Marco de Gobernanza de Cumplimiento Normativo

Compliance Governance Framework

Enpresa: Zabala Gailetak, S.L. **Dokumentu Mota:** Marco de Gobernanza **Bertsioa:** 1.0 **Data:** 2026-02-05 **Jabea:** CISO + Legal **Egoera:** Indarrean

---

1. XEDEA ETA IRISMENA

1.1 Helburua

Dokumentu honek Zabala Gailetak enpresaren **Gobernantza egitura** definitzen du, ziber-segurtasunaren eta araudiari dagokion betetzearen kudeaketarako.

Helburu nagusiak:

1. Araudiaren betetze-ardura eta rol argi eta garbiak ezartzea
2. Erabakien eskalaketarako fluxu egokiak finkatzea
3. Betetze mailan gobernu oneko printzipioak aplikatzea
4. Etika profesionala araudiaren betebeharrean txertatzea

1.2 Irismena

Aplikazio-eremua:

- ✅ Erakunde osoa (IT, OT, Admin, Ekoizpena)
- ✅ Compliance-aren kudeaketa estrategikoa eta operatiboa
- ✅ Araudia: GDPR, LOPD-GDD, ENS, NIS2, ISO 27001, IEC 62443
- ✅ Rol guztiak: Zuzendaritza, Kudeaketa, Langile teknikoak

---

2. GOBERNU ONEKO PRINTZIPIOAK

2.1 Printzipio Nagusiak (ISO 38500)

Zabala Gailetak ondorengo printzipioak aplikatzen ditu gobernantzan:

P1. ARDURA (Responsability)

- Zuzendaritzak ulertu eta onartu behar ditu segurtasun eta compliance ardurak
- Kanpoko eta barneko alderdiei emandako konpromisoak bete behar dira
- Liderrak accountable dira araudiaren urraketeengatik

P2. ESTRATEGIA (Strategy)

- Enpresaren estrategia negozio-beharretara lerrokatua
- Ziber-segurtasuna core business strategy integratua
- Compliance ez da oztopo, baizik eta lehiakortasun abantaila

P3. ESKURATZEA (Acquisition)

- Erabaki informatuak hartu behar dira arriskuen, kostuen eta aukeren analisi argia eginda
- Transparentzia hornitzaile eta zerbitzuen aukeraketan
- Due diligence ezarri behar da kanpoko hornitzaileekin

P4. ERRENDIMENDUA (Performance)

- Compliance neurriak KPI eta metrikak bitartez jarraitu behar dira
- Txostenak periodikoki egin behar dira zuzendaritzari
- Helburuak ezarri eta bete behar dira

P5. KONFORMITATEA (Conformance)

- Araudia eta estandarrak bete behar dira beti
- Politikak eta prozedurak errespetatu behar dira organizazio maila guztietan
- Auditoriak erregularki egin behar dira

P6. GIZA PORTAERA (Human Behaviour)

- Segurtasun politikak giza faktorea kontuan hartzen dute
- Awareness programak langile guztientzat
- Kultura: “Security & Compliance by Default”

---

3. EGITURA ORGANIZATIBOA - COMPLIANCE

3.1 Compliance Governance Committee (CGC)

Osaera:

- 👔 CEO (Jon Zabala) - Presidente

- 🔒 CISO (Mikel Etxebarria) - Compliance Lead
- 🛡️ DPO (Ainhoa Uriarte) - Data Protection Lead
- ⚖️ Legal Advisor (Itziar Sarasola) - Legal Compliance
- 💼 CFO (Eneko Garitano) - Financial & Audit
- 🏭 Operations Director (Koldo Agirre) - OT Compliance

Funtzioak:

- Compliance estrategiaren definizioa
- Arrisku nagusien erabaki-hartzea
- Araudiaren eguneraketen ebaluazioa
- Aurrekontuen onespena (compliance investments)
- Gobernantza politiken berrikuspena (urtero)

Bilera Maiztasuna:

