

# sop\_incident\_response

## Intzidentzien Erantzun Prozedura (SOP) - Zabala Gailetak

### 1. Helburua

Prozedura honen helburua segurtasun intzidentziak modu ordenatuan, eraginkorrean eta azkarrean kudeatzea da, kalteak minimizatzeko eta negozioaren jarraitutasuna bermatzeko.

### 2. Faseak (NIST Ereduan oinarrituta)

#### Fase 1: Prestaketa

- Taldea:** Intzidentzien Erantzun Taldea (CSIRT) definituta egon behar da (IKT arduraduna, Segurtasun arduraduna, Zuzendaritza).
- Tresnak:** Monitorizazio sistemak (SIEM), forentse tresnak, komunikazio bide alternatiboak.
- Formakuntza:** Simulakroak aldian-aldian egitea.

#### Fase 2: Detekzioa eta Analisia

- Alerta:** SIEM, IDS, Antibirus edo erabiltzaile baten bidez jasotako abisua.
- Triajea:**
  - Egiaztatu: Benetako intzidentzia da ala positibo faltsua?
  - Kategorizatu: (Adib. Ransomware, DDoS, Datu ihesa).
  - Lehenetsi: Larritasunaren arabera (Kritikoa, Altua, Ertaina, Baxua).
- Erregistroa:** Ireki intzidentzia berria incident\_log\_template.md erabiliz.

#### Fase 3: Euste-neurriak (Containment)

- Berehalakoa:** Isolatu kaltetutako sistemak saretik (kablea kendu edo VLAN isolatua). **Ez itzali ekipoa RAM memoria galduko delako** (forentserako garrantzitsua).
- Epe laburrera:** Blokeatu erasotzaileen IPak suebakian, aldatu kaltetutako pasahitzak.

#### Fase 4: Desagerraztea (Eradication)

- Identifikatu malwarearen jatorria eta sarrera puntuia.
- Garbitu sistemak: Antibirusa pasatu, rootkit-ak bilatu.
- Kasu larriean: Formateatu eta hutsetik instalatu (baina ebidentziak gorde ondoren).
- Ahultasuna partxeatu (segurtasun eguneraketak).

#### Fase 5: Berreskurapena (Recovery)

- Berrezarri sistemak babeskopietatik (ziurtatu babeskopia garbia dela).
- Monitorizatu sistema gertutik hurrengo ordu/egunetan, erasoa errepikatzen ez dela ziurtatzeko.
- Berrezarri zerbitzua erabiltzaileentzat.

## Fase 6: Ikasitako Lezioak (Post-Incident)

- Bilera intzidentzia itxi eta 2 asteko epean.
- Txostena idatzi: Zer funtzionatu du? Zer ez? Zer hobetu behar da?
- Eguneratu Segurtasun Plana eta prozedurak.

## 3. Komunikazio Plana

- **Barnekoa:** Langileei eta Zuzendaritzari informatu (informazio teknikoegia ekidin).
- **Kanpokoa:**
  - **Bezeroak:** Datu pertsonalak arriskuan egon badira (GDPR 72 orduko epea).
  - **Agintariak:** Datu Babeserako Bulegoa edo Zibersegurtasun Zentroa (Beharrezko bada).
  - **Prentsa:** Komunikazio arduradunaren bidez soilik.

## 4. NIS2 Jakinarazpen Protokoloa (EU 2022/2555)

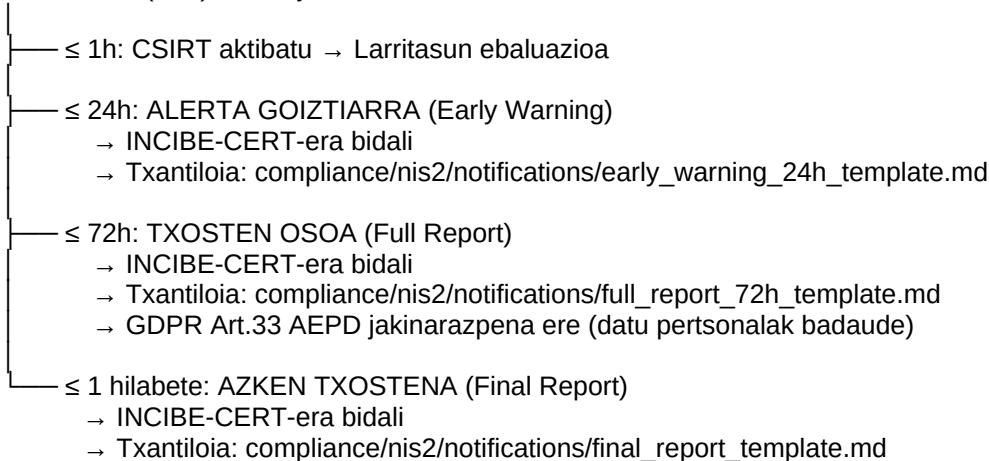
**GARRANTZITSUA:** NIS2 betebeharrok betetzea nahitaezkoa da 2026-10-17tik aurrera. Ez betetzeagatik zigorak: 10 milioi € arte edo fakturazioaren %2.

### 4.1 Noiz aktibatu — “Significant Incident” Irizpideak (Art. 23.3)

Intzidentzia **esanguratsua** da baldin eta: - Zerbitzu esanguratsuan etendura larria eragiten badu ( $\geq 30$  min) - Finantza galera garrantzitsua eragiten badu ( $> 5.000\text{€}$  estimazioa) - Beste pertsona fisiko edo juridiko bati kalte nabarmena eragin badezake - Datu pertsonalen ihesa badago (GDPR + NIS2 bikoitza)

### 4.2 Jakinarazpen Timeline-a

DETEKZIOA (T=0) — Erlojua hasten da



### 4.3 Hartzaileak

**Agintaria**

**Kontaktua**

**Noiz**

**INCIBE-CERT** incidencias@incibe-cert.es NIS2 intzidentzia esanguratsu guztietaan

**AEPD** www.aepd.es (sede elektronikoa) Datu pertsonalen ihesean (GDPR Art.33)

**BCSC** contacto@basquecybersecurity.eus Euskadi mailako koordinazioa

## 4.4 Procedura

1. **CSIRT Commander-ak** intzidentzia esanguratsua dela konfirmatzen du.
2. **Kronometroa** hasten da (T=0 = detekzio momentua).
3. **Automatizazioa:** SIEM alertak NIS2 timer-a aktibatzen du (ikus SOAR playbook-ak).
4. **24h baino lehen:** Early Warning txantiloia bete eta INCIBE-CERT-era bidali.
  - CISO-ak berrikusi eta onartzen du bidali baino lehen.
  - Kopia gorde: compliance/nis2/evidence-pack/notifications/
5. **72h baino lehen:** Full Report txantiloia osatu eta bidali.
6. **Hilabete barruan:** Final Report txantiloia osatu eta bidali.
7. **Erregistratu** bidalketa guztiak SIEM-ean eta evidence-pack-ean.

## 4.5 CSIRT Roster

CSIRT taldearen kontaktuak, guardia txandak eta eskalazio matrizea: →  
[compliance/nis2/csirt\\_roster.md](#)

## 4.6 SOAR Playbook-ak (Automatizazioa)

Automatizazioa eta korrelazio arauak: → [compliance/nis2/siem\\_soar/nis2\\_soar\\_playbooks.md](#) →  
[compliance/nis2/siem\\_soar/nis2\\_correlation\\_rules.json](#)