dipende dalla consapevolezza e dalla responsabilità delle persone che operano nell'organizzazione.

Zucchetti Healthcare promuove attività di informazione, formazione e sensibilizzazione finalizzate a sviluppare la conoscenza dei principi del Sistema di Gestione Integrato e a favorire comportamenti responsabili nella gestione delle informazioni e nell'utilizzo delle infrastrutture tecnologiche.

La Politica è resa disponibile sia all'interno dell'organizzazione sia alle parti interessate esterne, al fine di garantire trasparenza e diffusione degli impegni assunti dall'azienda.

Monitoraggio e miglioramento continuo

L'organizzazione verifica l'efficacia del Sistema di Gestione Integrato attraverso attività di misurazione delle prestazioni, audit interni e verifiche periodiche dei processi.

Sono inoltre effettuati test ed esercitazioni periodiche per verificare l'efficacia delle strategie di continuità operativa e delle procedure di ripristino dei servizi.

I risultati delle attività di monitoraggio sono valutati dalla Direzione nell'ambito del riesame del sistema di gestione, che consente di definire azioni di miglioramento e nuovi obiettivi organizzativi.

Riesame e aggiornamento della Politica

La presente Politica è oggetto di riesame periodico da parte della Direzione al fine di verificarne l'adeguatezza rispetto al contesto organizzativo, tecnologico e normativo.

Eventuali aggiornamenti sono approvati dalla Direzione e registrati nel sistema documentale aziendale, garantendo la tracciabilità delle revisioni e la disponibilità delle versioni aggiornate.

Rovereto, 03/07/2026

Paolo Galfione

(Amministratore Unico)

Nome: PAOLO GALFIONE
Emesso da: InfoCamere Qualified Electronic Signature CA
Località: Trento, Italia
Data: 03/07/2026