

README

NIS2 Ebidentzia Pakete Katalogoa / Evidence Pack Catalog

NIS2 Art. 20-23 — Compliance Evidence Collection

Dokumentu Kodea: NIS2-EVD-001

Bertsioa: 1.0

Data: 2026-02-06

Jabea: CISO

Berrikusketa: Hiruhilekoa

1. HELBURUA

Karpeta honek jasotzen ditu NIS2 compliance frogatzen duten ebidentziak: jakinarazpen kopiak, intzidentzia logak, BCP proba txostenak, hornitzaile DPAk, formakuntza erregistroak eta auditoretza emaitzak.

Auditoretza baterako behar diren dokumentu guztien erreferentzia leku bakarra da.

2. KARPETA EGITURA

```
evidence-pack/
├── README.md           # Dokumentu hau
├── incidents/          # Intzidentzia ebidentziak
│   ├── INC-YYYY-NNNN/  # Intzidentzia bakoitzeko karpeta
│   │   ├── early_warning.md  # 24h txantiloia beteta
│   │   ├── full_report.md    # 72h txostena beteta
│   │   ├── final_report.md   # Azken txostena
│   │   ├── siem_logs/        # SIEM alerta logak
│   │   ├── forensic/         # Forentse ebidentziak (RAM, disk)
│   │   ├── iocs.json          # Indicator of Compromise zerrenda
│   │   └── communications/    # Barneko/kanpoko komunikazioak
│   ├── notifications/      # INCIBE-CERT jakinarazpen kopiak
│   │   ├── YYYY-MM-DD_EW_INC-ID.pdf  # Early Warning bidalia (PDF kopia)
│   │   └── YYYY-MM-DD_FR_INC-ID.pdf  # Full Report bidalia (PDF kopia)
│   ├── bcp_tests/          # BCP proba txostenak
│   │   └── YYYY-QX_bcp_test_report.md
│   ├── supplier_assessments/  # Hornitzaile ebaluazioak
│   │   ├── YYYY_vendor_questionnaire_results.md
│   │   └── dpas/             # DPA kopia sinatuak (PDF)
│   ├── training/           # Formakuntza ebidentziak
│   │   ├── YYYY-QX_tabletop_report.md
│   │   ├── YYYY-QX_phishing_sim_results.md
│   │   └── attendance_records/
│   └── audits/              # Auditoretza txostenak
```

| |
|--|
| └─ YYYY_internal_audit.md |
| └─ YYYY_pentest_report.md |
| └─ metrics/ # NIS2 compliance metrikak |
| └─ YYYY-MM_nis2_kpis.md |
| └─ self_assessment/ # NIS2 self-assessment |
| └─ YYYY_nis2_self_assessment.md |

3. EBIDENTZIA CHECKLIST — Auditoria Prestaketarako

3.1 Gobernantza (Art. 20)

| # | Ebidentzia | Kokapena | Egoera |
|----------|---|-----------------------------|--------|
| E-GOV-01 | Segurtasun politika onarpen akta | sgsi/segurtasun_politika.md | ✓ |
| E-GOV-02 | CGC bilera aktak (arriskuen gainbegiratzea) | evidence-pack/audits/ | ⌚ |
| E-GOV-03 | Zuzendaritzaren formakuntza erregistroa | evidence-pack/training/ | ⌚ |
| E-GOV-04 | CISO/DPO izendapen agiria | Legal fitxategia | ✓ |

3.2 Arriskuak (Art. 21.2.a)

| # | Ebidentzia | Kokapena | Egoera |
|---------|---------------------------------|-----------------------------|--------|
| E-RM-01 | Arrisku ebaluazio txostena | sgsi/risk_assessment.md | ✓ |
| E-RM-02 | Arrisku tratamendu plana | sgsi/risk_treatment_plan.md | ✓ |
| E-RM-03 | Ahultasun eskaneaketa txostenak | evidence-pack/audits/ | ⌚ |
| E-RM-04 | Patch management erregistroa | SIEM/CMDB | ⌚ |
| E-RM-05 | EDR hedapen ebidentzia | CrowdStrike dashboard | ⌚ |

