

# supplier\_security\_register

## Hornitzaileen Segurtasun Erregistroa / Supplier Security Register

### NIS2 Art. 21.2.d — Supply Chain Security

Dokumentu Kodea: NIS2-SC-001

Bertsioa: 1.0

Data: 2026-02-06

Jabea: Legal Advisor + CISO + Procurement

Sailkapena: KONFIDENTZIALA

Berrikusketa: Urtekoa

#### 1. HELBURUA

Dokumentu honek identifikatzen ditu Zabala Gailetak-en hornitzaile kritikoak, haien segurtasun ebaluazioa egiten du, eta NIS2 Art. 21.2.d betebeharrak kudeatzeko erregistroaren jarraipena egiten du. Hornidura-katearen segurtasuna bermatzea da helburu nagusia.

#### 2. HORNITZAILE KRITIKOEN INBENTARIOA

##### 2.1 ICT Hornitzaileak (Kritikoak)

#	Hornitzailea	Zerbitzua	Kategoria	Kritikotasuna	DPA Sinatua	ISO 27001	Right to Audit	NIS2 SLA	Ebaluazio Egoera
1	Siemens	SCADA / PLC (S7-1500)	OT Hardware	KRITIKOA					Pendiente
2	AWS	Cloud Backup (S3)	Cloud IaaS	ALTUA			(kontratuan)		Pendiente
3	Cloudflare	WAF / CDN / DNS	Security SaaS	ALTUA					Pendiente
4	Google	Workspace (Email, Drive)	SaaS	ALTUA			Mugatua		Pendiente
5	CrowdStrike	EDR /	Security	ALTUA					Pendiente

#	Hornitzailea	Zerbitzua	Kategoria	Kritikotasuna	DPA Sinatua	ISO 27001	Right to Audit	NIS2 SLA	Ebaluazio Egoera
		Endpoint Security							
6	Wazuh	SIEM (Open Source)	Security	ERTAINA	N/A (OSS)	N/A	N/A	N/A	✅ OSS
7	HID Global	Badge / Access Control	Physical Sec.	ERTAINA	🕒	✅	🕒	🕒	🕒 Pendiente
8	ScadaBR	HMI (Open Source)	OT Software	ERTAINA	N/A (OSS)	N/A	N/A	N/A	✅ OSS

### 2.2 Non-ICT Hornitzaileak (Garrantzitsuak)

#	Hornitzailea	Zerbitzua	Kritikotasuna	Segurtasun Klausula
1	Elektrizitate hornitzailea	UPS / Energia	KRITIKOA	🕒 Berrikusi
2	Internet hornitzailea (ISP)	Konexioa	KRITIKOA	🕒 Berrikusi
3	Garbiketa enpresa	Instalazioen sarbidea	BAXUA	🕒 NDA sinatu
4	Segurtasun fisikoa (zaintzaileak)	Instalazioen babesa	ERTAINA	🕒 NDA sinatu

## 3. EBALUAZIO IRIZPIDEAK / Assessment Criteria

### 3.1 Segurtasun Galdetegia (100 puntu)

Kategoria	Puntuazioa	Galdera Kopurua	Gutxieneko Nota
Segurtasun Gobernantza	/20	10	14/20 (70%)
Sarbide Kontrola	/15	8	10/15 (67%)
Kriptografia eta Datuak	/15	7	10/15 (67%)
Intzidentzien Kudeaketa	/15	8	10/15 (67%)
Negozio Jarraitutasuna	/10	5	7/10 (70%)
Ahultasunen Kudeaketa	/10	5	7/10 (70%)
Langileen Segurtasuna	/10	5	7/10 (70%)
Compliance (ISO/GDPR)	/5	3	3/5 (60%)

Kategoria	Puntuazioa	Galdera Kopurua	Gutxieneko Nota
GUZTIRA	/100	51	68/100 (68%)

### 3.2 Arrisku Mailak

Arriskua	CVSS Mota	Galdetegia	Puntuazioa	Ekintza
BAXUA	Onartua	$\geq 80/100$		Jarraipena urtekoa
ERTAINA	Mugatua	68-79/100		Hobekuntza plana 6 hilabete
ALTUA	Garrantzitsua	50-67/100		Hobekuntza plana berehalakoa
KRITIKOA	Ezin onartua	$< 50/100$		Hornitzaile aldaketa planifikatu

## 4. KONTRATU KLAUSULA NAHITAEZKOAK / Required Contract Clauses

NIS2 betebeharrengatik, hornitzaile kritikoekiko kontratuak klausula hauek izan behar dituzte:

### 4.1 Segurtasun Klausulak

KLAUSULA 1 — Segurtasun Gutxienekoak  
Hornitzaileak neurri tekniko eta antolatzaile egokiak mantenduko ditu, ISO 27001 edo parekide bat betetzen dituen.

