nis2_controls_mapping

NIS2 Kontrolen Mapa / NIS2 Controls Mapping Matrix

Enpresa: Zabala Gailetak, S.L.
Direktiba: NIS2 (EU 2022/2555)
Dokumentu Kodea: NIS2-MAP-001
Bertsioa: 1.0
Data: 2026-02-06
Jabea: CISO

---

1. ARTIKULU 20 — Gobernantza / Governance

20.1 Zuzendaritzaren Ardurak

Kontrola	Deskribapena	ISO 27001 Mapaketa	Egoera	Ebidentzia
GOV-01	Zuzendaritzak ziber-segurtasun arriskuak onartzen ditu	A.5.1, A.5.2	✅	sgsi/segurtasun_politika.md
GOV-02	Zuzendaritzak formakuntza jasotzen du	A.6.3	⏳	Q2 2026 planifikatua
GOV-03	Arriskuen kudeaketa neurrien gainbegiratzea	A.5.4	✅	CGC aktak
GOV-04	Ziber-segurtasun politiken onarpena	A.5.1	✅	sgsi/segurtasun_politika.md
GOV-05	Erantzukizun pertsonala (Art.20.2)	—	⏳	Legal klausula behar

---

2. ARTIKULU 21 — Arriskuen Kudeaketa Neurriak / Risk Management Measures

21.2.a — Arriskuen Analisia eta Segurtasun Politikak

Kontrola	Deskribapena	ISO 27001	IEC 62443	Egoera	Ebidentzia
RM-01	Arrisku ebaluazio formala	A.5.7, A.8.8	SR 3.1	✅	sgsi/risk_assessment.md

Kontrola	Deskribapena	ISO 27001	IEC 62443	Egoera	Ebidentzia
RM-02	Arrisku tratamendu plana	A.5.7	—	✅	sgsi/ risk_treatment_plan.md
RM-03	Segurtasun politika eguneratua	A.5.1	—	✅	sgsi/ segurtasun_politika.md
RM-04	Mehatxu adimena (Threat Intelligence)	A.5.7	SR 3.1	⏳	SIEM + Honeypot feed
RM-05	MFA inplementazioa	A.8.5	SR 1.1	✅	JWT + TOTP + WebAuthn
RM-06	EDR hedapena	A.8.7	SR 3.1	⏳	CrowdStrike Q2 2026
RM-07	Adabaki kudeaketa (Patch mgmt)	A.8.8	SR 3.2	⏳ 70%	Automated + manual
RM-08	Ahultasunen eskaneatzea	A.8.8	SR 3.3	⏳	OWASP ZAP, Nessus

21.2.b — Intzidentzien Kudeaketa / Incident Handling

Kontrola	Deskribapena	ISO 27001	Egoera	Ebidentzia
INC-01	Intzidentzia SOP (NIST faseak)	A.5.24-28	✅	incidents/sop_incident_response.md
INC-02	CSIRT taldea operatiboa	A.5.24	⏳	nis2/csirt_roster.md
INC-03	24h alerta goiztiarra (early warning)	A.5.25	⏳	nis2/notifications/ early_warning_24h_template.md
INC-04	72h txosten osoa	A.5.26	⏳	nis2/notifications/ full_report_72h_template.md
INC-05	Azken txostena (hilabete 1)	A.5.27	⏳	nis2/notifications/final_report_template.md
INC-06	Intzidentzia erregistro automatizatua	A.5.28	⏳	SIEM → Ticket system
INC-07	SIEM alerta arauak NIS2rako	A.8.16	⏳	nis2/siem_soar/nis2_correlation_rules.json
INC-08	SOAR playbook-ak	A.8.16	⏳	nis2/siem_soar/nis2_soar_playbooks.md

21.2.c — Negozio Jarraitutasuna / Business Continuity

Kontrola	Deskribapena	ISO 27001	Egoera	Ebidentzia
BCP-01	Negozio inpaktuaren analisia (BIA)	A.5.29-30	✅	sgsi/business_continuity_plan.md
BCP-02	Berreskuratze plana (DR)	A.5.30	✅	BCP dokumentuan
BCP-03	RTO/RPO definizioak	A.5.30	✅	RTO 4h, RPO 1h
BCP-04	Hiruhileko simulakroak	A.5.30	⏳	Lehena Q2 2026
BCP-05	Babeskopiak enkriptatuak	A.8.13	✅	AES-256 + off-site

21.2.d — Hornidura-Kate Segurtasuna / Supply Chain Security

Kontrola	Deskribapena	ISO 27001	Egoera	Ebidentzia
SC-01	Hornitzaile kritikoen inbentarioa	A.5.19-22	⏳	nis2/ supplier_security_register.md
SC-02	Segurtasun galdetegia hornitzaileei	A.5.20	⏳	Galdetegi txantiloia
SC-03	DPA sinatuak (Data Processing Agreements)	A.5.20	⏳	Legal jarraipena
SC-04	“Right to audit” klausula	A.5.22	⏳	Kontratuen berrikusketa
SC-05	Intzidentzia jakinarazpen SLA (24h)	A.5.24	⏳	Kontratuan gehitu
SC-06	Hornitzaileen ebaluazio periodikoa	A.5.22	⏳	Urtero

