ZABALA GAILETAK

S.L. - Dokumentazio Akademikoa

Zibersegurtasun Gorabeherak Kudeatzea

2026(e)ko otsailaren 23(a)

MODULUA 04 — ZIBERSEGURTASUN-GORABEHERAK ETA ERANTZUNA

Proiektua: ER4 — Zabala Gailetak S.L. Zibersegurtasun Proiektua **Modulua:** 04 — Zibersegurtasun-Gorabeherak eta Erantzuna **Ikaslea:** Zabala Gailetak Taldea **Data:** 2025 **Bertsioa:** 1.0 **Egoera:** Osatua

AURKIBIDEA

1. Sarrera eta Helburuak

1.1 Moduluaren Deskribapena

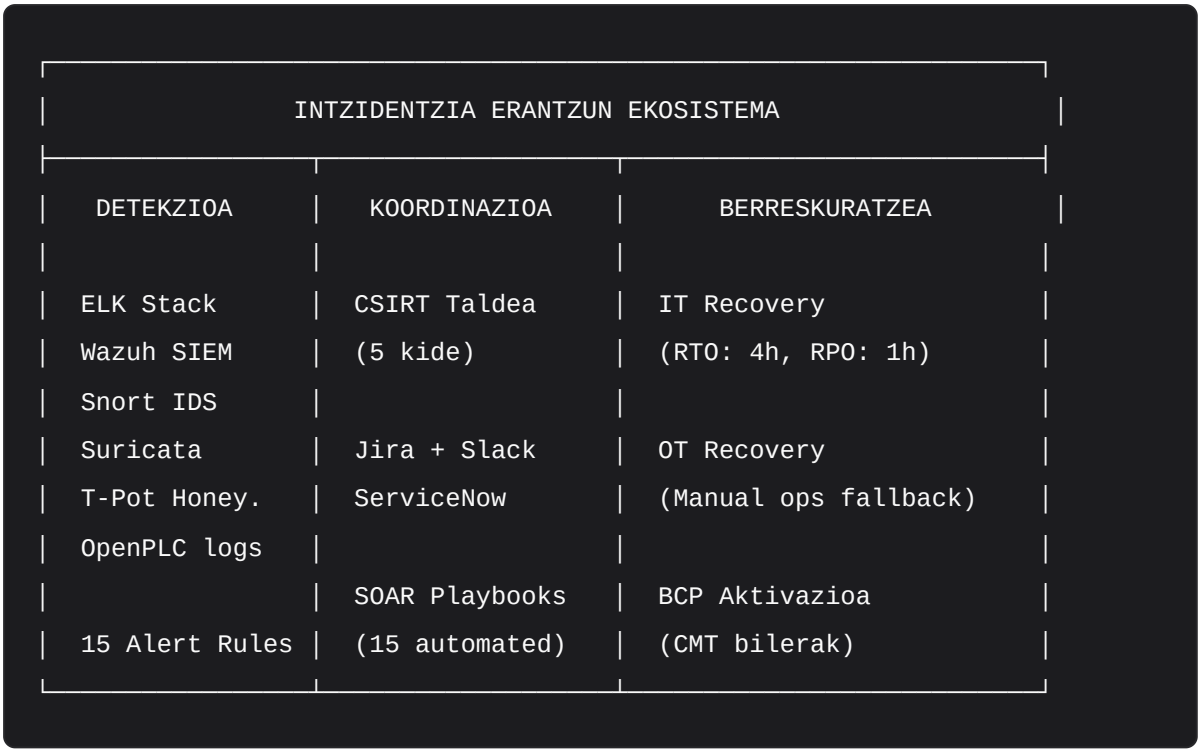
Modulu honek Zabala Gailetak S.L.-ren **Zibersegurtasun-Gorabeherak eta Erantzuna** dokumentatzen du. NIST SP 800-61r2 estandarrean oinarritutako intzidentzia erantzun prozedurak, CSIRT taldearen antolamendua, komunikazio planak eta negozio jarraitutasun plana (BCP) biltzen ditu.

Zabala Gailetak S.L.-k gaileta eta txokolate fabrikazio industria operatzen du 120 langile eta IT/OT azpiegitura konplexuarekin. Intzidentzia baten eragina IT sistemetan eta OT ekoizpen lineetan aldi berean gerta daitekeenez, erantzun prozedura integrala beharrezkoa da.

