Politica per la sicurezza delle informazioni

La seguente Politica integrata per la qualità e la sicurezza delle informazioni è stata sviluppata in conformità alle linee guida ISO 9001:2015 e ISO/IEC 27001:2022 e alle relative estensioni ISO/IEC 27017, ISO/IEC 27018, cui la società Develia Srl ha aderito. Lo scopo della presente politica è di proteggere da tutte le minacce, interne o esterne, intenzionali o accidentali, il patrimonio informativo dell'azienda, garantendo al contempo la qualità dei servizi erogati e la soddisfazione del cliente. Questa politica si applica a tutti i dipendenti, i contractor e i terzi che hanno accesso alle informazioni e ai processi dell'organizzazione. La politica è definita tenendo conto del contesto interno ed esterno dell'organizzazione e delle esigenze delle parti interessate rilevanti.

Premessa

Develia Srl progetta, sviluppa e commercializza servizi Saas per organizzazioni private e pubbliche. I servizi prevedono il trattamento di informazioni dei clienti e degli utenti finali, ovvero degli utenti dei propri clienti.

Consapevoli che i dati del cliente costituiscono informazioni il cui valore rappresenta il patrimonio aziendale della nostra organizzazione e di quella del cliente, abbiamo implementato un sistema di gestione per la sicurezza delle informazioni prevedendo la messa a punto di tutti i controlli di sicurezza applicabili al trattamento delle informazioni.

Campo di applicazione

Il Sistema di Gestione Integrato Qualità e Sicurezza delle Informazioni (SGI) di Develia Srl si applica alla totalità dei processi aziendali erogati dall'organizzazione, ivi compresi: la gestione commerciale e contrattuale, lo sviluppo software, la gestione dell'infrastruttura tecnologica e dei servizi cloud, l'assistenza e il supporto ai clienti, la gestione dei fornitori e dei partner, la gestione delle risorse umane, nonché i processi relativi alla sicurezza delle informazioni e alla protezione dei dati personali.

Il SGI copre la sede operativa e tutte le risorse — umane, tecnologiche e organizzative — coinvolte nell'erogazione dei suddetti processi, incluse le attività svolte da personale in modalità di lavoro agile (smart working) e quelle affidate a soggetti terzi nell'ambito di rapporti contrattuali con Develia.

1. I nostri principi fondamentali di sicurezza

Il nostro approccio alla sicurezza si basa sulla protezione dei tre pilastri fondamentali di ogni informazione che trattiamo:

- **Riservatezza:** assicuriamo che le informazioni siano accessibili solo a chi è legittimamente autorizzato.
- **Integrità:** salvaguardiamo l'accuratezza e la completezza delle informazioni e dei processi con cui vengono gestite.
- **Disponibilità:** garantiamo che gli utenti autorizzati possano accedere alle informazioni e ai servizi correlati quando necessario.

2. I nostri impegni strategici

Per attuare i nostri principi, l'Alta Direzione si impegna a:

- **Promuovere la cultura della sicurezza:** sviluppare e mantenere un'elevata consapevolezza della sicurezza a tutti i livelli dell'organizzazione, attraverso formazione e comunicazione continua, affinché ogni persona sia consapevole del proprio ruolo e delle proprie responsabilità.
- **Integrare la sicurezza nel ciclo di vita del prodotto:** progettare e sviluppare i nostri sistemi e servizi secondo i principi di "security-by-default" e "security-by-design", integrando i requisiti di sicurezza in ogni fase, dalla progettazione allo sviluppo del prodotto finale.
- **Assicurare la continuità operativa:** predisporre e mantenere piani di continuità operativa per garantire la resilienza dei servizi critici e dei prodotti sviluppati a fronte di incidenti o eventi avversi.
- **Garantire la conformità:** assicurare il pieno rispetto delle leggi e dei regolamenti vigenti in materia di sicurezza e protezione dei dati personali e più in generale di tutti i requisiti applicabili.
- **Adottare un approccio basato sulla valutazione del rischio:** gestire la sicurezza attraverso un processo continuo di valutazione dei rischi, per assicurare che le misure di controllo siano sempre adeguate alle minacce e commisurate al valore delle informazioni da proteggere.
- **Perseguire il miglioramento continuo:** riesaminare periodicamente l'efficacia del nostro SGI — sia nella componente di sicurezza delle informazioni che in quella della qualità — per identificare e attuare sistematicamente opportunità di miglioramento delle performance e dei risultati.
- **Orientarsi alla soddisfazione del cliente:** comprendere e soddisfare i requisiti dei clienti e delle parti interessate rilevanti, perseguire il superamento delle loro aspettative e misurare sistematicamente il loro grado di soddisfazione. Rientrano nei requisiti applicabili anche gli obblighi cogenti specifici del settore in cui opera Develia, tra cui il Regolamento UE 2016/679 (GDPR) in materia di protezione dei dati personali e la normativa vigente relativa ai servizi educativi per l'infanzia.