21.2.e — Ahultasunen Jakinarazpena / Vulnerability Disclosure

Kontrola	Deskribapena	ISO 27001	Egoera	Ebidentzia
VD-01	Ahultasunen jakinarazpen politika publikoa	A.8.8	⏳	nis2/ vulnerability_disclosure_policy.md
VD-02	Komunikazio kanala (security@)	A.8.8	⏳	Email + web formularioa
VD-03	Triage prozesua eta SLAk	A.8.8	⏳	SOP gehitu
VD-04	Koordinazio politika (CVE, CERT)	A.8.8	⏳	INCIBE koordinazioa

21.2.f — Kriptografia / Encryption

Kontrola	Deskribapena	ISO 27001	Egoera	Ebidentzia
CRY-01	TLS 1.3 transmisioan	A.8.24	✅	Nginx + HAProxy config
CRY-02	AES-256-GCM atsedenaldian	A.8.24	✅	PostgreSQL TDE, disk
CRY-03	Gako kudeaketa (Key management)	A.8.24	✅	HSM planifikatua
CRY-04	Pasahitz hashing (bcrypt/Argon2)	A.8.5	✅	Cost factor 12+
CRY-05	Gako errotazioa automatikoa	A.8.24	⏳	Q3 2026

21.2.g — Segurtasun Politikak / Security Policies

Kontrola	Deskribapena	ISO 27001	Egoera	Ebidentzia
POL-01	Informazio segurtasun politika	A.5.1	✅	SGSI
POL-02	Erabilera onargarria	A.5.10	✅	SGSI
POL-03	Urruneko lana (Remote work)	A.6.7	✅	SGSI
POL-04	BYOD politika	A.8.1	✅	SGSI

21.2.h — Sarbide Kontrola / Access Control

Kontrola	Deskribapena	ISO 27001	Egoera	Ebidentzia
AC-01	RBAC 5 rolekin	A.5.15-18	✅	ADMIN, RRHH, etc.
AC-02	MFA (TOTP + WebAuthn)	A.8.5	✅	Inplementatua
AC-03	Sarbide berrikuspen periodikoa	A.5.18	⏳	Hiruhileko
AC-04	Pribilegio gutxieneko printzipioa	A.8.2	✅	RBAC + JIT

---

3. ARTIKULU 23 — Intzidentzien Jakinarazpena / Incident Notification

Kontrola	Deskribapena	Epemuga	Egoera	Ebidentzia
NOT-01	Alerta goiztiarra CSIRT-era	≤ 24 ordu	⏳	Txantiloia sortuta
NOT-02	Jakinarazpen osoa	≤ 72 ordu	⏳	Txantiloia sortuta
NOT-03	Azken txostena	≤ 1 hilabete	⏳	Txantiloia sortuta

Kontrola	Deskribapena	Epemuga	Egoera	Ebidentzia
NOT-04	Erabiltzaileei jakinaraztea	“Undue delay” gabe	⏳	GDPR txantiloia existitzen da
NOT-05	Erregistro automatikoaren logak	Jarraia	⏳	SIEM integrazioa

---

4. COMPLIANCE LABURPENA / Summary

Kategoria	Guztira	✅ Eginak	⏳ Aurreratzen	❌ Falta	%
Gobernantza (Art.20)	5	3	2	0	60%
Arriskuak (21.2.a)	8	3	5	0	38%
Intzidentziak (21.2.b)	8	1	7	0	13%
Jarraitutasuna (21.2.c)	5	4	1	0	80%
Hornidura-katea (21.2.d)	6	0	6	0	0%
Ahultasunak (21.2.e)	4	0	4	0	0%
Kriptografia (21.2.f)	5	4	1	0	80%
Politikak (21.2.g)	4	4	0	0	100%
Sarbidea (21.2.h)	4	3	1	0	75%
Jakinarazpena (Art.23)	5	0	5	0	0%
GUZTIRA	**54**	**22**	**32**	**0**	**41%**

Target: 100% → 2026-10-17

---

5. Roadmap (12 Aste)

Astea	Ekintzak	Arduraduna
1-2	CSIRT roster, txantiloiak, VDP politika	CISO + Legal
3-4	Hornitzaile inbentarioa + galdetegia	Legal + Procurement
5-6	EDR hedapena, SIEM arauak, SOAR playbook-ak	Infra + Security
7-8	DPA sinatuak, kontratuen klausulak	Legal
9-10	BCP simulakroa, Pentesting, Formakuntza	Security + All

Astea	Ekintzak	Arduraduna
11-12	Self-assessment, Evidence pack, Audit prestaketa	CISO + Legal

---

Azken eguneratzea: 2026-02-06 | Zabala Gailetak, S.L.