- 📅 Quarterly Review (hiruhilekoa)
- 🚨 Ad-hoc (gorabeherak gertatu ezkero)

3.2 CISO (Chief Information Security Officer)

Ardura Nagusiak:

1. Segurtasun estrategiaren garapena eta exekuzioa
2. Compliance programa teknikoaren kudeaketa
3. SGSI (ISO 27001) jabetasuna
4. Arrisku teknikoen ebaluazioa eta tratamendua
5. Audit teknikoen koordinazioa
6. Gorabeheren erantzuna (Incident Response)

Reporta: CEO + CGC

KPIs:

- Security posture score (mensual)
- Compliance audit findings (quarterly)
- Incident response time (real-time)
- Vulnerability remediation rate (mensual)

3.3 DPO (Data Protection Officer)

Ardura Nagusiak:

1. GDPR eta LOPD-GDD betetzearen gainbegiraketa
2. Datu pertsonalen tratamenduen aholkularitza
3. Datu-babesaren arriskuen ebaluazioa (DPIAs)
4. AEPD eta DPA-ekin harremana (autoritate eskudunak)
5. Langile eta zuzendaritzaren formakuntza (GDPR)
6. Interesdunaren eskubideen kudeaketa (ARCO)

Reporta: CEO (independentzia bermatzeko)

KPIs:

- DPIA completion rate (100%)
- Data subject requests response time (<30 days)
- GDPR training completion (100% staff)
- Data breach notification compliance (72h)

3.4 Legal Advisor

Ardura Nagusiak:

1. Araudiaren interpretazio juridikoa
2. Kontratuen azterketa (compliance clauses)
3. Araudiaren aldaketen jarraipena (monitoring)
4. Akats administratiboen eta isunen kudeaketa
5. Kanpoko auditoreekin eta arautzaileekin koordinazioa

Reporta: CFO + CGC

3.5 IT Compliance Officer (barneko rola)

Ardura Nagusiak:

1. Politiken aplikazioa sisteman (implementazioa)
2. Teknologia kudeaketa (patching, hardening)
3. Log-ak eta jarraipena (SIEM, monitoring)
4. Backup eta berreskuratze planen exekuzioa
5. Security awareness programen entrega

Reporta: CISO

3.6 OT Compliance Officer (barneko rola)

Ardura Nagusiak:

1. IEC 62443 aplikazioa fabrika sisteman
2. PLCs eta SCADA sistemen segurtasuna
3. IT/OT segregazioaren mantenua
4. Intzidenteen detekzioa OT inguruan
5. Vendor management (OT suppliers)

Reporta: Operations Director + CISO (matrix)

---

4. RACI MATRIX - COMPLIANCE JARDUERAK

4.1 RACI Legenda

- **R** = Responsible (Erantzulea - exekutatzen duena)
- **A** = Accountable (Kontu-emaile - azken ardura duena)
- **C** = Consulted (Kontsultatua - informazioa ematen duena)
- **I** = Informed (Informatua - emaitzak jasotzen dituena)

4.2 RACI Taula

Jarduera	CEO	CISO	DPO	Legal	CFO	Ops Dir
Compliance Estrategia	A/R	C	C	C	C	C
SGSI Kudeaketa (ISO 27001)	I	A/R	C	C	I	C
GDPR Programak	I	C	A/R	C	I	I
Arriskuen Ebaluazioa	A	R	C	C	C	C
Politiken Onarpena	A	R	C	C	I	C
Gorabeheren Erantzuna	I	A/R	C	C	I	C
Audit Teknikoak	I	A/R	C	I	C	C
DPIA Garapen	I	C	A/R	C	I	C
Langile Formazioa	A	R	C	C	I	R
Araudiaren Jarraipena	I	C	C	A/R	I	I
Hornitzaile Kudeaketa	C	R	C	C	A	R
OT Segurtasuna (IEC 62443)	I	C	I	I	I	A/R

