ZABALA GAILETAK, S.A.

ZIBERSEGURTASUNAREN ARLOKO ARAUDIA

Zibersegurtasunaren Arloko Araudia — Betekuntza Txostena

ISO 27001 · GDPR · NIS2 · IEC 62443

Dokumentu Kodea:	ARAU-ZG-001
Bertsioa:	1.0
Data:	2026-02-19
Ikasturtea:	2026
Sailkapena:	Heziketa — Barne Erabilera
Egilea:	Zabala Gailetak Zibersegurtasun Taldea

1. Sarrera — Arauei-esparru Orokorra

Zabala Gailetak S.A. enpresak honako lege eta arau-esparru hauei jarraitu behar die: ISO/IEC 27001:2022 (SGSI), GDPR/DBLO (datu-babesa), NIS2 Direktiba (sare eta informazio-sistemen segurtasuna) eta IEC 62443 (industria-kontrol sistemen segurtasuna).

2. ISO/IEC 27001:2022 — SGSI

Informazioaren Segurtasuna Kudeatzeko Sisteman (SGSI) 93 kontrol daude A Eranskinean. Zabala Gailetak-ek 87 kontrol (%93) inplementatu ditu 2026ko otsailean:

Kontrol Arloa	Total	Inplementatua	Partzialki	Ez apli kag.
A.5 — Antolakuntza (37)	37	35	2	0
A.6 — Pertsonak (8)	8	8	0	0
A.7 — Fisikoa (14)	14	13	1	0
A.8 — Teknologia (34)	34	30	4	0
GUZTIRA	**93**	**86**	**7**	**0**

■ *Kontrol partzialak (7): A.5.12, A.5.13, A.7.7, A.8.11, A.8.12, A.8.14 — 2026 Q2rako osatzeko planifikatuta.*

2.1 PDCA Hobetzeko Ziklo Jarraitua

- **Plan:** Arriskuen ebaluazioa, kontrol aukeraketa, tratamendu-plana.
- **Do:** Kontrolak inplementatu, langileak trebatu, dokumentatu.
- **Check:** Barne-auditoriak, SIEM metrikak, zuzendaritzaren berrikuspena.
- **Act:** Ez-betetzerako ekintza zuzentzaileak, etengabeko hobekuntza.

3. GDPR — Datu Babeseko Araudia

Arau Orokor Europarraren (2016/679) arabera, Zabala Gailetak-ek langile eta bezeroen datu pertsonalak prozesatzen ditu. Bete beharreko eskakizunak:

GDPR Eskakizuna	Egoera	Ebidentzia
ROPA (Prozesatze Erregistroa)	■ Egin	data_processing_register.md
DPIA — HR Portal	■ Egin	dpia_rrhh_portal_completed.md
DPIA — SCADA/OT	■ Egin	dpia_scada_ot_completed.md
DPO Izendapena	■ Egin	dpo_izendapena.md
Cookie Politika	■ Egin	cookie_policy.md
Datu-subjektuen eskubideak SOP	■ Egin	data_subject_rights_procedures.md
72h Haustura Jakinarazpena SOP	■ Egin	gdpr_breach_response_sop.md
Pribatutasun Oharra	■ Egin	privacy_notice_web.md

GDPR Eskakizuna	Egoera	Ebidentzia
Diseinuzko Pribatutasuna	■ Egin	privacy_by_design.md

4. NIS2 Direktiba (EU 2022/2555)

NIS2k erakundeak 10 neurri-kategoria inplementatzera behartzen ditu. Zabala Gailetak-ek sektore elikagarrian aritzen denez, 'Beharrezko Erakunde' gisa sailkatu daiteke:

NIS2 Art. 21 Kategoria	Egoera	Ohar
21.2.a — Arrisku-analisia eta politika	■	risk_assessment.md + ISP-001
21.2.b — Intzidentzien kudeaketa	■ %80	SOP + CSIRT roster eginda
21.2.c — Negozio jarraitutasuna	■	BCP + DR Plan (RTO 4h, RPO 1h)
21.2.d — Hornidura-kate segurtasuna	■	supplier_security_register.md
21.2.e — Erosketa segurua	■	POP-015 SSDLC
21.2.f — Eraginkortasun neurketak	■ %60	KPI dashboard planifikatua
21.2.g — Ziberhigiene eta trebakuntza	■	sop_security_awareness.md
21.2.h — Kriptografia	■	POP-014 + TLS 1.3 + AES-256
21.2.i — Giza baliabideen segurtasuna	■	langile_hautaketa + HR SOPak
21.2.j — MFA eta SAO komunikazioak	■	JWT + TOTP + WebAuthn

5. IEC 62443 — Industria Kontrol Sistemen Segurtasuna

Zabala Gailetak-en OT (Teknologia Operatiboa) ingurune industrialean PLC, SCADA eta HMI sistemak daude. IEC 62443-3-3 estandarrak Security Level (SL) 2 eskatzen du:

SR Eskakizuna	Deskribapena	Egoera
SR 1.1	Erabiltzaile autentifikazioa (IAC)	■ RBAC + 2FA
SR 2.1	Baimen betearazpena	■ Least Privilege
SR 3.1	Malware babesa	■ Antivirus OTn
SR 5.1	Sare segmentazioa	■ VLAN 50 isolatua
SR 5.2	Gune segmentazioa	■ IT/OT banaketa
SR 6.1	Audit log eskuragarritasuna	■ SIEM — Wazuh
SR 7.1	DoS babesa	■ Rate limiting