industry_compliance_matrix

Industria Araudi Matrizea

Industry-Specific Compliance Matrix

Enpresa: Zabala Gailetak, S.L. **Dokumentu Kodea:** COMP-MATRIX-001 **Bertsioa:** 1.0 **Data:** 2026-02-05 **Jabea:** Legal Advisor + CISO **Egoera:** Indarrean

---

1. XEDEA ETA IRISMENA

1.1 Helburua

Dokumentu honek ezartzen du **araudia eta estandar aplikagarriak** industria mota desberdinetarako, gomendioak eta **best practices** emanda.

Helburu Espezifikoak: 1. ✅ Araudia mapeatzea industria sektore bakoitzerako 2. ✅ Gomendioak eman enpresa mota desberdinetarako 3. ✅ Compliance roadmap bat proposatzea 4. ✅ Kostu estimazioak ematea

1.2 Irismena

Sektoreak Aztertuak: - ✅ Elikagai Fabrikazioa (Zabala Gailetak - gure kasua) - ✅ Farmazioak (Guenaga Pharma - Erronka taldeko enpresa) - ✅ Upategiak (Kortabitarte - Erronka taldeko enpresa) - ✅ Medikuntza Industria (Unanue Hortz Sintetikoak - Erronka taldeko enpresa) - ✅ Finantza Zerbitzuak (referentzia) - ✅ Osasun Zerbitzuak (referentzia) - ✅ Industria Kritikoak (OT-heavy) (referentzia)

---

2. ELIKAGAI FABRIKAZIOA (Zabala Gailetak)

2.1 Ezaugarriak

Enpresa Profila: - Jarduera: Galletas eta txokolateak ekoiztu, saldu, banatu - Langileak: 120 (6 gerentzia, 10 admin, 5 IKT, 12 ikerketa, 87 ekoizpena) - Kokapena: Euskal Herria (Europa) - Merkatua: Nazionala + Europa Batasuna (B2B + B2C)

IT/OT Sistema: - IT: ERP, Portal RRHH, E-commerce web, Mobile app - OT: SCADA, PLCs (6x Siemens S7-1500), Sentsore, Robotika

2.2 Araudia Aplikagarria

2.2.1 Araudia KRITIKOA (Nahitaezkoa)

Araudia	Mota	Aplikagarritasuna	Prioritasuna
GDPR (EU 2016/679)	Reglamento	100% (Langileak + bezeroak)	**P0 - KRITIKAL**

Araudia	Mota	Aplikagarritasuna	Prioritasuna
LOPD-GDD (LO 3/2018)	Lege Organikoa	100% (Espainia)	**P0 - KRITIKAL**
Reg (EC) 178/2002 (Food Law)	Reglamento	100% (Elikagai fabrikante)	**P0 - KRITIKAL**
Reg (EC) 852/2004 (Hygiene)	Reglamento	100% (Fabrikazioa)	**P0 - KRITIKAL**
Reg (EU) 1169/2011 (Labeling)	Reglamento	100% (Produktu etiketak)	**P0 - KRITIKAL**
HACCP	Sistema	100% (Kalitate + segurtasun)	**P0 - KRITIKAL**
ENS (RD 311/2022)	Real Decreto	Gomendio (IT > 50 langileak)	**P1 - ALTUA**
NIS2 (EU 2022/2555)	Direktiba	Gomendio (>50 langile + food)	**P1 - ALTUA**

2.2.2 Estandar Profesionalak (Gomendioa)

Estandarra	Aplikagarritasuna	Onura	Prioritasuna
ISO 22000 (Food Safety)	100%	Bezeroen konfiantza, auditoriak	**P1 - ALTUA**
FSSC 22000	90%	Ziurtagiria (GFSI)	**P1 - ALTUA**
BRC Global Standard	80%	UK/EU merkatua	**P2 - ERTAINA**
IFS Food	70%	Alemania/Frantzia	**P2 - ERTAINA**
ISO 27001 (Security)	100%	Ziber-segurtasuna	**P1 - ALTUA**
IEC 62443 (OT Security)	100%	SCADA/PLC segurtasuna	**P1 - ALTUA**
ISO 22301 (BCP)	Gomendio	Business continuity	**P2 - ERTAINA**

