regulatory_monitoring_procedure

Araudiaren Jarraipena eta Monitorizazio Prozedura

Regulatory Monitoring and Compliance Procedure

Enpresa: Zabala Gailetak, S.L. **Dokumentu Kodea:** COMP-POP-001 **Bertsioa:** 1.0 **Data:** 2026-02-05
Jabea: Legal Advisor + CISO **Egoera:** Indarrean **Berrikusketa Maiztasuna:** Sei hilean behin (Biurteko)

---

1. XEDEA ETA IRISMENA

1.1 Helburua

Prozedura honek ezartzen du araudia zein da erakundeari aplikagarria den, nola jarraitzen den, eta nola kudeatu behar den araudiaren aldaketa bat.

Helburu Espezifikoak: 1. ✅ Enpresari aplikatu behar zaizkion araudia modu sistematikoan identifikatzea 2. ✅ Araudiaren aldaketen proaktiboa detektatzea 3. ✅ Inpaktuaren ebaluazio azkarra egitea 4. ✅ Erantzun plan eraginkorra inplementatzea 5. ✅ Datu-base juridiko aktualizatu bat mantentzea

1.2 Irismena

Aplikazio-eremua: - ✅ Araudia nazionala (Espainia) - ✅ Araudia europaarra (Batasuna Europarreko) - ✅ Estandar internazionalak (ISO, IEC, NIST) - ✅ Best practices sektorialak (OWASP, CIS)

Arau Multzoak: - Datuen babesa: GDPR, LOPD-GDD, ePrivacy - Ziber-segurtasuna: ENS, NIS2, CCN-STIC - Industria estandarrak: ISO 27001, IEC 62443, FSSC 22000 - Lan araudia: LPRL, Langileen Estatutua - Kodigo Penala: Delitu informatikoak (Art. 197-264)

---

2. ROLEN ETA ARDUREN DEFINIZIOA

2.1 RACI Matrix

Jarduera	Legal	CISO	DPO	CFO	CEO
Araudiaren Monitorizazioa	R	C	C	I	I
Inpaktu Ebaluazioa	R	R	C	C	A
Erantzun Planaren Garapena	C	R	C	C	A

Jarduera	Legal	CISO	DPO	CFO	CEO
Budget Esleipena	I	C	I	R	A
Kanpoko Aholkularitza Kontratatzea	R	C	C	A	A
Zuzendaritzari Reportatzea	R	R	C	I	A

2.2 Rol Deskribapenak

Legal Advisor (Arduradun Nagusia)

- Araudiaren interpretazio juridikoa
- BOE, DOUE eta aldizkari ofizialaren jarraipena
- Datu-base juridikoen kudeaketa
- Kanpoko legaleen koordinazioa

CISO (Compliance Technical Lead)

- Araudiaren inplikazio teknikoen ebaluazioa
- Kontrolen diseinu eta inplementazioa
- Teknologia-aldaketen kudeaketa
- Audit teknikoen koordinazioa

DPO (Data Protection Monitoring)

- GDPR eta LOPD-GDD aldaketen monitorizazioa
- AEPD irizpenen eta gidaliburuen jarraipena
- Europar jurisprudentziaren analisia

---

3. ARAUDIAREN INBENTARIOA

3.1 Enpresari Aplikagarria den Araudia

3.1.1 DATUEN BABESA

Araudia	Mota	Egoera	Azken Berrikusketa
RGPD (EU 2016/679)	Reglamento	Aktibo	2025-12-15
LOPD-GDD (LO 3/2018)	Lege Organikoa	Aktibo	2024-06-20
ePrivacy Directive (2002/58/EC)	Direktiba	Aktibo	2023-03-10
LSSI-CE (Ley 34/2002)	Lege	Aktibo	2022-01-18

Iturriak: - BOE: https://www.boe.es - AEPD: https://www.aepd.es - EUR-Lex: https://eur-lex.europa.eu

