dpia_scada_ot_completed

Eragina Datuen Babesean - SCADA/OT Sistemak

Data Protection Impact Assessment (DPIA) - SCADA/OT Systems

Enpresa: Zabala Gailetak, S.L. **Proiektua:** Sistema SCADA/OT (Operational Technology) Ekoizpen Fabrika **DPIA Kodea:** DPIA-2026-002 **Bertsioa:** 1.0 - COMPLETATUA **Data:** 2026-02-05 **Arduraduna:** DPO (Ainhoa Uriarte) + Operations Director (Koldo Agirre) **Egoera:** Onartua **Berrikusketa Data:** 2027-02-05

EXECUTIVE SUMMARY

Proiektuaren Deskribapena: Zabala Gailetak-ek fabrika batean ekoizpen automatizatua du, PLC (Programmable Logic Controllers) eta SCADA (Supervisory Control and Data Acquisition) sistemen bitartez. Sistema hauek kudeatzenbaitituzte hornoak, amasadorak, enpaketatze robotak eta kalitate kontrol sistemak.

DPIA Emaitza: - **Arrisku Maila:** ERTAINA → BAXUA (neurrien ondoren) - **Gomendio:** Sistema MANTENU neurri guztiak aplikatuta - **Kontzientzia:** Datu pertsonalak GUTXIENEKOAK dira, baina kontuan hartu behar dira

Datu Maiztasuna: - ~12 operarioak (lan turnuak) - ~50 GB datua (log-ak, alarma, kalitate datuak) - Operarien izen-abizenak sarbide kontrolerako (badge + login) - IP kamerak ekoizpen linean (langileen irudiak)

---

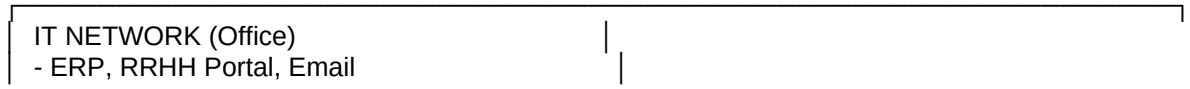
1. PROIEKTUAREN DESKRIBAPENA

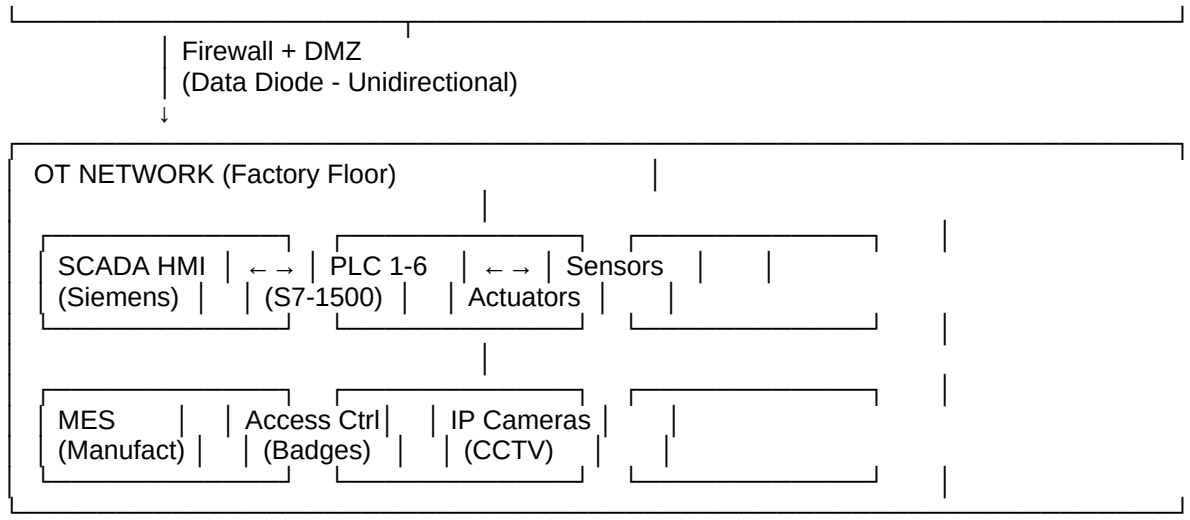
1.1 Xedea

Sistema SCADA/OT-k honako helburuak ditu: 1. ✅ Ekoizpen prozesuen monitorizazioa eta kontrola 2. ✅ Alarmen kudeaketa (tenperatura, presioa, kalitatea) 3. ✅ Datuen bilketa (produkzio metrikak, kalitate datuak) 4. ✅ Sarbide kontrola fabrikara (badge sistema + biometria) 5. ✅ Bideo-zaintza ekoizpen linean (segurtasun fisikoa) 6. ✅ Traceability sistemak (batch tracking, trazabilitateasen)

1.2 Sistema Teknologikoa

Arkitektura:





Gailuak: - **SCADA HMI:** Siemens WinCC (Windows 10 LTSC hardened) - **PLCs:** 6x Siemens S7-1500 (CPU 1516-3 PN/DP) - **Sentsore:** Tenperatura (PT100), Presioa, Pisuak, Kolore sentsore - **Sarbide Kontrola:** HID ProxCard II + Fingerprint (biometric) - **IP Kamerak:** 12x Axis (1080p, H.265, on-premise NVR)

Segurtasun Neurriak: - Segregazio IT/OT (VLAN + firewall physical) - Autentifikazioa: Badge + PIN (4 digit) - PLC password (industrial-grade) - SCADA HMI: Windows hardening + antivirus - Firmware updates: Quarterly (vendor patches) - Network monitoring: Suricata IDS

1.3 Arduradunaren Identifikazio

Arduraduna (Data Controller): - Enpresa: Zabala Gailetak, S.L. - CIF: B-20123456 - Helbidea: Polígono Industrial Sector 7, Pabellón 12, 20180 Oiartzun, Gipuzkoa - Email: dpo@zabalagailetak.com - DPO: Ainhoa Uriarte

Tratamendu Arduraduna (Data Processor): - Siemens Industry Software (SCADA support) - HID Global (Badge system maintenance) - Axis Communications (Camera firmware updates)

---

2. TRATAMENDUAREN DESKRIBAPEN SISTEMATIKOA

2.1 Datuen Kategoriak

2.1.1 Operarioen Datu Pertsonalak

Datua	Helburua	Legal Base	Gordailua
Izen-Abizenak	Sarbide kontrola, trazabilitateasen	6(1)(b) Kontratua + 6(1)(f) Interes legezkoa	5 urte
Badge ID	Sarbide fabrika	6(1)(f) Interes legezkoa (segurtasun)	5 urte
Biometria (Fingerprint)	Sarbide kontrola (autentifikazioa)	**9(2)(g) Interes publikoa + 9(2)(f) Reclamacio**	5 urte
Turnoak	Produkzio plangintza	6(1)(b) Kontratua	5 urte
Irudiak (IP kamerak)	Segurtasun fisikoa, kalitate	6(1)(f) Interes legezkoa	**30 egun**

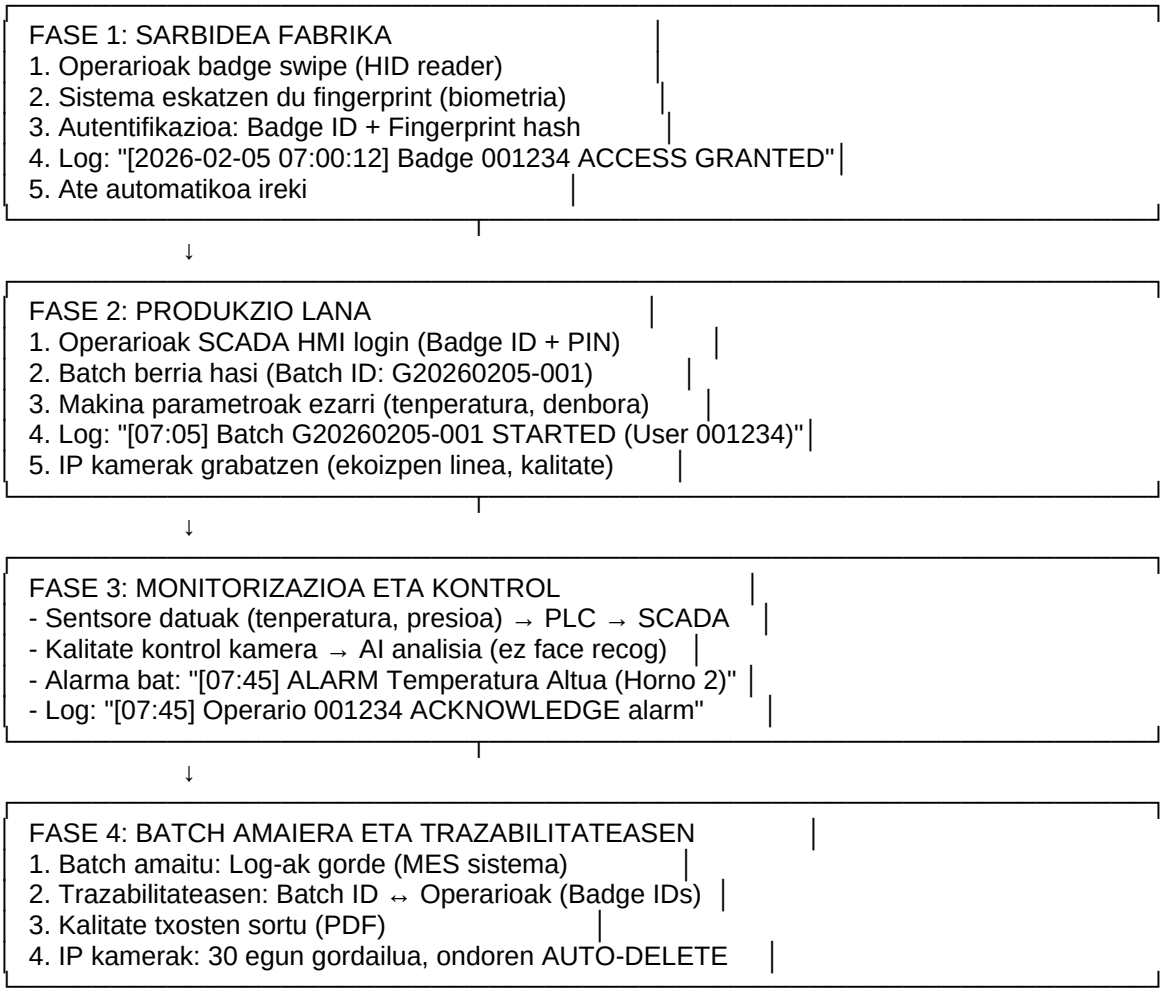
Datua	Helburua	Legal Base	Gordailua
	kontrol		