- **Garantire la qualità dei processi e dei servizi:** definire, monitorare e migliorare i processi aziendali al fine di garantire la conformità dei servizi erogati ai requisiti concordati, prevenire le non conformità e assicurare la coerenza tra gli obiettivi per la qualità e l'indirizzo strategico dell'organizzazione.
- **Diffondere e rendere disponibile la politica:** assicurare che la presente politica sia comunicata, compresa e applicata all'interno dell'organizzazione e resa disponibile alle parti interessate pertinenti, ove appropriato.

3. Aree di applicazione della sicurezza

Per dare attuazione pratica a questi impegni, l'organizzazione ritiene di fondamentale importanza l'adozione di adeguate misure di sicurezza, le quali insistono su 4 differenti ambiti:

- Controlli organizzativi
- Controlli sul personale
- Controlli fisici
- Controlli tecnologici

In virtù del business esercitato dall'organizzazione, le principali misure di sicurezza sono state implementate sviluppando i seguenti controlli:

- Individuazione di ruoli e responsabilità nella gestione della sicurezza delle informazioni
- Sicurezza delle informazioni nella gestione dei progetti e nello sviluppo dei prodotti
- Controllo degli accessi logici alle informazioni, alle reti ed ai sistemi ICT
- Privacy e protezione dei dati personali
- Formazione e consapevolezza del personale sulle tematiche di sicurezza
- Protezione fisica dei siti in cui risiede il patrimonio informativo
- Sviluppo sicuro e test del codice prodotto
- Diritti di accesso privilegiato ai sistemi ed ai servizi aziendali
- Protezione e ridondanza/backup dei sistemi
- Attività di monitoraggio e raccolta di log
- Mantenimento della continuità operativa dei servizi a seguito di eventi avversi

La tutela della sicurezza del patrimonio informativo aziendale è assicurata tramite l'attività combinata delle funzioni aziendali. Per garantire la sicurezza delle informazioni Develia Srl si basa anche sul contributo di clienti e terze parti.

4. Quadro di riferimento per gli obiettivi della sicurezza

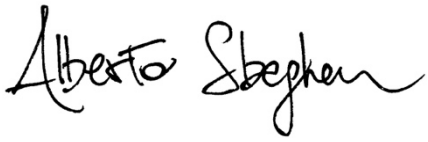
Questa politica fornisce il quadro di riferimento per la definizione e il riesame degli obiettivi misurabili per la sicurezza delle informazioni e per la qualità. I requisiti e i principi generali sono contestualizzati all'interno dell'organizzazione tramite obiettivi di carattere operativo finalizzati a supportare la realizzazione e il mantenimento del Sistema di Gestione Integrato (SGI) conforme alle norme ISO 9001:2015 e ISO/IEC 27001:2022.

5. Comunicazione ed applicabilità

Questa politica si applica a tutte le informazioni, i processi e le risorse tecnologiche inclusi nel campo di applicazione del Sistema di Gestione Integrato Qualità e Sicurezza delle Informazioni, come definito nell'apposita sezione del presente documento. L'organizzazione definisce obiettivi specifici, in linea con i principi qui espressi, che vengono formalizzati, monitorati tramite indicatori (KPI) e riesaminati almeno annualmente in sede di Riesame della Direzione per valutarne il raggiungimento e la continua pertinenza.

L'Alta Direzione si assume la piena responsabilità di guidare, sostenere e verificare l'applicazione di questa politica, assicurando che la sicurezza delle informazioni sia una responsabilità condivisa a tutti i livelli dell'organizzazione.

Pove del Grappa, lì 18/05/2026



L'AD Alberto Sbeghen