3.3 Intzidentziak (Art. 21.2.b, Art. 23)

| # | Ebidentzia | Kokapena | Egoera |
|----------|---------------------------------|------------------------------------|-------------|
| E-INC-01 | Intzidentzia SOP (NIST faseak) | incidents/sop_incident_response.md | ✓ |
| E-INC-02 | CSIRT roster operatiboa | nis2/csirt_roster.md | ✓ (sortuta) |
| E-INC-03 | Intzidentzia log erregistroak | evidence-pack/incidents/ | ⌚ |
| E-INC-04 | INCIBE-CERT jakinarazpen kopiak | evidence-pack/notifications/ | ⌚ |
| E-INC-05 | SIEM alerta arau konfigurazioa | nis2/siem_soar/ | ✓ (sortuta) |
| E-INC-06 | SOAR playbook ezarpenak | nis2/siem_soar/ | ✓ (sortuta) |

| # | Ebidentzia | Kokapena | Egoera |
|----------|------------------------------|-------------------------|--------|
| E-INC-07 | Tabletop simulakro txostenak | evidence-pack/training/ | 🕒 |

3.4 Jarraitutasuna (Art. 21.2.c)

| # | Ebidentzia | Kokapena | Egoera |
|----------|-----------------------------|----------------------------------|--------|
| E-BCP-01 | Negozio jarraitutasun plana | sgsi/business_continuity_plan.md | ✅ |
| E-BCP-02 | BCP proba txostenak | evidence-pack/bcp_tests/ | 🕒 |
| E-BCP-03 | DR proba emaitzak | evidence-pack/bcp_tests/ | 🕒 |

3.5 Hornidura-katea (Art. 21.2.d)

| # | Ebidentzia | Kokapena | Egoera |
|---------|---------------------------------|--|-------------|
| E-SC-01 | Hornitzaile erregistroa | nis2/supplier_security_register.md | ✅ (sortuta) |
| E-SC-02 | Segurtasun galdetegi emaitzak | evidence-pack/supplier_assessments/ | 🕒 |
| E-SC-03 | DPA kopia sinatuak | evidence-pack/supplier_assessments/dpas/ | 🕒 |
| E-SC-04 | Kontratuen segurtasun klausulak | Legal | 🕒 |

3.6 Ahultasunak (Art. 21.2.e)

| # | Ebidentzia | Kokapena | Egoera |
|---------|-------------------------------------|---|-------------|
| E-VD-01 | Vulnerability Disclosure Policy | nis2/vulnerability_disclosure_policy.md | ✅ (sortuta) |
| E-VD-02 | security.txt fitxategia (RFC 9116) | .well-known/security.txt | 🕒 |
| E-VD-03 | Jakinarazpen log (txostenak jasota) | evidence-pack/ | 🕒 |

4. FITXATEGIEN IZENDAPEN GIDA

Formatua: YYYY-MM-DD_MOTA_DESKRIBAPEN.ext

Adibideak:

- 2026-06-15_EW_INC-2026-0042.pdf (Early Warning jakinarazpena)
- 2026-06-17_FR_INC-2026-0042.pdf (Full Report)
- 2026-Q2_tabletop_ransomware.md (Tabletop exercise report)
- 2026-Q2_bcp_test_failover.md (BCP test report)
- 2026_siemens_vendor_assessment.md (Vendor assessment)
- 2026_aws_dpa_signed.pdf (DPA signed copy)

5. GORDEKETA ETA SEGURTASUNA

Irizpidea

Balioa

Gordetzeko epea: 5 urte (NIS2 + GDPR)

Enkriptazioa: AES-256-GCM (atsedenaldian)

Sarbidea: CISO, DPO, Legal, Auditoreak soilik

Babeskopia: Off-site enkriptatua, hilero

Integritatea: SHA-256 hash ebidentzia bakoitzeko

6. METRIKAK (KPI)

| Metrika | Helburua | Egungo Balioa |
|---|-------------|---------------|
| Ebidentzia pack osotasuna | $\geq 90\%$ | ~40% |
| Intzidentzia jakinarazpen kopiak (NIS2) | 100% | N/A |
| BCP probak eginda (urtea) | ≥ 2 | 0 |
| Tabletop exercises (urtea) | ≥ 4 | 0 |
| DPA sinatuak (hornitzaile kritikoak) | 100% | 0% |