

vulnerability_disclosure_policy

Ahultasunen Jakinarazpen Politika / Vulnerability Disclosure Policy

NIS2 Art. 21.2.e — Coordinated Vulnerability Disclosure

Enpresa: Zabala Gailetak, S.L.
Dokumentu Kodea: NIS2-VDP-001
Bertsioa: 1.0
Data: 2026-02-06
Jabea: CISO
Egoera: Indarrean

1. SARRERA / Introduction

Zabala Gailetak-ek ahultasunen jakinarazpen arduratsua (Coordinated Vulnerability Disclosure) sustatzen du. Segurtasun ikertzaileak eta erabiltzaileak gonbidatzen ditugu gure sistema eta produktuetan aurkitutako segurtasun ahultasunak modu arduratsuan jakinaraztera.

Politika hau NIS2 Direktibaren (EU 2022/2555) Art. 21.2.e betebeharrekin bat datoz.

2. IRISMENA / Scope

2.1 Programaren barruan dauden sistemak

Sistema	Domeinua / Helbidea	Oharra
Webgunea nagusia	*.zabala-gailetak.eus	Web aplikazioak
Portal RRHH (API)	api.zabala-gailetak.eus	REST API
Mobile App (Android)	Play Store aplikazioa	Android APK

2.2 Programatik KANPO dauden sistemak

- OT/SCADA sareak eta PLC kontroladoreak (segurtasun arrazoiengatik)
- Hirugarrenen zerbitzuak (Google Workspace, AWS, Cloudflare)
- Langileen email kontu pertsonalak
- Fisikoki instalazioetara sartzea

3. JAKINARAZPEN BIDEA / Reporting Channel

3.1 Kontaktua

Eremua	Xehetasuna
Email:	security@zabala-gailetak.eus
PGP Gako Publikoa:	[Eskuragarri: https://zabala-gailetak.eus/.well-known/security.txt]
PGP Fingerprint:	[XXXX XXXX XXXX XXXX XXXX]
Web Formularioa:	https://zabala-gailetak.eus/security/report
Hizkuntza:	Euskara, Gaztelania, Ingelesa

3.2 security.txt (RFC 9116)

Contact: <mailto:security@zabala-gailetak.eus>
Encryption: <https://zabala-gailetak.eus/.well-known/pgp-key.txt>
Preferred-Languages: eu, es, en
Canonical: <https://zabala-gailetak.eus/.well-known/security.txt>
Policy: <https://zabala-gailetak.eus/security/vulnerability-disclosure-policy>
Expires: 2027-02-06T00:00:00.000Z

3.3 Txostenean Sartu Beharreko Informazioa

Jakinarazpen bat bidaltzean, mesedez, eman informazio hau:

1. **Ahultasun mota** (e.g., XSS, SQLi, IDOR, RCE...)
2. **Kaltetutako sistema/URL**
3. **Erreproduktzio urratsak** (pausoz pauso)
4. **Ustiatze PoC** (kodea edo pantaila-argazkiak)
5. **Inpaktu estimazioa** (zer lor daiteke)
6. **Zure kontaktu datuak** (erantzun ahal izateko)

4. TRIAGE PROZESUA ETA SLAk

4.1 SLA (Service Level Agreement)

Fasea	Epemuga
Jasotze agiria (Acknowledgement)	≤ 3 egun
Hasierako triage	≤ 5 egun
Larritasun ebaluazioa	≤ 10 egun
Adabaki garapena (Critical/High)	≤ 30 egun
Adabaki garapena (Medium/Low)	≤ 90 egun

Fasea

Epemuga

Jakinarazpena ikertzaileari (konpondua) Konpondu ondoren ≤ 5 egun

Argitarapen publikoa (disclosure) Konpondu ondoren ≤ 90 egun

4.2 Larritasun Sailkapena

Maila	CVSS v3.1	Deskribapena	Erantzun Epemuga
Kritikoa	9.0 - 10.0	Urruneko kode exekuzioa, datu ihes masiboa	≤ 7 egun
Altua	7.0 - 8.9	Pribilegio eskalazio, sarbide ez-baimendua	≤ 14 egun
Ertaina	4.0 - 6.9	XSS biltegitratua, CSRF, informazio ihesa	≤ 30 egun
Baxua	0.1 - 3.9	Informatzaile txostena, minor issues	≤ 90 egun