Jarduera	CEO	CISO	DPO	Legal	CFO	Ops Dir
Urraketa Jakinarazpena	A	R	R	R	I	C
Budget Compliance	A	C	C	C	R	C

---

5. ERABAKIEN ESKALAKETA FLUXUA

5.1 Arrisku Matrize - Eskalaketa

```
┌──────────────────────┬──────────────────┬──────────────────────┐
│ KRITIKOTASUNA        │ ARDURA           │ EPEA                 │
├──────────────────────┼──────────────────┼──────────────────────┤
│ KRITIKAL (Gorria)    │ CEO + CGC        │ < 4 orduko erab.     │
│ ALTUA (Laranja)      │ CISO + DPO       │ < 24 orduko erab.    │
│ ERTAINA (Horia)      │ IT/OT Officer    │ < 1 asteko erab.     │
│ BAXUA (Berdea)       │ Team Lead        │ < 1 hileko erab.     │
└──────────────────────┴──────────────────┴──────────────────────┘
```

5.2 Eskalaketa Prozedurak

5.2.1 Kritikal (Kritikotasuna: GORRIA)

Adibideak:

- Ransomware incidentea
- Data breach masibo (>100 langileak)
- OT sistema konprometitua (produkzioa gelditu)
- AEPD ikuskapen bat

Fluxua:

```
1. Detekzioa (SIEM, SOC, Langile)
   ↓
2. IT/OT Officer berifikatu (15 min)
   ↓
3. CISO jakinarazi (30 min)
   ↓
4. CEO + CGC aktibatu (< 1 ordua)
   ↓
5. Crisis Management Team aktibatu
   ↓
6. Erabaki estrategikoa:
   - Sistemen isolamendua?
   - Erreskatea ordaindu?
```

```
   - AEPD jakinarazi?
   - PR komunikazioa?
```

Decision Makers: CEO (final word) + CISO + DPO + Legal

5.2.2 Altua (Kritikotasuna: LARANJA)

Adibideak:

- Phishing kanpaina arrakastatsua
- Ahulezia kritiko bat CVE altua
- Politika urraketa larria
- Audit finding critical

Fluxua:

```
1. Detekzioa
   ↓
2. IT/OT Officer maneiatu (1-4 ordu)
   ↓
3. CISO reportatu (< 24 ordu)
   ↓
4. Ekintza Plana proposatu
   ↓
5. DPO/Legal kontsultatu (behar izanez gero)
   ↓
6. CISO onartzen du plana
```

Decision Maker: CISO (DPO/Legal advice-rekin)

5.2.3 Ertaina (Kritikotasuna: HORIA)

Adibideak:

- Politika eguneraketa txikiak
- Ahulezia medium bat
- Log anomalia ez-kritikoak
- Formakuntza programen aldaketak

Fluxua:

```
1. Identifikazioa
   ↓
2. IT/OT Officer planifikazioa (< 1 astea)
   ↓
3. Konpontze plana gauzatu
```

```
   ↓
4. CISO reportatu (weekly report)
```

Decision Maker: IT/OT Compliance Officer

5.2.4 Baxua (Kritikotasuna: BERDEA)

Adibideak:

- Dokumentazio eguneraketak
- Ohiko mantenimendu lanak
- Awareness kanpainak
- Politika berrikusketa rutinak

Fluxua:

```
1. Identifikazioa
   ↓
2. Team Lead asignazioa
   ↓
3. Gauzatzea (< 1 hilea)
   ↓
4. IT/OT Officer reportatu (monthly)
```

Decision Maker: Team Lead

---

6. ETIKA PROFESIONALA

6.1 Kode Etikoa - Compliance

Zabala Gailetak-ek ondorengo balioetan oinarritzen da:

6.1.1 GARDENTASUNA (Transparency)

- Datuen tratamenduak argiak eta ulergarriak izan behar dira
- Compliance egoera reala reportatu behar da (ez “window dressing”)
- Akatsen aitortzea eta konpontzea (blameless culture)

