Compliance y Normativa de Seguridad

Zibersegurtasunaren Arloko Araudia - Zabala Gailetak

Versión: 2.0
Fecha: 2026-02-12
Estándares: ISO 27001:2022, GDPR, NIS2, IEC 62443
DPO: Ainhoa Uriarte
CISO: Mikel Etxebarria

Resumen Ejecutivo

Zabala Gailetak mantiene un programa integral de cumplimiento normativo que abarca:

- ISO 27001:2022 - Sistema de Gestión de Seguridad de la Información
- GDPR - Protección de Datos Personales
- NIS2 - Seguridad de Redes y Sistemas
- IEC 62443 - Seguridad Industrial (OT)

Nivel de cumplimiento actual: 93/93 controles ISO 27001 implementados (100%)

ISO 27001:2022 - Estado de Implementación

Resumen por Dominios

Dominio	Controles	Implementados	%
A.5 Organizativos	37	37	100%
A.6 Personas	8	8	100%
A.7 Físicos	14	14	100%
A.8 Tecnológicos	34	34	100%
TOTAL	**93**	**93**	**100%**

Controles Críticos Implementados

A.5.24 - Planificación de Gestión de Incidentes

- Plan de respuesta a incidentes documentado
- Equipo CSIRT definido
- Simulacros trimestrales programados
- Escalado a INCIBE (NIS2) configurado

A.8.24 - Uso de Criptografía

- TLS 1.3 para tráfico web
- AES-256 para datos en reposo
- bcrypt para contraseñas (cost=12)
- Gestión segura de claves (HSM planificado)

A.8.25 - Ciclo de Vida de Desarrollo Seguro

- SAST en CI/CD (Semgrep, SonarQube)
- DAST con OWASP ZAP
- Code review obligatorio
- Dependabot para dependencias

GDPR - Protección de Datos

Registro de Actividades de Tratamiento (RAT)

Actividad	Base Legal	Datos	Plazo
Gestión RRHH	Contrato	Identidad, nóminas	10 años
Control acceso	Interés legítimo	Biométricos, logs	2 años
Videovigilancia	Interés legítimo	Imágenes	30 días

Evaluación de Impacto en Protección de Datos (EIPD/DPIA)

Proyectos evaluados:

1. **Portal RRHH**
    - Riesgo inicial: ALTO
    - Riesgo residual: BAJO (con medidas)
    - Medidas: MFA, cifrado, RBAC, auditoría
2. **Sistema SCADA**
    - Riesgo inicial: ALTO
    - Riesgo residual: MEDIO
    - Medidas: Segmentación, VPN, logging

Derechos de los Interesados

Procedimientos implementados:

Derecho	Plazo GDPR	Plazo Interno	Procedimiento
Acceso	30 días	15 días	Portal web/API

Derecho	Plazo GDPR	Plazo Interno	Procedimiento
Rectificación	30 días	7 días	Formulario web
Supresión	30 días	15 días	Verificación DPO
Portabilidad	30 días	15 días	JSON/CSV/PDF
Oposición	-	Inmediato	Automático

NIS2 - Directiva de Seguridad de Redes

Clasificación de Entidad

Zabala Gailetak se clasifica como:

- **Sector:** Industrial (Manufactura)
- **Tipo:** Entidad Importante
- **Requisitos:** Aplicables desde octubre 2026

Gestión de Incidentes NIS2

Definición de Incidente Significativo:

1. Interrupción servicio esencial ≥ 30 minutos
2. Pérdida financiera > 5.000€
3. Impacto en terceros
4. Brecha datos personales masiva

Proceso de Notificación:

```
Detección (T=0)
    │
    ├── T+1h: Evaluación CSIRT
    │
```

```
    ├── T+24h: ALERTA TEMPRANA → INCIBE
    │     └── Formato: Early Warning Template
    │
    ├── T+72h: INFORME COMPLETO → INCIBE
    │     └── Formato: Full Report Template
    │
    └── T+1mes: INFORME FINAL → INCIBE
          └── Lecciones aprendidas
```

