

Ciberseguridad en OTEA

Funcionamiento distribuido, arquitecturas robustas o cumplimiento normativo son las principales características de seguridad de la plataforma.

Cumplimiento normativo

OTEA está certificada conforme a los estándares más estrictos de la industria y cumple normas como la ISO 27001 y el ENS (Esquema Nacional de Seguridad)



Ingesta segura de la información

- ✓ Dispositivos defendidos en profundidad con OTEA OS: puertos cerrados, blindaje de canales de comunicación entrantes y establecimiento de canales salientes seguros
- ✓ Comunicaciones externas HTTPS con SSL, TLS 1.3 /TLS



Seguridad y cifrado de datos

- ✓ Infraestructura organizada en silos para almacenamiento, cifrado, descifrado y transmisión de datos
- ✓ Datos encriptados según los estándares de la industria
- ✓ Registro centralizado de logs



Acceso seguro a la plataforma

- ✓ Acceso seguro a OTEA con permisos pormenorizados según rol de usuario
- ✓ Contraseñas robustas basadas el algoritmo criptográfico aprobado por ISO/IEC 10118-3



Protección frente a ataques

- ✓ Bloque de usuarios por intentos de Login incorrectos
- ✓ Filtrado y baneo automático por IP. Evitar posibles DDoS
- ✓ Integración opcional con SSO



Alojamiento de datos en la nube de Azure

- ✓ Protección de datos en tránsito y en reposo
- ✓ Redundancia geográfica de datos ante desastres
- ✓ Auditoría y gestión de registros



Disponibilidad de la plataforma

- ✓ SLA de disponibilidad de servidores de 99,9%
- ✓ Planes de continuidad, respaldo y recuperación frente a desastres o accidentes