6.1.2 INTEGRITATETASUNA (Integrity)

- Araudia betetzea nahitaezkoa da, baldin eta onuragarria ez bada ere
- Ez dago “atajos” compliance-an
- Security teatralitatea (checkbox compliance) EZ da onartzen

6.1.3 KONFIDENTZIALTASUNA (Confidentiality)

- Datu pertsonalek behar duten babesa jaso behar dute
- “Need-to-know” printzipioa aplikatzen da
- Informazio sentsibleak ez dira inoiz partekatu ezin bada justifikatu

6.1.4 ERRESPETUA (Respect)

- Langile guztien pribatutasuna errespetatzen da
- Monitoritzazioa egiten da, baina proportzionaltasun printzipioaz
- Interesdunaren eskubideak lehentasuna dute

6.1.5 ARDURA SOZIALA (Social Responsibility)

- Zabala Gailetak konprometitua da gizartearekin
- Datuak ez dira inoiz saldu edo partekatu hirugarrenei baldin legerik ez badago
- Kanpo-eragina positiboa: industria-estandarrak jarraitzea eta bultzatzea

6.2 Diziplina Prozedura

Politika urraketeengatik diziplina neurriak aplika daitezke:

Urraketa Maila	Lehen Aldiz	Bigarren Aldiz	Hirugarren Aldiz
Txikia	Ohartaraztea	Erreprimenda idatzia	Erreprimenda grabia
Ertaina	Erreprimenda idatzia	Suspendimendua (3 egun)	Kaleratze-espedientea
Larria	Kaleratze-espedientea	Kaleratzea	Salaketa penala
Oso Larria	Kaleratzea bertakoa	Salaketa penala	-

Adibideak:

- Txikia: Password partekatzea lankideekin
- Ertaina: USB zifratu gabeak erabiltzea datu pertsonalekin
- Larria: Intentional policy bypass, datuen exfiltrazioa
- Oso Larria: Sabotajea, espioitza, malware instalatzea

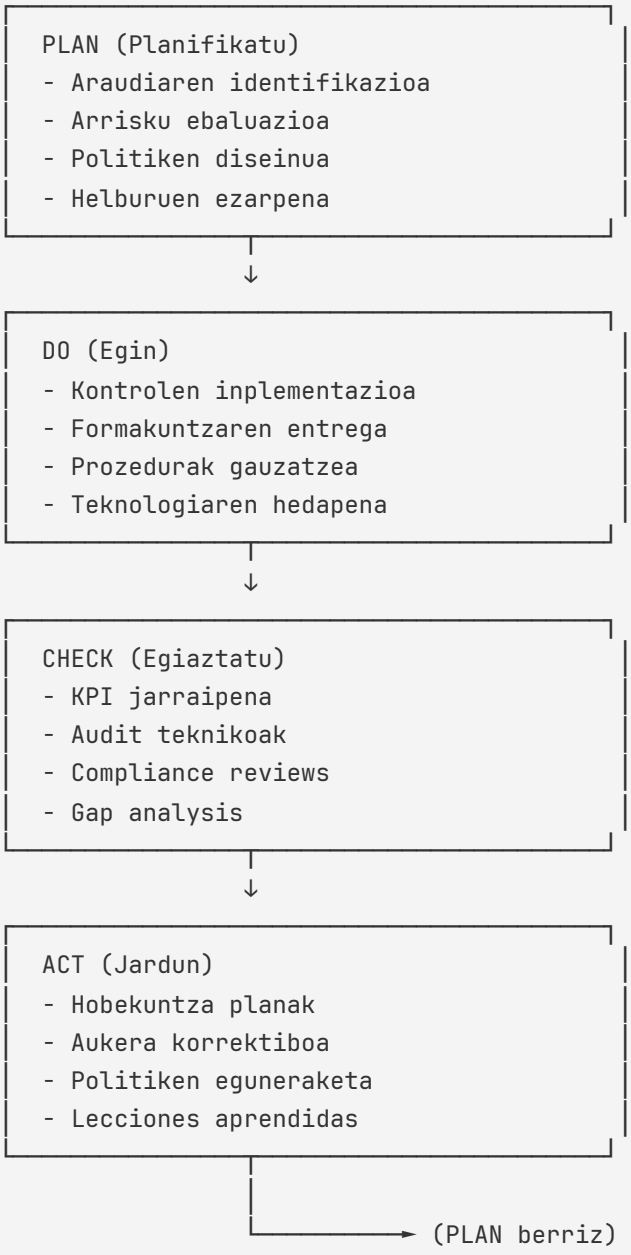
Dokumentazioa: `/Zabala Gailetak/compliance/sgsi/diziplina_prozedura.md`

