POL Politica di sicurezza delle informazioni

Storia della versione

Versione	Data	Autore	Approvato da
1	15/01/2025	Andrea Groppelli	Andrea Groppelli
2	27/05/2026	Andrea Groppelli	Andrea Groppelli

Indice

Descrizione della versione

Rispetto alla versione precedente, le principali modifiche sono:

- Ristrutturazione completa del documento secondo lo schema di una politica quadro del Sistema di Gestione della Sicurezza delle Informazioni, con introduzione delle sezioni formali di scopo, campo di applicazione, riferimenti normativi, termini e definizioni, e ruoli e responsabilità.
- Inserimento di una sezione dedicata agli obiettivi di sicurezza delle informazioni, allineata alla valutazione dei rischi e alla pianificazione strategica dell'organizzazione.
- Definizione esplicita dei principi fondamentali di sicurezza (approccio basato sul rischio, responsabilità condivisa, miglioramento continuo) che guidano l'intero corpo documentale del SGSI.
- Consolidamento della protezione degli asset fuori sede in una sezione autonoma, con indicazione dei principi di custodia, segnalazione e restituzione.
- Rimozione delle sezioni operative di dettaglio (uso accettabile e non accettabile, regole per la posta elettronica, dispositivi BYOD, conformità e violazioni), ora trattate nelle politiche specifiche per argomento e nelle procedure operative di riferimento.
- Allineamento alla struttura richiesta da ISO/IEC 27001:2022 e integrazione dei riferimenti alle politiche tematiche approvate dalla Direzione.

Scopo

La presente politica dichiara e comunica l'impegno del **CEO / Top Management** di iDigital3 verso la protezione degli asset informativi dell'organizzazione. Il documento costituisce il quadro di riferimento per istituire, attuare, mantenere e migliorare continuamente il Sistema di Gestione della Sicurezza delle Informazioni (SGSI), con l'obiettivo di preservare la riservatezza, l'integrità e la disponibilità delle informazioni trattate nell'ambito delle attività di consulenza IT, cybersecurity, gestione dell'infrastruttura e sviluppo software.

iDigital3 riconosce che una sicurezza efficace presuppone la partecipazione attiva di tutto il personale e dei collaboratori coinvolti nella gestione dei sistemi e delle informazioni aziendali. Attraverso questa politica, l'organizzazione intende fornire una direzione strategica chiara che supporti i propri obiettivi di business — tra i quali la trasformazione digitale dei clienti del settore Utility e delle PMI — e che garantisca la fiducia delle parti interessate nella capacità dell'azienda di proteggere adeguatamente il patrimonio informativo.

Campo di applicazione

La presente politica si applica a tutte le attività, i processi e gli asset informativi di iDigital3, inclusa la sede operativa di Largo della Pace 11C, 26013 Crema (CR). Coinvolge tutto il personale — dipendenti, collaboratori a contratto e terze parti — che accede alle informazioni o ai sistemi aziendali, indipendentemente dalla modalità di lavoro (in sede, da

remoto o in trasferta). Rientrano nel perimetro le attività di consulenza e supporto IT per la cybersecurity, la gestione dell'infrastruttura IT e degli asset informatici, nonché la progettazione, lo sviluppo e l'integrazione di soluzioni software per i clienti.

Riferimenti normativi

- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- Regolamento (UE) 2016/679

Termini e definizioni

- **Sistema di Gestione della Sicurezza delle Informazioni (SGSI)** : insieme di politiche, processi e controlli adottati dall'organizzazione per gestire sistematicamente i rischi relativi alla sicurezza delle informazioni.
- **Riservatezza** : proprietà per cui le informazioni non sono rese disponibili o divulgate a individui, entità o processi non autorizzati.
- **Integrità** : proprietà di accuratezza e completezza delle informazioni.
- **Disponibilità** : proprietà di essere accessibile e utilizzabile su richiesta da parte di un'entità autorizzata.
- **Rischio** : effetto dell'incertezza sugli obiettivi, espresso in termini di combinazione della probabilità di un evento e delle sue conseguenze.
- **Asset informativo** : qualsiasi elemento che ha valore per l'organizzazione, inclusi informazioni, software, hardware, servizi, personale, risorse intangibili e reputazione.
- **Evento di sicurezza delle informazioni** : occorrenza identificata nello stato di un sistema, servizio o rete che indica una possibile violazione della politica di sicurezza, un fallimento dei controlli o una situazione precedentemente sconosciuta che può essere rilevante per la sicurezza.
- **Incidente di sicurezza delle informazioni** : uno o più eventi di sicurezza delle informazioni indesiderati o inattesi che hanno una significativa probabilità di compromettere le operazioni aziendali e di minacciare la sicurezza delle informazioni.