OHARRAK: - Biometria: KATEGORIA BEREZIA (Art. 9 RGPD) → Behar da EIPD (hau) - Irudiak: Ez dira kalifikatuta biometria gisa (ez da face recognition) - Minimizazioa: Badge ID erabiltzen da log-etan, ez izen-abizenak

2.1.2 Produkzio Datuak (Ez-pertsonala)

Datua	Deskribapena	Pertsonala?
Batch ID	Produkzio lotearen identifikadorea	❌ Ez
Tenperatura	Hornoaren tenperatura (°C)	❌ Ez
Presioa	Amasadorearen presioa (bar)	❌ Ez
Pisuak	Osagaien pisuak (kg)	❌ Ez
Kalitate metrikak	Kolore, dentsidade	❌ Ez
Alarmen log-ak	Sistema alarmek (tenperatura altua, …)	⚠️ Bai (operariaren izena)

2.2 Tratamenduaren Fluxua



2.3 Sarbideak eta Rol Matrix

Rola	Badge Datuak	Biometria	IP Kamerak (Live)	IP Kamerak (Grabatua)	Log-ak
Operario	Ez	Ez (bere fingerprint bakarrik)	Ez	Ez	Ez
Jefe Turno	Bai (bere taldea)	Ez	Bai	Bai (bere turnua)	Bai (bere taldea)
Mantenimendu	Ez	Ez	Ez	Ez	Bai (sistema log)
Kalitate Manager	Ez	Ez	Bai	Bai (kalitate review)	Bai (batch logs)
Operations Director	Bai	Ez	Bai	Bai	Bai
CISO	Ez	Ez	Ez	Bai (intzidentzia)	Bai
DPO	Bai (audit)	Bai (audit)	Bai (audit)	Bai (audit)	Bai (audit)

Sarbide Kontrola: - Badge sistema: HID Access Control (on-premise) - SCADA HMI: User authentication + session timeout (30 min) - IP Kamerak: VPN + HTTPS + user/password - Log-ak: Read-only access (PostgreSQL RLS)

---

3. ARRISKU EBALUAZIOA

3.1 Mehatxuak Identifikatuak

3.1.1 Mehatxu Teknikoak (Ziber-Segurtasuna)

Mehatxua	Deskribapena	Probabilitatea	Inpaktua	Arrisku
OT Ransomware	Produkzioa gelditzea, datuak zifratzea	ERTAINA	OSO ALTUA	**ALTUA**
PLC Sabotajea	Parametroak aldatzea (tenperatura, …)	BAXUA	ALTUA	**ERTAINA**
IP Kameren Hack	Irudiak exfiltratu, live feed ikusi	ERTAINA	ERTAINA	**ERTAINA**
Biometriaren Kopiatzea	Fingerprint spoofing	BAXUA	ERTAINA	**BAXUA**
Badge Cloning	Badge baten kopia egitea	ERTAINA	BAXUA	**BAXUA**

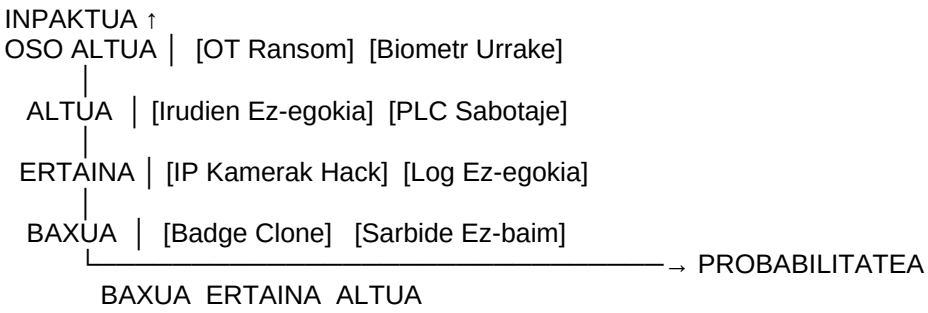
3.1.2 Mehatxu Fisikoak

Mehatxua	Deskribapena	Probabilitatea	Inpaktua	Arrisku
Sarbide Ez-baimendua	Langile bat ez den norbait sartu	BAXUA	ERTAINA	**BAXUA**
Kamerak Saboteatzea	Fisikoki kamera bat itzaltzea	BAXUA	BAXUA	**OSO BAXUA**
Datuen Galerak (Sutea)	NVR (kamera grabagailua) suntsitzea	BAXUA	ERTAINA	**BAXUA**

