Misure tecniche e organizzative

per la sicurezza
e la protezione dei dati

yousign

Introduzione

Yousign si impegna a rispettare la riservatezza dei dati dei clienti e la loro privacy. Una serie di misure tecniche e organizzative è stata messa in atto **per garantire la sicurezza dei dati personali forniti dai clienti**. Queste misure possono cambiare man mano che la soluzione di Yousign si evolve tecnicamente e si perfeziona. A questo proposito, Yousign potrà introdurre altre misure appropriate.

Certificazioni e audit

In qualità di terzo di fiducia, Yousign soddisfa i requisiti e dispone delle certificazioni **eIDAS per la firma elettronica, il sigillo elettronico e la marcatura temporale**. Tutta la documentazione tecnica è accessibile alla seguente pagina: Documentazione tecnica delle certificazioni.

Elenco degli standard rispettati da Yousign:

Sigillo elettronico e firma avanzata	Marcatura temporale qualificata	Certificati qualificati per sigillo e firma
EN 319 401 V2.2.1	EN 319 401 V2.2.1	EN 319 401 V2.2.1
EN 319 403 V2.2.2	EN 319 403 V2.2.2	EN 319 403 V2.2.2
EN 319 411-1 V1.2.2	EN 319 421 V1.1.1	EN 319 411-1 V1.2.2
		EN 319 411-2 V2.2.2

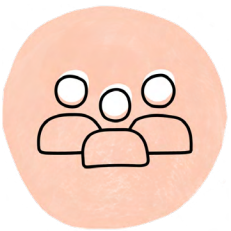
Qualunque sia il livello di firma, Yousign utilizza un HSM Proteccio (un server che permette di proteggere le transazioni crittografiche). L'HSM è certificato:
- Common Criteria a livello EAL4+
- Certificazione NATO SECRET
- Certificazione EU RESTRICTED
- Qualifica rafforzata dall'ANSSI

Al fine di garantire il mantenimento della nostra conformità, conduciamo regolarmente alcuni audit.

- Audit esterni di sicurezza e di conformità eIDAS
- Audit interni di sicurezza e di conformità eIDAS

Gestione del personale e ruolo

I collaboratori di Yousign **sono consapevoli della sicurezza e della protezione dei dati personali**.



- Formazione sulla sicurezza delle informazioni e sulla protezione dei dati personali per i nuovi collaboratori
- Comunicazioni regolari a tutti i team
- Designazione di referenti tecnici all'interno dei team per garantire l'attuazione delle buone pratiche e delle regole interne

Abbiamo implementato una politica di gestione dei ruoli, sulla base della quale limitiamo l'accesso al ruolo di ciascun dipendente secondo il principio del minor privilegio. Con cadenza trimestrale viene effettuata una revisione della gestione dei diritti.

- Politica di gestione delle password
- Impegni di riservatezza

Infrastrutture e controllo accessi

Yousign si affida a partner di hosting per garantire **la sicurezza ottimale delle proprie infrastrutture**, avendo in particolare implementato una politica di sicurezza dei sistemi informativi che soddisfa i requisiti di diversi standard e certificazioni (certificazione PCI-DSS, certificazione ISO/IEC 27001, certificati SOC 1 TYPE II e SOC 2 TYPE II, ecc.).

Controllo dell'accesso fisico

- Verifica dell'identità
- Gestione centralizzata delle porte di accesso tramite un sistema di badge
- Cabine individuali per l'accesso controllato
- Sistemi di sorveglianza

Controllo di accesso logico ai dati

- Processo di autenticazione in due fasi
- Politica di gestione delle password
- Firewall e antivirus aggiornati regolarmente
- Politica di registrazione e controllo degli accessi documentata

Sicurezza delle transazioni e crittografia

L'intero percorso di transazione è **protetto da crittografia**. Yousign si avvale di moderne tecnologie di crittografia conformi agli standard stabiliti dall'ANSSI.

- Transazioni sicure tramite crittografia TLS da e verso i nostri servizi
- Crittografia a riposo dei documenti prima e dopo la firma tramite crittografia AES-256-bit
- Utilizzo di chiavi di dimensioni superiori a 2048 bit e di protocolli sicuri come RSA

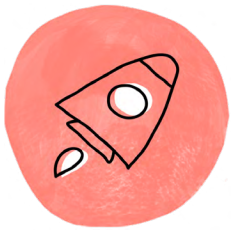
Gestione delle vulnerabilità e degli incidenti

Abbiamo implementato politiche di gestione delle vulnerabilità e degli incidenti. Esse consentono di **prevenire, rilevare e risolvere questi eventi**.

- Scansioni di vulnerabilità
- PenTest da parte di una società specializzata
- Tracciamento delle rilevazioni tramite un programma di Bug bounty
- Allarmi e sorveglianza delle vulnerabilità
- Verifiche e revisioni del codice
- Processo di notifica delle violazioni ai nostri clienti e alle autorità competenti

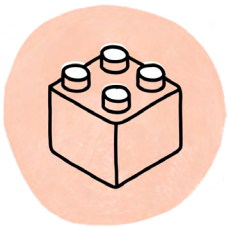
Disponibilità e continuità del servizio

Yousign si adopererà al massimo per garantire **un'elevata disponibilità e continuità dei servizi**.



- Infrastruttura ridondante e scalabile
- Processo di monitoraggio delle prestazioni
- Regolari prove di stress dei servizi
- Test di vulnerabilità e di intrusione esterna
- Gestione delle informazioni e degli eventi di sicurezza
- Piano di continuità operativa
- Piano di ripristino in caso di disastro

Sicurezza dello sviluppo



Mettiamo in atto processi interni di sviluppo per i nostri team, al fine di garantire lo sviluppo sicuro della nostra soluzione.

- Applicazione delle buone pratiche dettate dall'Open Web Application Security Project (OWASP)
- Approccio “Security by Design”
- Test automatici e manuali
- Revisioni e modifiche del codice
- Revisione tra pari


yousign