---

7. GOBERNANTZA ZIKLOA (Governance Cycle)

7.1 Plan-Do-Check-Act (PDCA)

Zabala Gailetak-ek PDCA zikloa aplikatzen du compliance gobernantzan:



7.2 Urteko Gobernantza Egutegia

Hilabetea	Jarduera Nagusia
Urtarrila	Urteko planning (Compliance Roadmap)
Otsaila	Q1 CGC Review + Budget review
Martxoa	Awareness campaign (GDPR)
Apirila	Internal audit (ISO 27001)

Hilabetea	Jarduera Nagusia
Maiatza	Q2 CGC Review + Risk assessment
Ekaina	Politiken eguneraketa (urteko berrikusketa)
Uztaila	Formakuntza (summer session)
Abuztua	Q3 CGC Review
Iraila	Araudiaren monitorizazioa (legal update review)
Urria	External audit prep (ISO 27001)
Azaroa	Q4 CGC Review + Lessons learned
Abendua	Urteko txostena + 2027ko helburuak

---

8. KOMUNIKAZIO KANALAK

8.1 Komunikazio Hierarkia

8.1.1 Gorantz (Upward Communication)

- IT/OT Officer → CISO (weekly, astero)
- CISO → CEO (monthly, hilero)
- DPO → CEO (monthly, hilero)
- CGC → Board of Directors (quarterly, hiruhilekoa)

8.1.2 Beherantz (Downward Communication)

- CEO → CGC (strategic decisions)
- CISO → IT/OT Officers (tactical decisions)
- All Management → Staff (policies, awareness)

8.1.3 Alborantz (Horizontal Communication)

- CISO ↔ DPO (weekly sync)
- IT Officer ↔ OT Officer (daily stand-ups)
- Legal ↔ CISO (as needed - contractual reviews)

8.2 Txosten Motak

8.2.1 Executive Dashboard (CEO + CGC)

Maiztasuna: Monthly **Edukia:**

- Compliance posture (%)
- Top 5 risk indicators
- Budget vs actual (compliance spend)
- Regulatory updates
- Key incidents (if any)

8.2.2 Technical Compliance Report (CISO)

Maiztasuna: Weekly **Edukia:**

- Vulnerability status
- Patch compliance (%)
- Security events (SIEM)
- Audit findings remediation
- Open action items

8.2.3 GDPR Compliance Report (DPO)

Maiztasuna: Quarterly **Edukia:**

- Data subject requests (ARCO)
- DPIA status
- Breaches (if any)
- Training completion
- Third-party processor reviews

---

9. BALIABIDE KUDEAKETA

9.1 Compliance Budget

Zabala Gailetak compliance aurrekontua esleituko du urtero:

Kategoria	% Aurrekontu	2026 Budget
Personal (CISO, DPO, Officers)	60%	300.000 €
Teknologia (SIEM, EDR, DLP)	25%	125.000 €

Kategoria	% Aurrekontu	2026 Budget
Formazioa (Awareness, certs)	5%	25.000 €
Auditoriak (Internal + External)	5%	25.000 €
Legalak (Lawyer, fines coverage)	3%	15.000 €
Hobetzeak (Projects)	2%	10.000 €
TOTALA	100%	**500.000 €**