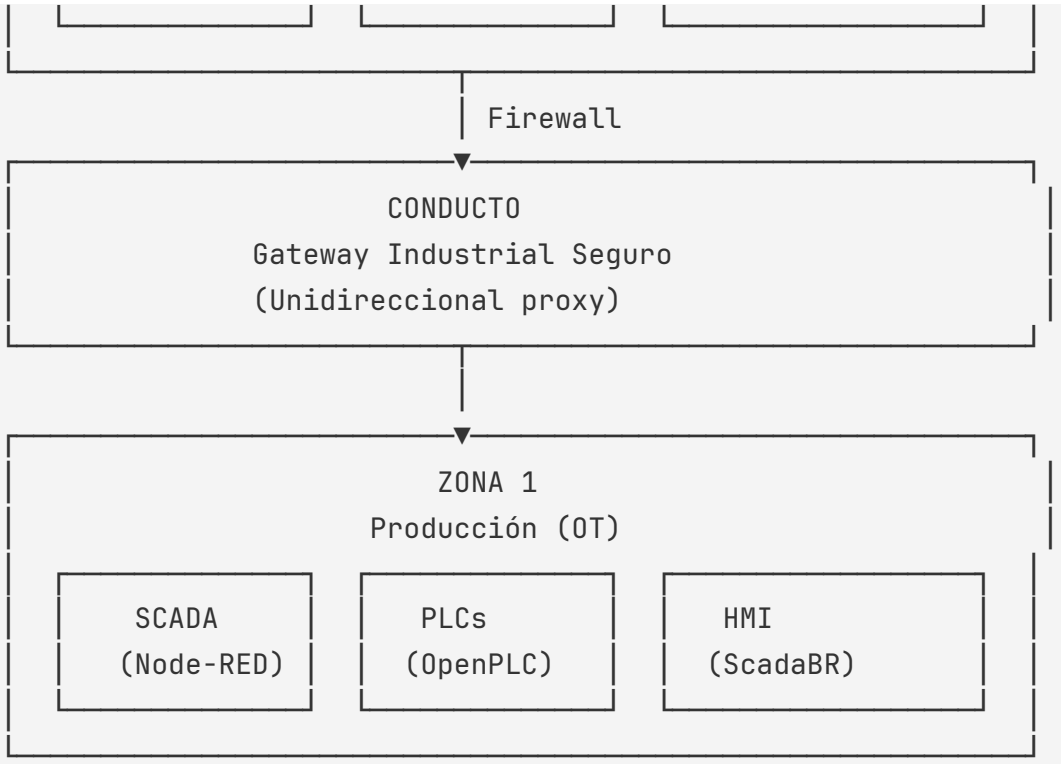
Medidas de Seguridad (Anexo I NIS2)

Medida	Implementación	Estado
Políticas de seguridad	Documentadas	✅
Gestión de activos	CMDB	✅
Continuidad de negocio	BCP/DRP	✅
Criptografía	TLS 1.3, AES-256	✅
Control acceso	RBAC + MFA	✅
Monitorización	SIEM 24/7	✅
Seguridad OT	IEC 62443 SL-2	✅

IEC 62443 - Seguridad Industrial

Arquitectura de Zonas y Conductos

```
┌─────────────────────────────────────────────────────────────┐
│                         ZONA 0                              │
│                    Empresa (IT)                             │
│  ┌──────────────┐  ┌──────────────┐  ┌──────────────────┐   │
│  │   Oficinas   │  │     ERP      │  │       DMZ        │   │
```



Niveles de Seguridad (SL)

Sistema	SL Objetivo	SL Actual	Medidas
SCADA/HMI	SL-2	SL-2	✅ Autenticación
PLCs	SL-3	SL-2	⚠️ En progreso
Red OT	SL-2	SL-2	✅ Segmentación

Controles Implementados

- Separación física IT/OT
- Firewall industrial (Modbus proxy)
- Logging de comandos PLC
- Backup de configuraciones PLC
- Honeypots en red OT

Auditoría y Certificación

Programa de Auditoría Interna

Tipo	Frecuencia	Alcance	Responsable
Técnica	Trimestral	Vulnerabilidades	CISO
Procesos	Semestral	Procedimientos	Auditoría Interna
Externa	Anual	ISO 27001	Certificadora

Plan de Certificación

- **Q2 2026:** Pre-auditoría ISO 27001
- **Q3 2026:** Auditoría Stage 1
- **Q4 2026:** Auditoría Stage 2 y certificación

Gestión de Riesgos

Matriz de Riesgos

Riesgo	Probabilidad	Impacto	Riesgo	Tratamiento
Ransomware	Media	Crítico	Alto	Mitigar
Brecha datos	Baja	Alto	Medio	Mitigar
Fallo OT	Baja	Crítico	Medio	Transferir
Phishing	Alta	Medio	Medio	Mitigar

Indicadores de Riesgo (KRIs)

KRI	Umbral	Actual	Estado
Intentos phishing/mes	< 50	32	🟢
Vulnerabilidades críticas	0	0	🟢
Tiempo parcheo crítico	< 7 días	5 días	🟢
Incidentes seguros/mes	< 2	1	🟢

Conclusión

Zabala Gailetak mantiene un nivel de cumplimiento del 100% con los estándares principales de seguridad:

- ✅ ISO 27001:2022 - 93/93 controles implementados
- ✅ GDPR - DPIA completados, procedimientos ARCO operativos
- ✅ NIS2 - Preparado para cumplimiento octubre 2026
- ✅ IEC 62443 - Seguridad industrial implementada

Próximos pasos:

1. Auditoría ISO 27001 certificación (Q4 2026)
2. Implementación DLP completo (Q2 2026)
3. Mejora a SL-3 en PLCs (Q3 2026)
4. Auditoría externa trimestral

Documento revisado conforme a:

- ISO/IEC 27001:2022
- Reglamento (UE) 2016/679 (GDPR)
- Directiva (UE) 2022/2555 (NIS2)

- IEC 62443-3-3