Politica Aziendale

Sistema di Gestione della Sicurezza delle Informazioni (SGSI o ISMS), esteso alla protezione delle informazioni personali (PIMS)

Scopo della Politica

La presente Politica definisce i principi e gli indirizzi adottati dall'organizzazione per garantire la sicurezza delle informazioni e dei sistemi informativi, nel rispetto dei requisiti del *Sistema di Gestione della Sicurezza delle Informazioni* (SGSI) conforme alla norma ISO/IEC 27001, con riferimento alle linee guida ISO/IEC 27017 e ISO/IEC 27018.

La Politica stabilisce il quadro di riferimento per la gestione dei rischi, la protezione del patrimonio informativo e il miglioramento continuo del SGSI, assicurando la tutela della riservatezza, dell'integrità e della disponibilità delle informazioni trattate dall'organizzazione.

Essa costituisce inoltre un riferimento interno per l'individuazione, la classificazione e la gestione delle informazioni e dei sistemi che le trattano, in coerenza con le prescrizioni normative applicabili, incluse quelle in materia di protezione dei dati personali e sicurezza delle infrastrutture digitali.

Il Sistema di Gestione della Sicurezza delle Informazioni costituisce inoltre il riferimento per la gestione dei rischi cyber relativi alle reti, ai sistemi informativi e ai servizi digitali, in coerenza con i requisiti normativi applicabili.

La Politica costituisce inoltre il riferimento per l'estensione del Sistema di Gestione della Sicurezza delle Informazioni alla gestione delle informazioni personali, secondo i principi del Privacy Information Management System, con l'obiettivo di rafforzare il governo dei trattamenti, la tutela dei diritti degli interessati, la gestione dei ruoli privacy, la tracciabilità delle evidenze e la dimostrazione dell'accountability dell'organizzazione.

Ambito di applicazione

La presente Politica si applica a tutte le informazioni trattate dall'organizzazione, indipendentemente dalla forma o dal supporto utilizzato, nonché ai sistemi, alle infrastrutture tecnologiche e ai servizi che ne consentono la gestione, l'elaborazione, la conservazione e la trasmissione.

Essa riguarda il personale interno, i collaboratori, i fornitori e tutte le parti che operano nell'ambito dei processi aziendali e dei servizi erogati, in relazione alle informazioni e ai sistemi utilizzati nello svolgimento delle attività.

Con riferimento alle informazioni personali, la Politica si applica ai trattamenti svolti da ZHC nell'ambito dei propri processi interni e ai trattamenti effettuati nell'erogazione dei servizi software, cloud, assistenza, manutenzione, formazione, consulenza e gestione applicativa, tenendo conto dei diversi ruoli assunti dall'organizzazione, anche quale titolare, responsabile o sub-responsabile del trattamento.

Principi generali

L'organizzazione riconosce il patrimonio informativo come un asset strategico e adotta misure organizzative, tecniche e procedurali volte a garantirne:

- riservatezza, prevenendo accessi non autorizzati alle informazioni;

- integrità, assicurando l'accuratezza e la completezza delle informazioni;
- disponibilità, garantendo l'accesso alle informazioni e la continuità dei servizi, nonché la capacità di prevenzione, rilevazione, risposta e ripristino rispetto a eventi di sicurezza informatica.

La sicurezza delle informazioni costituisce parte integrante della governance aziendale ed è integrata nei processi di sviluppo, gestione ed erogazione dei servizi.

Censimento delle informazioni e dei trattamenti

Elemento fondamentale della sicurezza delle informazioni è la conoscenza del patrimonio informativo gestito.

L'organizzazione mantiene un censimento aggiornato delle informazioni, dei sistemi e dei trattamenti effettuati, identificando per ciascun ambito:

- le informazioni trattate e il relativo valore per l'organizzazione;
- i processi e i sistemi coinvolti nel trattamento e nella gestione delle informazioni;
- i soggetti che vi accedono nell'ambito delle attività operative;
- le responsabilità associate alla gestione e alla protezione delle informazioni.

Il censimento costituisce la base per le attività di classificazione delle informazioni, analisi del rischio e definizione delle misure di sicurezza, nonché per la gestione complessiva degli asset informativi nell'ambito del SGSI.

Protezione delle informazioni personali e PIMS

L'organizzazione integra nel Sistema di Gestione della Sicurezza delle Informazioni i principi e i presidi relativi alla protezione delle informazioni personali, al fine di assicurare che i trattamenti siano governati in modo conforme, sicuro, documentato e verificabile.

In tale ambito, ZHC mantiene il censimento dei trattamenti, individua i ruoli e le responsabilità privacy, valuta i rischi per i diritti e le libertà degli interessati, definisce misure tecniche e organizzative adeguate, gestisce le richieste relative all'esercizio dei diritti, presidia le informative, le nomine, i rapporti con fornitori e subfornitori, la conservazione, la cancellazione, la restituzione e l'eventuale comunicazione dei dati personali.

