POL Politica di sicurezza delle informazioni

Storia della versione

Versione	Data	Autore	Approvato da
1	10/03/2026	Massimo Demelas	Massimo Demelas

Indice

Scopo

La presente politica esprime e formalizza l'impegno del Top Management di DB PROJECT DI DEMELAS MASSIMO S.A.S verso la protezione del patrimonio informativo aziendale. Attraverso questo documento, l'organizzazione dichiara la propria volontà di istituire, attuare, mantenere e migliorare continuamente un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) che tuteli la riservatezza, l'integrità e la disponibilità delle informazioni trattate nell'ambito della fornitura e commercializzazione di soluzioni hardware e software, dei servizi di installazione, configurazione, consulenza, assistenza tecnica, gestione di infrastrutture IT e servizi cloud correlati.

Questa politica costituisce il quadro di riferimento strategico al quale si conformano tutte le policy e le procedure di sicurezza di livello subordinato. Essa stabilisce i principi che orientano le decisioni in materia di protezione degli asset informativi e promuove una cultura della sicurezza che coinvolge ogni soggetto operante nel contesto aziendale, nella convinzione che la sicurezza delle informazioni rappresenti un fattore abilitante per la qualità dei servizi erogati e per la fiducia dei clienti.

Campo di applicazione

La presente politica si applica a tutte le attività, i processi, gli asset informativi e i sistemi tecnologici dell'organizzazione, presso la sede operativa di Via Antonio Ballero 15, 09044 Quartucciu (CA). Essa coinvolge il titolare, eventuali collaboratori a contratto e le terze parti che accedono a informazioni o sistemi aziendali, indipendentemente dalla loro ubicazione fisica, inclusi i contesti di lavoro da remoto e di intervento presso le sedi dei clienti.

Riferimenti normativi

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

Termini e definizioni

- **Sistema di Gestione della Sicurezza delle Informazioni (SGSI)** : insieme di politiche, procedure, linee guida e risorse correlate, gestite collettivamente dall'organizzazione allo scopo di proteggere i propri asset informativi.
- **Sicurezza delle informazioni** : preservazione della riservatezza, dell'integrità e della disponibilità 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 delle conseguenze di un evento e della relativa probabilità di accadimento.
- **Asset informativo** : qualsiasi elemento che abbia valore per l'organizzazione, inclusi informazioni, software, hardware, servizi e reputazione.
- **Evento di sicurezza delle informazioni** : occorrenza identificata in un sistema, servizio o rete che indica una possibile violazione della politica di sicurezza o un guasto dei controlli.
- **Incidente di sicurezza delle informazioni** : uno o più eventi di sicurezza delle informazioni che hanno una significativa probabilità di compromettere le operazioni e di minacciare la sicurezza delle informazioni.
- **Controllo** : misura che modifica il rischio, comprendente processi, politiche, dispositivi, pratiche o altre condizioni e azioni.

Ruoli e responsabilità

- **Responsabile IT e sicurezza delle informazioni** : definisce e attua i controlli di sicurezza previsti dalla presente politica, monitorando l'efficacia delle misure di protezione degli asset informativi.
- **Responsabile del sistema di gestione** : cura la documentazione del SGSI e verifica, attraverso audit interni e riesami periodici, la conformità delle attività ai principi enunciati in questa politica.
- **Responsabile servizi tecnici e operazioni** : garantisce che l'erogazione dei servizi tecnici ai clienti avvenga nel rispetto dei requisiti di sicurezza delle informazioni stabiliti dalla presente politica.
- **Responsabile commerciale e gestione fornitori** : assicura che i rapporti con fornitori e partner tecnologici includano requisiti di sicurezza delle informazioni coerenti con gli impegni dichiarati in questa politica.

Obiettivi di sicurezza delle informazioni

L'organizzazione persegue obiettivi di sicurezza delle informazioni misurabili, coerenti con il proprio contesto operativo e allineati agli indirizzi strategici aziendali. Tali obiettivi discendono dall'analisi dei rischi, dalle aspettative delle parti interessate e dalle prestazioni rilevate nel SGSI, e vengono riesaminati periodicamente in sede di riesame della direzione.

