Politica Aziendale

Sistema di Gestione per la Cybersicurezza

Scopo della Politica

La presente Politica definisce gli indirizzi aziendali per il governo della cybersicurezza e della resilienza dei sistemi informativi e di rete di Zucchetti Healthcare S.r.l., in coerenza con il Sistema di Gestione Integrato, con il Sistema di Gestione per la Sicurezza delle Informazioni, con ISO/IEC 27001:2022, con le estensioni applicabili ai servizi cloud e con il quadro normativo derivante dalla Direttiva NIS2 e dal D.Lgs. 138/2024.

La Politica ha lo scopo di assicurare che la cybersicurezza sia gestita come componente strutturale dei processi aziendali, con particolare attenzione alla protezione dei servizi cloud, dei servizi gestiti, delle applicazioni software, delle infrastrutture tecnologiche, degli ambienti di sviluppo, test e produzione, delle identità digitali, degli accessi, dei dati trattati, dei fornitori ICT e dei processi che concorrono alla continuità operativa.

La Politica non si limita alla gestione tecnica delle vulnerabilità, dei Vulnerability Assessment e dei Penetration Test, ma definisce il quadro di governo entro cui sono pianificate, attuate, monitorate e migliorate le misure organizzative, tecniche e procedurali finalizzate alla prevenzione, rilevazione, gestione e mitigazione dei rischi cyber.

Perimetro NIS2

Zucchetti Healthcare S.r.l. rientra nel perimetro NIS2 quale soggetto essenziale, come da comunicazione ACN relativa alla Dichiarazione DNISA00041373, con codice univoco identificativo del soggetto ZHC ITM4TMH2.

Il perimetro NIS2 dichiarato riguarda le seguenti tipologie di soggetto: Gestione dei servizi TIC – Fornitori di servizi gestiti; Infrastrutture digitali – Fornitori di servizi di cloud computing.

Ai fini della presente Politica, rientrano nel perimetro NIS2 i servizi cloud e i servizi gestiti erogati da ZHC, insieme agli asset, alle risorse, ai sistemi informativi e di rete, ai processi e ai fornitori che ne consentono progettazione, erogazione, gestione, manutenzione, monitoraggio, assistenza, continuità e ripristino.

Per i servizi applicativi cloud, il perimetro comprende le applicazioni, gli ambienti di produzione, i database, l'infrastruttura cloud, i sistemi di autenticazione, le reti, i backup, il logging, il monitoraggio, gli strumenti di amministrazione, le procedure di rilascio, l'assistenza tecnica, il personale autorizzato e i fornitori infrastrutturali coinvolti.

Per i servizi gestiti, il perimetro comprende le attività con cui ZHC assicura configurazione, aggiornamento, manutenzione, monitoraggio, supporto, gestione delle anomalie e interventi correttivi su sistemi o servizi rilevanti per i clienti. Sono pertanto ricompresi anche strumenti di ticketing, utenze tecniche, accessi privilegiati, documentazione operativa, procedure di escalation e risorse umane coinvolte.

L'identificazione degli elementi riconducibili al perimetro NIS2 avviene secondo un criterio di dipendenza funzionale. Un asset, una risorsa, un processo o un fornitore è rilevante quando la sua indisponibilità, compromissione, alterazione o gestione non adeguata può incidere sulla sicurezza,

disponibilità, integrità, riservatezza o continuità dei servizi cloud o dei servizi gestiti dichiarati da ZHC.

La presente Politica ha comunque applicazione più ampia rispetto al solo perimetro NIS2, in quanto disciplina il presidio della cybersicurezza in modo trasversale all'intera organizzazione, includendo anche servizi, asset e processi non formalmente ricompresi nel perimetro NIS2 ma rilevanti per la sicurezza delle informazioni, la continuità operativa, la protezione dei dati, la gestione degli accessi o il Sistema di Gestione Integrato.

Principi generali

Zucchetti Healthcare adotta un approccio alla cybersicurezza fondato su prevenzione, proporzionalità, responsabilizzazione delle funzioni aziendali, integrazione nei processi e miglioramento continuo.

Le misure di sicurezza sono definite tenendo conto della criticità degli asset, dei dati trattati, dell'esposizione dei sistemi, della continuità dei servizi, delle dipendenze da fornitori, degli obblighi normativi e contrattuali applicabili e del perimetro NIS2 dichiarato.

La gestione della cybersicurezza è basata sul rischio. Gli aspetti cyber sono considerati nelle fasi di identificazione, analisi, valutazione, trattamento, monitoraggio e riesame dei rischi aziendali, con riferimento agli impatti su riservatezza, integrità, disponibilità, continuità operativa, conformità normativa, rapporti contrattuali e tutela dei clienti e degli utenti.

