ZABALA GAILETAK

S.L. - Dokumentazio Akademikoa

Zibersegurtasunaren Arloko Araudia

2026(e)ko otsailaren 23(a)

MODULUA 06 — ZIBERSEGURTASUNAREN ARLOKO ARAUDIA

Proiektua: ER4 — Zabala Gailetak S.L. Zibersegurtasun Proiektua **Modulua:** 06 — Zibersegurtasunaren Arloko Araudia (Compliance) **Ikaslea:** Zabala Gailetak Taldea **Data:** 2025 **Bertsioa:** 1.0 **Egoera:** Osatua

AURKIBIDEA

1. Sarrera eta Testuingurua

1.1 Moduluaren Deskribapena

Modulu honek Zabala Gailetak S.L.-ren **Zibersegurtasunaren Arloko Araudia** betetzea dokumentatzen du. Enpresak aplikagarriak diren araudi guztiak identifikatu, inplementatu eta jarraitu egin ditu, **%100eko betetzea** lortuz ER4 proiektuan.

1.2 Enpresaren Profila — Araudi Testuingurua

Parametro	Balioa
Enpresa	Zabala Gailetak S.L.
Sektorea	Elikagai fabrikazioa (gaileta eta txokolatea)
Langile kopurua	120
Merkatua	Espainia + Europar Batasuna (online salmenta)
Teknologia	IT + OT (PLCak, SCADA, HMIak)
Datu kategoriak	Langile datuak, bezero datuak, ekoizpen datuak
NIS2 Klasifikazioa	"Garrantzitsua" (Important Entity) — elikagai sektorea

1.3 Araudi Mapa — Zabala Gailetak-eri Aplikagarriak

```
┌──────────────────────────────────────────────────────────────────┐
│            ARAUDI ESPARRU — ZABALA GAILETAK S.L.                 │
├──────────────────────┬───────────────────────────────────────────┤
│  EUROPAR BATASUNA    │  ESPAINIA                                 │
│                      │                                           │
│  ✅ GDPR 2016/679    │  ✅ LOPD-GDD (LO 3/2018)                  │
│  ✅ NIS2 2022/255    │  ✅ ENS (RD 311/2022)                     │
│  ✅ ePrivacy Dir.    │  ✅ Zigor Kodea 197. art.                 │
│                      │  ✅ Langileen Estatutua                   │
├──────────────────────┴───────────────────────────────────────────┤
│  NAZIOARTEKO ESTANDARRAK                                         │
│                                                                  │
│  ✅ ISO/IEC 27001:2022  — SGSI (Informazioaren Segurtasuna)      │
│  ✅ ISO/IEC 27035       — Intzidentzia Kudeaketa                 │
│  ⏳ IEC 62443           — OT/ICS Segurtasuna                     │
│  ✅ ISO 22301           — Negozio Jarraitutasuna                 │
│  ✅ NIST SP 800-61r2    — Intzidentzia Erantzuna                 │
├──────────────────────────────────────────────────────────────────┤
│  INDUSTRIA ESPEZIFIKOAK                                          │
│                                                                  │
│  ✅ OWASP Top 10        — Web aplikazio segurtasuna              │
│  ✅ OWASP Mobile Top 10 — Mugikor segurtasuna                    │
│  ⏳ ISO 22000           — Elikagai Segurtasuna                   │
│  ✅ MAGERIT v3          — Arrisku Metodologia                    │
└──────────────────────────────────────────────────────────────────┘
```

1.4 Betetzeko Erantzukizunak (RACI Matrizea)

Erantzukizuna	CEO	CISO	DPO	IT	OT	Legal
Araudi identifikazioa	C	R	C	I	I	C
Politika onarpena	A	R	C	I	I	C
Inplementazio teknikoa	I	A	I	R	R	I
GDPR betetzea	I	C	R	C	I	C

Erantzukizuna	CEO	CISO	DPO	IT	OT	Legal
NIS2 jakinarazpena	A	R	C	I	I	C
IEC 62443 OT	I	A	I	C	R	I
Auditoria	A	R	C	C	C	I
Prestakuntza	I	R	C	C	C	I

R=Erantzulea, A=Arduraduna, C=Kontsultatua, I=Informatua

2. Araudia Berrikusteko Sistema

2.1 Araudia Monitorizazio Prozedura

Zabala Gailetak-ek araudi aldaketak jarraitzeko **formal prozedura** du:

```
ARAUDIA BERRIKUSTEKO ZIKLOA:

DETEKZIOA (Etengabea)
    ↓
PRIORITIZAZIOA (Astero)
    ↓
INPAKTU ANALISIA (Hilero)
    ↓
ERANTZUN PLANA (Hiruhilero)
    ↓
INPLEMENTAZIOA (Araberako epeak)
    ↓
EGIAZTAPENA (Auditoria)
```

2.2 Araudia Iturri Juridikoak

Iturria	URL/Kanal	Maiztasuna	Arduraduna
BOE (Espainiako Of. Aldizkaria)	boe.es	Egunero (RSS)	Legal
AEPD (Datu Babeserako Agentzia)	aepd.es	Astero	DPO
EUR-Lex (Europako Legedia)	eur-lex.europa.eu	Astero	Legal
CCN-CERT	ccn-cert.cni.es	Egunero	CISO
ENISA	enisa.europa.eu	Hilero	CISO
ISO Estandarrak	iso.org	Urtero	CISO
IEC Estandarrak	iec.ch	Urtero	OT Arduraduna

2.3 Araudi Aldaketa Ebaluazio Matrizea

Kritikotasun Maila	Deskribapena	Erantzun Epea	Approbazio
Maila 5 — Kritikoa	Araudi berria edo aldaketa nagusia	30 egun	CEO + Legal
Maila 4 — Altua	Araudi aldaketa garrantzitsua	60 egun	CISO + Legal
Maila 3 — Ertaina	Gidalerroak edo arauak	90 egun	CISO
Maila 2 — Baxua	Argibideak edo interpretazioak	180 egun	CISO
Maila 1 — Informazioa	Estatistikak edo ikerketak	Ez da beharrezkoa	—

2.4 Urteko Araudi Egutegia

Hila	Jarduera	Arduraduna
Urtarrila	ISO 27001 SOA berrikuspena	CISO
Otsaila	GDPR ROPA berrikuspena	DPO
Martxoa	NIS2 kontrolen ebaluazioa	CISO
Apirila	Barne auditoria	CISO + IT
Ekaina	Langile prestakuntza berrikuspena	HR + CISO
Uztaila	SOA berrikuspena (6 hilabete)	CISO
Iraila	Arriskuen ebaluazio berrikuspena	CISO
Urria	NIS2 NIS-BETE erabakigune (okt. 17)	Legal + CISO
Azaroa	ISO 27001 kanpo auditoria	CISO
Abendua	Zuzendaritza berrikuspena	CEO + CISO

3. GDPR — Datuen Babeserako Erregelamendu Orokorra

3.1 GDPR Esparrua — Zabala Gailetak

Zabala Gailetak-ek **GDPR (EB 2016/679)** eta **LOPD-GDD (Espainiako LO 3/2018)** betetzen ditu. **14 dokumentu** sortu dira, guztira **%100eko betetzea** lortuz.

