nis2_implementation_plan

NIS2 Inplementazio Plana

NIS2 Directive Implementation Plan

Enpresa: Zabala Gailetak, S.L. **Direktiba:** NIS2 (EU 2022/2555) **Deadline:** 2026-10-17 **Status:** ⏳ IN PROGRESS (60%) **Budget:** 85.000€

---

1. NIS2 APLIKAGARRITASUNA

Zabala Gailetak: - Jarduera: Elikagai fabrikazioa - Langileak: 120 - Sektorea: Critical infrastructure (elikagai hornidura-katea) - Entitate Mota: **“IMPORTANT ENTITY”** (Art. 3)

Obligazio Nagusiak: - Risk management measures (Art. 21) - Incident notification (Art. 23): 24h early warning, 72h full report - Supply chain security (Art. 21.2.e) - Cyber hygiene (Art. 21.2.a)

---

2. NIS2 GAP ANALYSIS

Requirement (NIS2)	Egungo Egoera	Gap	Prioritasuna
Art. 21.2.a - Cyber hygiene	Partial (MFA 100%, patching 70%)	EDR, SIEM 24/7	P0
Art. 21.2.b - Incident handling	SOP exists	CSIRT team, 24h notification	P0
Art. 21.2.c - Business continuity	BCP exists	Test quarterly	P1
Art. 21.2.d - Supply chain security	Informal	Vendor assessment program	P0
Art. 21.2.e - Vulnerability disclosure	No policy	Public disclosure policy	P1
Art. 21.2.f - Encryption	TLS 1.3, disk encryption	Full E2EE	P2
Art. 21.2.g - Security policies	✅ Comprehensive	Minor updates	P3
Art. 21.2.h - Access control	✅ MFA + RBAC	Periodic review	P2
Art. 23 - Incident notification	Template exists	Automated workflow	P0

Compliance: 60% → Target: 100% by Oct 2026

---

3. IMPLEMENTATION ROADMAP

Q1 2026 (Martxoa)

- ✅ Gap analysis completed
- ⏳ Cyber hygiene baseline (MFA 100%) ✅
- ⏳ Incident notification SOP

Q2 2026 (Apirila-Ekaina)

- ⏳ EDR deployment (CrowdStrike)
- ⏳ SIEM + SOC 24/7
- ⏳ CSIRT team formation
- ⏳ Supplier security assessment program

Q3 2026 (Uztaila-Iraila)

- ⏳ Vulnerability disclosure policy
- ⏳ BCP quarterly testing
- ⏳ Penetration testing (annual)
- ⏳ NIS2 compliance self-assessment

Q4 2026 (Urria)

- ✅ NIS2 COMPLIANCE DEADLINE (Oct 17)
- ⏳ External audit (optional but recommended)
- ⏳ Report to National Authority

---

4. KEY ACTIONS

4.1 CSIRT Team

Osaera: - CISO (Incident Commander) - IT Officer (Technical Lead) - DPO (Privacy Lead) - Legal (Legal Advisor) - External SOC (24/7 monitoring)

Training: Q2 2026

4.2 Incident Notification (24/72h)

Workflow:

Incident Detected → CSIRT activated (< 1h)
↓
Initial Assessment (< 4h)
↓
Early Warning (< 24h) → National Authority
↓
Full Investigation (< 72h)
↓
Final Report (< 72h) → National Authority

4.3 Supply Chain Security

Vendor Assessment: - Siemens (SCADA) - HID (Badge system) - AWS (Backup) - Cloudflare (WAF)

Criteria: - ISO 27001 certification - Security questionnaire (100 questions) - Right to audit clause - Incident notification SLA (24h)

---

5. BUDGET

Item	Cost
EDR (CrowdStrike)	25.000€
SIEM + SOC 24/7	40.000€
Vulnerability scanning	5.000€
Pentesting	10.000€
Training	5.000€
TOTAL	**85.000€**

---

6. SANZIOAK (Ez betetze)

NIS2 Art. 34: - Administrative fines: up to **10 million €** or **2% annual turnover** - For Zabala Gailetak: Est. max fine ~200.000€

Gomendio: ✅ COMPLY (kostu < isun)

ONARPENA: CEO (Jon Zabala) + CISO (Mikel Etxebarria) - 2026-02-05 **STATUS REVIEW:** Monthly (CGC) **DEADLINE:** 2026-10-17 ⚠️

Dokumentu hau sortu da RA5 (Normativa Nazionala/Internazionala) betebeharrak betetzeko.