2.3 Gomendioak Zabala Gailetak-entzat

2.3.1 GDPR + LOPD-GDD

Status: ✅ INPLEMENTATUA (92%)

Neurri Nagusiak: - ✅ DPO izendatu (Ainhoa Uriarte) - ✅ Privacy Notice (web + langileak) - ✅ DPIA (Portal RRHH + SCADA/OT) - ✅ Data Retention Schedule - ✅ ARCO Prozedura - ⏳ Formakuntza (Q1 2026)

Budget: 0€ (indarrean)

2.3.2 Food Safety (HACCP + ISO 22000)

Status: ⏳ HACCP inplementatua, ISO 22000 planifikatua

Neurri Nagusiak: - ✅ HACCP plana (7 printzipioak) - ✅ Trazabilitateasen (batch tracking) - ✅

Supplier management - ⏳ ISO 22000 ziurtagiria (2026-2027)

Budget: 25.000€ (ziurtagiria + consultancy)

Gomendio: ISO 22000 lortzea da prioritate altua bezero korporatiboentzat (B2B)

2.3.3 Ziber-Segurtasuna (ISO 27001 + IEC 62443)

Status: ⏳ PLANIFIKATUA

Neurri Nagusiak: - ⏳ ISO 27001 ziurtagiria (2026-2027) - ⏳ IEC 62443 aplikazioa OT-rako (2026-2027) - ✅ SGSI dokumentazioa (90% osatua) - ⏳ Audit teknikoa (Q2 2026)

Budget: 60.000€ (ziurtagiria + audit + consultancy)

Gomendio: ISO 27001 da kritikoa E-commerce webgunearentzat (bezero datuak)

2.3.4 NIS2 Directive

Status: ⏳ GAP ANALYSIS

Aplikagarritasuna: Gomendio altua (>50 langile + elikagai)

Neurri Nagusiak: - ⏳ Risk management framework - ⏳ Incident notification procedure (24h) - ⏳ Supply chain security assessment - ⏳ Cyber hygiene measures (MFA 100%, EDR, …)

Budget: 85.000€ (ikus /compliance/nis2_implementation_plan.md)

Gomendio: NIS2 transposizioa 2024ko Urrian, aplikazioa 2026an

2.4 Compliance Roadmap (Zabala Gailetak)

2026 Q1: ✅ GDPR + LOPD-GDD (inplementatua)
✅ HACCP (inplementatua)
⏳ ISO 27001 prep (gap analysis)

2026 Q2: ⏳ ISO 27001 audit Stage 1
⏳ IEC 62443 OT assessment
⏳ NIS2 gap analysis

2026 Q3: ⏳ ISO 27001 audit Stage 2 → Ziurtagiria
⏳ NIS2 implementation start

2026 Q4: ⏳ ISO 22000 prep (gap analysis)
⏳ NIS2 compliance (deadline: Oct 2026)

2027 Q1: ⏳ ISO 22000 audit → Ziurtagiria
⏳ IEC 62443 compliance review

2027 Q2: ⏳ FSSC 22000 certification (optional)

2.5 Kostu Estimazioa (Zabala Gailetak)

Proiektua	Budget	Timeline
GDPR compliance	0€ (indarrean)	-
ISO 27001	60.000€	2026-2027

Proiektua	Budget	Timeline
IEC 62443	40.000€	2026-2027
NIS2	85.000€	2026
ISO 22000	25.000€	2027
FSSC 22000 (opt)	15.000€	2027 (opt)
TOTALA (2026-2027)	**225.000€**	2 urteak

---

3. FARMAZIOAK (Guenaga Farmazeutika)

3.1 Ezaugarriak

Enpresa Profila: - Jarduera: Farmazia-banaketa - Langileak: 50 (5 gerentzia, 3 admin, 4 IKT, 12 ikertzaile, 26 ekoizpena) - Kokapena: Espainia (Europa talde batekoa) - Merkatua: Europako farmaziak (B2B)

IT/OT Sistema: - IT: ERP (stock automatiko), Web E-commerce, Mobile app - OT: Robotika (zerbitzatu automatikoa), Inbentario sistema

