Kontrol Diseinua eta Aukera Prozedura

Security Control Design and Selection Procedure

Enpresa: Zabala Gailetak, S.L. **Dokumentu Kodea:** COMP-POP-002 **Bertsioa:** 1.0 **Data:** 2026-02-05 **Jabea:** CISO **Egoera:** Indarrean

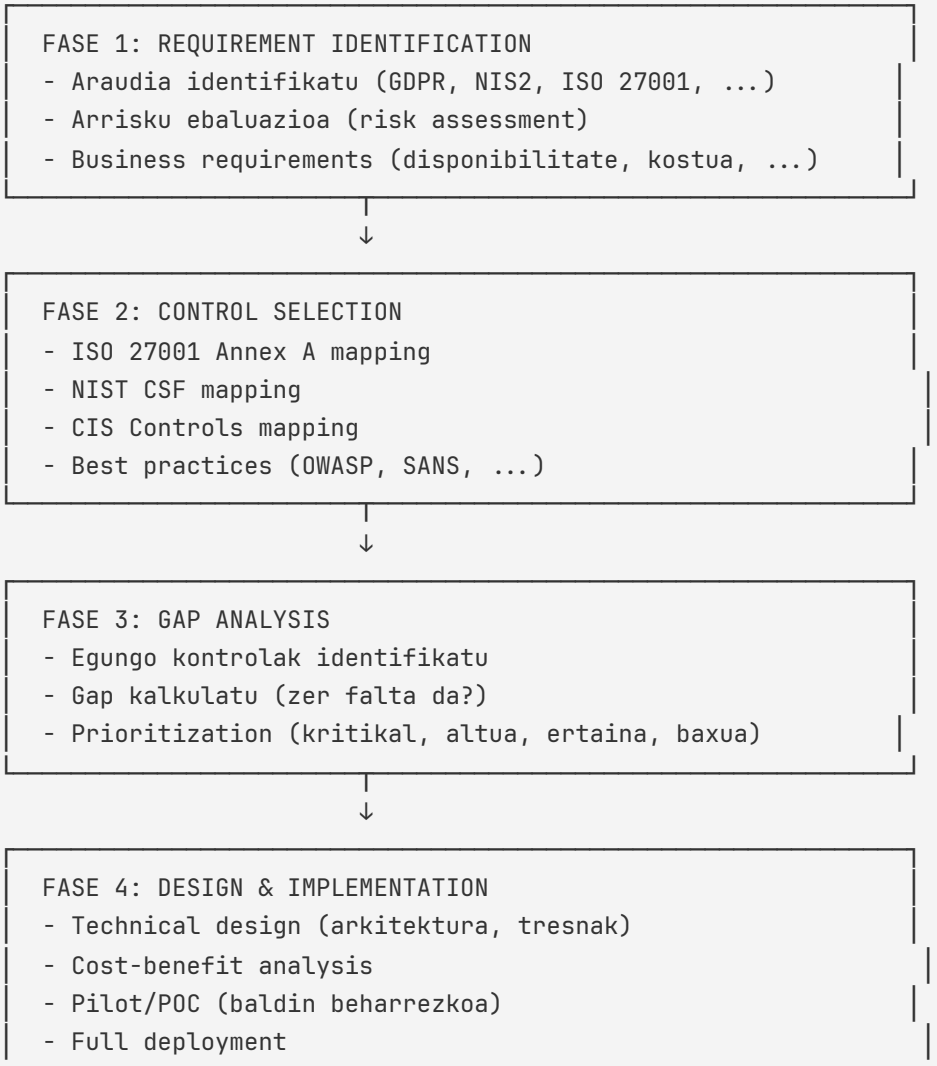
---

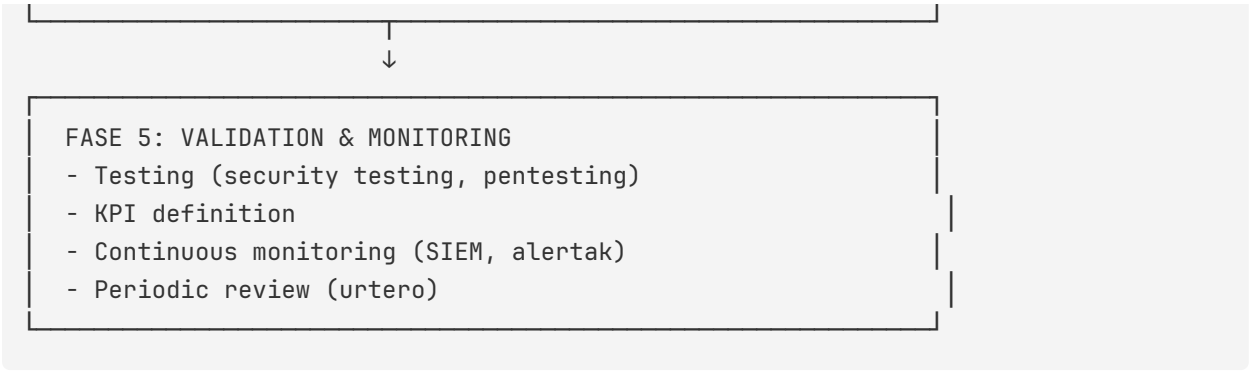
1. XEDEA

Prozedura honek ezartzen du nola diseinatzen eta aukeratzen diren **segurtasun kontrolak** araudia eta arriskuak betetzeko.

---

2. CONTROL DESIGN LIFECYCLE





---

3. CONTROL FRAMEWORKS

3.1 ISO 27001:2022 Annex A

Kategoriak:

- A.5: Organizational controls (37 kontrolak)
- A.6: People controls (8 kontrolak)
- A.7: Physical controls (14 kontrolak)
- A.8: Technological controls (34 kontrolak)

TOTALA: 93 kontrolak

Erabilera: Statement of Applicability (SOA) sortu

3.2 NIST Cybersecurity Framework

Funtzionak:

- Identify (ID)
- Protect (PR)
- Detect (DE)
- Respond (RS)
- Recover (RC)

Erabilera: Maturity assessment

3.3 CIS Controls v8

Kategoriak:

- Implementation Group 1 (IG1): 56 safeguards (basic)
- Implementation Group 2 (IG2): 74 safeguards (intermediate)
- Implementation Group 3 (IG3): 153 safeguards (advanced)