Zucchetti Healthcare applica i principi di security by design e security by default nella progettazione, sviluppo, configurazione, modifica e rilascio di sistemi, applicazioni, infrastrutture e servizi. Tali principi sono integrati nei processi di sviluppo software, change management, gestione sistemistica, servizi cloud e qualifica dei fornitori.

L'accesso a sistemi, dati e ambienti è regolato secondo il principio del privilegio minimo, con assegnazione delle autorizzazioni coerente con ruolo, responsabilità e necessità operative. Sono inoltre promosse la segregazione degli ambienti, la separazione dei compiti, la tracciabilità delle attività rilevanti, la gestione controllata degli accessi privilegiati e l'adozione di misure di autenticazione adeguate al rischio.

Il monitoraggio della cybersicurezza è assicurato attraverso verifiche tecniche, audit, analisi degli incidenti, valutazione delle vulnerabilità, Vulnerability Assessment, Penetration Test, simulazioni, indicatori e riesami periodici. Gli esiti delle verifiche alimentano la valutazione dei rischi, i piani di remediation, le azioni correttive e il miglioramento continuo.

Ruoli, responsabilità e consapevolezza

L'Alta Direzione assume la responsabilità complessiva del governo della cybersicurezza, assicurando indirizzo, risorse, priorità e riesame periodico dell'efficacia delle misure adottate, anche in relazione agli obblighi derivanti dalla qualificazione di Zucchetti Healthcare come soggetto essenziale NIS2.

Il Board Compliance e Certificazioni costituisce la sede di raccordo aziendale per il presidio della cybersicurezza, con il coinvolgimento dei responsabili delle funzioni interessate. In tale ambito sono valutati gli aspetti organizzativi, tecnici, normativi, contrattuali e operativi rilevanti, nonché le priorità di intervento, lo stato delle azioni, gli esiti degli audit, le vulnerabilità, gli incidenti, i change significativi, le verifiche sui fornitori e le esigenze di miglioramento.

Il Referente per la Cybersecurity coordina l'applicazione della presente Politica e delle procedure operative collegate. Supporta l'Alta Direzione e il Board Compliance e Certificazioni, promuove l'integrazione della cybersicurezza nei processi aziendali, coordina le verifiche tecniche, monitora le vulnerabilità, segue l'avanzamento delle remediation, raccoglie le evidenze e contribuisce al riesame dell'efficacia delle misure adottate.

Le funzioni aziendali sono responsabili dell'attuazione delle misure di cybersicurezza pertinenti al proprio ambito operativo. La Direzione Servizi Digitali, l'area sistemistica, i team di sviluppo, l'assistenza, HR, amministrazione/procurement e le funzioni coinvolte nella gestione dei fornitori concorrono, secondo le rispettive competenze, alla protezione dei sistemi informativi e di rete, alla gestione degli accessi, allo sviluppo sicuro, alla continuità operativa, alla qualifica dei fornitori, alla formazione e alla rilevazione di anomalie o incidenti.

Tutto il personale è tenuto a rispettare le politiche aziendali di sicurezza, proteggere le credenziali, utilizzare correttamente gli strumenti messi a disposizione, segnalare tempestivamente anomalie, sospetti incidenti, tentativi di phishing, accessi non autorizzati o altre situazioni potenzialmente rilevanti per la cybersicurezza.

La consapevolezza del personale è promossa attraverso attività formative, iniziative di awareness, comunicazioni interne, simulazioni phishing e interventi mirati in funzione del ruolo, delle responsabilità e del livello di esposizione al rischio. Il piano formativo tiene conto delle esigenze del personale generale, della Direzione, dei responsabili di processo, degli sviluppatori, dei sistemisti, degli amministratori di sistema, dell'assistenza e delle figure coinvolte nella gestione degli incidenti.

Sistema di Gestione per la Cybersicurezza

Il Sistema di Gestione per la Cybersicurezza è parte integrante del Sistema di Gestione Integrato di Zucchetti Healthcare e opera in coordinamento con il Sistema di Gestione per la Sicurezza delle Informazioni, il sistema qualità, il sistema di gestione dei servizi IT, i processi di gestione del rischio, il change management, lo sviluppo software, la gestione sistemistica e cloud, la qualifica dei fornitori, l'incident management, la business continuity, il disaster recovery, la formazione, gli audit e il riesame della Direzione.

Il Sistema di Gestione per la Cybersicurezza assicura l'identificazione e la classificazione dei servizi, degli asset e dei sistemi informativi e di rete rilevanti; la valutazione e il trattamento dei rischi cyber; l'applicazione di politiche e controlli di sicurezza; la gestione delle vulnerabilità e delle attività VA/PT; la gestione degli incidenti e delle comunicazioni; il presidio della continuità operativa e del disaster recovery; la sicurezza della supply chain; la formazione e la consapevolezza del personale; la raccolta delle evidenze; il monitoraggio degli indicatori; la gestione delle non conformità e delle azioni correttive.

