final_report_template

Azken Txostena — Final Incident Report (≤ 1 hilabete)

NIS2 Art. 23.4.d — Informe Final

Dokumentu Kodea: NIS2-NOT-003
Txantiloi Mota: Final Report
Epemuga: ≤ 1 hilabete txosten osotik (edo ikerketaren amaieran)
Hartzailea: INCIBE-CERT (incidencias@incibe-cert.es)
CC: BCSC, AEPD

---

1. IDENTIFIKAZIOA

Eremua	Edukia
Intzidentzia ID:	INC-YYYY-NNNN
Early Warning ID:	EW-YYYY-NNNN
Full Report ID:	FR-YYYY-NNNN
Enpresa:	Zabala Gailetak, S.L. (B-XXXXXXXX)
CSIRT Kontaktua:	[CISO] — ciso@zabala-gailetak.eus
Txosten data:	YYYY-MM-DD
Detekzio data:	YYYY-MM-DD HH:MM
Ebazpen data:	YYYY-MM-DD HH:MM
Guztizko iraupena:	XX egun, XX ordu

---

2. LABURPEN EXEKUTIBOA (Executive Summary)

> [Intzidentziaren laburpen exekutiboa: zer gertatu zen, noiz, nola detektatu zen, zer inpaktu izan zuen, nola ebatzi zen, eta zer neurri prebentzio hartu diren. 300-500 hitz, ez-teknikoa, zuzendaritzarentzat eta agintarientzat ulergarria.]

---

3. KRONOLOGIA OSOA (Detailed Timeline)

#	Data/Ordua (UTC+1)	Fasea	Gertaera	Iturria	Arduraduna
1		Prestaketa			
2		Detekzioa	Lehenengo alerta SIEM-ean	SIEM	SOC
3		Detekzioa	Triage eta baieztapena	SIEM+Manual	IT Lead
4		Eustea	CSIRT aktibatua	—	CISO
5		Eustea	Sistemak isolatuta	Firewall	IT Lead
6		Jakinaraz.	Early Warning bidali (24h)	Email	CISO
7		Eustea	RAM/Disko irudiak	Forensic	IT
8		Desagerr.	Root cause identifikatua	Forensic	Security
9		Desagerr.	Malware/backdoor kendu	AV/EDR	IT
10		Jakinaraz.	Full Report bidali (72h)	Email	CISO
11		Berresk.	Babeskopietatik berrezarri	Backup	IT
12		Berresk.	Zerbitzuak berrabiarazi	—	IT
13		Berresk.	Monitorizazio areagotua	SIEM	SOC
14		Amaiera	Intzidentzia itxita	—	CISO
15		Post	Azken txosten hau bidalia	Email	CISO

---

4. ROOT CAUSE ANALYSIS (Jatorriaren Analisia)

4.1 Erasoaren Bektorea

Eremua	Edukia
Hasierako sarbidea:	[e.g., Phishing, RDP zabalik, ahultasun ustiatua]
Ahultasuna:	[CVE-XXXX-XXXXX edo deskribapena]
Nola eskalatu:	[Lateral movement teknikak]
Helburua:	[e.g., Data exfiltration, ransomware, sabotage]

4.2 Root Cause

> [Azalpen zehatza jatorri kausaz: zergatik posible izan zen erasoa, zer kontrolek huts egin zuten,
> zer ahultasunak existitzen ziren. Erabili “5 Whys” metodologia.]