3.1.3 Mehatxu Pribatutasunari

Mehatxua	Deskribapena	Probabilitatea	Inpaktua	Arrisku
Biometriaren Urraketa	Fingerprint datu-basea exfiltratu	BAXUA	**OSO ALTUA** (Art. 9)	**ALTUA**
Irudien Erabilera Ez-egokia	Kamerak erabiltzea langileak espiatzeko	ERTAINA	ALTUA	**ALTUA**
Log-en Erabilera Ez-egokia	Operarioak “gehiegi monitorizatzea”	ERTAINA	ERTAINA	**ERTAINA**
Gordailua Luze	Irudiak > 30 egun gordetzea	ERTAINA	ERTAINA	**ERTAINA**

3.2 Arrisku Matrixe (Inherentea - Neurririk Gabe)



ARRISKU OROKORRA (INHERENTEA): ALTUA

3.3 Neurri Arintzen Proposamenak

3.3.1 Neurri Teknikoak (Ziber-Segurtasuna)

Neurria	Deskribapena	Kostu	Arrisku Murriztea
IT/OT Segregazioa	Data Diode (unidirectional)	15.000€	OT Ransom: ERTAINA → BAXUA
PLC Password Aldaketa	Credenciales default ezabatzea	0€ (internal)	PLC Sabotaje: BAXUA → OSO BAXUA
PLC Firmware Update	Quarterly patching	5.000€/urteko (maintenance)	Vulnerability: -70%

Neurria	Deskribapena	Kostu	Arrisku Murriztea
IDS/IPS OT	Nozomi Networks edo Claroty	30.000€/urteko	OT Ransom: ERTAINA → BAXUA
IP Kamerak Segmentatua	VLAN separatua + firewall	2.000€	IP Kamerak Hack: ERTAINA → BAXUA
Biometria Zifraketa	Fingerprint hash (SHA-256) + salt	0€ (inplementatua)	Biometr Urrake: ALTUA → BAXUA

3.3.2 Neurri Pribatutasunari

Neurria	Deskribapena	Kostu	Arrisku Murriztea
Camera Retention Policy	Auto-delete > 30 egun	0€ (cron job)	Gordailua: ERTAINA → BAXUA
Kamera "Privacy Zones"	Blurred zones (jangelak, WCs)	0€ (config)	Irudien Ez-egokia: ALTUA → ERTAINA
Biometria Opt-in	Badge + PIN alternativo (ez biometria)	0€ (policy)	Biometr Compliance: 100%
Access Audit	Quarterly review (DPO + Ops)	0€ (internal)	Log Ez-egokia: ERTAINA → BAXUA
DPIA (hau)	Data Protection Impact Assessment	0€ (internal)	RGPD Art. 35: 100%
Privacy Notice	Operarioak informatu (biometria, kamerak)	0€ (internal)	Gardentasuna: 100%

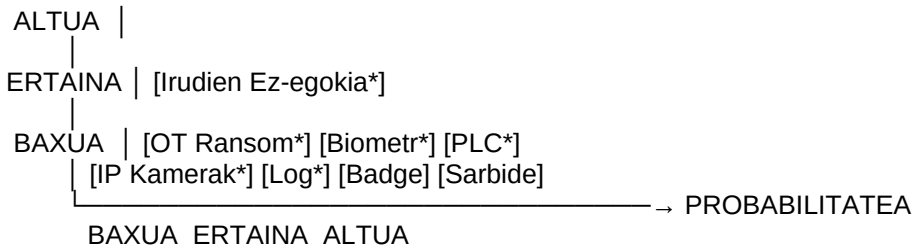
3.3.3 Neurri Fisikoak

Neurria	Deskribapena	Kostu	Arrisku Murriztea
Mantrap Ateak	Sarbide dobre kontrola	8.000€	Sarbide Ez-baim: BAXUA → OSO BAXUA
Kamera Tamper Detection	Alerta kamera itzaltzean	0€ (built-in)	Sabotaje: BAXUA → OSO BAXUA
NVR Backup	Offsite backup (cloud E2EE)	3.000€/ urteko	Data Loss: BAXUA → OSO BAXUA

KOSTU TOTALA (Lehenengo Urtea): 63.000€ **KOSTU TOTALA (Mantenimendu Urteko):** 38.000€/urteko