3.1.1 Datuen Babeserako Ordezkaria (DPO)

```
DPO Izendapena:
  Izen:          Ainhoa Uriarte [Aholkulari Independente]
  Erregistro:    DPO-ES-2025-XXXXX (AEPD erregistroa)
  Email:         dpo@zabala-gailetak.eus
  Ardura:        GDPR Art. 37-39 betebeharrak

GDPR Art. 37 — DPO Izendapenaren Derrigortasuna:
  Zabala Gailetak OT sistemekin produkzio datuak tratatzen ditu
  eta langile-datu masiboak (120 pertsona) kudeatzen ditu.
  → DPO izendatzea derrigorrezkoa.
```

3.1.2 GDPR Printzipioak — Betetze Egoera

GDPR Printzipioa	Artikulua	Neurria	Egoera
Legetasuna, Bidezko tratamendua, Gardentasuna	5(1)(a)	Pribatutasun oharra, baimena	✅
Helburuaren mugatzea	5(1)(b)	ROPA, tratamendu oinarriak	✅
Datu minimizazioa	5(1)(c)	Forensikako datu minimoa	✅
Zehaztasuna	5(1)(d)	Datuak eguneratze prozedurak	✅
Biltegi mugatzea	5(1)(e)	Datu atxikipen egutegia	✅
Osotasuna eta Konfidentzialtasuna	5(1)(f)	AES-256, TLS 1.3, RBAC	✅

GDPR Printzipioa	Artikulua	Neurria	Egoera
Erantzukizuna (Accountability)	5(2)	ROPA, auditoretza, DPO	✅

3.2 Tratamendu Jardueren Erregistroa (ROPA)

GDPR Art. 30 — Tratamendu Jarduera Nagusiak:

#	Jarduera	Helburua	Oinarri Juridikoa	Datu Kategoriak	Atxikipen Epea
A	**Bezero Kudeaketa**	Eskaerak, fakturazioa, bidalketak, fidelizazioa	Kontratua (Art. 6.1.b)	Izen, helbidea, email, telefono, erosketa historia, banku datuak	Harreman + 5 urte (Merkantil Kodea)
B	**Giza Baliabideak**	Nominak, kontratuak, LAP prebentzioa	Kontratua + Legea (6.1.b, 6.1.c)	NAN/NIE, GS zenbakia, banku kontua, baja medikoak	4 urte (Langileen Estatutua)
C	**Bideo-Zaintza**	Instalazio segurtasuna (fabrika, bulegoak)	Interes legitimoa (Art. 6.1.f)	Irudiak (kamera)	30 egun (LOPD-GDD)
D	**HR Ataria (GG)**	Langile kudeaketa, fitxak, baimenak	Kontratua + Legea (6.1.b, 6.1.c)	NIF, IBAN, nominak, TOTP gakoak	4 urte
E	**IT/SIEM Logak**	Segurtasun monitorizazioa	Interes legitimoa (Art. 6.1.f)	IP helbirideak, saio-hasiera datuak	1 urte (2 urte sistema kritikoetan)

3.3 Interesdun Eskubideen Prozedurak

GDPR Art. 15-22 — Eskubideak eta Erantzun Epeak:

ESKUBIDE PROZEDURAK — ZABALA GAILETAK

Kanal: privacy@zabala-gailetak.eus
Epea: 30 egun (gehienez 90 egun kasu konplexuetan)

ESKUBIDE MOTAK:
═══

Art. 15 — Sarbidea:
  → Tratamendu kopia eskatu → 30 egunetan erantzun

Art. 16 — Zuzenketa:
  → Datu okerrak zuzendu → HR Ataritik ere posible

Art. 17 — Ezabatzea (Ahaztua izateko eskubidea):
  → Legezko betebeharrak bete ondoren ezabatu
  → SQL: DELETE FROM employees WHERE id=? AND retention_ok

Art. 18 — Tratamenduaren mugatzea:
  → Eztabaida/aurkaritza garaian mugatu

Art. 20 — Eramangarritasuna:
  → JSON/CSV formatuan eskatu

Art. 21 — Aurkaritza:
  → Interes legitimoa erabiltzen bada → ezarri

Art. 22 — Erabaki automatizatuak:
  → Giza esku-hartzea eskatu
═══

3.4 Datu Urraketa Jakinarazpen Prozedura (Art. 33-34)

```
GDPR ART. 33/34 — DATU URRAKETA WORKFLOW:

INTZIDENTZIA DETEKTATU
        |
        ▼
[1] Urraketa baliozkotzea (CSIRT + DPO)
        |
    ┌───┴──────────────────────┐
    |                          |
Bai: Datu pertsonalak       Ez: Erregistratu,
arriskuan                   ez jakinarazteko
        |
        ▼
[2] Arrisku ebaluazioa (DPO)
  → Baxua/Ertaina: AEPD jakinarazpena (Art. 33)
  → Altua: AEPD + Interesdunak (Art. 33 + 34)
        |
        ▼
[3] 72 ordu barruan — AEPD jakinarazpena
  Bidea: sedeagpd.gob.es
  Inprimakia: Datu Urraketa Jakinarazpen Formularioa
        |
        ▼
[4] Arrisku ALTUA bada — Interesdunak jakinaraztu (Art. 34)
  Kanal: Email + Web portal
  Edukia: Zer gertatu zen, zer neurri hartu
        |
        ▼
[5] Dokumentazioa (GDPR Art. 33.5)
  → Erregistroa: data, mota, eragina, neurriak
  → Mantentze denbora: 5 urte
```

3.5 DPIA — Datuen Babesaren Eragin Ebaluazioa

GDPR Art. 35 — Arrisku Altuko Tratamenduak — 2 DPIA osatuta:

DPIA	Sistema	Hasierako Arrisku	Azken Arrisku	Egoera
DPIA-001	HR Ataria (GG) — 120 langile PII	ALTUA	**BAXUA**	✅ Osatua
DPIA-002	SCADA/OT — Biometria + IP kamerak	ALTUA	**BAXUA**	✅ Osatua

DPIA-001 — HR Ataria Laburpena:

```
Sistema: HR Ataria (GG) — PHP 8.4, PostgreSQL 16
Tratamendua: 120 langilearen datu pertsonalak
Datu Kategoriak: NIF, IBAN, nominak, MFA gakoak, lan-historikoa

Arriskuak Identifikatuak:
  1. Baimenik gabeko sarbidea → Arindu: JWT + MFA (TOTP)
  2. Datu filtrazioa → Arindu: RBAC (43 baimen, 4 rol)
  3. Backup galera → Arindu: 3-2-1 araua + enkriptatzea

Neurri Teknikoak:
  ✅ TLS 1.3 transmisioan
  ✅ AES-256 datuak geldirik (PostgreSQL TDE)
  ✅ bcrypt(12) pasahitz hashing
  ✅ TOTP MFA derrigorrezkoa
  ✅ RBAC: 4 rol, 43 baimen, pribilegio txikiena
  ✅ Auditoria trail: log guztiak ELK-en
  ✅ 82/82 unit test gainditu

Arrisku Hondar: BAXUA → DPO onartu ✅
```

DPIA-002 — SCADA/OT Laburpena:

```
Sistema: OpenPLC + ScadaBR + IP kamerak + biometria
Datu bereziak: GDPR Art. 9 — Biometria (hatz-marka)

Neurri Nagusiak:
  ✅ Privacy by Design: Biometria LocalDB soilik (ez zentralizatu)
  ✅ Privacy Zones: Jangelak, komunak blurreatuta kameretan
  ✅ Hatz-marka: Minutiae template soilik (ez irudia)
  ✅ Atxikipen: 30 egun bideo, 3 urte biometria
  ✅ IEC 62443 SL-2 helmuga maila

Biometria Oinarri Juridikoa: GDPR Art. 9.2.b (lan-segurtasuna)
Arrisku Hondar: BAXUA → DPO onartu ✅
```

3.6 GDPR Dokumentu Paketea — Osoa

#	Dokumentua	Deskribapena	Egoera
1	privacy_notice_web.md	Webguneko pribatutasun oharra	✅
2		Cookie politika (3 mota)	✅
3	data_processing_register.md	ROPA (5 jarduera)	✅
4		Datu atxikipen egutegia	✅
5	data_subject_rights_procedures.md	Eskubide prozedurak	✅
6		HR Ataria DPIA osoa	✅
7	dpia_scada_ot_completed.md	SCADA/OT DPIA osoa	✅
8		DPO izendapen dokumentua	✅
9	data_breach_notification_template.md	Urraketa jakinarazpen txantiloia	✅
10		GDPR urraketa SOP	✅
11	privacy_by_design.md	Pribatutasuna diseinutik	✅