3.1.2 ZIBER-SEGURTASUNA

Araudia	Mota	Egoera	Azken Berrikusketa
ENS (RD 311/2022)	Real Decreto	Aktibo	2024-09-12
NIS2 Directive (EU 2022/2555)	Direktiba	Transposizioan	2025-10-17
CCN-STIC Guides	Gida Teknikoa	Aktibo	2025-11-05
Código Penal (Art. 197-264)	Lege	Aktibo	2023-07-01

Iturriak: - CCN-CERT: https://www.ccn-cert.cni.es - INCIBE: https://www.incibe.es - ENISA: https://www.enisa.europa.eu

3.1.3 KUDEAKETA ESTANDARRAK

Estandarra	Mota	Egoera	Azken Berrikusketa
ISO/IEC 27001:2022	Estandar	Inplementatzen	2023-10-25
ISO/IEC 27002:2022	Gida	Aktibo	2023-10-25
IEC 62443 (OT Security)	Estandar	Planifikatuta	2024-12-01
ISO 22301 (BCP)	Estandar	Planifikatuta	2025-03-15

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

3.1.4 SEKTORE ESPEZIFIKOA (Alimentazioa)

Araudia	Mota	Egoera	Aplikagarritasuna
FSSC 22000	Estandar	Ez inplementatua	Gomendioa
BRC Global Standard	Estandar	Ez inplementatua	Aukera
HACCP	Reglamento	Inplementatua	Nahitaezkoa
Reg (EC) 178/2002 (Food Law)	Reglamento	Aktibo	Nahitaezkoa

Oharra: Arau hauek ez dira ZG-ren parte, baina industria osotasunean beharrezkoak dira.

---

4. ARAUDIAREN JARRAIPENA - PROZEDURAK

4.1 Datu-Base Juridikoen Kontsulta

4.1.1 Iturriak Nazionalak

BOE (Boletín Oficial del Estado): - URL: https://www.boe.es - Kontsulta maiztasuna: **EGUNERO** (automated alert) - Arduraduna: Legal Advisor - Alertak: Email notifikazioak gako-hitzetan oinarrituak -

“protección de datos” - “ciberseguridad” - “seguridad de la información” - “sistemas de información”

AEPD (Agencia Española de Protección de Datos): - URL: https://www.aepd.es - Irizpenak eta jarraibideak - Kontsulta maiztasuna: **ASTERO** - Arduraduna: DPO - Aztertu behar da: - Irizpen bateratuak (nuevas) - Guías prácticas - Sanciones publicadas (jurisprudencia)

CCN-CERT (Centro Criptológico Nacional): - URL: https://www.ccn-cert.cni.es - CCN-STIC gidak - Kontsulta maiztasuna: **HILERO** - Arduraduna: CISO - Alertak: Bulletin suscription

4.1.2 Iturriak Europearrak

EUR-Lex (EU Legislation): - URL: https://eur-lex.europa.eu - Kontsulta maiztasuna: **HILERO** - Arduraduna: Legal Advisor - Gako-hitzak: - “data protection” - “cybersecurity” - “NIS directive”

ENISA (European Network and Information Security Agency): - URL: https://www.enisa.europa.eu - Threat landscapes, guides - Kontsulta maiztasuna: **HIRUHILEKOA** - Arduraduna: CISO

EDPB (European Data Protection Board): - URL: https://edpb.europa.eu - Guidelines, opinions - Kontsulta maiztasuna: **HILERO** - Arduraduna: DPO

4.1.3 Iturriak Internazionalak

ISO Updates: - URL: https://www.iso.org/news - Standard revisions - Kontsulta maiztasuna: **HIRUHILEKOA** - Arduraduna: CISO

NIST (National Institute of Standards and Technology): - URL: https://www.nist.gov/cybersecurity - Cybersecurity Framework updates - Kontsulta maiztasuna: **HIRUHILEKOA** - Arduraduna: CISO