Il PIMS è attuato secondo un approccio proporzionato al rischio e integrato con i processi di sicurezza delle informazioni, gestione dei servizi cloud, continuità operativa, cybersicurezza, sviluppo software, AI, gestione fornitori, audit e miglioramento continuo.

Gestione del rischio per la sicurezza delle informazioni

L'organizzazione adotta un approccio sistematico alla gestione del rischio per la sicurezza delle informazioni, conforme ai principi della norma ISO/IEC 27001.

Attraverso processi strutturati di identificazione, analisi, valutazione e trattamento dei rischi, vengono individuate le minacce e le vulnerabilità che possono compromettere la sicurezza delle informazioni, definendo le misure di controllo più adeguate alla loro mitigazione.

La gestione del rischio costituisce un elemento centrale del Sistema di Gestione della Sicurezza delle Informazioni e orienta la definizione, l'implementazione e il monitoraggio delle misure organizzative, tecniche e procedurali adottate dall'organizzazione.

Nell'ambito di tale processo sono considerati anche i rischi derivanti da minacce cyber, dalle dipendenze da fornitori e servizi ICT, dall'utilizzo di infrastrutture cloud e dalle interconnessioni tra sistemi e organizzazioni.

Conformità normativa e regolatoria

La sicurezza delle informazioni è perseguita nel rispetto delle normative applicabili e dei requisiti contrattuali.

In particolare, il Sistema di Gestione della Sicurezza delle Informazioni tiene conto dei principi e degli obblighi derivanti da:

- Regolamento (UE) 2016/679 (GDPR) in materia di protezione dei dati personali;
- Direttiva (UE) 2022/2555 (NIS2) relativa alla sicurezza delle reti e dei sistemi informativi;
- normative nazionali e settoriali applicabili ai servizi digitali e ai servizi sociosanitari.

L'organizzazione promuove inoltre l'adozione di codici di condotta e di schemi di certificazione riconosciuti, quando utili a rafforzare la fiducia delle parti interessate e a dimostrare la conformità ai requisiti normativi e di sicurezza applicabili.

Sicurezza dei servizi cloud

Per i servizi erogati o utilizzati in ambiente cloud, l'organizzazione applica i controlli e le buone pratiche indicati nelle norme ISO/IEC 27017 e ISO/IEC 27018, con particolare attenzione a:

- separazione logica e protezione dei dati dei clienti;
- chiara definizione e gestione delle responsabilità tra provider e utilizzatori dei servizi cloud;
- protezione dei dati personali trattati in ambienti cloud.

L'organizzazione assicura inoltre che i servizi cloud adottati o erogati siano gestiti in modo coerente con i requisiti del Sistema di Gestione della Sicurezza delle Informazioni e con le normative applicabili.

Ruoli, responsabilità e consapevolezza

La sicurezza delle informazioni è una responsabilità condivisa da tutta l'organizzazione.

La Direzione assicura il supporto al Sistema di Gestione della Sicurezza delle Informazioni e mette a disposizione le risorse necessarie per il suo funzionamento e il suo miglioramento continuo, mentre tutto il personale è chiamato a operare nel rispetto delle politiche, delle procedure e delle misure di sicurezza definite.

La Direzione assicura la supervisione dei rischi cyber rilevanti e promuove l'integrazione della sicurezza delle informazioni nei processi decisionali e strategici dell'organizzazione.

L'organizzazione promuove attività continuative di formazione, informazione e sensibilizzazione sulla sicurezza delle informazioni, al fine di garantire un adeguato livello di consapevolezza e di responsabilità nell'utilizzo dei sistemi e nella gestione delle informazioni.

Miglioramento continuo

Il Sistema di Gestione della Sicurezza delle Informazioni è soggetto a monitoraggio continuo attraverso audit interni, riesami della Direzione, analisi degli incidenti, incluse le valutazioni post-evento e le azioni di miglioramento derivanti da eventi di sicurezza informatica.

I risultati di tali attività sono utilizzati per migliorare costantemente l'efficacia del sistema e l'adeguatezza delle misure di sicurezza adottate, assicurando l'evoluzione del SGSI in relazione ai cambiamenti organizzativi, tecnologici e normativi.

Diffusione della Politica

La presente politica è comunicata all'interno dell'organizzazione ed è resa disponibile a tutto il personale e ai collaboratori che operano nell'ambito dei processi aziendali e dei servizi erogati.

L'organizzazione assicura che i contenuti della politica siano conosciuti e compresi dalle persone che trattano informazioni o utilizzano sistemi informativi nell'ambito delle proprie attività.

La politica è inoltre resa disponibile alle parti interessate rilevanti quando necessario o opportuno, in coerenza con le modalità di comunicazione previste dall'organizzazione.

Integrazione nel Sistema di Gestione

Il Sistema di Gestione della Sicurezza delle Informazioni 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, 03/07/2026

Paolo Galfione

(Amministratore Unico)

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

[1] Si rimanda in generale alla Politica Aziendale integrata PAC01, alla Politica Aziendale PAC03 per il Sistema di Gestione della Continuità Operativa, 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.