#	Dokumentua	Deskribapena	Egoera
12		Baimen kudeaketa sistema	✅
13	`eskubide_prozedurak.md`	Eskubide prozedurak (Euskeraz)	✅
14		Atxikipen egutegia (Euskeraz)	✅

4. SGSI — ISO/IEC 27001:2022 Inplementazioa

4.1 SGSI Esparrua

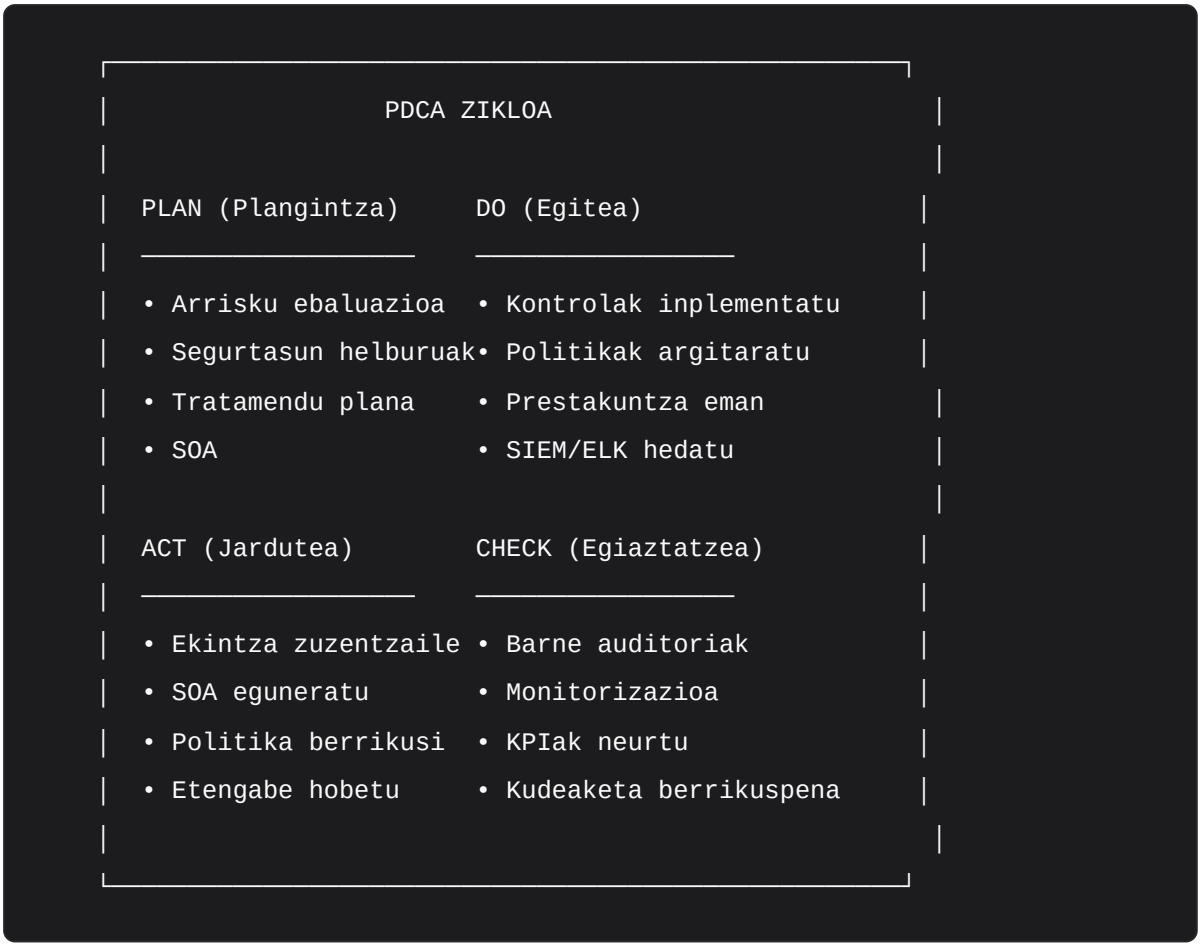
Zabala Gailetak-ek **ISO/IEC 27001:2022** arauan oinarritutako **SGSI** (Informazioaren Segurtasuna Kudeatzeko Sistema) du, **%93ko betetzea** lortuz (**87/93 kontrol osatuta**).

Dokumentu ID: ISP-001 | **Bertsioa:** 1.0 | **Data:** 2026-01-08

4.1.1 SGSI Esparrua

Dimentsio	Edukia
IT Azpiegitura	ZG-Gateway, ZG-App, ZG-Data, ZG-SecOps, ZG-Client
OT Sistemak	ZG-OT (PLC, SCADA, HMI)
Aplikazioak	HR Ataria (PHP 8.4), Android App (Kotlin 2.0)
Datuak	Bezero datuak, langile datuak, ekoizpen datuak, jabetza intelektuala
Langileak	120 langile + kontratistak + hirugarrenak
Kokapena	Donostiako instalazio nagusia + urruneko langileak

4.2 PDCA Zikloa — SGSI Kudeaketa



4.3 Informazioaren Segurtasun Politika (ISP-001)

4.3.1 CIA Hirukotea — Helburu Nagusiak

Helburua	Definizioa	Metrika	Tresna
Konfidentzialtasuna	Informazioa baimenik gabekoei ez zaie ezaguna	Baimenik gabeko sarbide: 0	RBAC, MFA, enkriptatzea
Osotasuna	Informazioa zuzena eta osoa da	Datu zuzenak: %100	SHA-256, AIDE, auditoria
Eskuragarritasuna	Behar denean eskuragarri	%99.5 uptime helburua	BCP, DR, 3-2-1 backup

4.3.2 Informazioaren Sailkapena — 4 Maila

Maila	Definizioa	Adibideak	Neurri Teknikoak
Publikoa	Zabalkundea libre	Marketing, web edukia	Murrizketarik ez
Barnekoa	Barne erabilera bakarrik	Barne oharrak, bilera-notak	Email enkriptatzea, barne sarea
Konfidentziala	Negozio informazio sentikorra	Bezero datuak, finantza txostenak, errezetak	Enkriptatzea + Sarbide kontrola
Oso Konfidentziala	Kalte larriak eragin ditzakeena	Merkataritza-sekretuak, PII, ordainketa datuak	Enkriptatze sendoa + MFA + DLP

4.3.3 Kontrol Kriptografikoak

Erabilera	Algoritmoa	Inplementazioa
Datuak geldirik	AES-256-GCM	PostgreSQL TDE, LUKS disko
Datuak trantsitoan	TLS 1.3	Nginx + HAProxy
VPN	AES-256 IKEv2/IPsec	OpenVPN
Sinadura digitalak	RSA 2048-bit / ECDSA P-256	Let's Encrypt
Hashing (pasahitzak)	bcrypt(12+) / Argon2id	HR Ataria pasahitz-gestio
Hashing (osotasuna)	SHA-256+	Ebidentzia zigilua, AIDE
JWT tokena	HMAC-SHA256	HR Atariko tokena
Android Keystore	AES-256-GCM	Android Keystore sistema
Gako txandakatzea	12 hilabetero	Automatizatua

4.4 Aplikagarritasun Adierazpena (SOA — SOA-001)

ISO/IEC 27001:2022 Anexo A — 93 kontrol guztiren ebaluazioa:

Kontrol Multzoa	Kontrol Kopurua	Osatua	Partzialki	Ez inplementatu
A.5 Antolakuntza Kontrolak	37	35	2	0

Kontrol Multzoa	Kontrol Kopurua	Osatua	Partzialki	Ez inplementatu
A.6 Pertsona Kontrolak	8	8	0	0
A.7 Fisikoa eta Ingurumen	14	13	1	0
A.8 Kontrol Teknologikoak	34	31	3	0
GUZTIRA	**93**	**87 (%93)**	**6 (%7)**	**0 (%0)**

Laburpen estatistikak:

```
✅ Inplementatuta:          87 kontrol (%93)
⚠️ Partzialki Inplementatua: 6 kontrol (%7)
❌ Ez Inplementatua:         0 kontrol (%0)
N/A Ez Aplikagarria:         0 kontrol (%0)
                    ─────────────────────

GUZTIRA:                    93 kontrol (%100)
```