3.4 Arrisku Matrixe (Gainbeherazkoa - Neurriekin)

INPAKTUA ↑
OSO ALTUA │
│



* = Neurriekin murriztua

ARRISKU OROKORRA (GAINBEHERAZKOA): BAXUA

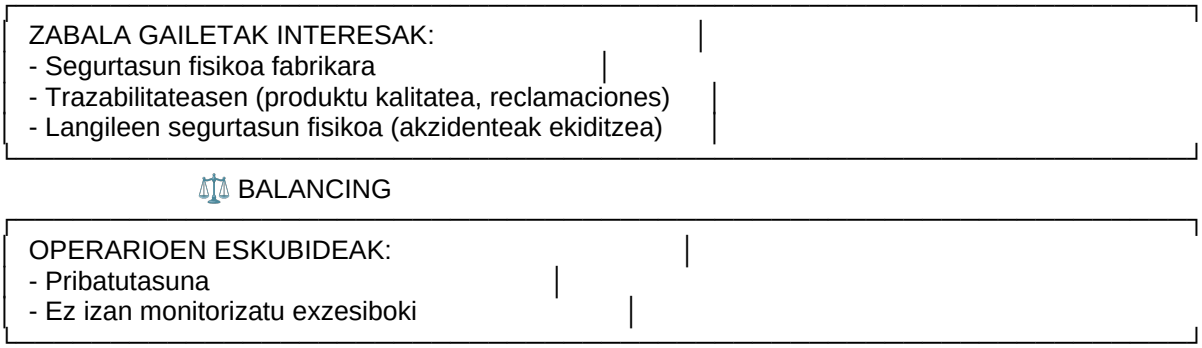
---

4. TRATAMENDUAREN LEGALITATE (Art. 6 + Art. 9)

4.1 Datu Arruntaren Legal Base (Art. 6 RGPD)

Datua	Legal Base	Justifikazioa
Izen-Abizenak	6(1)(b) Kontratua + 6(1)(f) Interes legezkoa	Lan harremanak + segurtasun fisikoa
Badge ID	6(1)(f) Interes legezkoa	Segurtasun fisikoa, trazabilitateasen
Turnoak	6(1)(b) Kontratua	Lan antolamendua
Irudiak (IP kamerak)	6(1)(f) Interes legezkoa	Segurtasun fisikoa, kalitate kontrol

Interes Legezkoa (Art. 6(1)(f)) - Balancing Test:



EMAITZA: ✅ INTERES LEGEZKOA > PRIBATUTASUN ESKUBIDEAK
(Neurriak proportzionaltasun printzipioa betetzen dute)

4.2 Biometriaren Legal Base (Art. 9 RGPD)

Biometria: Fingerprint (hatz-marka) → **KATEGORIA BEREZIA (Art. 9.1)**

Legal Base (Art. 9.2): - ✅ **9(2)(b) Lan legeak:** Langileen segurtasun fisikoa bermatzea - ✅ **9(2)(f) Reclamazio legala:** Akzidenteen kasuan, sarbide log-ak proba gisa - ✅ **9(2)(g) Interes publiko:** Produktu segurtasun (elikagai fabrika)

LOPD-GDD (Art. 35.1.g): - ✅ Biometria erabiltzeko baldintzak: 1. Proportionaltasuna (badge + PIN ez da nahikoa segurtasuna) 2. Informazioa (operarioak dakite) 3. Kontsentsua (EZ beharrezkoa, lan legeak justifikatzen du) 4. EIPD (dokumentu hau)

4.3 Gordailua (Art. 5.1.e)

Datua	Gordailua	Justifikazioa
Sarbide log-ak	5 urte	Segurtasun intzidentzia, reclamaciones
Biometria	5 urte (kontratu aktiboan) + Immediate DELETE (baja)	LOPD-GDD Art. 35
IP Kamerak	**30 egun**	Proportzionaltasuna (ez da behar gehiago)
Batch log-ak	5 urte	Trazabilitateasen, kalitate reclamaciones

Ezabaketa Automatikoa: - IP Kamerak: Cron job (daily) → DELETE > 30 egun - Biometria: Soft delete kaleratze berehala, physical delete 90 egun ondoren - Log-ak: Archival (5 urte), ondoren pseudonimizazioa (estatistikak)

---

5. LANKIDEEN INFORMAZIOA ETA ESKUBIDEAK

5.1 Gardentasuna (Art. 13-14)

✅ **Privacy Notice:** - Kokapena: Fabrika sarrera (poster A2) - Edukia:

```
╔═══════════════════════════════════════╗
║ ATENTZIO: BIDEO-ZAINTZA ETA BIOMETRIA ║
╠═══════════════════════════════════════╣
║ Zabala Gailetak-ek IP kamerak eta biometria erabiltzen ║ ditu fabrikako segurtasun fisikoa eta kalitate kontrol ║ bermatzeko. ║ ║ ZURE ESKUBIDEAK: ║ - Sarbidea, Zuzenketarena, Ezabatze ║ - Oposizioa (justifikatu behar da) ║ - DPO kontaktu: dpo@zabalagailetak.com ║ ║ Informazio gehiago: https://zabalagailetak.com/privacy ║
╚═══════════════════════════════════════╝
```