KLAUSULA 2 — Intzidentzien Jakinarazpena  
Hornitzaileak segurtasun intzidentziak Zabala Gailetak-i jakinaraziko dizkio  $\leq 24$  orduko epean detekziotik, NIS2 Art. 23 betebeharrekin bat etorriz.

KLAUSULA 3 — Auditoretza Eskubidea (Right to Audit)  
Zabala Gailetak-ek eskubidea izango du hornitzailearen segurtasun neurriak auditatzeko, zuzenean edo hirugarren auditore baten bidez, urtean behin gutxienez.

KLAUSULA 4 — Datu Babesaren Akordio (DPA)  
GDPR Art. 28 arabera DPA bat sinatu beharko da datu pertsonalak tratatzen diren guztietan.

KLAUSULA 5 — Sub-hornitzaile Kontrola  
Hornitzaileak sub-hornitzaile berriak Zabala Gailetak-i jakinaraziko dizkio, eta segurtasun neurri berdinak exijituko ditu sub-hornitzaileei.

KLAUSULA 6 — Kontratu Amaiera  
Kontratua amaitzean, hornitzaileak Zabala Gailetak-en datu guztiak itzuliko edo modu seguruan suntsituko ditu, berreste txostenarekin.

## 5. EBALUAZIO EGUTEGIA / Assessment Schedule

Hornitzailea   Lehenengo Ebaluazioa   Maiztasuna   Hurrengo Berrikusketa

Siemens	2026-Q2	Urtekoa	2027-Q2
AWS	2026-Q2	Urtekoa	2027-Q2
Cloudflare	2026-Q2	Urtekoa	2027-Q2
Google	2026-Q2	Urtekoa	2027-Q2
CrowdStrike	2026-Q2	Urtekoa	2027-Q2
HID Global	2026-Q3	Bi urtekoa	2028-Q3

## 6. DPA JARRAIPENA / DPA Tracking

Hornitzailea	DPA Beharrezkoa	DPA Bidalia	DPA Sinatua	Oharrak
Siemens	✅ Bai (OT datuak)	🕒	❌	Lehentasuna
AWS	✅ Bai (backup)	🕒	❌	AWS DPA estandarra
Cloudflare	✅ Bai (WAF logs)	🕒	❌	Cloudflare DPA
Google	✅ Bai (email, docs)	🕒	❌	Google Workspace DPA
CrowdStrike	✅ Bai (endpoint data)	🕒	❌	CS DPA estandarra
HID Global	✅ Bai (badge data)	🕒	❌	—

## 7. METRIKEN JARRAIPENA

Metrika	Helburua	Egungo Balioa	Azken Data
Hornitzaile kritikoak ebaluatuta	100%	0%	2026-02-06
DPA sinatuak (kritikoak)	100%	0%	2026-02-06
Right to audit klausulak	100%	0%	2026-02-06
Intzidentzia SLA klausulak (24h)	100%	0%	2026-02-06
Galdetegi nota minimoa (68/100)	100%	N/A	—

## 8. ERREFERENTZIAK

- NIS2 (EU 2022/2555) Art. 21.2.d — Supply chain security
- ISO 27001:2022 A.5.19-A.5.22 — Supplier relationships
- GDPR Art. 28 — Data Processing Agreements
- ENISA: Good Practices for Supply Chain Cybersecurity

---

### ONARPENA:

- CISO: Mikel Etxebarria — Data: \_\_\_\_
- Legal: \_\_\_\_\_ — Data: \_\_\_\_
- Procurement: \_\_\_\_\_ — Data: \_\_\_\_

*Dokumentu hau KONFIDENTZIALA da. Zabala Gailetak, S.L. — 2026-02-06*