In questa cornice, l'organizzazione si impegna a:

- tutelare la riservatezza delle informazioni dei clienti e dell'organizzazione stessa, prevenendo accessi e divulgazioni non autorizzati;
- preservare l'integrità dei dati amministrativi, contabili, tecnici e della documentazione dei clienti gestita attraverso le proprie infrastrutture e piattaforme cloud;

- assicurare la disponibilità dei servizi IT e delle informazioni critiche, riducendo i tempi di indisponibilità entro soglie compatibili con le esigenze operative dei clienti;
- contenere i rischi legati alle minacce informatiche entro livelli accettabili, adottando un approccio sistematico di valutazione e trattamento del rischio;
- migliorare continuamente l'efficacia del SGSI attraverso il monitoraggio degli indicatori di prestazione, l'analisi degli incidenti e l'attuazione di azioni correttive.

Principi fondamentali di sicurezza delle informazioni

L'organizzazione fonda il proprio SGSI su principi che permeano ogni attività, decisione e relazione con le parti interessate, nella consapevolezza che la sicurezza delle informazioni è una condizione necessaria per la qualità e l'affidabilità dei servizi offerti al mercato B2B.

Approccio basato sul rischio. Ogni decisione in materia di sicurezza delle informazioni trae origine dalla valutazione sistematica dei rischi, condotta secondo scale di probabilità e impatto definite e con una soglia di accettazione stabilita. L'organizzazione identifica le minacce e le vulnerabilità pertinenti ai propri asset, valuta le possibili conseguenze e adotta misure di trattamento proporzionate al livello di rischio rilevato, privilegiando la prevenzione e il contenimento.

Responsabilità condivisa. La protezione delle informazioni è responsabilità di chiunque operi per conto dell'organizzazione o acceda ai suoi sistemi. Ciascun soggetto è tenuto a conoscere e rispettare le politiche e le procedure di sicurezza applicabili al proprio ruolo, contribuendo attivamente al mantenimento di un ambiente sicuro.

Classificazione e trattamento delle informazioni. Le informazioni sono classificate in base alla loro sensibilità e criticità, secondo i livelli Pubblico, Limitato e Riservato. A ciascun livello corrispondono requisiti specifici di protezione per l'accesso, la trasmissione, la conservazione e la distruzione, così come definiti nella *POL Politica di classificazione ed etichettatura delle informazioni* .

Uso accettabile delle risorse. Le risorse informatiche e informative dell'organizzazione sono messe a disposizione per finalità operative legittime. L'organizzazione promuove un utilizzo responsabile e consapevole dei sistemi, delle informazioni e dei dispositivi, nel rispetto delle regole stabilite dalla *POL Politica di sicurezza operativa* e dei principi di riservatezza, integrità e disponibilità.

Protezione dello schermo e della postazione. L'organizzazione adotta misure tecniche e organizzative per prevenire l'accesso non autorizzato alle informazioni visibili a schermo o presenti sulla postazione di lavoro. I dispositivi sono configurati con il blocco automatico dello schermo dopo cinque minuti di inattività, e le informazioni riservate su supporto fisico non vengono lasciate esposte in aree accessibili.

Segnalazione degli eventi di sicurezza. L'organizzazione promuove una cultura della segnalazione tempestiva di qualsiasi evento, osservato o sospetto, che possa indicare una compromissione della sicurezza delle informazioni. A tale scopo mette a disposizione canali appropriati per la comunicazione e registra ogni evento nel *MOD Registro degli incidenti di sicurezza delle informazioni* , attivando le procedure di risposta definite nella *PRO Procedura di gestione degli incidenti di sicurezza delle informazioni* .

