csirt_roster

CSIRT Roster — Zabala Gailetak

Computer Security Incident Response Team

Dokumentu Kodea: NIS2-CSIRT-001
Bertsioa: 1.0
Data: 2026-02-06
Sailkapena: KONFIDENTZIALA
NIS2 Artikulua: Art. 21.2.b, Art. 23

---

1. CSIRT Osaera / Team Composition

1.1 Talde Nagusia (Core Team)

Rola	Izena	Postua	Telefonoa	Email	Guardia
Incident Commander	Mikel Etxebarria	CISO	+34 6XX XXX XX1	ciso@zabala-gailetak.eus	24/7
Technical Lead	[Izendatu]	IKT Arduraduna	+34 6XX XXX XX2	it-lead@zabala-gailetak.eus	L-V 08-20
Privacy Lead (DPO)	Ainhoa Uriarte	DPO	+34 6XX XXX XX3	dpo@zabala-gailetak.eus	L-V 09-18
Legal Advisor	[Izendatu]	Legal	+34 6XX XXX XX4	legal@zabala-gailetak.eus	L-V 09-18
Communications	[Izendatu]	Komunikazio Ard.	+34 6XX XXX XX5	comms@zabala-gailetak.eus	L-V 09-18
OT Specialist	[Izendatu]	OT Ingeniaria	+34 6XX XXX XX6	ot-eng@zabala-gailetak.eus	L-V 08-20

1.2 Kanpo Laguntza / External Support

Hornitzailea	Zerbitzua	Kontaktua	SLA
SOC 24/7 (kontratatzeko)	SIEM monitorizazioa, Alerta triage	soc@provider.com	15 min erantzun
CrowdStrike	EDR incident response	support@crowdstrike.com	1h P1
INCIBE-CERT	CSIRT Nazionala	incidencias@incibe-cert.es	NIS2 Art.23

Hornitzailea	Zerbitzua	Kontaktua	SLA
BCSC	Euskadi CERT	contacto@basquecybersecurity.eus	—
Epeldegi Abogados (adib.)	Legal zibersegurtasuna	—	4h respuesta
Forensic Provider (kontratatzeko)	Analisi forensea	—	8h on-site

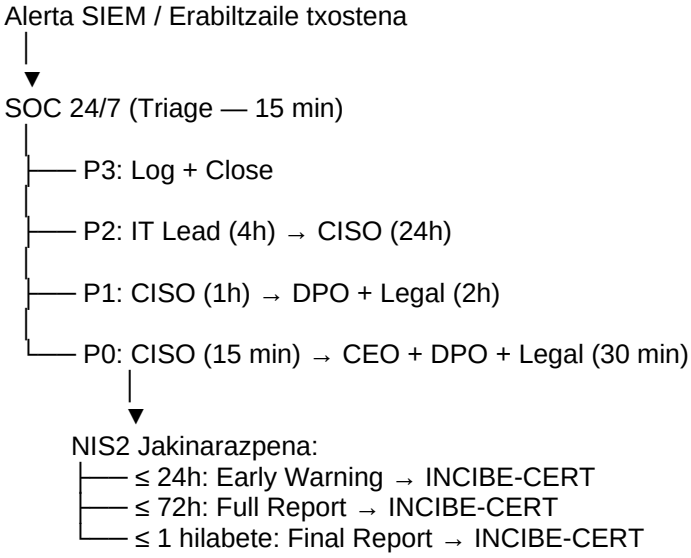
---

2. Eskalazio Matrizea / Escalation Matrix

2.1 Larritasun Mailak

Maila	Deskribapena	Erantzun Denbora	Eskalazio Denbora
P0 — KRITIKOA	Ransomware, datu ihes masiboa, OT erasoa	≤ 15 min	→ CEO berehala
P1 — ALTUA	Sarbide ez-baimendua, datu ihes txikia, DDoS	≤ 1 h	→ CISO ≤ 30 min
P2 — ERTAINA	Malware isolatua, brute force, phishing arrakastatsua	≤ 4 h	→ IT Lead ≤ 2 h
P3 — BAXUA	Positibo faltsua, scan-a, phishing huts egin	≤ 24 h	—