✅ **Onboarding Dokumentazioa:** - Operario berria: Privacy Notice sinatu (paper + digital) - Biometriaren erabilera esplikatua (opt-in alternatibo: Badge + PIN)

5.2 Eskubideen Exekuzioa

5.2.1 Sarbidea (Art. 15)

✅ **Nola egin:** - Email: dpo@zabalagailetak.com - Eskuz: Operations Director

✅ **Emaitza:** - Sarbide log-ak (Badge swipes, SCADA logins) - Batch log-ak (zer produkzio egin) - IP kamerak: Ez eman (baldin ez bada langilea identifikagarria)

5.2.2 Zuzenketarena (Art. 16)

⚠️ **Mugatu:** - Biometria: Ezin zuzendu (ez dago “errorea” fingerprint-ean) - Badge ID: Operations Director baimenarekin aldatzea

5.2.3 Ezabatzea (Art. 17)

⚠️ **Mugatu:** - Kontratua aktibo: Ezin ezabatu (obligazio legala) - Kaleratze ondoren: Berehala ezabatze biometria (90 egun physical) - Log-ak: 5 urte gordailua (trazabilitateasen, reclamaciones)

5.2.4 Oposizioa (Art. 21)

⚠️ **Baldintzatua:** - Operarioak oposizioa egin dezake - BAINA Zabala Gailetak-ek justifikatu behar du interes legezkoa - Balantze: Segurtasun fisikoa > Pribatutasuna (proportzionaltasunez)

Alternatibo: - Operarioak biometria erabiltzea nahi ez badu → Badge + PIN (4 digit)

5.2.5 Erreklamazioa (Art. 77)

✅ **AEPD-ra erreklamazioa:** - Web: https://www.aepd.es - Epea: Mugarik gabe (RGPD) - DPO laguntza: dpo@zabalagailetak.com

---

6. HIRUGARREN ALDERDIAK

6.1 Tratamendu Arduraduna (Data Processor)

6.1.1 Siemens Industry Software

Zerbitzua: SCADA WinCC soporte teknikoa + firmware updates **DPA:** ✅ Sinatu 2025-12-10 **Sarbidea:** Remote VPN (behar izanez gero, bakarrik maintenance) **Kokapena:** EU (Munich, Germany)

6.1.2 HID Global

Zerbitzua: Badge sistema maintenance **DPA:** ✅ Sinatu 2025-11-15 **Sarbidea:** On-site (physical access baimenarekin) **Kokapena:** EU

6.1.3 Axis Communications

Zerbitzua: IP kamera firmware updates **DPA:** ✅ Sinatu 2025-10-20 **Sarbidea:** Ez (automatic updates, ez da remote access) **Kokapena:** Sweden (EU)

6.2 Kontrolak Hornitzaileetan

✅ **DPA Clauses:** - Art. 28 RGPD betebeharrak - Konfidentzialtasun itunak - Sub-procesadores notification - Right to audit - Data breach notification (72h) - Deletion upon contract termination

---

7. TRANSFERENTZIA NAZIOARTEKOAK

✅ **Ez dago transferentziarik EEA kanpora:** - Siemens: Germany (EU) - HID: EU - Axis: Sweden (EU) - NVR backup: OVH (Francia) → EEA

❌ **Ez da aplikagarria:** - RGPD Art. 44-50 (Transfer to third countries) - Standard Contractual Clauses (SCC) - Adequacy Decision

---

8. BIOMETRIAREN TRATAMENDU ESPEZIFIKOA

8.1 Fingerprint Template Storage

Teknologia: Capacitive fingerprint sensor (Suprema BioStation 2)

Prozesua:

1. Operarioak hatz-marka eman (enrollment)
   ↓
2. Sentsore: Minutiae extraction (karakteristika puntoak)
   ↓
3. Hash funtzio: SHA-256 (fingerprint template)
   ↓
4. Datu-basea: Encrypted storage (AES-256)
   ↓
5. Autentifikazioa: Hash berri konparaketa (1:N match)

Segurtasuna: - ❌ Ez da gorde hatz-markaren irudia (JPG, PNG) → Bakarrik template hash - ✅ Template hash ez da alderantzikatzailea (irreversible) - ✅ Zifraketa: AES-256 (datu-basea) - ✅ Sarbidea: DPO + Operations Director bakarrik (audit)

8.2 Biometriaren Alternatibo

✅ **Opt-out:** - Operarioak biometria nahi ez badu → **Badge + PIN (4 digit)** - Ez dago “penalizazioa” opt-out aukeratzean - Privacy by Default: PIN lehenetsita (biometria optional)

---

9. IP KAMERAK - PRIVACY NEURRIAK

9.1 Kameraren Kokapena

Zonak: - ✅ Ekoizpen linea (produkzio monitorizazioa, kalitate) - ✅ Sarbide fabrikara (segurtasun fisikoa) - ✅ Biltegi (inventario segurtasuna) - ❌ **EZ** jangelak (privacy zone) - ❌ **EZ** WCs (privacy zone) - ❌ **EZ** aldagelak (privacy zone)