OWASP (Open Web Application Security Project): - URL: https://owasp.org - Top 10, ASVS updates - Kontsulta maiztasuna: **URTERO** - Arduraduna: Development Lead

4.2 Automatizazio Tresnak

4.2.1 Alerta Sistema

RSS Feeds: - BOE RSS: Gako-hitzen araberako iragazkia - EUR-Lex RSS: “cybersecurity”, “data protection” - AEPD Newsletter: Email subscription

Tresna: Feedly, Inoreader, edo custom script (Python)

Eskema:

```
# Pseudo-kodea
feeds = [
    "https://www.boe.es/rss/boe/",
    "https://www.aepd.es/rss/novedades",
    "https://www.ccn-cert.cni.es/rss"
]

keywords = ["protección datos", "ciberseguridad", "RGPD", "NIS2"]

for feed in feeds:
    entries = parse_feed(feed)
    for entry in entries:
        if any(keyword in entry.title for keyword in keywords):
            send_alert(legal_team, entry)
```

4.2.2 Datu-Basea Kudeaketa

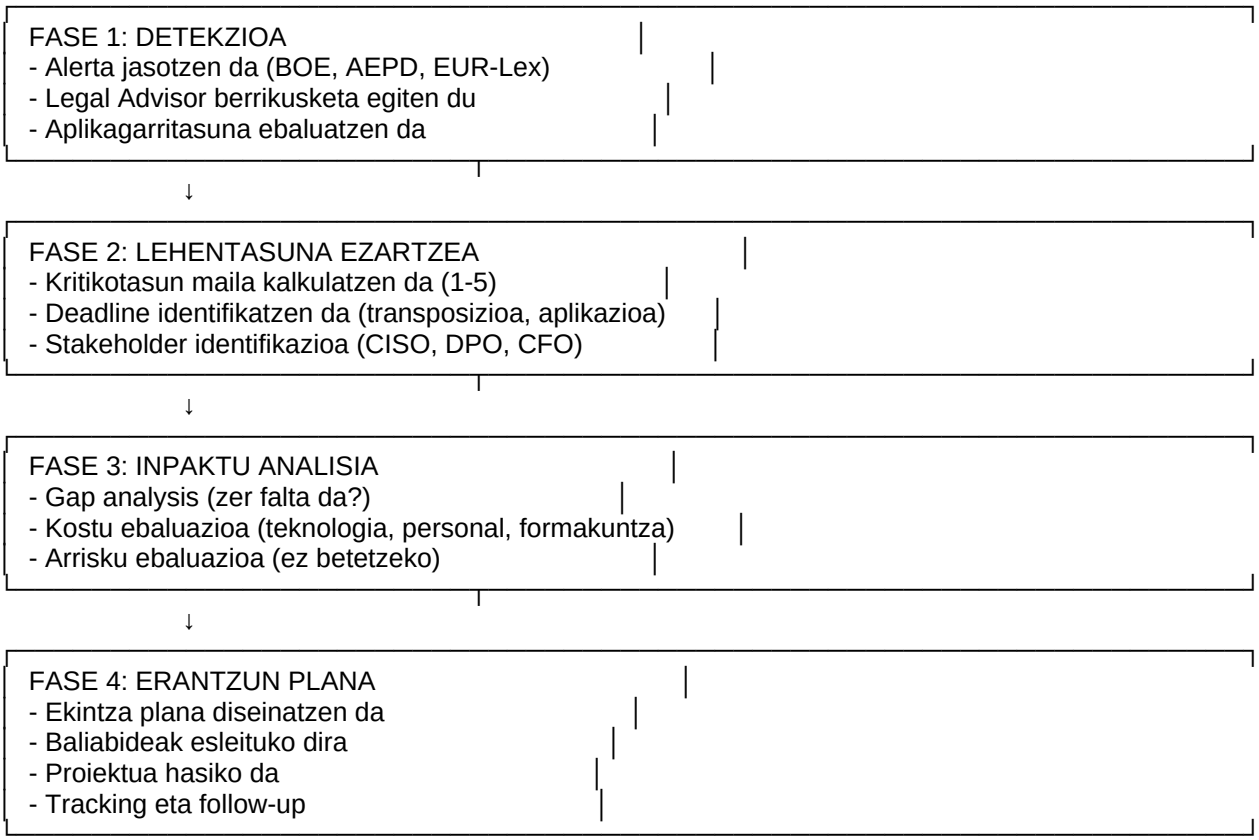
Tresna: Dokumentu Kudeaketa Sistema (Sharepoint, Confluence, edo custom)