4.3 MITRE ATT&CK Mapa

Fasea	Teknika	ID	Deskribapena
Initial Access		T1XXX	
Execution		T1XXX	
Persistence		T1XXX	
Privilege Escalation		T1XXX	
Defense Evasion		T1XXX	
Lateral Movement		T1XXX	
Collection		T1XXX	
Exfiltration		T1XXX	
Impact		T1XXX	

---

5. INPAKTU ZEHATZA (Detailed Impact Assessment)

5.1 Zerbitzu Inpaktua

Zerbitzua	Etendura Hasiera	Etendura Amaiera	Guztira	RTO bete?
				[ ] Bai / [ ] Ez

5.2 Datu Inpaktua

Datu Mota	Erregistroak	Mota (ikusi/galdu/aldatu)	GDPR Art.4(12)?
			[ ] Bai / [ ] Ez

5.3 Kalte Ekonomikoa (Behin betiko)

Kontzeptua	Kostua (€)	Oharrak
Zerbitzu etendura (ekoizpen galera)		
Forensic eta incident response		

Kontzeptua	Kostua (€)	Oharrak
Adabakiak eta hobekuntzak		
Legal eta komunikazio		
GDPR isunak (baldin badago)		
Ospe galera (estimazioa)		
GUZTIRA	**€**	

---

6. HARTUTAKO NEURRIAK (Actions Taken)

6.1 Erantzun Neurriak (Reactive)

#	Neurria	Data	Eraginkortasuna
1			[ ] Eraginkorra / [ ] Partziala / [ ] Eragingabea

6.2 Prebentzio Neurriak (Proactive — implementatuak ondoren)

#	Neurria	Data	Egoera
1	[e.g., MFA zabaldu sistema guztietara]		[ ] Eginak / [ ] Prozesuan
2	[e.g., EDR hedatu endpoint guztietara]		[ ] Eginak / [ ] Prozesuan
3	[e.g., Segmentazio arauak estutu]		[ ] Eginak / [ ] Prozesuan
4	[e.g., Langileentzako phishing formakuntza]		[ ] Eginak / [ ] Prozesuan
5	[e.g., SIEM arau berriak gehitu]		[ ] Eginak / [ ] Prozesuan

---

7. IKASITAKO LEZIOAK (Lessons Learned)

7.1 Zer funtzionatu zuen ongi?

1.

7.2 Zer hobetu behar da?

1.

7.3 Ekintza Plana (Hobekuntza)

#	Ekintza	Arduraduna	Epemuga	Egoera
1				
2				
3				

---

8. CONFORMITY NEURRIAK (NIS2 Compliance Confirmation)

NIS2 Betebeharra	Bete da?	Ebidentzia
Art. 23.4.a Early Warning ≤ 24h	[ ] Bai / [ ] Ez	EW-YYYY-NNNN timestamp
Art. 23.4.b Full Report ≤ 72h	[ ] Bai / [ ] Ez	FR-YYYY-NNNN timestamp
Art. 23.4.d Final Report ≤ 1 month	[ ] Bai / [ ] Ez	Dokumentu hau
Art. 23.3 Cross-border notification	[ ] Bai / [ ] Ez / [ ] N/A	
GDPR Art. 33 AEPD notification ≤ 72h	[ ] Bai / [ ] Ez / [ ] N/A	
GDPR Art. 34 Data subject notification	[ ] Bai / [ ] Ez / [ ] N/A	

---

9. ERANSKINAK

#	Dokumentua	Kokapena
A	Early Warning kopia (24h)	evidence-pack/
B	Full Report kopia (72h)	evidence-pack/
C	SIEM alerta logak	evidence-pack/
D	IOC zerrenda osoa	evidence-pack/
E	Forensic txostena	evidence-pack/
F	Komunikazio erregistroak	evidence-pack/
G	MITRE ATT&CK Navigator export	evidence-pack/

SINADURA ETA ONARPENA

Rola	Izena	Sinadura	Data
Incident Commander / CISO			
CEO	Jon Zabala		
DPO	Ainhoa Uriarte		
Legal Advisor			

> **NIS2 Art. 23.4.d:** “[…] a final report shall be submitted not later than one month after the submission of the incident notification […] including a detailed description of the incident, including its severity and impact; the type of threat or root cause that is likely to have triggered the incident; applied and ongoing mitigation measures […]”