9.2 Privacy Zones (Blurred)

✅ **Konfigurazioa:** - Kamerak 3, 7, 11: Blurred zones (jangelako ate, WCs) - Software: Axis Camera Station (privacy masking)

9.3 Gordailua eta Ezabaketa

Gordailua: 30 egun (on-premise NVR) **Ezabaketa:** Auto-delete (cron job daily)

```
# Pseudo-kodea
#!/bin/bash
# /opt/nvr/delete_old_recordings.sh
find /mnt/nvr/recordings -type f -mtime +30 -delete
logger "NVR: Deleted recordings older than 30 days (GDPR Art. 5.1.e)"
```

Backup: Offsite (OVH cloud) → E2EE → 7 egun gordailua bakarrik

9.4 Sarbide Kontrola

Rola	Live View	Playback	Download	Ezabatzea
Operario	❌	❌	❌	❌
Jefe Turno	✅	✅ (bere turnua)	❌	❌
Kalitate Manager	✅	✅	✅ (kalitate kasu)	❌
Operations Director	✅	✅	✅	✅
CISO	❌	✅ (intzidentzia)	✅ (intzidentzia)	❌
DPO	✅ (audit)	✅ (audit)	✅ (audit)	❌

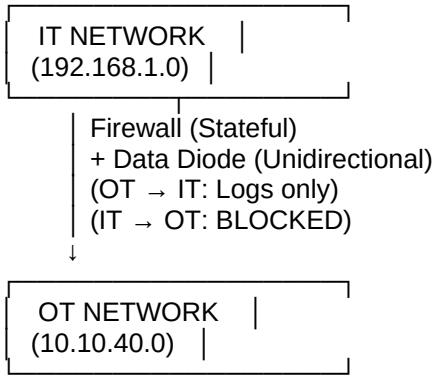
---

10. SEGURTASUN NEURRIAK (RGPD Art. 32)

10.1 Neurri Teknikoak

10.1.1 Segregazioa IT/OT

Diseinua:



Arauak: - ❌ Ez dago sarbide IT-tik OT-ra (inbound blocked) - ✅ OT-tik IT-ra: Log shipping bakarrik (unidirectional) - ✅ Firewall: Palo Alto PA-220 (industrial-grade)

10.1.2 PLC Segurtasuna

Neurria	Inplementazioa
Password aldaketa	✅ Default “admin/admin” aldatu
Firmware updates	✅ Quarterly (Siemens patches)
Physical security	✅ PLC gabinete giltzaduna
Network segmentation	✅ VLAN separatua PLC bakoitzeko
Access control	✅ SCADA HMI bakarrik (ez Ethernet direkta)

10.1.3 SCADA HMI Hardening

Neurria	Inplementazioa
Windows hardening	✅ CIS Benchmark Level 2
Antivirus	✅ Kaspersky Industrial CyberSecurity
Application whitelisting	✅ WinCC bakarrik, beste guztiak blokeatuta
USB disabled	✅ BIOS + GPO
Automatic updates	⚠️ Delayed (test environment lehenengo)

10.1.4 IP Kamerak Segurtasuna

Neurria	Inplementazioa
Password aldaketa	✅ Default “root/pass” aldatu
Firmware updates	✅ Quarterly
HTTPS	✅ TLS 1.3 (HTTP disabled)
VLAN separatua	✅ Kamerak isolatu
Access control	✅ VPN + user/password

10.2 Neurri Organisatoriak

10.2.1 Politikak

- ✅ /compliance/sgsi/information_security_policy.md
- ✅ /infrastructure/ot/sop_ot_security.md
- ✅ /security/mobile_security_sop.md (badge system)

10.2.2 Formazioa

Programa	Maiztasuna	Audience
OT Security Awareness	Urtero	Operarioak, Mantenimendu
Privacy & Biometrics	Onboarding	Operario berria
Incident Response (OT)	Bi-urteko	Jefe Turno, Operations

---

11. PRIVACY BY DESIGN ETA BY DEFAULT

11.1 Diseinuan Pribatutasuna (Art. 25.1)

✅ **Inplementatua:**

1. **Data Minimization:**
   - Badge ID erabiltzea log-etan, EZ izen-abizenak
   - IP kamerak: Ez face recognition (ez beharrezkoa)
2. **Pseudonimization:**
   - Badge ID: Zenbaki bat, ez langilearen izena
   - Batch log-ak: “User 001234”, ez “Iker Zabala”
3. **Encryption:**
   - Biometria: Hash (SHA-256) + AES-256 storage
   - IP kamerak backup: E2EE (GPG)
4. **Access Control:**
   - RBAC + Least Privilege
   - Segregation of Duties (Ops ≠ DPO)
5. **Logging:**
   - Audit trail (sarbidea, aldaketak)