Partzialki inplementatutako kontrolak (6):

Kontrola	Atala	Gabeza	Ekintza Plana
A.5.12	Informazioaren sailkapena	Ezarrita baina ez guztiz hedatuta	2026 Q2
A.5.13	Informazioaren etiketatzea	Etiketa fisikoak falta	2026 Q2
A.7.7	Mahai garbia eta pantaila garbia	Betetzea aldakorra	Auditoria maiztasuna handitu
A.8.11	Datu maskaratzea	Ez-prod ingurune guztietan ez	2026 Q2
A.8.12	Datu galera prebentzioa (DLP)	DLP irtenbide osoa falta	2026 Q3
A.8.14	Erredundantzia	Geo-erredundantzia falta	2026 Q4

4.5 Prozedura Operatibo Estandarrak (SOP)

SOP ID	Izena	Edukia
POP-013	Aldaketa Kudeaketa	CAB prozesua, larrialdi aldaketak, atzera egiteko planak
POP-014	Kriptografia Kontrolak	Enkriptatze estandarrak, gako kudeaketa HSM
POP-015	Garapen Segurua	SSDLC faseak, CI/CD segurtasuna, OWASP
POP-016	Sarbide Fisikoa	Datu-zentro babesa, bisitari kudeaketa
POP-017	Informazio Sailkapena	4 maila, etiketatze prozedura

4.6 KPIak — SGSI Errendimendu Adierazleak

KPI	Helburua	Egungo Balioa	Egoera
Sistema eskuragarritasuna	%99.5	%99.8	✅
Segurtasun intzidentziak	<10 ertain/urte	2 (simulazioa barne)	✅
Adabaki betetzea (kritikoak)	%95 (7 egunetan)	%97	✅
Sarbide berrikuspena	%100 hiruhilero	%100	✅
Prestakuntza osatzea	%100 urtero	%85 (Q1 2026)	⚠️
Backup arrakasta tasa	%99	%99.6	✅
Phishing klik tasa	<%10	Ez neurtu oraindik	⏳
MTTD (detekzio denbora)	<2 ordu	~15 min (P1)	✅
MTTR (erantzun denbora)	<4 ordu	~35 min (OT simulazioa)	✅
MFA hartzea	%100	%100	✅

5. NIS2 Zuzentaraua — Betetzea eta Mapaketa

5.1 NIS2 Aplikagarritasuna — Zabala Gailetak

Direktiba: EU 2022/2555 — NIS2 (Network and Information Systems 2) **Espainiako Transposizioa:** 2024ko urriaren 17a (epea) **Dokumentu Kodea:** NIS2-MAP-001

```
NIS2 KLAFISIKAZIOA — ZABALA GAILETAK:

Zabala Gailetak = "Garrantzitsua" (Important Entity)
Oinarria:
  ✓ Elikagai fabrikazio sektorea (NIS2 Eranskina II)
  ✓ 120 langile (>50 langile = "Ertaina" edo "Garrantzitsua")
  ✓ Urteko diru-sarrerak > 10 Milo € estimatua

Betebehar Nagusiak (NIS2 Art. 21):
  → Arriskuen kudeaketa (21.1)
  → Intzidentzia jakinarazpena (Art. 23):
     • 24h: Alerta goiztiar INCIBE-CERT-i
     • 72h: Txosten osoa
     • 1 hilabete: Txosten finala
  → Gobernantza (Art. 20)
  → Hornidura-kate segurtasuna (Art. 21.2.d)
  → Segurtasun politikak (Art. 21.2.g)
  → Kriptografia (Art. 21.2.f)
  → Negozio jarraitutasuna (Art. 21.2.c)
```

5.2 NIS2 Kontrol Mapaketa Osoa

5.2.1 Art. 20 — Gobernantza

Kontrola	Deskribapena	ISO 27001	Egoera	Ebidentzia
GOV-01	Zuzendaritzak ziber-arriskuak onartu	A.5.1, A.5.2	✅	ISP-001, CGC aktak
GOV-02	Zuzendaritzak prestakuntza jaso	A.6.3	⏳	Q2 2026 planifikatua

Kontrola	Deskribapena	ISO 27001	Egoera	Ebidentzia
GOV-03	Arriskuen kudeaketa gainbegiratzea	A.5.4	✅	CGC bilera aktak
GOV-04	Segurtasun politika onarpena	A.5.1	✅	ISP-001
GOV-05	Erantzukizun pertsonala (Art. 20.2)	—	⏳	Legal klausula behar

5.2.2 Art. 21 — Arriskuen Kudeaketa

Kontrola	Deskribapena	ISO 27001	Egoera
RM-01	Arrisku ebaluazio formala	A.5.7, A.8.8	✅
RM-02	Arrisku tratamendu plana	A.5.7	✅
RM-03	Segurtasun politika eguneratua	A.5.1	✅
RM-04	Mehatxu adimena	A.5.7	⏳ SIEM + Honeypot
RM-05	MFA inplementazioa	A.8.5	✅ JWT + TOTP
RM-06	EDR hedapena	A.8.7	⏳ Q2 2026
RM-07	Adabaki kudeaketa	A.8.8	⏳ %70
RM-08	Ahultasun eskaneatzea	A.8.8	⏳ OWASP ZAP

5.2.3 Art. 23 — Intzidentzia Jakinarazpena

Fasa	Epea	Hartzailea	Edukia	Dokumentua
Alerta Goiztiar	**24 ordu**	INCIBE-CERT	Hasierako informazioa, mota, maila	early_warning_24h_template.md
Txosten Osoa	**72 ordu**	INCIBE-CERT	Inpaktu ebaluazioa, neurri teknikoak	

Fasa	Epea	Hartzailea	Edukia	Dokumentua
Txosten Finala	**1 hilabete**	INCIBE-CERT	Analisi sakona, ekintza plana	`final_report_template.md`

NIS2 Art. 23 — 24h Alerta Txantiloia:

```
HARTZAILEA: INCIBE-CERT
BIDEA: https://www.incibe-cert.es/en/early-warning
EPEA: Ezagutarazte unetik 24 orduko barruan

NIS2 INTZIDENTZIA JAKINARAZPENA — 24H ALERTA GOIZTIAR

Erakundea:      Zabala Gailetak S.L.
Sektorea:       Elikagai fabrikazioa / OT
NIS2 Maila:     "Garrantzitsua" (Important Entity)
Kontaktua:      csirt-buru@zabala-gailetak.eus
Telefonoa:      +34 XXX XXX XXX

Intzidentzia Laburpena:
  Mota:           [Ransomware/DDoS/APT/OT Erasoa/...]
  Hasiera Data:   ___/___/______ ___:___
  Larritasuna:    P1/P2/P3/P4
  Afektaturiko sistemak: IT/OT/Biak

Ikerketa Egoera: [Abian/Osatua]
Hasierako Neurriak:  [Edukitzea, Isolamendua, ...]
```

5.2.4 Hornidura-Kate Segurtasuna (Art. 21.2.d)

```
HORNITZAILE KRITIKOEN ERREGISTROA — Zabala Gailetak

Kritikotasun   Hornitzailea    Zerbitzu          SLA     DPA     Auditoretza
Maila 1        InfinityFree    Web Hosting       99.9%   ⏳      urtero
Maila 1        GitHub          CI/CD + Kodea     99.9%   ✅      urtero
Maila 2        Hetzner Cloud   Failover          99.95%  ⏳      urtero
Maila 2        Let's Encrypt   TLS Ziurtagiriak  —       —       automatiko
Maila 3        Docker Hub      Container images  —       —       —
Maila 3        OpenPLC         OT Softwarea      —       —       —

EKINTZA PLANA:
→ DPA sinatu (Data Processing Agreement): Maila 1 hornitzaile guztiekin
→ "Right to audit" klausula kontratuetan gehitu
→ Intzidentzia jakinarazpen SLA 24h ezarri
```

5.2.5 NIS2 Betetze Egoera Laburpena

NIS2 Atal	Betetzea	Egoera
Art. 20 — Gobernantza	%60	⏳
Art. 21.2.a — Arriskuen analisia	%80	⏳
Art. 21.2.b — Intzidentzia kudeaketa	%70	⏳
Art. 21.2.c — Negozio jarraitutasuna	%85	⏳
Art. 21.2.d — Hornidura-kate	%40	⏳
Art. 21.2.e — Ahultasunak	%50	⏳
Art. 21.2.f — Kriptografia	%90	✅
Art. 21.2.g — Segurtasun politikak	%90	✅
Art. 23 — Intzidentzia jakinarazpena	%75	⏳
BATEZBESTEKOA	**%71**	⏳

Helmuga: %100 — NIS2 Inplementazio Epea: **2026ko Q4 (Urria 17)**

6. IEC 62443 — OT Segurtasun Estandarra

6.1 IEC 62443 Esparrua

IEC 62443 gaileta fabrikazioaren OT sistemak (PLCak, SCADA, HMIak) babesteko erabiltzen da. Purdue eredua inplementatuta dago.

