full_report_72h_template

Txosten Osoa — Full Incident Report (≤ 72h)

NIS2 Art. 23.4.b — Notificación Completa

Dokumentu Kodea: NIS2-NOT-002
Txantiloi Mota: Full Incident Report
Epemuga: ≤ 72 ordu intzidentzia detektatutik
Hartzailea: INCIBE-CERT (incidencias@incibe-cert.es)
CC: BCSC, AEPD (datu pertsonalak inplikatzen badira)

FORMULARIOA / NOTIFICATION FORM

1. IDENTIFIKAZIOA

Eremua	Edukia
Intzidentzia ID:	INC-YYYY-NNNN
Early Warning ID:	EW-YYYY-NNNN (aurreko jakinarazpena)
Enpresa:	Zabala Gailetak, S.L. (B-XXXXXXXX)
CSIRT Kontaktua:	[CISO izena] — ciso@zabala-gailetak.eus
Txosten data:	YYYY-MM-DD HH:MM (UTC+1)
Detekzio data:	YYYY-MM-DD HH:MM (UTC+1)
Denbora detekziotik:	XX ordu, XX minutu

---

2. INTZIDENTZIAREN DESKRIBAPEN ZEHATZA

2.1 Kronologia (Timeline)

Data/Ordua (UTC+1)	Gertaera	Iturria
YYYY-MM-DD HH:MM	Lehenengo adierazle susmagarria (e.g., SIEM alerta)	SIEM/Wazuh
YYYY-MM-DD HH:MM	Bigarren adierazlea / Ikerketaren hasiera	IT Team
YYYY-MM-DD HH:MM	Intzidentzia konfirmatu	CSIRT

Data/Ordua (UTC+1)	Gertaera	Iturria
YYYY-MM-DD HH:MM	Euste neurriak hartu (containment)	CSIRT
YYYY-MM-DD HH:MM	Early Warning bidalia (≤24h)	CISO → INCIBE
YYYY-MM-DD HH:MM	Desagerrarazte neurriak (eradication)	IT/Security
YYYY-MM-DD HH:MM	Berreskurapena hasi	IT
YYYY-MM-DD HH:MM	Txosten hau bidalia (≤72h)	CISO → INCIBE

2.2 Intzidentzia Mota

- Ransomware
- DDoS (Denial of Service)
- Datu pertsonalen ihesa (Data breach)
- Sarbide ez-baimendua (Unauthorized access)
- Malware / Trojan / Backdoor
- Phishing arrakastatsua
- Supply chain erasoa
- OT / SCADA erasoa
- Beste: _____

2.3 Deskribapen Teknikoa

> [Goiko ataleko mota guztiak zehaztu: erasoaren bektorea, ustiapen teknikak, malware identifikazioark (hash, IOC), sistema kaltetuak, sarbide metodoa, denbora dagokion xehetasun guztiekin. Gutxienez 200 hitz.]

Atala	Xehetasuna
Erasoaren bektorea:	[e.g., Phishing email → payload → lateral movement]
Ustiatutako ahultasuna:	[CVE-XXXX-XXXXX edo deskribapena]
Malware/Tresnak identifikatuak:	[Izena, SHA256, C2 domain/IP]
Erasotzailearen IOC-ak:	[IP, domain, hash, email, TTP]
MITRE ATT&CK teknikak:	[e.g., T1566.001, T1059.001, T1486]

---

3. INPAKTUAREN EBALUAZIOA

3.1 Zerbitzu Inpaktua

Zerbitzua	Egoera	Etendura Denbora	RPO txarra?
Web zerbitzaria	[ ] Kaltetuta / [ ] Ondo	**_h** _min	[ ] Bai / [ ] Ez
Posta elektronikoa	[ ] Kaltetuta / [ ] Ondo	**_h** _min	[ ] Bai / [ ] Ez