Ruoli e responsabilità

- **CEO / Top Management** : approva la presente politica, assicura le risorse necessarie al SGSI e promuove il miglioramento continuo della sicurezza delle informazioni.
- **CTO** : definisce gli indirizzi tecnologici per la sicurezza, supervisiona le misure di protezione degli asset informatici e garantisce la conformità normativa dei sistemi IT.
- **Responsabile del sistema di gestione** : gestisce la documentazione del SGSI, pianifica gli audit interni e coordina le attività di riesame e aggiornamento della presente politica.

- **Responsabile IT** : attua le misure tecniche di sicurezza, gestisce l'infrastruttura e i dispositivi aziendali e interviene in caso di segnalazioni relative a eventi di sicurezza.

Obiettivi di sicurezza delle informazioni

iDigital3 persegue obiettivi di sicurezza delle informazioni coerenti con la propria strategia aziendale, con il contesto di mercato in cui opera e con i risultati della valutazione dei rischi. Tali obiettivi sono misurabili, comunicati a tutto il personale e riesaminati a intervalli pianificati.

L'organizzazione si impegna a:

- Mantenere un livello di rischio residuo accettabile, attraverso l'identificazione, l'analisi e il trattamento sistematico dei rischi di sicurezza delle informazioni, classificandoli secondo la formula R = Probabilità × Impatto e intervenendo ogni qual volta il livello superi la soglia di accettabilità definita.
- Prevenire violazioni della riservatezza, dell'integrità e della disponibilità delle informazioni trattate, anche mediante l'adozione di tecnologie avanzate di rilevamento e risposta (SOC, monitoraggio delle vulnerabilità, sistemi XDR) e l'autenticazione a più fattori per l'accesso ai sistemi.
- Garantire la continuità dei servizi IT erogati ai propri clienti del settore Utility e delle PMI, riducendo i tempi di indisponibilità attraverso piani di continuità operativa e di ripristino di emergenza.
- Assicurare la conformità alla normativa applicabile in materia di protezione dei dati personali e sicurezza delle informazioni, aggiornando periodicamente procedure e controlli a fronte dell'evoluzione del quadro regolamentare.
- Promuovere la consapevolezza e la competenza del personale in materia di sicurezza, attraverso programmi di formazione continua e campagne di sensibilizzazione sulle minacce emergenti.
- Integrare la sicurezza delle informazioni nella progettazione e nello sviluppo di soluzioni software, adottando un approccio di sicurezza fin dalle prime fasi del ciclo di vita applicativo.

Principi fondamentali di sicurezza delle informazioni

L'intero impianto del SGSI di iDigital3 poggia su un insieme di principi che orientano le decisioni, i controlli e i comportamenti di tutto il personale. Tali principi informano ogni politica tematica e procedura operativa adottata dall'organizzazione.

Approccio basato sul rischio. Ogni decisione in materia di sicurezza delle informazioni parte dalla valutazione dei rischi — condotta almeno una volta all'anno — e dal conseguente piano di trattamento. L'organizzazione classifica i rischi su scala di probabilità e impatto e adotta misure proporzionate al livello di rischio individuato, ricorrendo alla mitigazione, all'accettazione, al trasferimento o all'eliminazione del rischio secondo il criterio di costo-beneficio.

Responsabilità condivisa. La sicurezza delle informazioni non è esclusiva di una funzione aziendale: ogni persona che accede a informazioni o risorse dell'organizzazione è responsabile della loro protezione nell'ambito delle proprie mansioni. Ciascun dipendente e collaboratore è tenuto a conoscere e rispettare le politiche e le procedure applicabili al proprio ruolo.

Minimo privilegio e necessità di conoscere. L'accesso alle informazioni e ai sistemi è concesso esclusivamente nella misura necessaria allo svolgimento delle attività assegnate. I diritti di accesso sono riesaminati periodicamente e revocati al cessare della necessità operativa.

Protezione su più livelli. L'organizzazione adotta controlli di sicurezza combinati — fisici, logici, organizzativi e procedurali — affinché il fallimento di un singolo controllo non comprometta la protezione complessiva dell'informazione.

Uso accettabile delle risorse. Le risorse informatiche aziendali sono destinate a scopi di lavoro e il loro utilizzo è regolato da regole specifiche volte a prevenire usi impropri che possano compromettere sistemi o dati. L'organizzazione mantiene un *Registro degli utenti autorizzati all'uso delle informazioni* che documenta gli utenti, i sistemi e le repository a cui ciascuno può accedere; all'assegnazione di dotazioni hardware si procede mediante il *MOD Modulo di assegnazione dei beni* .

