Medidas técnicas y organizativas

para garantizar la seguridad y la protección de los datos

yousign

Introducción

Yousign se compromete a respetar la confidencialidad de sus datos y su privacidad. Hemos adoptado una serie de medidas técnicas y organizativas para **garantizar la seguridad de los datos personales que usted nos proporciona**.
Estas medidas pueden cambiar en función de los avances técnicos y las mejoras de la solución de Yousign. A este respecto, Yousign puede aplicar otras medidas apropiadas.

Certificaciones y auditorías

Como tercero de confianza, Yousign cumple los requisitos del Reglamento **eIDAS para expedir certificados de firma electrónica, sello electrónico y sello de tiempo**. Toda la documentación técnica está disponible en la siguiente página:
Documentación técnica de certificaciones

Lista de normas que cumple Yousign:

Sello electrónico y firma electrónica avanzada	Sello cualificado de tiempo	Certificados cualificados de firma electrónica y sello electrónico
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

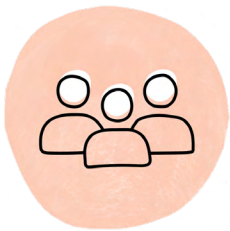
Independientemente del nivel de firma, Yousign utiliza un HSM Proteccio (un servidor que permite proteger las transacciones criptográficas). El HSM cuenta con las siguientes certificaciones:
- Criterios comunes con nivel EAL4+.
- Aprobación NATO SECRET.
- Aprobación UE RESTRICTED.
- Cualificación reforzada por la ANSSI (Agencia francesa de seguridad de los sistemas de información).

Para garantizar el cumplimiento continuo de la normativa, realizamos auditorías de forma regular.

- Auditorías externas de seguridad y cumplimiento del Reglamento eIDAS.
- Auditorías internas de seguridad y cumplimiento del Reglamento eIDAS.

Gestión del personal y funciones

Los empleados de Yousign son **conscientes de la importancia de la seguridad y la protección de los datos personales**.



- Formación en seguridad de la información y protección de datos personales para los nuevos empleados.
- Comunicaciones periódicas a todos los equipos.
- Nombramiento de coordinadores técnicos dentro de los equipos para garantizar la aplicación de las buenas prácticas y normas internas.

Hemos adoptado una política de gestión de funciones y, a este respecto, limitamos el acceso según la función de cada empleado de acuerdo con el principio de mínimo privilegio. Examinamos la gestión de los derechos trimestralmente.

- Política de gestión de contraseñas.
- Compromisos de confidencialidad.

Infraestructura y control de acceso

Yousign recurre a socios de alojamiento para garantizar **la máxima seguridad de sus infraestructuras**, con una política de seguridad de los sistemas de información que responde a las exigencias de varias normas y certificaciones (certificación PCI-DSS, certificación ISO/IEC 27001, certificados SOC 1 TIPO II y SOC 2 TIPO II, etc.).

Control de acceso físico

- Verificación de la identidad.
- Gestión centralizada de las puertas de acceso mediante un sistema de tarjetas de identificación.
- Esclusa unipersonal.
- Equipo de vigilancia.

Control de acceso lógico a los datos

- Proceso de autenticación en dos pasos.
- Política de gestión de contraseñas.
- Actualización periódica de cortafuegos y antivirus.
- Registro y política de control de acceso documentado.

Seguridad de las transacciones y cifrado

Toda la cadena de transacciones está **protegida mediante cifrado**. Yousign utiliza tecnologías modernas de cifrado que cumplen con las normas establecidas por la ANSSI.

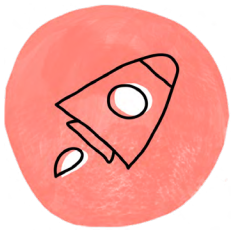
- Transacciones seguras mediante el protocolo de cifrado TLS hacia y desde nuestros servicios.
- Cifrado en reposo de los documentos antes y después de la firma a través del cifrado AES-256 bits.
- Uso de claves superiores a 2048 bits y protocolos seguros como el RSA.

Gestión de vulnerabilidades y de incidentes

Se han adoptado políticas de gestión de vulnerabilidades y de incidentes que ayudan a **prevenir, detectar y resolver estos sucesos**.

- Escáneres de vulnerabilidades.
- Auditoría de pruebas de penetración por parte de una empresa especializada.
- Seguimiento de la detección de vulnerabilidades a través de un programa de recompensas (bug bounty).
- Alertas y supervisión de vulnerabilidades.
- Auditorías y revisiones de códigos.
- Procedimiento de notificación de violaciones de seguridad a los clientes y autoridades competentes.

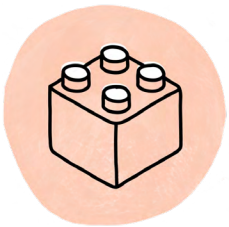
Disponibilidad y continuidad del servicio



Yousign se esfuerza por garantizar una **alta disponibilidad y la continuidad de los servicios**.

- Infraestructura redundante y escalable.
- Proceso de seguimiento del rendimiento.
- Pruebas de estrés periódicas de los servicios.
- Pruebas de vulnerabilidad e intrusión externa.
- Gestión de la información y de incidentes de seguridad.
- Plan de continuidad empresarial.
- Plan de recuperación de desastres.

Seguridad del desarrollo



Establecemos procesos de desarrollo interno para nuestros equipos con el fin de desarrollar de forma segura nuestra solución.

- Supervisión de las buenas prácticas establecidas por el Open Web Application Security Project (OWASP).
- Principio de seguridad desde el diseño.
- Pruebas automáticas y manuales.
- Revisiones y cambios de código.
- Revisión por pares.


yousign