11.2 Lehenespenik Pribatutasuna (Art. 25.2)

✅ **Inplementatua:**

1. **Biometria Opt-in:**
   - Lehenetsita: Badge + PIN
   - Biometria: Opt-in (explicitu baimena)
2. **IP Kamerak Retention:**
   - Lehenetsita: 30 egun (ez 90 egun)
   - Auto-delete (ez manual)
3. **Privacy Zones:**
   - Jangelak, WCs: Blurred (ez grabatu)
4. **Access Restrictions:**
   - Operarioak ez dute sarbide IP kamera grabaketetara

---

12. CONSULTATIONS ETA AHOLKULARITZA

12.1 Barneko Stakeholders

Kontsultatuak (DPIA garapena): - ✅ Operations Director (Koldo Agirre) - 2026-01-25 - ✅ CISO (Mikel Etxebarria) - 2026-01-26 - ✅ Jefe Turno x3 (Operarioak ordezkari) - 2026-01-27 - ✅ Mantenimendu Team Lead - 2026-01-28 - ✅ Legal Advisor (Itziar Sarasola) - 2026-01-29 - ✅ Komitea Sindikalki (langile ordezkari) - 2026-01-30 - ✅ CEO (Jon Zabala) - 2026-02-01

Feedback Integratua: - Operations: Badge + PIN alternatibo (onartua) - Operarioak: Privacy zones jangeletan (inplementatua) - Sindikalki: 30 egun retention bakarrik (onartua) - CISO: IT/OT segregazioa data diode-rekin (planifikatua Q2)

12.2 AEPD Kontsulta Aurretiazko (Art. 36)

❌ **Ez beharrezkoa:** - DPIA honek arrisku altua identifikatu du (biometria) - Baina neurriak ezarrita, arrisku baxua da - RGPD Art. 36.3(b): Neurriak arriskua efectibo murrizten du

✅ **Kontsulta egingo litzateke baldin:** - Biometria face recognition (ez fingerprint bakarrik) - Kamerak > 100 (ez 12) - Retention > 90 egun (ez 30)

---

13. EBALUAZIOAREN EMAITZAK ETA GOMENDIOAK

13.1 Laburpena

Arrisku Maila: - Inherentea (Neurririk gabe): **ALTUA** - Gainbeherazkoa (Neurriekin): **BAXUA**

Gomendio Nagusia: ✅ **SISTEMA MANTENU** neurriak aplikatuta

13.2 Ekintza Plana (2026)

Ekintza	Epemuga	Arduraduna	Budget
✅ Privacy Notice poster	2026-01-05	Ops Dir	0€
✅ Biometria opt-out	2026-01-10	Ops Dir	0€
✅ IP kamerak privacy zones	2026-01-12	CISO	0€
✅ NVR auto-delete 30 days	2026-01-15	IT Officer	0€
✅ PLC password aldaketa	2026-01-20	Mantenimendu	0€
✅ DPIA (hau)	2026-02-05	DPO	0€
⏳ IT/OT data diode	2026-04-30	CISO	15k€
⏳ IDS/IPS OT (Nozomi)	2026-06-01	CISO	30k€
⏳ Mantrap ateak	2026-07-01	Ops Dir	8k€
⏳ NVR cloud backup (OVH)	2026-05-15	IT Officer	3k€

Budget Total: 56k€ (2026)

13.3 Berrikusketa

Maiztasuna: Urtero (Otsaila) **Arduraduna:** DPO + Operations Director **Trigger-ak (ad-hoc):** - Biometria teknologia aldaketa (face recognition) - Kamera kopurua aldaketa (> 15) - Data breach edo incident - Araudiaren aldaketa (GDPR, LOPD-GDD)

---

14. ONARPENA ETA SINADURA

Dokumentu hau Compliance Governance Committee-ak onartu du:

Rola	Izena	Sinadura	Data
DPO	Ainhoa Uriarte	_____	2026-02-05
Operations Director	Koldo Agirre	_____	2026-02-05

Rola	Izena	Sinadura	Data
CISO	Mikel Etxebarria	_____	2026-02-05
CEO	Jon Zabala	_____	2026-02-05
Komitea Sindikalki	Ane Larrauri	_____	2026-02-05

ONARPENA: Sistema ONARTUA - Mantenu operazioan neurriak aplikatuz.

HURRENGO BERRIKUSKETA: 2027-02-05

ERANSKINAK

Eranskina A: Network Diagram (IT/OT)

(Ikus sekzioa 1.2)

Eranskina B: Privacy Notice (Poster)

(Kokapena: Fabrika sarrera)

Eranskina C: Biometria Opt-out Form

Template: /compliance/gdpr/biometric_opt_out_form.pdf

Eranskina D: IP Kamerak Map

Kokapena: 12 kamerak mapa fabrikarekin

Eranskina E: Vendor DPA Contracts

- Siemens DPA (sinatu 2025-12-10)
- HID DPA (sinatu 2025-11-15)
- Axis DPA (sinatu 2025-10-20)

DPIA hau sortu da RGPD Art. 35 betebeharrak betetzeko (Biometria + Bideo-Zaintza), Erronka 4 - ZG (Zibersegurtasunaren Arloko Araudia) atalean.