Scrivania e schermo puliti. L'organizzazione promuove l'applicazione sistematica del principio di scrivania pulita e schermo pulito: i documenti e i supporti classificati non devono rimanere esposti sulle postazioni di lavoro e i dispositivi si bloccano automaticamente dopo cinque minuti di inattività, richiedendo l'autenticazione al risveglio.

Segnalazione tempestiva degli eventi. Ogni persona che osservi o sospetti un evento di sicurezza delle informazioni — incluse debolezze, tentativi di phishing o violazioni delle politiche — è tenuta a segnalarlo immediatamente al **Responsabile del sistema di gestione** tramite i canali di comunicazione predisposti dall'organizzazione. La segnalazione viene formalizzata attraverso un ticket nel sistema di gestione e registrata nel *MOD Registro degli incidenti di sicurezza delle informazioni* . L'organizzazione assicura che nessuna conseguenza negativa ricada su chi segnala in buona fede.

Miglioramento continuo. L'organizzazione si impegna a valutare costantemente l'efficacia del SGSI mediante audit interni, riesami della Direzione, analisi degli incidenti e monitoraggio degli indicatori di prestazione, traducendo i risultati in azioni correttive e opportunità di miglioramento.

Protezione degli asset fuori sede

iDigital3 riconosce la necessità di proteggere gli asset informativi anche quando essi si trovano al di fuori della sede operativa — in contesti di smart working, telelavoro, trasferta o manutenzione remota. L'organizzazione adotta i seguenti principi a tutela dei dispositivi e delle informazioni utilizzate in tali circostanze.

Custodia. I dispositivi aziendali (notebook, tablet, telefoni cellulari) non sono mai lasciati incustoditi in veicoli, mezzi pubblici, aree comuni di hotel o spazi di coworking. In trasferta, il personale assegnatario custodisce gli asset in luogo chiuso a chiave o nella cassaforte della struttura. L'accesso fisico alla postazione di lavoro remota è limitato esclusivamente alle persone autorizzate.

Protezione logica in ambiente remoto. Il personale che opera da remoto utilizza la VPN aziendale per qualsiasi accesso ai sistemi interni e l'autenticazione a più fattori per tutti gli applicativi aziendali. Il router domestico deve impiegare protocolli di cifratura aggiornati (almeno WPA2) e le credenziali predefinite (nome rete, password, accesso amministratore) devono essere modificate. L'installazione o l'utilizzo di tecnologie di accesso remoto non autorizzate è vietata su qualsiasi sistema aziendale. Le comunicazioni aziendali contenenti informazioni classificate transitano unicamente attraverso canali approvati dall'organizzazione.

Segnalazione di smarrimento, furto o danneggiamento. Il personale notifica immediatamente al **Responsabile IT** ogni smarrimento, furto o danneggiamento di asset aziendali fuori sede. La segnalazione attiva le procedure di blocco remoto del dispositivo, revoca degli accessi e sostituzione delle credenziali. L'evento è registrato come incidente di sicurezza delle informazioni nel *MOD Registro degli incidenti di sicurezza delle informazioni* .

Restituzione. Al termine della trasferta, del progetto o del rapporto di lavoro, gli asset assegnati sono restituiti all'organizzazione attraverso il *MOD Modulo di assegnazione dei beni* . Il personale cessante elimina tutte le informazioni e gli account aziendali da eventuali dispositivi personali.

Archiviazione e aggiornamento

La presente politica è un documento controllato del SGSI. Il **Responsabile del sistema di gestione** ne cura l'archiviazione all'interno del sistema documentale aziendale, garantendone la disponibilità a tutto il personale interessato e la comunicazione agli stakeholder esterni ove previsto. La politica è riesaminata con cadenza annuale nell'ambito del riesame della Direzione, oppure in occasione di cambiamenti significativi nel contesto organizzativo, tecnologico, normativo o nel profilo delle minacce. Ogni revisione è approvata dal **CEO / Top Management** e le modifiche sono comunicate tempestivamente al personale e alle parti interessate.

Documenti di riferimento

- POL Politica di sicurezza operativa
- POL Politica di classificazione ed etichettatura delle informazioni
- POL Politica di gestione del rischio della sicurezza delle informazioni
- POL Politica di gestione patrimoniale
- POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni
- POL Politica delle risorse umane sulla sicurezza delle informazioni
- POL Politica di sicurezza delle informazioni per gli ex dipendenti
- POL Politica di gestione delle terze parti
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni
- PRO Procedura di gestione e controllo degli accessi logici

- PRO Procedura di sviluppo sicuro
- PRO Valutazione rischi per la sicurezza delle informazioni
- PRO Procedura di sicurezza fisica e ambientale