Edukia: - Araudiaren inbentario taula (eguneratua) - Aldaketen log-a (changelog) - Inpaktu ebaluazio txostenak - Erantzun planaren dokumentuak

---

5. ARAUDIAREN ALDAKETA DETEKTATZEA

5.1 Detekzio Prozesu Fluxua



5.2 Kritikotasun Maila (Prioritization Matrix)

Kritikotasuna	Aplikagarritasun Epea	Isun Arriskua	Ekintza Berehala
5 - Kritikala	< 3 hileak	Oso Altua (>500k €)	Berehala (< 1 astea)
4 - Altua	3-6 hileak	Altua (100k-500k €)	Lehentasuna (< 1 hilea)
3 - Ertaina	6-12 hileak	Ertaina (10k-100k €)	Planifikatua (< 3 hileak)
2 - Baxua	1-2 urteak	Baxua (<10k €)	Gomendioa (< 6 hileak)
1 - Informatiboa	> 2 urteak	Ez dago	Monitorizazioa

Adibide Kalkulua:

NIS2 Transposizioa (2024):
- Aplikagarritasun Epea: 6 hileak geratzen → 4 puntuak

- Isun Arriskua: 10M € arte (2% cifra) → 5 puntuak
- Inpaktua: IT + OT sistemak → 5 puntuak
- KRITIKOTASUNA = (4 + 5 + 5) / 3 = 4.67 → KRITIKAL (5)

---

6. INPAKTU EBALUAZIOA

6.1 Impact Assessment Template

Dokumentua: Araudiaren Aldaketa Impact Assessment

Atalak	Deskribapena
1. Araudiaren Identifikazioa	Izena, zenbakia, data
2. Laburpena	Araudiaren helburua (executive summary)
3. Aplikagarritasuna	Zabala Gailetak-i aplikatzen zaio?
4. Deadlines	Noiz sartu behar da indarrean?
5. Gap Analysis	Zer falta da gaur egun?
6. Kontrolen Beharrak	Zer kontrol teknikoa behar da?
7. Kostuen Estimazioa	Teknologia, personal, formakuntza
8. Arrisku Ez-betetzearen	Zer gertatzen da ez badugu betetzen?
9. Gomendioak	Ekintza planaren proposamena
10. Onarpenaren Beharrak	Nor behar du onartu? (CGC, CEO)

6.2 Gap Analysis Prozesua

Pausuak: 1. **Araudiaren Requirement listatu** (artikulu bakoitza) 2. **Egungo egoera ebaluatu** (zer daukagu?) 3. **Gap identifikatu** (zer falta da?) 4. **Prioritizatu** (zer da kritikoena?) 5. **Kostu estimatu** (zenbat kostatu?) 6. **Plan diseinatu** (nola konpondu?)

