Cybersecurity in OTEA

Distributed operation, robust architecture and regulatory compliance are core to the platform's security.

Regulatory compliance

OTEA is certified to rigorous industry standards and complies with ISO 27001 and Spain's National Security Framework (ENS).

Secure data ingestion

- ✓ OTEA OS provides defense in depth: closed ports, protected inbound communication channels and secure outbound connections
- ✓ External communications use HTTPS with SSL/TLS, including TLS 1.3

Data security and encryption

- ✓ Infrastructure separated into silos for data storage, encryption, decryption and transmission
- ✓ Data encrypted to industry standards
- ✓ Centralized log collection

Secure platform access

- ✓ Secure access to OTEA with granular permissions based on user roles
- ✓ Strong passwords based on cryptographic algorithms approved under ISO/IEC 10118-3

Protection against attacks

- ✓ Users locked out after repeated failed login attempts
- ✓ Automatic IP filtering and blocking to mitigate potential DDoS attacks
- ✓ Optional SSO integration

Azure cloud data hosting

- ✓ Data protected in transit and at rest
- ✓ Geographic data redundancy for disaster recovery
- ✓ Log auditing and management

Platform availability

- ✓ 99.9% server availability SLA
- ✓ Continuity, backup and recovery plans for disasters or incidents