2.2 Eskalazio Fluxua



---

3. Guardia Txandak / On-Call Schedule

3.1 Txanda Eskema

Ordua	Erantzukizuna	Kontak Ordena
L-V 08:00 - 20:00	IT Lead → CISO	Zuzenean
L-V 20:00 - 08:00	SOC 24/7 → CISO (guardia)	SOC-ak eskalatzen du
Asteburua / Jaiak	SOC 24/7 → CISO (guardia)	SOC-ak eskalatzen du

3.2 Guardia Errotazioa

Astea	Guardia Nagusia	Backupa
Aste 1	CISO	IT Lead
Aste 2	IT Lead	CISO
Aste 3	CISO	OT Specialist
Aste 4	IT Lead	CISO

Egutegia: Google Calendar talde partekatuan + PagerDuty (kontratatu behar).

---

4. Komunikazio Kanalak

4.1 Kanal Nagusiak

Kanala	Erabilera	Noizko
Telefono / WhatsApp taldea	Berehalako alertak	P0, P1
Email segurua (PGP)	Txostenak, jakinarazpenak	P0-P3
Signal taldea	Backup komunikazioa (email erori bada)	P0
Zoom / Teams (pasahitz bidez)	War room bilera	P0, P1
SIEM Dashboard (Kibana)	Denbora errealeko jarraipena	Beti

4.2 Kanpo Jakinarazpenak (NIS2)

Hartzailea	Modua	Epemuga	Txantiloia
INCIBE-CERT	Web formularioa + email	≤ 24h (early warning)	notifications/ early_warning_24h_template.md
INCIBE-CERT	Web formularioa +	≤ 72h (full	notifications/full_report_72h_template.md

Hartzailea	Modua	Epemuga	Txantiloia
	email	report)	
INCIBE-CERT	Email + Plataforma	≤ 1 hilabete (final)	notifications/final_report_template.md
AEPD	Sede elektronikoa	≤ 72h (GDPR Art.33)	gdpr/ data_breach_notification_template.md
Erabiltzaileak	Email + Web	“Undue delay” gabe	GDPR Art.34 txantiloia

---

5. CSIRT Formakuntza / Training

Jarduera	Maiztasuna	Parte-hartzaileak	Hurrengo Data
Tabletop Exercise (TTX)	Hiruhilekoa	CSIRT osoa	2026-Q2
Intzidentzia Simulakroa (Live)	Seihilekoa	CSIRT + IT	2026-Q3
NIS2 Jakinarazpen Drill	Hiruhilekoa	CISO + DPO + Legal	2026-Q2
Forensic Workshop	Urtekoa	IT Lead + CISO	2026-Q3
Phishing Simulation	Hilero	Langile guztiak	Hilero

---

6. Aktibazio Protokoloa

Intzidentzia bat gertatzen denean:

1. **DETEKZIOA:** SIEM alertak, SOC alertak, edo erabiltzaile txostenak.
2. **AKTIBAZIO IRIZPIDEAK:**
   - Datu pertsonalen ihesa?
   - Zerbitzu kritikoaren etendura?
   - OT sistemen arriskua?
   - Kalte ekonomiko garrantzitsua?
3. **CSIRT AKTIBATU** (P0/P1 kasuetan berehalakoa):
   - Incident Commander-ak War Room deia egiten du.
   - Rolak esleitzen dira.
   - Komunikazio kanalak aktibatzen dira (Signal/Zoom).
4. **NIS2 ERLOJUA HASTEN DA:** Intzidentzia detektatu den momentutik.
   - ≤ 24h: Early Warning prestatu eta bidali.
   - ≤ 72h: Full Report prestatu eta bidali.

---

7. Dokumentu Loturaak

- Incident Response SOP
- Incident Log Template
- 24h Early Warning Template
- 72h Full Report Template
- GDPR Breach Response SOP
- NIS2 Controls Mapping

ONARPENA:
- CISO: Mikel Etxebarria — Data: ____
- CEO: Jon Zabala — Data: ____

Dokumentu hau KONFIDENTZIALA da. Ez partekatu baimenik gabe.