Adibidea: NIS2 Directive Gap Analysis

Requirement (NIS2)	Egungo Egoera	Gap	Kostua	Epea
Incident notification (24h)	Ez dago prozedura	SOP sortu	5.000€	2 hileak
Supply chain risk mgmt	Informal	Vendor assessment program	20.000€	4 hileak
Cyber hygiene measures	Partial (MFA 60%)	MFA 100% + EDR	50.000€	3 hileak
Business continuity plan	Badago baina ez testatua	Testing + improvement	10.000€	3 hileak

Requirement (NIS2)	Egungo Egoera	Gap	Kostua	Epea
TOTALA	-	-	**85.000€**	**4 hileak**

---

7. ERANTZUN PLANA GAUZATZEA

7.1 Ekintza Planaren Garapena

Template: Regulatory Compliance Action Plan

Elementua	Deskribapena
Araudiaren Izena	Adib: NIS2 Directive (EU 2022/2555)
Helburua	NIS2 betetze osoa lortu Zabala Gailetak-en
Scope	IT + OT sistemak, incidenteen kudeaketa
Owner	CISO
Stakeholders	CEO, Legal, CFO, Ops Director
Budget	85.000€
Deadline	2026-10-17 (NIS2 transposition)
Milestones	- M1: Gap analysis (Complete)

- M2: MFA 100% (2026-04-30)
- M3: EDR deployment (2026-05-31)
- M4: SOP incident notification (2026-06-30)
- M5: Vendor assessment (2026-08-31)
- M6: BCP testing (2026-09-30)
- M7: Final audit (2026-10-15) | | **Arriskuak** | Budget insufizientea, baliabide eskasia | | **KPIs** | - MFA adoption: 100%
- EDR coverage: 100%
- Incident response SOP: Approved
- Vendor assessments: 10/10 completed |

7.2 Proiektu Kudeaketa

Metodologia: PRINCE2 edo Agile (Scrum)

Tresnak: - Jira, Asana, Microsoft Project

Tracking: - Weekly status meetings - Monthly progress reports (CGC) - Risk log (updated weekly) - Issue log (resolved < 1 week)

---

8. URTEKO BERRIKUSKETA EGUTEGIA

8.1 Quarterly Legal Review (Hiruhilekoa)

Noiz: Q1, Q2, Q3, Q4 amaieran **Nor:** Legal Advisor + CISO + DPO **Iraupena:** 2-3 orduak

Agenda: 1. Azken hiruhilekoan argitaratutako araudiak berrikusi (15 min) 2. Aplikagarritasuna ebaluatu (30 min) 3. Indarreko ekintza planen progress review (45 min) 4. Gap identification berria (30 min) 5. Budget review eta adjustments (20 min) 6. Next quarter priorities (10 min)

Deliverable: Quarterly Compliance Report (CGC-ra bidal)

8.2 Annual Comprehensive Review (Urtekoa)

Noiz: Abenduan **Nor:** CGC (Compliance Governance Committee) osoa **Iraupena:** 1 egun (workshop)

Agenda: 1. Urteko berrikusketa: Aplikatutako araudia (1h) 2. Compliance posture assessment (ISO 27001, GDPR, ENS, NIS2) (2h) 3. Lecciones aprendidas (incidents, audits) (1h) 4. Budget review: Gastua vs. Planifikatua (1h) 5. 2027ko priorities ezartzea (2h) 6. Araudiaren Roadmap (2027-2029) (1h)

Deliverable: - Annual Compliance Report (Board of Directors) - 2027 Compliance Budget - 2027 Compliance Roadmap

---

9. DOKUMENTAZIO ETA ERREGISTROAK

9.1 Dokumentu Erregistroak

Kokapena: /compliance/regulatory_monitoring/

Fitxategiak: - regulatory_inventory.xlsx - Araudiaren zerrenda - regulatory_changelog.md - Aldaketen log-a - impact_assessments/ - Karpeta IA dokumentuekin - action_plans/ - Karpeta ekintza planarekin - quarterly_reviews/ - Karpeta hiruhileko txostenekin - annual_reports/ - Karpeta urteko txostenekin

9.2 Metadata Erregistroak

Datu-Basean (Sharepoint, Confluence):

Aldaketa bakoitzeko: - Araudiaren izena - Argitaratze data - Aplikagarritasun epea - Kritikotasuna (1-5) - Assigned owner - Egoera (Open, In Progress, Closed) - Budget allocated - Actual spend - Comments