Erabilera: Quick wins prioritization

---

4. CONTROL SELECTION CRITERIA

4.1 Prioritization Matrix

Criteria	Pisua (%)	Deskribapena
Compliance Requirement	40%	Araudia obligatorio? (GDPR, NIS2, …)
Risk Reduction	30%	Arrisku murriztapen ehunekoa
Cost-Benefit	15%	ROI (Return on Investment)
Implementation Complexity	10%	Konplexutasuna (baxua > altua)
Business Impact	5%	Eragina negozio operazioetan

Kalkulua:

```
Control Score = (Compliance × 0.4) + (Risk Reduction × 0.3) +
                (Cost-Benefit × 0.15) + (Complexity × 0.1) +
                (Business Impact × 0.05)
```

Adibidea: MFA Implementation

- Compliance: 10/10 (GDPR, ENS obligatorio) → 4 puntuak
- Risk Reduction: 9/10 (phishing -80%) → 2.7 puntuak
- Cost-Benefit: 10/10 (kostu 0€, onura altua) → 1.5 puntuak
- Complexity: 8/10 (erraz implementatzea) → 0.8 puntuak
- Business Impact: 7/10 (pixkat inkonbenioa) → 0.35 puntuak
- **TOTAL: 9.35/10 → PRIORITATE OSO ALTUA**

4.2 Prioritization Thresholds

Score	Prioritate	Epemuga
9-10	P0 - KRITIKAL	< 1 hilea
7-8.9	P1 - ALTUA	< 3 hileak
5-6.9	P2 - ERTAINA	< 6 hileak
3-4.9	P3 - BAXUA	< 12 hileak