9.2 Vendor Management

Kanpoko hornitzaileak CGC-k onartu behar ditu:

- ✅ Legal contracts dituzten compliance clauses
- ✅ Due diligence (security assessment)
- ✅ SLA (Service Level Agreements)
- ✅ Right to audit clauses
- ✅ Data Processing Agreements (GDPR)

Hornitzaile Kritikoak:

- SOC/SIEM provider
- Cloud providers (AWS, Azure)
- Auditing firms
- Legal advisors
- OT vendors (Siemens, Allen Bradley)

---

10. KPI ETA METRIKA

10.1 Compliance KPIs

KPI	Target	Maiztasuna
ISO 27001 Compliance	95%+	Quarterly
GDPR Compliance	100%	Monthly
Policy Adherence	90%+	Monthly
Training Completion	100%	Annual

KPI	Target	Maiztasuna
Audit Findings (Critical)	0	Quarterly
Incident Response Time	< 1h	Real-time
Patch Compliance	95%+	Weekly
MFA Adoption	100%	Monthly
DPIA Completion	100%	Quarterly
Vulnerability Remediation (Critical)	< 7 days	Weekly

10.2 Governance Maturity Model

```
Level 5: OPTIMIZED (Hobekuntza etengabea)
  ↑
Level 4: MANAGED (Neurgarria eta kontrolatua)
  ↑
Level 3: DEFINED (Prozesuak definituak eta dokumentatuak)
  ↑
Level 2: REPEATABLE (Ad-hoc baina errepikagarria)
  ↑
Level 1: INITIAL (Kaotikoa, erreaktiboak)
```

Zabala Gailetak Current State: Level 3 (Defined) **Zabala Gailetak Target (2027):** Level 4 (Managed)

---

11. BERRIKUSKETA ETA EGUNERAKETA

11.1 Dokumentuaren Berrikusketa

Maiztasuna: Urtero (Ekaina) **Arduraduna:** CISO + Legal **Prozesua:**

1. Araudiaren aldaketen analisia
2. Egitura organizatiboaren aldaketak
3. Lessons learned azken urtekoak
4. KPI review eta target adjustment
5. CGC-k berrikuspena eta onarpena

11.2 Eguneraketa Historikoa

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

---

12. ERREFERENTZIAK

12.1 Araudia

- ISO/IEC 38500:2015 - Governance of IT
- ISO/IEC 27001:2022 - Information Security Management
- GDPR (EU 2016/679)
- LOPD-GDD (Ley Orgánica 3/2018)
- ENS (Real Decreto 311/2022)

12.2 Best Practices

- COBIT 5 (Control Objectives for IT)
- NIST Cybersecurity Framework
- COSO Framework (Internal Controls)
- ITIL v4 (IT Service Management)

12.3 Barneko Dokumentuak

- `/compliance/sgsi/information_security_policy.md`
- `/compliance/sgsi/risk_assessment.md`
- `/compliance/gdpr/privacy_notice_web.md`
- `/compliance/sgsi/diziplina_prozedura.md`

---

13. ONARPENA

Dokumentu hau Compliance Governance Committee-ak onartu du:

Rola	Izena	Sinadura	Data
CEO	Jon Zabala	_____	2026-02-05
CISO	Mikel Etxebarria	_____	2026-02-05
DPO	Ainhoa Uriarte	_____	2026-02-05

Rola	Izena	Sinadura	Data
Legal	Itziar Sarasola	_____	2026-02-05
CFO	Eneko Garitano	_____	2026-02-05
Ops Dir	Koldo Agirre	_____	2026-02-05

ONARPENA: Dokumentu hau indarrean dago 2026-02-05tik aurrera.

HURRENGO BERRIKUSKETA: 2027-06-30

Dokumentua sortu da Zabala Gailetak-en Compliance Governance Program-aren parte gisa, Erronka 4 - ZG (Zibersegurtasunaren Arloko Araudia) betebeharrak betetzeko.