3.2 Araudia Aplikagarria

3.2.1 Araudia KRITIKOA

Araudia	Mota	Aplikagarritasuna	Prioritasuna
GDPR	Reglamento	100% (Paziente datuak!)	**P0 - KRITIKAL**
LOPD-GDD	Lege Organikoa	100%	**P0 - KRITIKAL**
Reg (EU) 2016/161 (Falsified Medicines)	Reglamento	100%	**P0 - KRITIKAL**
Reg (EC) 726/2004 (Medicinal Products)	Reglamento	100%	**P0 - KRITIKAL**
GDP (Good Distribution Practice)	Gida	100%	**P0 - KRITIKAL**
NIS2 (EU 2022/2555)	Direktiba	**100% (Kritikoa!)**	**P0 - KRITIKAL**
ENS (RD 311/2022)	Real Decreto	ALTUA (datu sentsibleak)	**P0 - KRITIKAL**

OHARRAK: - Farmazioak NIS2-ren **Entitate Essentiala** dira (Art. 3) - GDPR Art. 9: Osasun datuak (kategoria berezia) - Isun arriskua oso altua (osasun publikoa)

3.2.2 Estandar Profesionalak

Estandarra	Aplikagarritasuna	Onura	Prioritasuna
ISO 27001	100%	NAHITAEZKOA (osasun datuak)	**P0 - KRITIKAL**
ISO 13485 (Medical Devices)	Baldin medical devices	Ziurtagiria	**P1 - ALTUA**
ISO 22301 (BCP)	100%	Business continuity	**P1 - ALTUA**
IEC 62443 (OT)	100%	Robotika segurtasuna	**P1 - ALTUA**
NIST CSF	Gomendio	Ziber-segurtasuna framework	**P2 - ERTAINA**

3.3 Gomendioak Farmaziako

3.3.1 GDPR + Osasun Datuak

Status: KRITIKAL - BEREHALA

Neurri Nagusiak: - ✅ DPO izendatu (OBLIGATORIO Art. 37) - ✅ DPIA (osasun datuak) - NAHITAEZKOA (Art. 35) - ✅ Data Processing Agreement (DPA) zerbitzari guztiekin - ✅ Encryption at rest + in transit (osasun datuak) - ✅ Audit log (tamper-proof) - ✅ Access control (RBAC + MFA 100%)

Budget: 100.000€ (consultancy + teknologia)

Gomendio: GDPR urraketa farmaziako = Isun OSO ALTUA (>2M €)

3.3.2 NIS2 Directive

Status: OBLIGATORIO - DEADLINE 2026-10-17

Neurri Nagusiak: - ✅ CISO izendatu (OBLIGATORIO) - ✅ Risk management framework (ISO 27005) - ✅ Incident notification (24h alerta, 72h txosten) - ✅ Supply chain security (vendor assessment) - ✅ Security operations center (SOC 24/7) - ✅ Cyber hygiene (patching, MFA, EDR, SIEM)

Budget: 250.000€ (teknologia + SOC outsourcing)

Gomendio: NIS2 ez betetzea = Isun 10M € arte

3.3.3 ISO 27001 + ISO 22301

Status: KRITIKAL

Gomendio: ISO 27001 ziurtagiria **NAHITAEZKOA** farmaziako

Budget: 80.000€ (ISO 27001 + ISO 22301)

3.4 Compliance Roadmap (Farmaziako)

2026 Q1: ⚠️ GDPR osasun datuak (EMERGENCY)
⚠️ NIS2 gap analysis (BEREHALA)

2026 Q2: ⏳ ISO 27001 audit Stage 1
⏳ NIS2 implementation
⏳ SOC 24/7 setup

2026 Q3: ⏳ NIS2 compliance (deadline approaching!)
⏳ ISO 27001 audit Stage 2

2026 Q4: ✅ NIS2 compliance (DEADLINE Oct)
✅ ISO 27001 ziurtagiria

2027 Q1: ⏳ ISO 22301 (BCP) ziurtagiria
⏳ ISO 13485 (if medical devices)

3.5 Kostu Estimazioa (Farmaziako)

Proiektua	Budget	Prioritasuna
GDPR (osasun datuak)	100.000€	**P0 - KRITIKAL**
NIS2	250.000€	**P0 - KRITIKAL**
ISO 27001	80.000€	**P0 - KRITIKAL**
ISO 22301	40.000€	**P1 - ALTUA**
IEC 62443 (OT)	50.000€	**P1 - ALTUA**
TOTALA (2026)	**520.000€**	-