Zerbitzua	Egoera	Etendura Denbora	RPO txarra?
ERP sistema	[ ] Kaltetuta / [ ] Ondo	**_h** _min	[ ] Bai / [ ] Ez
Portal RRHH	[ ] Kaltetuta / [ ] Ondo	**_h** _min	[ ] Bai / [ ] Ez
SCADA / PLC	[ ] Kaltetuta / [ ] Ondo	**_h** _min	[ ] Bai / [ ] Ez
Ekoizpen linea	[ ] Kaltetuta / [ ] Ondo	**_h** _min	[ ] Bai / [ ] Ez
Datu pertsonalak	[ ] Kaltetuta / [ ] Ondo	—	[ ] Bai / [ ] Ez

3.2 Datu Inpaktua

Datu Mota	Erregistro Kopurua	Kaltetutakoak	Sailkapena
Langileen datuak			Konfidentziala
Bezeroen datuak			Konfidentziala
Finantza datuak			Oso Konfidentziala
OT konfigurazioak			Konfidentziala
Kredentzialak			Oso Konfidentziala

3.3 Kalte Ekonomikoa (Estimazioa)

Kontzeptua	Estimazioa (€)
Zerbitzu etendura	
Ekoizpen galera	
Forensic eta erantzun kostuak	
Jakinarazpen kostuak	
Osorik kalte-ordainak	
GUZTIRA	**€**

---

4. HARTUTAKO NEURRIAK

4.1 Euste Neurriak (Containment)

Neurria	Egoera	Data	Arduraduna
Kaltetutako sistemak isolatu (sareko deskonexioa)	[ ] Eginak / [ ] Ezin		

Neurria	Egoera	Data	Arduraduna
IP/domain susmagarriak blokeatu firewall-ean	[ ] Eginak		
Kredentzialak berrezarri (kaltetutako kontuak)	[ ] Eginak		
RAM dumpak egin (forentse ebidentzia)	[ ] Eginak		
Disko irudiak egin (forentse ebidentzia)	[ ] Eginak		

4.2 Desagerrarazte Neurriak (Eradication)

Neurria	Egoera	Data
Malware kendu / garbitu	[ ] Eginak / [ ] Prozesuan	
Ahultasuna partxeatu (patch)	[ ] Eginak / [ ] Prozesuan	
Backdoor-ak bilatu eta kendu	[ ] Eginak / [ ] Prozesuan	
Lateral movement bideak itxi	[ ] Eginak / [ ] Prozesuan	

4.3 Berreskuratze Neurriak (Recovery)

Neurria	Egoera	Data
Babeskopietatik berrezarri	[ ] Eginak / [ ] Prozesuan	
Zerbitzuak berrabiarazi	[ ] Eginak / [ ] Prozesuan	
Monitorizazio areagotua aktibatuta	[ ] Eginak	

---

5. MUGAZ GAINDIKO INPAKTUA (NIS2 Art. 23.3)

Eremua	Edukia
Beste EU estatu kideak kaltetuak?	[ ] Bai / [ ] Ez
Zein estatu?	
Beste sektore kaltetuak?	[ ] Bai / [ ] Ez
Zergatik mugaz gaindiko?	[Hornidura katea, cloud zerbitzuak, etab.]

---

6. ERANSKINAK

#	Dokumentua	Lotu
A	SIEM alerta logak	[Erantsi]
B	IOC zerrenda (hash, IP, domain)	[Erantsi]
C	Kronologia xehatua	[Erantsi]
D	RAM dump analisiaren emaitzak	[Erantsi]
E	Komunikazioak (barnekoak eta kanpokoak)	[Erantsi]

BIDALKETA

1. **Bete** formulario hau ≤ 72 orduan.
2. **Bidali** INCIBE-CERT-era (incidencias@incibe-cert.es) PGP bidez.
3. **CC** DPO-ari (GDPR Art.33 jakinarazpena ere bete behar bada).
4. **Gorde kopia** compliance/nis2/evidence-pack/ karpetan.
5. **Prestatu** azken txostena hilabete barruan (Art. 23.4.d).

> **NIS2 Art. 23.4.b:** “[…] without undue delay, and in any event within 72 hours of becoming aware of the significant incident, submit an incident notification, which shall, where applicable, update the information referred to in the early warning […]”

Txantiloi hau: 2026-02-06 | Zabala Gailetak, S.L. — NIS2 Compliance