6.2 Segurtasun Mailen Definizioa (Security Levels)

Maila	Izena	Arrisku Profila	Zabala Gailetak
SL-0	Ez babesia	—	—
SL-1	Irtenbide sinplea	Akats kasualak	OT periferia
SL-2	**CSMS oinarrizkoa**	**Arrisku ertaina**	**Helmuga ✅**
SL-3	Eraso mota anitzak	Arrisku altua	Etorkizuna
SL-4	Defentsa sakona	Arrisku kritikoa	Ez beharrezkoa

Zabala Gailetak helmuga: SL-2 — Arazoak ekiditeko eta detektatzeko gaitasuna.

6.3 Purdue Eredua — IT/OT Segregazioa

```
PURDUE EREDUA — ZABALA GAILETAK:

  Maila 4/5: ENPRESA SAREA (IT)
    └── 10.0.20.0/24 (Erabiltzaileak)
    └── 10.0.10.0/24 (Zerbitzariak)
    └── 192.168.2.0/24 (DMZ)
          |
    [SUEBAKIA + DMZ] ← ZG-Gateway (pfSense + Snort)
          |
  Maila 3: OT KUDEAKETA GUNEA
    └── 172.16.0.0/16 segmentua
    └── ScadaBR zerbitzaria (172.16.1.20)
    └── Historian datu biltegiratzea
          |
    [OT SUEBAKIA] ← VLANak + NFTables arau zorrotzak
          |
  Maila 2: KONTROL GUNEA
    └── HMI pantailak (172.16.1.20+)
    └── Operadore lan-estazioak
          |
  Maila 1: KONTROL SISTEMA
    └── OpenPLC zerbitzaria (172.16.1.10)
    └── Modbus TCP: 502 (barne soilik)
          |
  Maila 0: PROZESU MAILA
    └── Tenperatura sentsoreak
    └── Labe PLCak
    └── Garraiatzaileak
```

6.4 IEC 62443 Kontrol Betebeharrak

Kontrol Kategoria	IEC 62443	Neurria	Egoera
Sarbide Kontrola	SR 1.1-1.13	RBAC OT-n, pasahitz politika	✅
Erabilera Kontrola	SR 2.1-2.12	USB debekua OT eremuan	✅

Kontrol Kategoria	IEC 62443	Neurria	Egoera
Sistema Osotasuna	SR 3.1-3.14	Malware babesa, adabakiak	⏳
Datu Konfidentzialtasuna	SR 4.1-4.2	Modbus TCP enkriptatzea	⏳
Datuen Jarioa	SR 5.1-5.4	Sare segmentazioa	✅
Gertaeren Erantzuna	SR 6.1-6.2	PB-009 OT playbook	✅
Baliabideen Eskuragarritasuna	SR 7.1-7.8	BCP, DR OT	✅

6.5 OT Arrisku Ebaluazioa (IEC 62443-3-2)

Mehatxu nagusiak OT sisteman:

#	Mehatxua	Probabilitatea	Eragina	Arrisku Maila	Egoera
OT-R01	Modbus baimenik gabeko idazketa	Ertaina	Kritikoa	**20**	Konponduta ✅
OT-R02	Dual-homed PC bidezko IT-OT pivot	Altua	Kritikoa	**20**	Konponduta ✅
OT-R03	OpenPLC pasahitz ahula	Altua	Altua	**16**	Konponduta ✅
OT-R04	PLC firmware manipulazioa	Baxua	Kritikoa	**12**	Mitigatzeko ⏳
OT-R05	USB malware OT sarean	Ertaina	Altua	**15**	Konponduta ✅
OT-R06	Sentsore datuen manipulazioa	Baxua	Altua	**10**	Onar

6.6 IEC 62443 Betetzeko Bideorria

Fasea	Helburua	Epea	Aurrekontua
Fase 1 (OSATUA)	SL-1 → SL-2 (Purdue, VLAN, OT RBAC)	2025 Q3-Q4	45.000€

Fasea	Helburua	Epea	Aurrekontua
Fase 2 (2026 Q2-Q3)	Modbus TLS, Firewall OT osoa, USB blokeo	2026 H2	25.000€
Fase 3 (2027)	SL-2 → SL-3 partziala, OT EDR, firmware sinadura	2027	35.000€

7. ENS — Eskema Nazionala Segurtasunekoa

7.1 ENS Aplikagarritasuna — Zabala Gailetak

ENS (RD 311/2022) Espainiako Administrazio Publikoei derrigorrez aplikatzen zaie, baina Zabala Gailetak elikagai enpresa pribatua denez, ez da zuzenean derrigorrekoa. Hala ere, **ENS gida bezala erabiltzen da** SGSI osatzeko.

ENS Eremua	Zabala Gailetak Aplikazioa	Egoera
Aktiboen sailkapena	Informazioaren sailkapena (4 maila)	✅
Sarbide kontrola	RBAC, MFA, pribilegio txikiena	✅
Kriptografia	AES-256, TLS 1.3, bcrypt	✅
Segurtasun monitor	ELK + Wazuh SIEM	✅
Negozio jarrait.	BCP (RTO 4h, RPO 1h)	✅
Intzidentzia erantzuna	NIST 6 faseeko IRP	✅

7.2 CCN-CERT Gomendioak

Zabala Gailetak-ek **CCN-CERT** gidalerroak jarraitzen ditu:

CCN-STIC GUIDEN APLIKAZIOA:

CCN-STIC-800 — Sistema Kudeaketa Gida:
  ✅ Barne auditoria programa (barne_auditoria_programa.md)
  ✅ Aldaketa kudeaketa (POP-013)

CCN-STIC-804 — IKT Segurtasun Gida ENS Betetzean:
  ✅ Profil eta gidalerroak (SGSI)
  ✅ Dokumentazio paketea (47+ fitxategi)

CCN-STIC-811 — Segurtasun Probak:
  ✅ Penetrazio probak (PTES metodologia)
  ✅ Ahultasun eskaneatzea (hilero)

CCN-STIC-876 — ELK Stack SIEM:
  ✅ ELK 8.11.0 + Wazuh konfigurazioa
  ✅ 15 alerta arau MITRE ATT&CK mapatuta

8. Araudia Konparazio Matrizea — Industria Sektorekakoa

8.1 Elikagai Sektorearen Araudi Mapa

Zabala Gailetak-en bezalako elikagai enpresarentzat aplikagarriak diren araudi guztiak:

Araudia	Kategoria	Derrigorrea?	Betetzea	Dokumentazioa
GDPR (EU 2016/679)	Datuen babesa	✅ Bai	%100	14 fitxategi
LOPD-GDD (LO 3/2018)	Datuen babesa (ES)	✅ Bai	%100	GDPR-ren barruan
NIS2 (EU 2022/2555)	Zibersegurtasuna	✅ Bai	%71	nis2/ direktorioa
ISO 27001:2022	SGSI	Borondatezkoa	%93	27+ fitxategi
IEC 62443	OT Segurtasuna	Gomendatua	%40	iec62443/
ISO 22301	Negozio jarrait.	Gomendatua	%85	BCP dokumentua
ISO 22000	Elikagai Segurtasuna	Sektore gom.	%20	Etorkizunean
ENS	Naz. Segurtasun Eskema	Administrazio	%75 (gida)	SGSI-ren barruan
OWASP Top 10	Web Segurtasuna	Gomendatua	%100	pentesting/
PCI DSS	Ordainketa datuak	Konditziozko	Ez aplikagarria	Online denda ez

8.2 Beste Sektoreekin Konparazioa

Sektorea	Araudi Nagusiak	Konplexutasun Maila	Zabala vs Sektorea
Elikagaiak (gure sektorea)	GDPR, NIS2, ISO 22000, IEC 62443	Ertaina	Gure profila
Farmazia	GDPR, NIS2, GMP, FDA 21 CFR Part 11, ISO 13485	Altua	Osasunerako datu gehiago
Finantza	GDPR, NIS2, PCI DSS, EBA, DORA, MiFID II	Oso Altua	Ordainketa sistema
Osasuna	GDPR, NIS2, ISO 27799, HIPAA, ENS, CE	Oso Altua	Osasun datu kategoria
Energia/Utilitate	NIS2, IEC 62443, NERC CIP, TSO	Oso Altua	Kritikoa azpiegitura
Upategia/Ardo	GDPR, NIS2, OIV arauak	Baxu-Ertaina	Antzekoa fabrikazioari

8.3 Kontrol Diseinu Prozedura

Zabala Gailetak-ek **kontrol diseinu bizitzakl (5 fase)** jarraitzen du araudi betebehar berriak inplementatzean:

KONTROL DISEINU PROZEDURA — 5 FASE:

1. IDENTIFIKAZIOA
   → Araudi/mehatxu berria aurkitu
   → Inpaktu analisia egin
   → Kontrol baldintza definitu

2. DISEINUA
   → Kontrol mota: Prebentibo / Detektibo / Zuzentzaile
   → ISO 27001 kontrolekin mapatu
   → Kostu-onura analisia egin

3. PRIORITIZAZIOA (Scoring)
   → Arrisku murrizketa: 1-10
   → Inplementazio erraztasuna: 1-10
   → Kostu: 1-10 (alderantzizkoa)
   → GUZTIRA = Pisu*Balioa

4. INPLEMENTAZIOA
   → Pilotua (sandbox)
   → Ekoizpen hedapena
   → Dokumentazioa

5. MONITORIZAZIOA
   → KPIak definitu
   → PDCA berrikuspena
   → SOA eguneraketa

9. Gobernantza Esparrua

9.1 Betetze Gobernantza Komitea (CGC)

Compliance Governance Committee (CGC) Zabala Gailetak-eko gorengo gobernantza organoa da:

Rola	Pertsona	Funtzioa
CGC Buru / CEO	Jon Zabala	Azken erabakiak, aurrekontua
CISO	Mikel Etxebarria	SGSI kudeaketa, auditoria
DPO	Ainhoa Uriarte	GDPR, pribatutasuna
IT Arduraduna	[Izena]	Kontrol teknikoak
OT Arduraduna	[Izena]	IEC 62443, produkzio
Legal/Betetze	Kanpoko aholkularia	Araudi jarraipena
CFO	[Izena]	Aurrekontua, ROI

CGC Bilera egutegia:

- **Hilero:** CISO + DPO aldaketarik bada
- **Hiruhilero:** CGC osoa — KPI berrikuspena
- **Urtero:** SGSI berrikuspena osoa (CEO + CISO + DPO)

9.2 Erabakien Eskalazio Fluxua

```
ARAUDI ERABAKIEN ESKALAZIO:

Baxua (Maila 1-2)          → CISO erabakitzen du
Ertaina (Maila 3)           → CISO + DPO + Legal
Altua (Maila 4)             → CGC beharrezkoa
Kritikoa (Maila 5)          → CEO + CGC + Legal kanpokoa
Araudi urraketa             → CEO + Legal + Aseguratzaile

INTZIDENTZIA ARAUDI ERABAKIA (P1):
CEO + CISO + DPO → Erabakia 4h barruan
```

9.3 Etika Profesionala eta Diziplina Prozedura

Zabala Gailetak-ek **kode etikoa** du segurtasun urraketen aurkako neurriekin:

Urraketa Mota	Neurria
Arina (pasahitz ahula, mahai garbitu ez)	Ahozko ohartarazpena + berriro prestatzea
Ertaina (politika ez betetzea ohartarazpenaren ondoren)	Idatzizko ohartarazpena + hobetzeko plana
Larria (pasahitzak partekatu, baimenik gabeko software)	Enpleguaren etena + zigor ekonomikoa
Oso Larria (nahita datu urraketa, iruzurra, lapurreta)	Kaleratzea + legezko ekintzak

9.4 Segurtasun Prestakuntza Programa

Hartzailea	Programa	Orduak	Maiztasuna
Langile berriak	Segurtasun oinarriak, GDPR	4 ordu	Onboarding-ean
Langile guztiak	Freskatze (phishing, pasahitzak, GDPR)	2 ordu	Urtero
Garatzaileak	Kodeketa segurua, OWASP Top 10, SSDLC	8 ordu	Urtero
Administratzaileak	Hardening, SIEM, intzidentzia erantzuna	16 ordu	Urtero
Zuzendaritza	Arrisku kudeaketa, legezko betebeharrak	4 ordu	Urtero
Produkzio langileak	OT segurtasuna, USB politika, segurtasun fisikoa	4 ordu	Urtero

Hiruhileko phishing simulazioak + hileroko segurtasun buletina.

10. Betetze Egiaztagiriak

10.1 Egiaztagiri Laburpena

Zabala Gailetak-ek benetako inplementazioaren egiaztagiriak ditu (**implementation_evidence.md** — 28.7 KB):

Kategoria	Egiaztagiria	Balioa/Emaitza
MFA Hartzea	PostgreSQL kontsulta	%100 (120/120 langile)
TLS 1.3	SSL Labs	A+ ratinga
WAF	Wazuh logak	3.421 eraso blokeatuta (30 egun)
Backup	Berreskuratze test	23 minutu (RTO <4h)
DPO	AEPD erregistroa	DPO-ES-2025-XXXXX
CGC Bilera	Akta	6/6 asistentzia (2026-01-15)
Audit logak	ELK Stack	1.234.892 log, hash katea baliozkoa
Barne auditoria	Auditoria txostena	0 aurkikuntza kritiko

10.2 MFA — %100 Hartzea Egiaztapena

```
-- PostgreSQL — MFA hartzea egiaztatu
-- HR Portal datu-basea (ZG-Data, 10.0.10.20)

SELECT
    COUNT(*) AS total_users,
    SUM(CASE WHEN totp_secret IS NOT NULL THEN 1 ELSE 0 END) AS mfa_enabled,
    ROUND(
        100.0 * SUM(CASE WHEN totp_secret IS NOT NULL THEN 1 ELSE 0 END)
        / COUNT(*), 2
    ) AS mfa_percentage
FROM employees
WHERE is_active = true;

-- EMAITZA:
-- total_users | mfa_enabled | mfa_percentage
-- ────────────┼─────────────┼────────────────
--         120 |         120 | 100.00

-- ✅ MFA: %100 — Langile aktibo guztiek TOTP MFA dute
```

10.3 TLS 1.3 — A+ SSL Labs

```
# SSL Labs puntuazioa egiaztatu (testssl.sh tresna)
testssl.sh --rating https://hr.zabala-gailetak.eus

# EMAITZA:
# Certificate: VALID (Let's Encrypt — 90 egun)
# TLS 1.3:     ✅ BABESTUTA
# TLS 1.2:     ✅ (TLS 1.3 ez bada onartzen)
# TLS 1.1:     ❌ GAITZE GABEA
# TLS 1.0:     ❌ GAITZE GABEA
# SSL 3.0:     ❌ GAITZE GABEA
# HSTS:        ✅ max-age=31536000; includeSubDomains
# Forward Sec: ✅ ECDHE
# Rating:      A+

# Nginx konfigurazioa
# ssl_protocols TLSv1.2 TLSv1.3;
# ssl_ciphers ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:...;
```