KRITIKOA: Farmaziako compliance kostu oso altua da osasun datuak + NIS2

---

4. UPATEGIAK (Kortabitarte)

4.1 Ezaugarriak

Enpresa Profila: - Jarduera: Ardoa ekoiztu eta esportatu - Langileak: 65 (5 gerentzia, 4 admin, 5 IKT, 12 enologo, 39 mahastizainak) - Kokapena: Bierzo (Leon) + Ourense - Merkatua: Esportazioak (UK, Europa, Asia)

IT/OT Sistema: - IT: ERP, E-commerce web, Mobile app - OT: Upategi kontrola (tenperatura, humitate), Upelak monitorizazioa

4.2 Araudia Aplikagarria

4.2.1 Araudia KRITIKOA

Araudia	Mota	Aplikagarritasuna	Prioritasuna
GDPR	Reglamento	100%	**P0 - KRITIKAL**
LOPD-GDD	Lege Organikoa	100%	**P0 - KRITIKAL**
Reg (EU) 1308/2013 (Wine)	Reglamento	100%	**P0 - KRITIKAL**

Araudia	Mota	Aplikagarritasuna	Prioritasuna
Reg (EC) 606/2009 (Wine production)	Reglamento	100%	**P0 - KRITIKAL**
Organic Regulation (EU 2018/848)	Reglamento (if organic)	Baldin organic	**P1 - ALTUA**
ENS (RD 311/2022)	Real Decreto	Gomendio	**P2 - ERTAINA**

4.2.2 Estandar Profesionalak

Estandarra	Aplikagarritasuna	Onura	Prioritasuna
ISO 22000 (Food Safety)	80%	Esportazioak	**P1 - ALTUA**
IFS Food	70% (if EU export)	Alemanian, Frantzia	**P1 - ALTUA**
BRC	60% (if UK export)	UK merkatua	**P1 - ALTUA**
ISO 27001	Gomendio	E-commerce segurtasuna	**P2 - ERTAINA**
IEC 62443 (OT)	Gomendio	Upategi automatizazioa	**P3 - BAXUA**

4.3 Gomendioak Upategientzat

4.3.1 GDPR

Status: ⏳ INPLEMENTATU BEHAR

Neurri Nagusiak: - ✅ DPO izendatu (gomendio) - ✅ Privacy Notice (web + bezeroak) - ✅ Cookie Policy (E-commerce) - ✅ ARCO Prozedura - ⏳ DPIA (baldin tratamendu masibo)

Budget: 20.000€ (consultancy)

4.3.2 Export Compliance (IFS, BRC)

Status: PRIORITATE ALTUA (esportazioetarako)

Gomendio: UK esportatzeko, BRC ziurtagiria **NAHITAEZKOA**

Budget: - IFS Food: 25.000€ - BRC: 30.000€

4.3.3 Ziber-Segurtasuna

Status: BAXUA (ez kritikal)

Gomendio: ISO 27001 ez da nahitaezkoa, baina gomendio E-commerce-rako

Budget: 50.000€ (baldin nahi bada)

4.4 Compliance Roadmap (Upategiak)

2026 Q1: ✅ GDPR compliance

⏳ IFS Food prep

2026 Q2: ⏳ IFS Food audit
⏳ BRC prep (if UK export)

2026 Q3: ⏳ BRC audit
⏳ ISO 22000 (optional)

2026 Q4: ✅ Ziurtagiriak osatu
⏳ E-commerce security review

4.5 Kostu Estimazioa (Upategiak)

Proiektua	Budget	Prioritasuna
GDPR	20.000€	**P0 - KRITIKAL**
IFS Food	25.000€	**P1 - ALTUA**
BRC (if UK)	30.000€	**P1 - ALTUA**
ISO 27001 (opt)	50.000€	**P2 - ERTAINA**
TOTALA (2026)	**125.000€**	-