---

10. ESKALAKETA PROZEDURA

10.1 Araudiaren Aldaketa Kritikala

Eszenarioa: Araudia berria edo aldaketa kritikala (Kritikotasun 4-5)

Fluxua:

1. Legal Advisor detekta aldaketa → BEREHALA
   ↓
2. Impact Assessment azkar (< 48h)

↓
3. CISO + DPO kontsulta (< 72h)
↓
4. Compliance Governance Committee alerta (< 1 astea)
↓
5. Emergency meeting konbokatu (< 2 astek)
↓
6. Ekintza plana onartu eta Budget esleitu (< 3 astek)
↓
7. Proiektua hasi → BEREHALA ondoren

Komunikazio Kanala: - Email + SMS (urgent) - Slack/Teams channel (#compliance-alerts) - Phone call (if > 1M € fine risk)

10.2 Araudiaren Aldaketa Ez-Kritikala

Eszenarioa: Araudia aldaketa txikia edo gomendioa (Kritikotasun 1-3)

Fluxua:

1. Legal Advisor detekta aldaketa
↓
2. Quarterly Review biltzarrean eztabaidatu
↓
3. Ekintza plana diseinatu (if needed)
↓
4. Normal project flow (backlog → sprint → delivery)

---

11. KANPOKO AHOLKULARIEN KUDEAKETA

11.1 Legala Asesoria Externa

Noiz erabili: - Araudia konplexua edo anbiguoa da - Isun arriskua oso altua da (> 500k €) - Epaitegiaren kasua da (jurisprudentzia) - Kanpoko auditoriari aurre egin behar zaio

Hornitzaileak: - Bufete Garmendia & Asociados (Madrid) - Privacy Legal (Bilbo) - ECIJA Abogados (Barcelona)

Budget: 15.000€/urteko (2026)

11.2 Teknologia Kontsultantak

Noiz erabili: - Gap analysis tekniko konplexua (ISO 27001, IEC 62443) - Implementazio teknikoa behar da (MFA, EDR, SIEM) - Penetration testing edo audit tekniko bat

Hornitzaileak: - S2 Grupo (Valencia) - Tarlogic (Madrid) - ElevenPaths (Telefónica)