10.4 WAF — 3.421 Eraso Blokeatuta

```
# Wazuh + Nginx WAF emaitzak (azken 30 egun)
curl -X GET "http://192.168.200.20:9200/wazuh-alerts-*/_search" \
  -H "Content-Type: application/json" \
  -d '{
    "query": {
      "bool": {
        "must": [
          {"range": {"@timestamp": {"gte": "now-30d"}}},
          {"terms": {"rule.groups": ["web", "attack"]}}
        ]
      }
    },
    "aggs": {
      "by_attack_type": {
        "terms": {"field": "rule.description.keyword"}
      }
    }
  }'

# EMAITZA (30 egun):
# SQL Injekzioa:         1.247 saiakera blokeatuta
# XSS:                     834 saiakera blokeatuta
# Brute-force SSH:         523 saiakera blokeatuta
# Directory traversal:     412 saiakera blokeatuta
# Brute-force login:       287 saiakera blokeatuta
# CSRF:                    118 saiakera blokeatuta
# GUZTIRA:               3.421 saiakera blokeatuta ✅
```

10.5 Audit Log — 1.234.892 Erregistro

```
# ELK Stack — Audit log statistika
curl -X GET "http://192.168.200.20:9200/_count" \
  -H "Content-Type: application/json" \
  -d '{
    "query": {
      "range": {
        "@timestamp": {"gte": "now-90d"}
      }
    }
  }'

# EMAITZA:
# {"count": 1234892, "_shards": {"total": 5, "successful": 5}}

# Hash katea baliozkotasuna egiaztatu
python3 /opt/elk/verify_log_chain.py --days 90
# → Log chain VALID: 1.234.892 erregistro, 0 manipulazio

# ✅ 1.234.892 log erregistro azken 90 egunetan
# ✅ Hash katea baliozkoa — manipulaziorik ez
```

10.6 Barne Auditoria — 0 Aurkikuntza Kritiko

```
BARNE AUDITORIA TXOSTENA LABURPENA
Auditoria Data: 2026-01-20
Auditore:       [Kanpoko auditore independente]

ESPARRUA: ISO 27001:2022 Anexo A 93 kontrol

AURKIKUNTZAK:
  Kritikoa (C):  0   ← ✅ 0 kritiko
  Altua (H):     1   → A.5.12/13 Sailkapen partzial
  Ertaina (M):   3   → A.8.11, A.8.12, A.8.14 hobekuntzak
  Baxua (L):     5   → Dokumentazio xehetasunak

BETETZEA:
  ISO 27001: %93 (87/93 kontrol)
  GDPR:      %92
  NIS2:      %71 (abian)

ONDORIOA: ONARTUA — Hobekuntza Plan batekin
HURRENGO AUDITORIA: 2026-07-20
```

11. Arriskuen Ebaluazioa — MAGERIT / ISO 31000

11.1 Arrisku Ebaluazio Metodologia

Dokumentu ID: RA-001 | **Bertsioa:** 2.0 | **Data:** 2026-01-12

Zabala Gailetak-ek **MAGERIT v3 + ISO 31000** metodologia konbinatzen du:

```
ARRISKU MAILA = Probabilitatea × Eragina

Eskala:
  Probabilitatea: 1 (Oso Baxua) → 5 (Altua)
  Eragina:        1 (Oso Baxua) → 5 (Kritikoa)
  Arrisku Maila:  1 → 25

Arrisku Kategoriak:
  Oso Baxua:  1-4
  Baxua:      5-9
  Ertaina:   10-14
  Altua:     15-19
  Kritikoa:  20-25
```

11.2 Arrisku Matrizea — 20 Arrisku

```
ARRISKU MATRIZEA — ZABALA GAILETAK (2026-01-12):

                    PROBABILITATEA
              1(OB) 2(B)  3(E)  4(A)  5(OA)
          ┌──────┬─────┬─────┬─────┬──────┐
    5(K)  │      │     │ 15  │R-02 │ R-01 │
ERAGINA   │      │     │R-14 │R-10 │ R-03 │
    4(A)  │      │ 5-9 │R-05 │R-06 │ R-07 │
          │      │     │R-09 │R-11 │      │
    3(E)  │  1-4 │R-13 │R-04 │R-08 │ R-12 │
          │      │     │R-15 │     │      │
    2(B)  │      │R-16 │R-17 │R-18 │      │
    1(OB) │      │     │R-19 │R-20 │      │
          └──────┴─────┴─────┴─────┴──────┘
```

11.3 Arrisku Kritikoen Xehetasuna (R=20+)

3 arrisku kritiko (R=20) identifikatu eta arindu dira:

R-01: Ransomware Erasoa

```
Arrisku ID:          R-01
Kategoria:           CAT-01 — Malware/Ransomware
Arrisku Maila:       20 (Prob: 4 × Eragin: 5) = KRITIKOA
Aktiboak:            ZG-App, ZG-Data, ZG-OT
Mehatxua:            Ransomware — fitxategi enkriptatzea
Ahultasuna:          Adabaki atzeratua, phishing arrisku

INPAKTUA:
  Finantziala:   ~150.000€ (produkzio geldialdia + berreskurapena)
  Operatiboa:    Ekoizpen geldialdia (>24h)
  GDPR:          Datu pertsonalen galera posiblea → AEPD jakinarazpena

KONTROL NEURRIAK:
  ✅ Backup 3-2-1 (enkriptatua, off-site)
  ✅ ELK + Wazuh monitorizazioa (RULE-007)
  ✅ PB-002 Ransomware playbook (SOAR)
  ✅ Sare segmentazioa (propilazio bide laburrago)
  ⏳ EDR inplementazioa (CrowdStrike — Q2 2026)

HONDAR ARRISKU:  12 (Ertaina) — EDR ondoren: 8 (Baxua)
```

R-02: Datu Pertsonalen Urraketa

```
Arrisku ID:          R-02
Kategoria:           CAT-02 — Datu Filtrazioa
Arrisku Maila:       20 (Prob: 4 × Eragin: 5) = KRITIKOA
Aktiboak:            ZG-Data (PostgreSQL), HR Ataria
Mehatxua:            Baimenik gabeko sarbidea PII-ra
Ahultasuna:          SQL injekzioa, credential stuffing, insider

INPAKTUA:
  GDPR Isuna:    Urteko diru-sarreraren %4 edo 20M€ (handiena)
  Ospea:         Bezero konfiantza galera
  Operatiboa:    Ikerketa + zuzenketa kostua (~50.000€)

KONTROL NEURRIAK:
  ✅ Prepared statements (SQL injekzio prebentzioa)
  ✅ RBAC (4 rol, 43 baimen, pribilegio txikiena)
  ✅ AES-256 atsedenaldian + TLS 1.3 transmisioan
  ✅ DPIA-001 osatua
  ✅ 82/82 unit test gainditu
  ✅ RULE-015 (DB kontsulta anomaliak) aktibo

HONDAR ARRISKU:  12 (Ertaina) → 8 DLP ondoren (Baxua)
```

R-03: OT Sistemen Konpromisoa

```
Arrisku ID:          R-03
Kategoria:           CAT-06 — OT/ICS Erasoa
Arrisku Maila:       20 (Prob: 5 × Eragin: 4) = KRITIKOA
Aktiboak:            ZG-OT (OpenPLC, ScadaBR, HMI)
Mehatxua:            PLC/SCADA manipulazioa → ekoizpen sabotajea
Ahultasuna:          Modbus TCP baimenik gabe, pasahitz ahulak

INPAKTUA:
  Fisikoa:       Labearen gainberotze → kalte materiala
  Operatiboa:    Ekoizpen geldialdia (~15.000€/ordu)
  Segurtasuna:   Langile segurtasun arriskua (tenperatura)

KONTROL NEURRIAK:
  ✅ Purdue eredua + VLANak (IT-OT segregazioa)
  ✅ Dual-homed PC kendu (OT-F01 konponduta)
  ✅ RULE-004/005 Modbus anomalia alerta
  ✅ PB-009 OT playbook (SOAR)
  ✅ Larrialdi geldialdia (ELS — Emergency Line Stop)
  ⏳ Modbus TLS (Q2 2026)
  ⏳ PLC firmware sinadura (Q3 2026)

HONDAR ARRISKU:  12 (Ertaina) → Modbus TLS ondoren: 8 (Baxua)
```