---

5. MEDIKUNTZA INDUSTRIA (Unanue Hortz Sintetikoak)

5.1 Ezaugarriak

Enpresa Profila: - Jarduera: Hortz sintetikoak diseinatu, ekoiztu, banatu (Europa) - Langileak: 55 (5 gerentzia, 12 admin, 8 IKT, 10 ikerketa, 10 diseinua, 10 ekoizpena) - Kokapena: Euskal Herria - Merkatua: Hortz klinikak (Europa)

IT/OT Sistema: - IT: ERP berria, 3D diseinua softwarea, Trazabilitateasen sistema - OT: Mekanizazio makinak (CNC), Kalitate kontrol

5.2 Araudia Aplikagarria

5.2.1 Araudia KRITIKOA

Araudia	Mota	Aplikagarritasuna	Prioritasuna
GDPR	Reglamento	100% (Paziente datuak!)	**P0 - KRITIKAL**
LOPD-GDD	Lege Organikoa	100%	**P0 - KRITIKAL**
MDR (EU 2017/745) (Medical Devices)	Reglamento	100%	**P0 - KRITIKAL**
ISO 13485	Estandar	**OBLIGATORIO (MDR)**	**P0 - KRITIKAL**
EN ISO 14971 (Risk Management)	Estandar	OBLIGATORIO	**P0 - KRITIKAL**
NIS2 (baldin digital)	Direktiba	Gomendio altua	**P1 - ALTUA**

Araudia	Mota	Aplikagarritasuna	Prioritasuna
ENS	Real Decreto	ALTUA (osasun datuak)	**P1 - ALTUA**

OHARRAK: - Medical Devices Regulation (MDR) **oso zorrotza** da - Hortz sintetikoak = Class IIa Medical Device - ISO 13485 ziurtagiria OBLIGATORIO da MDR-rako - Trazabilitateasen 10-15 urtean OBLIGATORIO

5.2.2 Estandar Profesionalak

Estandarra	Aplikagarritasuna	Onura	Prioritasuna
ISO 27001	100%	Osasun datuak + diseinuak	**P0 - KRITIKAL**
ISO 9001 (Quality)	100%	Kalitate kudeaketa	**P1 - ALTUA**
ISO 22301 (BCP)	Gomendio	Continuity (trazabilitateasen)	**P2 - ERTAINA**
IEC 62443 (OT)	Gomendio	CNC segurtasuna	**P2 - ERTAINA**

5.3 Gomendioak Medikuntza Industriarako

5.3.1 MDR + ISO 13485

Status: KRITIKAL - SIN ESTO EZ DA LEGALA

Neurri Nagusiak: - ✅ ISO 13485 Quality Management System - ✅ Technical File (Technical Documentation) - ✅ Risk Management (ISO 14971) - ✅ Post-Market Surveillance - ✅ Notified Body audit (TÜV, BSI, …) - ✅ CE Marking

Budget: 150.000€ (consultancy + Notified Body + ziurtagiria)

Timeline: 12-18 hileak

Gomendio: Hau da LEHENTASUNA ABSOLUTOA

5.3.2 GDPR + Osasun Datuak

Status: KRITIKAL

Neurri Nagusiak: - ✅ DPO izendatu (OBLIGATORIO) - ✅ DPIA (3D diseinuak + paziente datuak) - ✅ Encryption (diseinuak + paziente identifikazioa) - ✅ Access control (RBAC + MFA) - ✅ Trazabilitateasen (10-15 urte gordailua)

Budget: 80.000€

5.3.3 ISO 27001

Status: OBLIGATORIO (praktikan)

Gomendio: Hortz klinikak eskatzen dute ISO 27001 (osasun datuak)