Score	Prioritate	Epemuga
0-2.9	P4 - OPTIONAL	Backlog

---

5. CONTROL DESIGN TEMPLATE

5.1 Control Specification Document

Template: `/compliance/controls/CTRL-XXX-specification.md`

Edukia:

1. **Control ID:** CTRL-001 (adib: MFA)
2. **Control Name:** Multi-Factor Authentication
3. **Control Category:** ISO 27001 A.5.18 (Access rights)
4. **Compliance Mapping:**
    - GDPR Art. 32 (Security of processing)
    - ENS mp.ac.2 (Autentifikazioa)
    - ISO 27001 A.5.18
5. **Risk Addressed:** Phishing, credential stuffing, password theft
6. **Description:** Obligar autentifikazioa bikoitza (password + TOTP)
7. **Technical Design:**
    - Teknologia: Google Authenticator (TOTP RFC 6238)
    - Integrazio: JWT middleware + MFA check
    - Rollout: Phased (Admin lehenengo, ondoren guztiak)
8. **Implementation Plan:**
    - Phase 1: Admin (2 asteak)
    - Phase 2: RRHH + IKT (2 asteak)
    - Phase 3: Guztiak (4 asteak)
9. **Cost:** 0€ (library free)
10. **KPIs:**
    - MFA adoption rate (target: 100%)
    - Failed login attempts (target: -70%)
    - Phishing success rate (target: -85%)
11. **Testing Plan:** Pentesting phishing simulation

12. **Maintenance:** Quarterly review
13. **Owner:** CISO
14. **Status:** ✅ Implemented (2026-01-15)

---

6. CONTROL INVENTORY

6.1 Zabala Gailetak Controls (Implemented)

Control ID	Izena	Kategoria	Status	Priority
CTRL-001	MFA (TOTP)	Authentication	✅	P0
CTRL-002	WAF (Cloudflare)	Network Security	✅	P0
CTRL-003	Encryption TLS 1.3	Data Protection	✅	P0
CTRL-004	Password Policy	Authentication	✅	P0
CTRL-005	RBAC + RLS	Access Control	✅	P0
CTRL-006	Backup Offline	Data Protection	✅	P0
CTRL-007	Audit Logging	Monitoring	✅	P0
CTRL-008	SIEM (Planned)	Monitoring	⏳ Q2	P1
CTRL-009	EDR (Planned)	Endpoint Security	⏳ Q2	P1
CTRL-010	DLP (Planned)	Data Protection	⏳ Q2	P1

6.2 Gap Analysis Results

Implemented: 7/10 (70%) **Planned:** 3/10 (30%) **Total Coverage:** 100% (by Q2 2026)

---

7. COST-BENEFIT ANALYSIS

7.1 Template

Kontrola: EDR (Endpoint Detection and Response)

Kostua:

- Lizentziak: 25.000€/urteko (CrowdStrike)
- Implementazio: 10.000€ (one-time)

- Mantenimendu: 5.000€/urteko (internal)
- **TOTAL (5 urteak):** 160.000€

Onura:

- Ransomware murriztapen: 95% (arrisku 2M€ → 100k€)
- Incident response time: -80% (6h → 1h)
- Compliance: NIS2, ISO 27001 betetzen
- ROI: (1.9M€ saved - 160k€ cost) / 160k€ = **1087% ROI**

Erabakia: ✅ ONARTUA (ROI oso altua)

---

8. ERREFERENTZIAK

- ISO/IEC 27001:2022 Annex A
- NIST Cybersecurity Framework v1.1
- CIS Controls v8
- `/compliance/sgsi/risk_assessment.md`
- `/compliance/sgsi/statement_of_applicability.md`

ONARPENA: CISO (Mikel Etxebarria) - 2026-02-05 **HURRENGO BERRIKUSKETA:** 2027-02-05

Dokumentu hau sortu da RA2 (Diseño de Sistemas de Cumplimiento) betebeharrak betetzeko.