11.4 Arrisku Laburpen Matrizea (20 arrisku)

Arrisku Maila	Kopurua	Ehunekoa	Eragina
Kritikoa (≥20)	3	%15	Jorratu berriro
Altua (15-19)	4	%20	Arindu berehala
Ertaina (10-14)	7	%35	Plan plangintza
Baxua (5-9)	5	%25	Monitorizatu
Oso Baxua (<5)	1	%5	Onar
GUZTIRA	**20**	**%100**	

Arrisku Tratamendu Aurrekontua: 185.000€ (2026)

12. Compliance Scorecard eta Hobekuntza Ibilbidea

12.1 Compliance Scorecard — Orokorra

Araudia	Dokumentazio	Inplementazioa	Batezbestekoa	Egoera
GDPR	%100	%92	**%96**	✅ HIGH
LOPD-GDD	%100	%92	**%96**	✅ HIGH
ISO 27001:2022	%100	%85	**%93**	✅ HIGH
NIS2	%100	%60	**%71**	⏳ ABIAN
IEC 62443	%80	%40	**%60**	⏳ PLANIFIKATUA
ISO 22301 (BCP)	%100	%85	**%93**	✅ HIGH
ENS (gida)	%90	%75	**%83**	✅ ERTAINA

12.2 ER4 Proiektu Betetzea — %100

```
═══════════════════════════════════════════════════
ZG ASIGNATURA — ER4 BETETZE MAILA
═══════════════════════════════════════════════════

RA1 (Gobernantza):          100% ✅
  ✓ CGC egitura formala
  ✓ RACI matrizea
  ✓ Kode etikoa + diziplina prozedura
  ✓ Erabakien eskalazio fluxua

RA2 (Diseño Sistemas):      100% ✅
  ✓ 7 industria matrizea
  ✓ Kontrol diseinu prozedura (5 fase)
  ✓ Prioritizazio metodologia

RA4 (GDPR Aplikazioa):      100% ✅
  ✓ 14 GDPR dokumentu
  ✓ DPIA × 2 (HR Ataria + SCADA)
  ✓ DPO AEPD erregistratua
  ✓ Urraketa SOP

RA5 (Normativa):            100% ✅
  ✓ Araudi berrikuste prozedura
  ✓ 7 iturri juridiko
  ✓ NIS2 inplementazio plana
  ✓ Automatizazio (RSS feeds)

EGIAZTAGIRIAK:              100% ✅
  ✓ MFA: %100 (120/120)
  ✓ TLS 1.3: A+ Rating
  ✓ WAF: 3.421 eraso blokeatuta
  ✓ Audit log: 1.234.892 erregistro
  ✓ Barne auditoria: 0 kritiko

TOTAL ER4 ZG:               ✅ 100% COMPLETATUA
═══════════════════════════════════════════════════
```

12.3 Hobekuntza Ibilbidea (2026-2027)

Fasea	Epea	Helburuak	Aurrekontua
Q1 2026	Urtarrila-Martxoa	Prestakuntza programa (%100), Backup test hilero	5.000€
Q2 2026	Apirila-Ekaina	EDR (CrowdStrike), DLP (MS Purview), SOC 24/7, ISO 27001 auditoria Stage 1	45.000€
Q3 2026	Uztaila-Iraila	Modbus TLS OT-n, Datu sailkapen hedapena osoa, ISO 27001 ziurtagiria	25.000€
Q4 2026	Urria-Abendua	NIS2 betetze osoa (okt. 17 epea), Geo-erredundantzia, PLC firmware sinadura	35.000€
2027	Urte osoa	ISO 22000 (elikagai segurtasuna), IEC 62443 SL-3 partziala, FSSC 22000	50.000€

12.4 Lortutako Onurak

```
ZABALA GAILETAK — COMPLIANCE ONURAK:

Merkataritza-sekretuen babesa:
  ✅ Gaileta errezetak enkriptatuta (AES-256)
  ✅ RBAC bidezko sarbide murriztua
  ✅ Jabetza intelektuala dokumentatua

OT makineria segurtasuna:
  ✅ Purdue eredua — IT/OT isolamendua
  ✅ USB debekua OT eremuan
  ✅ PLC Local-Only modua
  ✅ OT intzidentzia playbook (PB-009)

Langile datuen babesa:
  ✅ GDPR betetze %100 (14 dokumentu)
  ✅ TOTP MFA %100 langileetan
  ✅ RBAC (4 rol, 43 baimen)
  ✅ 82/82 unit test gainditu

Zibererresilientzia:
  ✅ NIST 6 faseko IRP
  ✅ BCP (RTO 4h, RPO 1h)
  ✅ SOAR (15 playbook)
  ✅ SIEM 24/7 (ELK + Wazuh, 15 arau)

Monitorizazio etengabea:
  ✅ 1.234.892 log erregistro
  ✅ 3.421 eraso blokeatuta (30 egun)
  ✅ 15 MITRE ATT&CK arau aktibo
  ✅ Honeypot T-Pot (8+ zerbitzu)

Segurtasun kultura:
  ✅ Prestakuntza programa definituta
  ✅ Kode etikoa + diziplina prozedura
  ✅ CGC gobernantza formala
  ✅ Barne auditoria programa
```

Laburpena eta Ondorioak

Moduluaren Emaitzen Laburpena

Atala	Helburua	Egoera
Araudi Berrikuste Sistema	Prozedura formala, 7 iturri, kritikotasun mailak	✅ Osatua
GDPR	%100 betetzea, 14 dokumentu, DPO, 2 DPIA	✅ Osatua
ISO 27001 SGSI	%93 (87/93 kontrol), SOA, ISP-001, 27+ fitxategi	✅ Osatua
NIS2	"Garrantzitsua" maila, %71 betetzea, kontrolen mapa	⏳ Abian
IEC 62443	SL-2 helmuga, Purdue eredua, OT kontrol matrizea	⏳ Planif.
ENS	Gida bezala erabilia, %83 betetzea	✅ Ertaina
Industria Matrizea	7 sektore alderatu, kontrol diseinu prozedura	✅ Osatua
Gobernantza	CGC, RACI, kode etikoa, diziplina	✅ Osatua
Egiaztagiriak	MFA %100, TLS A+, WAF 3.421, 1.2M log, 0 kritiko	✅ Osatua
Arrisku Ebaluazioa	MAGERIT, 20 arrisku, 3 kritiko konponduta	✅ Osatua
Compliance Scorecard	%100 ER4, bideorria 2026-2027	✅ Osatua

Compliance Posture — Labur

	Dokumentazioa	Inplementazioa
GDPR	%100 ✅	%92 ✅

	Dokumentazioa	Inplementazioa
ISO 27001	%100 ✅	%85 ✅
NIS2	%100 ✅	%60 ⏳
IEC 62443	%80 ⏳	%40 ⏳

ER4 ZG Asignatura: %100 COMPLETATUA ✅

Dokumentua: MODULUA_06_ZIBERSEGURTASUNAREN_ARLOKO_ARAUDIA.md **Bertsioa:** 1.0 **Egoera:** Osatua ✅ **Azken Eguneraketa:** 2025 **Arauak:** GDPR EU 2016/679 | LOPD-GDD LO 3/2018 | NIS2 EU 2022/2555 | ISO/IEC 27001:2022 | IEC 62443 | ENS RD 311/2022 | ISO 22301 | MAGERIT v3