Le misure previste sono applicate secondo un criterio di proporzionalità, tenendo conto della criticità degli asset, dei dati trattati, dell'esposizione dei sistemi, della continuità dei servizi, delle dipendenze da fornitori, degli obblighi normativi e contrattuali, del perimetro NIS2 dichiarato e dell'impatto potenziale su clienti, utenti e organizzazione.

Gestione degli incidenti e obblighi NIS2

La gestione degli incidenti di cybersicurezza è integrata nel processo aziendale di incident management e nelle procedure dedicate al Comitato di Crisi. Gli eventi rilevanti devono essere

rilevati, segnalati, classificati, analizzati e gestiti con tempestività, tracciabilità e coordinamento delle responsabilità.

Per gli incidenti qualificabili come significativi ai fini NIS2, Zucchetti Healthcare assicura la gestione degli adempimenti previsti per i soggetti essenziali, inclusi pre-notifica, notifica, eventuali aggiornamenti intermedi e relazione finale, secondo le modalità e le tempistiche applicabili.

La valutazione della significatività dell'incidente considera l'impatto sui servizi, la durata, l'estensione, il numero di utenti o clienti interessati, la compromissione di dati o sistemi, gli effetti sulla continuità operativa e le possibili conseguenze economiche, operative, contrattuali o reputazionali.

Il Referente per la Cybersecurity supporta la qualificazione tecnica degli eventi e degli incidenti, coordina la raccolta delle evidenze tecniche, contribuisce alla valutazione degli impatti cyber e supporta la definizione delle misure di contenimento, ripristino e remediation, in raccordo con le funzioni competenti, il Comitato di Crisi, il Board Compliance e Certificazioni e l'Alta Direzione.

Miglioramento continuo

Zucchetti Healthcare assicura il miglioramento continuo del Sistema di Gestione per la Cybersicurezza attraverso il monitoraggio delle misure adottate, la valutazione degli indicatori, gli audit, le verifiche tecniche, gli esiti di VA/PT, l'analisi degli incidenti, i risultati delle campagne phishing, le verifiche sui fornitori, i test di continuità, il riesame dei rischi e il trattamento delle non conformità.

Gli esiti delle attività di controllo alimentano azioni correttive, preventive o di miglioramento, con responsabilità definite, tempi di attuazione, priorità, criteri di verifica e modalità di chiusura documentate.

Il miglioramento continuo deve consentire di mantenere il Sistema di Gestione per la Cybersicurezza coerente con l'evoluzione del contesto aziendale, delle minacce, degli obblighi normativi e contrattuali, delle tecnologie, dei servizi erogati e del perimetro NIS2 dichiarato.

Diffusione della Politica

La presente Politica è approvata dall'Alta Direzione ed è diffusa ai soggetti interessati attraverso i canali aziendali previsti dal Sistema di Gestione Integrato.

La Politica è resa disponibile al personale autorizzato e comunicata, per quanto applicabile, alle funzioni aziendali, ai collaboratori, ai fornitori e alle terze parti coinvolte nei processi che possono incidere sulla sicurezza dei sistemi informativi e di rete.

La diffusione della Politica è accompagnata da iniziative di sensibilizzazione e formazione, al fine di assicurare comprensione, consapevolezza e corretta applicazione dei principi e delle responsabilità in materia di cybersicurezza.

Integrazione nel Sistema di Gestione

Il Sistema di Gestione per la Cybersicurezza opera in coordinamento con gli altri sistemi di gestione adottati dall'organizzazione, assicurando coerenza tra gli obiettivi di sicurezza, gli indirizzi strategici aziendali, i requisiti normativi e contrattuali, il perimetro NIS2 dichiarato e i processi operativi[1].

Le politiche, le procedure e le misure di sicurezza sono applicate in modo trasversale ai processi aziendali, contribuendo al miglioramento continuo dell'organizzazione, alla resilienza dei sistemi informativi e di rete, alla qualità dei servizi erogati e alla tutela dei clienti e degli utenti.

La Politica è riesaminata periodicamente e aggiornata in caso di modifiche normative, evoluzioni del perimetro NIS2, cambiamenti organizzativi, nuovi servizi, variazioni rilevanti dei rischi cyber, esiti di audit, incidenti significativi, riesami della Direzione o altre esigenze di miglioramento.

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 PAC03 per il Sistema di Gestione della Continuità Operativa, alla Politica Aziendale PAC04 per il Sistema di Gestione della Intelligenza Artificiale e alla Politica Aziendale PAC05 per il Sistema di Gestione dei Servizi.