

ZABALA GAILETAK, S.A.
ZIBERSEGURTASUN-GORABEHERAK

Zibersegurtasun-gorabeherak — Intzidentziei Erantzuteko Plana

NIST SP 800-61 · ISO 27035 · NIS2 Art. 23 · CSIRT

Dokumentu Kodea: GORB-ZG-001

Bertsioa: 1.0

Data: 2026-02-19

Ikasturtea: 2026

Sailkapena: Heziketa — Barne Erabilera

Egilea: Zabala Gaietak Zibersegurtasun Taldea

1. Intzidentziei Erantzuteko Plana (IEP)

NIST SP 800-61 eta ISO/IEC 27035 estandarren arabera, Zabala Gaietak-en Intzidentziei Erantzuteko Planak sei fase ditu:

Fasea	Ekintzak	Erantzule
1. Prestakuntza	Tresnak, eskumenak, trebakuntza, plan dokumentatua	CISO + CSIRT
2. Detekzioa	SIEM alerta, erabiltzaile txostena, honeypot	SOC / IT
3. Mugatzea	Sistema isolatu, sarbideak eten, backup babestu	IT + CSIRT
4. Desagerraraztea	Erro-kausa kendu, sistema garbitu, patch-ak	IT + CISO
5. Berrestea	Sistema itzuli ekoizpenera, egiaztapenak egin	IT + Negozio
6. Ikaskuntzak	Txostena, prozesua hobetu, agintariei jakinarazi	CISO + Leg.

2. Intzidentzien Sailkapena eta Erantzun Denborak

Maila	Deskribapena	Erantzun	Konponketa
P0 — KRIT.	Ransomware, OT erasoa, datu-ihes masiboa (>500 pertsona)	15 min	4 ordu
P1 — ALTUA	Baimenik gabeko sarbidea, DDoS, datu-ihes txikia	1 ordu	24 ordu
P2 — ERT.	Malware isolatua, brute force arrakastatsua	4 ordu	72 ordu
P3 — BAXUA	Positibo faltsua, port scan, phishing huts	24 ordu	1 aste

2.1 NIS2 Notifikazio Epealdiak

- **24 ordu:** Early Warning — INCIBE-CERT eta BCSC-ri gertaera jakinarazi (Art. 23.1.a).
- **72 ordu:** Txosten osoa — intzidentziaren eragina, kausa eta ezarritako neurriak.
- **30 egun:** Azken txostena — ikaskuntzak, hobukuntzak, ekintzak.

3. CSIRT Taldea — Zabala Gaietak

Rola	Izena	Telefona	Guardia
Incident Commander (IC)	Mikel Etxebarria	+34 6XX XXX XX1	24/7
Technical Lead (IT)	[Izendatu]	+34 6XX XXX XX2	L-V 08-20
DPO (Privacy Lead)	Ainhoa Uriarte	+34 6XX XXX XX3	L-V 09-18
Legal Aholkularia	[Izendatu]	+34 6XX XXX XX4	L-V 09-18

Rola	Izena	Telefonia	Guardia
OT Espezialist.	[Izendatu]	+34 6XX XXX XX6	L-V 08-20
Forensik Analista	[Izendatu]	+34 6XX XXX XX7	Deituta

4. Intzidentzia Kasuetan — Playbook Adibideak

4.1 Ransomware Playbook

Urratsa	Ekintza	Nork
1	Alerta jaso (SIEM / erabiltzaile) — denbora erregistratu	SOC
2	Kutsatutako sistema(k) sare-kabletik fisikoki atera	IT
3	Backup freskoena egiaztatu — oraindik garbi dagoen?	IT
4	IC (CISO) eta CEO jakinarazi — P0 eskalazio	SOC
5	Auzitegi irudi forensea egin (kutsatutako diskoak)	DFIR
6	24h early warning INCIBE-CERT-i	DPO+Legal
7	Sistema garbi batetik itzulera (DR Plan)	IT
8	Ziber-asegurua jakinarazi	CISO
9	Ikaskuntza-txostena idatzi	CISO

4.2 Datu-ihes Playbook (GDPR Art. 33)

- Datuak identifikatu: zenbat, noren, zer motatakoak (ROPA kontsultatu).
- 72 orduan: AEPD/agintaritzari jakinarazi (gdpr_breach_response_sop.md).
- Babes-neurriak: pasahitzak aldatu, sarbidea revokatu, sistema garbitu.
- Kaltetutako pertsonen jakinarazi (arrisku altua badago).
- Gertatutako guztia dokumentatu ROPA-n.

5. OT Intzidentzia — Simulazio Txostena

2026ko urtarrilean OT intzidentzia-simulazio bat egin da Zabala Gaietak-en ekoizpen-ingurune probaketan:

Eszenarioa	SCADA-n baimenik gabeko sarrera eta PLC formula aldaketa
Eragin Simulatua	Galleta nahasketa-errezeta aldaketa — osasun-arrisku hipotetioa
Detekzio Denbora	23 minutu (SIEM Wazuh alertak ez zuen OT sarerako araurik)
Mugaketa Denbora	47 minutu — manuz isolatu behar izan zen OT sarea
Ondorio Nagusia	OT sare-monitoreo automatikorako araurik ez zegoen — berehala konpondu
Hobekuntza Neurria	Conpot honeypot gehitu OT sarean + SIEM arau berriak ezarri

6. Ikaskuntza-Txostena eta Hobekuntzak

- OT sareko SIEM monitoring arauak sortu (SR 6.1 IEC 62443).
- CSIRT kideen zerrenda osatu eta 24/7 berme-sistema ezarri.
- Intzidentzia-simulazio ariketak hiruhilekero egitea planifikatua.
- Ransomware simulazio tailor-made bat egin 2026 Q2an.
- Ziber-aseguruaren poliza berrikusi — OT intzidentziak babesten ditu?
- NIS2 Art. 23 jakinarazpen-txantiloak prestatu — betetze-denborak gorde.