Budget: 70.000€

5.4 Compliance Roadmap (Medikuntza)

2026 Q1: ⚠️ MDR gap analysis (EMERGENCY)
⚠️ ISO 13485 prep (KRITIKAL)

2026 Q2: ⏳ ISO 13485 implementation
⏳ Technical File preparation
⏳ GDPR osasun datuak

2026 Q3: ⏳ ISO 13485 audit Stage 1
⏳ Risk Management (ISO 14971)
⏳ ISO 27001 prep

2026 Q4: ⏳ ISO 13485 audit Stage 2 → Ziurtagiria
⏳ Notified Body submission

2027 Q1: ⏳ Notified Body audit
⏳ ISO 27001 audit

2027 Q2: ✅ CE Marking
✅ ISO 27001 ziurtagiria

5.5 Kostu Estimazioa (Medikuntza)

Proiektua	Budget	Prioritasuna
ISO 13485 + MDR	150.000€	**P0 - KRITIKAL**
GDPR (osasun)	80.000€	**P0 - KRITIKAL**
ISO 27001	70.000€	**P0 - KRITIKAL**
ISO 9001	30.000€	**P1 - ALTUA**
ISO 22301 (opt)	40.000€	**P2 - ERTAINA**
TOTALA (2026-2027)	**370.000€**	-

OHARRAK: Medikuntza industria compliance oso garestia da

---

6. FINANTZA ZERBITZUAK (Erreferentzia)

6.1 Araudia Aplikagarria

Araudia	Mota	Aplikagarritasuna
GDPR	Reglamento	100%
PSD2 (EU 2015/2366)	Direktiba	100% (ordainketak)
AMLD5 (EU 2015/849)	Direktiba	100% (money laundering)
MiFID II (if investment)	Direktiba	Baldin inbertsioak
NIS2	Direktiba	**100% (Kritikoa!)**

Araudia	Mota	Aplikagarritasuna
ISO 27001	Estandar	**OBLIGATORIO (praktikan)**
PCI-DSS	Estandar	**OBLIGATORIO (txartelak)**

6.2 Gomendioak

- **ISO 27001:** NAHITAEZKOA finantza sektorean
- **PCI-DSS:** OBLIGATORIO txartel datuak tratatzeko
- **SOC 2 Type II:** Gomendio altua (auditoriak)
- **ISO 22301:** KRITIKAL (business continuity)

Budget Estimazioa: 500.000€ - 1.000.000€ (tamainu handiko entitate)

---

7. OSASUN ZERBITZUAK (Erreferentzia)

7.1 Araudia Aplikagarria

Araudia	Mota	Aplikagarritasuna
GDPR	Reglamento	100% (osasun datuak - Art. 9)
LOPD-GDD	Lege Organikoa	100%
ENS	Real Decreto	**ALTUA kategoría**
NIS2	Direktiba	**100% (Kritikoa!)**
ISO 27001	Estandar	**OBLIGATORIO**
ISO 27799 (Health)	Estandar	Gomendio altua
HL7 FHIR (if digital health)	Estandar	Interoperabilitate

7.2 Gomendioak

- **ENS Kategoria ALTUA:** OBLIGATORIO (datu sentsibleak)
- **ISO 27001 + ISO 27799:** Gomendio oso altua
- **DPIA:** OBLIGATORIO osasun datuak tratatzeko (Art. 35)
- **DPO:** OBLIGATORIO (Art. 37)

Budget Estimazioa: 300.000€ - 800.000€

---

8. INDUSTRIA KRITIKOAK (OT-heavy) (Erreferentzia)

8.1 Araudia Aplikagarria

Araudia	Mota	Aplikagarritasuna
NIS2	Direktiba	**100% (Kritikoa!)**
ENS	Real Decreto	ALTUA kategoría
IEC 62443	Estandar	**OBLIGATORIO (praktikan)**
ISO 27001	Estandar	OBLIGATORIO
NERC CIP (if energy)	Estandar	Energia sektorea

8.2 Gomendioak

- **IEC 62443:** NAHITAEZKOA OT sistemetarako
- **IT/OT Segregazioa:** KRITIKAL (data diode)
- **OT-specific SIEM:** Nozomi Networks, Claroty
- **Incident Response (OT):** Specialized playbook

Budget Estimazioa: 400.000€ - 1.500.000€ (tamainuaren arabera)