Budget: Proiektu bakoitzeko

---

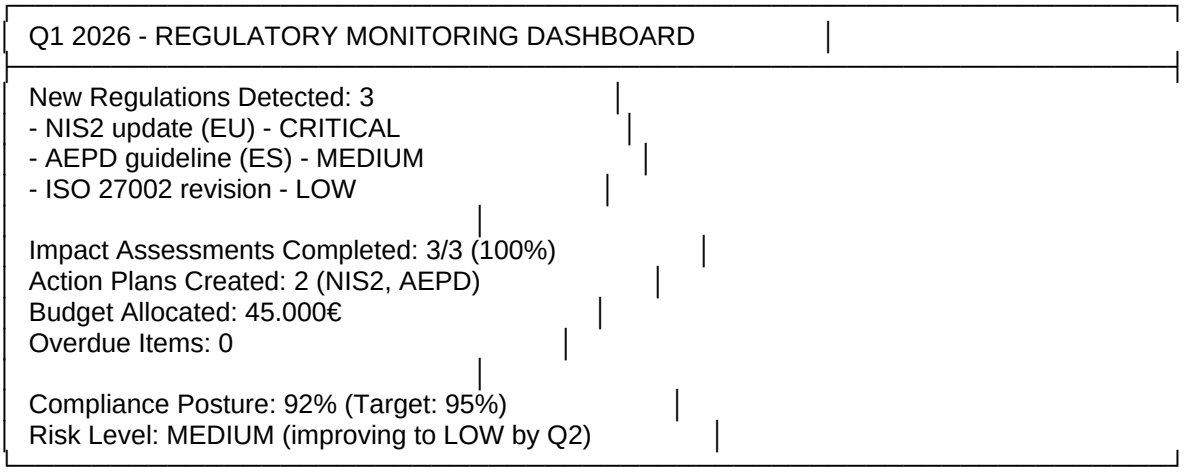
12. METRIKA ETA KPI

12.1 Araudiaren Monitorizazio KPIs

KPI	Target	Maiztasuna
Regulatory sources monitored	100% (guztiak)	Egunero
New regulations detected	-	Tracking
Time to impact assessment	< 72h	Per regulation
Compliance gap closure rate	> 90%	Quarterly
Budget vs. actual (compliance)	± 10%	Quarterly
Overdue action items	0	Monthly
Regulatory fines	0 €	Annual

12.2 Quarterly Dashboard

CEO + CGC-rako txostena:



---

13. LECCIONES APRENDIDAS ETA HOBEKUNTZA

13.1 Post-Implementation Review

Proiektu bakoitzaren ondoren (adib: NIS2 implementation):

Galderak: 1. Prozedura hau funtzionatu al du? 2. Impact assessment zehatza izan zen? 3. Budget eta timeline errealistak ziren? 4. Zer hobetu genezake?

Dokumentazioa: Lessons Learned Report (Sharepoint)

13.2 Prozedura Hobekuntza

Maiztasuna: Urtero (Annual Review-en)

Fokoa: - Automatizazioa hobetu (alertak, reportak) - Datu-basea egitura optimize - Stakeholder communication hobetu - Training eta awareness programak

---

14. FORMAKUNTZA ETA AWARENESS

14.1 Legal Team Training

Maiztasuna: Biurtekoa **Edukia:** - Araudia berrien interpretazioa - Datu-base juridikoen erabilea - Impact assessment teknikak - Compliance governance best practices

Hornitzailea: Kanpoko aholkulariak edo ICAB/ICAM

14.2 Technical Team Awareness

Maiztasuna: Quarterly (hiruhilekoa) **Edukia:** - Araudia aldaketen laburpenak - Kontrolen implementazio beharrak - Case studies (beste enpresak) - Q&A session

Formatua: Webinar edo in-person session (1h)

---

15. ERREFERENTZIAK

15.1 Datu-Base Juridikoak

Nazionala: - BOE: https://www.boe.es - AEPD: https://www.aepd.es - CCN-CERT: https://www.ccn-cert.cni.es - INCIBE: https://www.incibe.es

Europaarra: - EUR-Lex: https://eur-lex.europa.eu - EDPB: https://edpb.europa.eu - ENISA: https://www.enisa.europa.eu

Internazionala: - ISO: https://www.iso.org - IEC: https://www.iec.ch - NIST: https://www.nist.gov - OWASP: https://owasp.org

15.2 Barneko Dokumentuak

- /compliance/compliance_governance_framework.md
- /compliance/sgsi/information_security_policy.md
- /compliance/sgsi/risk_assessment.md
- /compliance/gdpr/privacy_notice_web.md

---

16. BERRIKUSKETA ETA EGUNERAKETA

Berrikusketa Maiztasuna: Sei hilean behin (Ekaina eta Abendua) **Arduraduna:** Legal Advisor + CISO **Onarpena:** CGC

16.1 Aldaketa Log-a

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

---

17. ONARPENA

Prozedura hau Compliance Governance Committee-ak onartu du:

Rola	Izena	Sinadura	Data
Legal Advisor	Itziar Sarasola	_____	2026-02-05
CISO	Mikel Etxebarria	_____	2026-02-05
CEO	Jon Zabala	_____	2026-02-05

HURRENGO BERRIKUSKETA: 2026-08-05

Prozedura hau sortu da RA5 (Araudiaren Aplikazioa) betebeharrak betetzeko, Erronka 4 - ZG (Zibersegurtasunaren Arloko Araudia) atalean.