Miglioramento continuo. L'organizzazione si impegna a riesaminare periodicamente l'adeguatezza e l'efficacia del SGSI, tenendo conto dell'evoluzione delle minacce, dei cambiamenti tecnologici e organizzativi, degli esiti degli audit interni e delle lezioni apprese dagli incidenti. Ogni riesame è occasione per aggiornare le misure di sicurezza e innalzare il livello di protezione complessivo.

Conformità normativa. L'organizzazione persegue la piena conformità ai requisiti legali, regolamentari e contrattuali applicabili alla sicurezza delle informazioni e alla protezione dei dati personali, adeguando tempestivamente il proprio SGSI a ogni evoluzione del quadro normativo di riferimento.

Protezione degli asset fuori sede

L'organizzazione riconosce che gran parte dell'attività operativa si svolge al di fuori della sede aziendale — presso i clienti, in mobilità o in contesti di lavoro da remoto — e si impegna a garantire che gli asset informativi mantengano un livello di protezione equivalente a quello assicurato all'interno dei propri locali. Il rischio di furto, smarrimento o accesso non autorizzato ai dispositivi mobili rappresenta una minaccia significativa, che l'organizzazione affronta attraverso i seguenti principi:

Custodia e controllo fisico. I dispositivi aziendali — notebook, smartphone, supporti di memorizzazione rimovibili — non vengono mai lasciati incustoditi in luoghi accessibili a terzi. Quando utilizzati fuori sede, restano sotto la diretta custodia del personale assegnatario, che ne impedisce la visibilità a persone non autorizzate e ne assicura il riparo in luogo chiuso a chiave durante le assenze.

Protezione logica dei dispositivi. Ogni dispositivo utilizzato fuori sede è protetto da credenziali personali, password complesse e autenticazione a più fattori ove disponibile, software antivirus e firewall attivi, aggiornamenti automatici del sistema operativo e dei software applicativi. Lo schermo si blocca automaticamente dopo cinque minuti di inattività. È vietato l'utilizzo di reti Wi-Fi pubbliche non protette; l'accesso ai servizi aziendali avviene esclusivamente tramite connessioni sicure, con impiego di VPN ove necessario.

Backup e continuità dei dati. I dati trattati durante le attività fuori sede sono oggetto di backup periodico su sistemi aziendali o piattaforme cloud sicure, in modo da preservarne la disponibilità anche in caso di perdita o danneggiamento del dispositivo.

Segnalazione di smarrimento, furto o danneggiamento. Qualsiasi evento di smarrimento, furto o danneggiamento di un asset aziendale fuori sede viene comunicato tempestivamente al **Responsabile IT e sicurezza delle informazioni** , che attiva le misure di blocco remoto del dispositivo, revoca degli accessi e aggiornamento delle credenziali. L'evento è registrato come incidente di sicurezza delle informazioni nel *MOD Registro degli incidenti di sicurezza delle informazioni* .

Restituzione degli asset. Al termine di un incarico, di un progetto o della cessazione di un rapporto contrattuale, gli asset sono restituiti all'organizzazione secondo le modalità stabilite, affinché il patrimonio informativo resti sotto il pieno controllo dell'organizzazione in ogni fase del ciclo di vita della collaborazione.

Archiviazione e aggiornamento

La presente politica è un documento controllato del SGSI, conservato nella piattaforma documentale aziendale e soggetto alle regole di gestione delle informazioni documentate definite nella *PRO Procedura di gestione delle informazioni documentate* . Il **Responsabile del sistema di gestione** ne cura la revisione con cadenza annuale, oppure in occasione di cambiamenti significativi nel contesto organizzativo, nell'evoluzione delle minacce o nel quadro normativo applicabile. Ogni aggiornamento è approvato dal Top Management prima della diffusione al personale interessato e alle parti esterne coinvolte.

Documenti di riferimento

- POL Politica di classificazione ed etichettatura delle informazioni
- POL Politica di sicurezza operativa
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni
- PRO Procedura di gestione delle informazioni documentate
- MOD Registro degli incidenti di sicurezza delle informazioni