

Politica per la Sicurezza delle Informazioni di XFORGE

ISO/IEC 27001:2022

Revisioni					
ID	Versione	Data	Classificazione	Autore	Breve descrizione modifica
DS_02_ISO_27001	1.0	08/09/2025	Pubblico	RSGSI	Prima scrittura

Via Francesco Arese 16
20159 Milano 
info@xforge.it 
www.xforge.it 

P. Iva 10147400963
Reg. Impr. Milano N° 2509700
amministrazione@pec.xforge.it

1. Scopo e Finalità

La presente Politica per la Sicurezza delle Informazioni definisce i principi, gli impegni e gli obiettivi di alto livello che guidano l'approccio di XFORGE alla gestione della sicurezza delle informazioni. Lo scopo è istituire un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) conforme alla norma ISO/IEC 27001:2022 , al fine di proteggere la riservatezza, l'integrità e la disponibilità dei propri asset informativi e di quelli affidati dai clienti.

Questa politica costituisce il quadro di riferimento per la definizione di obiettivi specifici e per l'implementazione di controlli adeguati, garantendo che la sicurezza delle informazioni sia un pilastro fondamentale della proposta di valore di XFORGE e un fattore abilitante per il raggiungimento dei suoi obiettivi strategici .

2. Campo di Applicazione

In conformità con l'analisi del contesto interno ed esterno e delle esigenze delle parti interessate, il campo di applicazione del SGSI di XFORGE è definito come segue:

"Gestione dell'infrastruttura tecnologica e dei processi informativi a supporto alle attività di: Gestione delle infrastrutture SAP e applicazioni software in cloud; Servizi di monitoraggio remoto per la sicurezza e prestazioni dei sistemi SAP; Supporto personalizzato al cliente."

Il SGSI si applica a tutte le persone, i processi e le tecnologie che rientrano in questo perimetro.

3. Principi Guida e Impegni della Direzione

L'Alta Direzione di XFORGE si impegna a stabilire, attuare, mantenere e migliorare continuamente il SGSI, aderendo ai seguenti principi fondamentali :

- **Protezione degli Asset Informativi:** Garantire un livello adeguato di riservatezza, integrità e disponibilità per tutte le informazioni trattate, in particolare per i dati critici dei clienti gestiti all'interno delle infrastrutture SAP e cloud .
- **Approccio Basato sul Rischio:** Adottare un processo sistematico di valutazione e trattamento del rischio per la sicurezza delle informazioni, che consenta di identificare, analizzare e mitigare le minacce in modo proporzionato al loro potenziale impatto . Le decisioni sul trattamento del rischio saranno documentate e riesaminate periodicamente .
- **Conformità a Requisiti Applicabili:** Impegnarsi a soddisfare tutti i requisiti legali, regolamentari e contrattuali pertinenti per la sicurezza delle informazioni. Ciò include ma non si limita a:
 - **Regolamento Generale sulla Protezione dei Dati (GDPR - UE 2016/679):** Operare in qualità di "Responsabile del trattamento" fornendo garanzie sufficienti per l'adozione di misure tecniche e organizzative adeguate a tutela dei dati personali .

- **Obblighi Contrattuali:** Rispettare e superare le aspettative dei clienti definite negli Accordi sui Livelli di Servizio (SLA) in materia di sicurezza, performance e disponibilità .
- **Miglioramento Continuo:** Impegnarsi nel miglioramento continuo dell'efficacia del SGSI attraverso il monitoraggio delle prestazioni, gli audit interni e il riesame periodico da parte della direzione .

4. Obiettivi per la Sicurezza delle Informazioni

In linea con i principi guida e gli impegni assunti, l'Alta Direzione stabilisce i seguenti obiettivi strategici per la sicurezza delle informazioni, che forniscono un quadro per la definizione di traguardi misurabili a tutti i livelli dell'organizzazione :

1. Garantire la Resilienza e la Continuità Operativa dei Servizi Erogati:

- **Obiettivo:** Assicurare la massima disponibilità e performance delle infrastrutture SAP e dei servizi gestiti, in linea con gli obiettivi aziendali di "garantire alte performance, sicurezza e continuità operativa" .
- **Attuazione:** Implementare e testare regolarmente piani di continuità operativa e di disaster recovery per ripristinare tempestivamente la disponibilità dei dati e dei servizi in caso di incidente, in conformità con i requisiti del GDPR.

2. Assicurare e Dimostrare la Conformità Normativa e Contrattuale:

- **Obiettivo:** Mantenere un quadro di controlli che soddisfi pienamente i requisiti della Direttiva NIS 2 e del GDPR, nonché gli impegni contrattuali con i clienti .
- **Attuazione:** Integrare i requisiti normativi nel processo di valutazione del rischio. Pur riconoscendo il valore della certificazione ISO 27001 come elemento qualificante, XFORGE si impegna a dimostrare l'effettiva adeguatezza delle misure adottate, consapevole che la certificazione non garantisce di per sé la conformità, ma assicura l'adozione di controlli basati su una valutazione del rischio .

3. Rafforzare la Gestione degli Incidenti di Sicurezza e delle Vulnerabilità:

- **Obiettivo:** "Anticipare le criticità" attraverso il monitoraggio proattivo e garantire una capacità di risposta rapida ed efficace per rilevare, contenere e risolvere gli incidenti di sicurezza .
- **Attuazione:** Mantenere processi formalizzati di Incident Management, definire ruoli e responsabilità chiari e condurre analisi post-incidente per trarre insegnamenti e migliorare le difese.

4. Promuovere una Cultura della Sicurezza e Sviluppare le Competenze:

- **Obiettivo:** Assicurare che tutto il personale, in particolare gli "esperti con elevata seniority", possieda le competenze e la consapevolezza necessarie per gestire i rischi di sicurezza delle informazioni .
- **Attuazione:** Erogare programmi di formazione continua in materia di cibersicurezza e "igiene informatica di base", come richiesto dalla Direttiva NIS 2 . Definire politiche chiare sull'uso degli strumenti aziendali.

5. Implementare e Mantenere Controlli Tecnici Avanzati:

- **Obiettivo:** Proteggere le infrastrutture gestite e i dati dei clienti attraverso l'adozione di soluzioni di sicurezza allo stato dell'arte.
- **Attuazione:** Implementare e gestire soluzioni come Single Sign-On (SSO), Multifactor Authentication (MFA) e crittografia, in linea con l'offerta di servizi di XFORGE e i requisiti della Direttiva NIS 2.

5. Ruoli e Responsabilità

L'Alta Direzione di XFORGE assume la responsabilità ultima per l'efficacia del SGSI . Essa assicura che le responsabilità e le autorità per i ruoli pertinenti alla sicurezza delle informazioni siano assegnate, comunicate e comprese all'interno dell'organizzazione . Ogni dipendente e collaboratore ha la responsabilità di aderire alla presente politica e alle procedure di sicurezza correlate.

6. Comunicazione, Riesame e Miglioramento

La presente Politica per la Sicurezza delle Informazioni è documentata, comunicata a tutto il personale interno e resa disponibile alle parti interessate pertinenti, come clienti e autorità di regolamentazione, secondo opportunità .

Questa politica sarà riesaminata ad intervalli pianificati, e comunque in caso di cambiamenti significativi, per assicurarne la continua idoneità, adeguatezza ed efficacia. Il riesame terrà conto dei risultati degli audit, degli incidenti, delle nuove minacce e delle evoluzioni del contesto di business e normativo .

XFORGE S.R.L.
Via Francesco Arese, 16
20159 Milano (MI) - ITALY
P.Iva/Cod. Fisc.: 10147400963