---

9. LABURPEN MATRIZEA - INDUSTRIA GUZTIAK

9.1 Araudia Aplikagarritasun Matrizea

Araudia	Elikagai	Farmazioak	Upategiak	Medikuntza	Finantza	Osasuna	OT-heavy
GDPR	✅	✅	✅	✅	✅	✅	✅
NIS2	⚠️	✅	❌	⚠️	✅	✅	✅
ENS	⚠️	✅	❌	⚠️	✅	✅	✅
ISO 27001	⚠️	✅	❌	✅	✅	✅	✅
IEC 62443	⚠️	⚠️	❌	❌	❌	❌	✅
ISO 22000	✅	❌	⚠️	❌	❌	❌	❌
ISO 13485	❌	⚠️	❌	✅	❌	❌	❌
PCI-DSS	❌	❌	❌	❌	✅	❌	❌
MDR	❌	⚠️	❌	✅	❌	⚠️	❌

Legenda: - ✅ OBLIGATORIO edo KRITIKAL - ⚠️ Gomendio altua - ❌ Ez aplikagarria

9.2 Budget Estimazioa Matrizea

Industria	Compliance Budget (2 urteak)	Kritikotasuna
Elikagai	225.000€	ERTAINA
Farmazioak	520.000€	**OSO ALTUA**
Upategiak	125.000€	BAXUA-ERTAINA
Medikuntza	370.000€	**OSO ALTUA**
Finantza	750.000€ (avg)	**OSO ALTUA**
Osasuna	550.000€ (avg)	**OSO ALTUA**
OT-heavy	850.000€ (avg)	**OSO ALTUA**

---

10. GOMENDIO OROKORRAK

10.1 Gomendio Enpresa Txikiak (< 50 langile)

Lehentasunak: 1. ✅ GDPR + LOPD-GDD (OBLIGATORIO) 2. ⚠️ Sector-specific regulations (Food Law, Wine Reg, …) 3. ⚠️ ISO 27001 (baldin E-commerce edo datu sentsibleak) 4. ❌ Ez gastu gehiegi ziurtagiri guztiak (fokuatu kritikoan)

Budget: 50.000€ - 150.000€

10.2 Gomendio Enpresa Ertainak (50-250 langile)

Lehentasunak: 1. ✅ GDPR + Sector regulations (OBLIGATORIO) 2. ✅ ISO 27001 (gomendio oso altua) 3. ⚠️ NIS2 (baldin aplikagarria) 4. ⚠️ IEC 62443 (baldin OT) 5. ⚠️ ISO 22301 (BCP)

Budget: 200.000€ - 500.000€

10.3 Gomendio Enpresa Handiak (> 250 langile)

Lehentasunak: 1. ✅ GDPR + Sector regulations (OBLIGATORIO) 2. ✅ ISO 27001 (OBLIGATORIO) 3. ✅ NIS2 (baldin aplikagarria) 4. ✅ IEC 62443 (baldin OT) 5. ✅ ISO 22301 (BCP) 6. ✅ SOC 24/7

Budget: 500.000€ - 2.000.000€

---

11. ERREFERENTZIAK

11.1 Araudia Iturriak

- **GDPR:** https://eur-lex.europa.eu/eli/reg/2016/679/oj
- **NIS2:** https://eur-lex.europa.eu/eli/dir/2022/2555/oj
- **MDR:** https://eur-lex.europa.eu/eli/reg/2017/745/oj

- **Food Law:** https://eur-lex.europa.eu/eli/reg/2002/178/oj

11.2 Estandar Iturriak

- **ISO:** https://www.iso.org
- **IEC:** https://www.iec.ch
- **AENOR:** https://www.aenor.com

11.3 Barneko Dokumentuak

- /compliance/compliance_governance_framework.md
- /compliance/regulatory_monitoring_procedure.md
- /compliance/sgsi/information_security_policy.md

---

12. BERRIKUSKETA ETA EGUNERAKETA

Berrikusketa Maiztasuna: Urtero (Ekaina) **Arduraduna:** Legal Advisor + CISO **Onarpena:** CGC

12.1 Aldaketa Log-a

Bertsioa	Data	Aldaketak	Egilea
1.0	2026-02-05	Dokumentu initial	Legal + CISO

HURRENGO BERRIKUSKETA: 2027-06-30

Dokumentu hau sortu da RA2 (Diseño de Sistemas de Cumplimiento) betebeharrak betetzeko, Erronka 4 - ZG (Zibersegurtasunaren Arloko Araudia) atalean.