4.3 Triage Fluxua

Txostena jasotzen da (security@)



Jasotze agiria bidali (≤ 3 egun)



Triage: Baliozko ahultasuna? (≤ 5 egun)

— EZ → Ikertzaileari jakinarazi (ez da ahultasuna / out of scope)

— BAI → Larritasun sailkapena (CVSS)



Garapen taldeari esleitu



Adabakia garatu + testatu



Adabakia hedatu (produkzioan)



Ikertzaileari jakinarazi (konpondua)











Jakinarazpen koordinatu (publikoa — 90 egun ondoren ikertzailearen baimenarekin)

5. ARAUAK / Rules of Engagement

5.1 Baimendutako Jarduerak

- ✓ Ahultasunen analisisa irismen barruko sistemetan
- ✓ PoC (Proof of Concept) sortzea ez-kaltegarria
- ✓ Txostenak bidaltzea email edo web formularioaren bidez

5.2 DEBEKATUTAKO Jarduerak

-  Zerbitzu ukapena (DoS/DDoS) probak
-  Datu pertsonalen atzipena, kopiatzea edo aldatzea
-  Phishing edo ingeniari-tza soziala gure langileen kontra
-  Fisikoki instalazioetara sartzea
-  OT/SCADA sistemekin interakzioa
-  Hirugarrenen zerbitzuak erasotzea
-  Backdoor-ak instalatzea
-  Ahultasunak publikoki zabaltzea konpondu baino lehen

5.3 Safe Harbor / Babes Juridikoa

Politika hau betetzen duten ikertzaileei:

- **EZ dugu** ekintza legal abiaraziko baldin eta arau hauek betetzen badira.
- **EZ dugu** poliziari jakinaraziko ikertzailearen izaera baliabideen kontra baldin eta jarduerak **on fede** eta **arau hauen barruan** egiten badira.
- **Jakinaraziko dugu** ikertzaileari edozein arazo identifikatuz gero prozesu teknikoan.

|OHARRA: Arau hauen urraketak lege-ekintza ekar dezake.

6. AITORPENA / Recognition

6.1 Hall of Fame

Baimena ematen duten ikertzaileak gure **Security Hall of Fame** orrian agertuko dira: <https://zabalagaitak.eus/security/hall-of-fame>

6.2 Sari Ekonomikoa (Bug Bounty)

Momentu honetan **EZ dugu** sari ekonomikoko programa formalik.
Etorkizunean inplementatzea baloratuko da ikertzaileen interesaren arabera.

7. KOORDINAZIOA / Coordination

7.1 CVE Esleipena

Kalifikatutako ahultasunetarako CVE identifikatzaileak eskatuko ditugu: - **CNA:** INCIBE (Espainiako CNA nazionala) - **Kontaktua:** cve@incibe.es

7.2 CERT Koordinazioa

Entitatea	Funtzioa
-----------	----------

INCIBE-CERT	Koordinazio nazionala
-------------	-----------------------

ENISA	EU mailako koordinazioa
-------	-------------------------

BCSC	Euskadiko CERT
------	----------------

8. DOKUMENTU LOTURAAK

- [NIS2 Controls Mapping](#)
- [Incident Response SOP](#)
- [CSIRT Roster](#)
- [OWASP Vulnerability Disclosure Cheat Sheet](#)

ONARPENA:

- CISO: Mikel Etxebarria — Data: ____
- CEO: Jon Zabala — Data: ____
- Legal: _____ — Data: ____

Dokumentu hau NIS2 (EU 2022/2555) Art. 21.2.e betebeharrak betetzeko sortu da.
Zabala Gailetak, S.L. — 2026-02-06