1.2 Helburuak

#	Helburua	Estandarra
H-01	Intzidentziei erantzuteko prozedura formalizatua ezartzea	NIST SP 800-61r2
H-02	CSIRT taldea antolatzea eta erantzukizunak definitzea	ISO/IEC 27035
H-03	Intzidentzien sailkapena eta triajea automatizatzea	CVSS v3.1, MITRE ATT&CK
H-04	Komunikazio plan integratua garatzea (barne/kanpo)	GDPR Art. 33/34, NIS2
H-05	OT intzidentzia simulazioa burutzea	IEC 62443-2-4
H-06	Negozio jarraitutasuna bermatzea (RTO=4h, RPO=1h)	ISO 22301, BCP
H-07	SOAR automatizazioa hedatzea 15 playbook-ekin	SANS, MITRE

1.3 Intzidentzia Erantzun Arkitektura



1.4 Arau-esparrua

Araudia	Aplikazioa	Betebehar nagusia
GDPR Art. 33	Datu pertsonalak	72h jakinarazpen AEPD-ri
GDPR Art. 34	Arrisku handiko incidenteak	Afektatuei jakinarazpen
NIS2 Zuzentaraua	Ezinbesteko zerbitzu hornitzaile	24h hasierako alerta INCIBE
ISO/IEC 27035	Intzidentzia kudeaketa	Prozesu formala
IEC 62443-2-4	OT intzidentziak	OT-espezifikoa
NIST SP 800-61r2	Erantzun prozedura	6 faseetan oinarritua

2. CSIRT Taldea eta Prestaketa

2.1 CSIRT Taldea — Antolaketa

CSIRT (Computer Security Incident Response Team) Zabala Gailetak-en 5 kidez osatuta dago:

Rola	Izena	Erantzukizuna	Kontaktua
CSIRT Buru	IT Zuzendaria	Koordinazio orokorra, komunikazio exekutiboa	csirt-buru@zabala-gailetak.eus
Analistalari Senior	SecOps Teknikaria	Intzidentzia azterketa, forensika	analista@zabala-gailetak.eus
Sareak Espezialista	Sare Administradorea	Sare isolamendua, firewall arauak	sareak@zabala-gailetak.eus
OT Espezialista	SCADA Teknikaria	PLC/SCADA erantzuna, ekoizpen jarraitutasuna	ot-sec@zabala-gailetak.eus
Legea eta Komunikazioa	Betetze Arduraduna / DPO	GDPR/NIS2 jakinarazpenak, prentsa	dpo@zabala-gailetak.eus

2.2 Arduradun Eskalazio Matrizea

```
MAILAK:
  Maila 1 (L1) → SOC Analista (1. erantzuna, triajea)
  Maila 2 (L2) → CSIRT Analistalari Senior (sakoneko azterketa)
  Maila 3 (L3) → CSIRT Buru + Exekutiboa (P1 intzidentziak)

ESKALAZIO DENBORA:
  P4 (Baxua)    → L1: 24h → L2: 72h (beharrezkoa bada)
  P3 (Ertaina)  → L1: 4h  → L2: 8h  → L3: 24h
  P2 (Altua)    → L1: 1h  → L2: 2h  → L3: 4h
  P1 (Kritikoa) → L1: 15m → L2: 30m → L3: 1h (berehalakoa)
```

2.3 Prestaketa Faseko Jarduerak

2.3.1 Tresnen Prestaketa

Tresna	Helburua	Konfigurazioa
ELK Stack 8.11.0	SIEM – log zentralizazioa	ZG-SecOps (192.168.200.20)
Wazuh Agent	Endpoint detekzioa	Denbora errealeko alerta
Snort IDS/Suricata	Sareko intrusioak	ZG-Gateway (192.168.2.1)
T-Pot Honeypot	Mehatxu hasierako detekzioa	Cowrie + Conpot aktibo
Velociraptor	Endpoint forensika	Volatile datuak batzea
TheHive/Cortex	Intzidentzia kudeaketa	SOAR integrazioa
MISP	Mehatxu adimena	IoC partekatze
Volatility	Memoriaren analisia	RAM dump azterketa

2.3.2 Playbook Liburutegia

```
/playbooks/
  ├── PB-001_malware_detekzioa.yml
  ├── PB-002_ransomware_erantzuna.yml
  ├── PB-003_datu_filtrazioa.yml
  ├── PB-004_sarerako_intrusioa.yml
  ├── PB-005_priibilegio_eskalazio.yml
  ├── PB-006_phishing_kampaina.yml
  ├── PB-007_ddos_erasoa.yml
  ├── PB-008_ot_anomalia.yml
  ├── PB-009_plc_manipulazioa.yml
  ├── PB-010_credential_stuffing.yml
  ├── PB-011_sql_injekzioa.yml
  ├── PB-012_apt_detekzioa.yml
  ├── PB-013_insider_threat.yml
  ├── PB-014_cloud_baimenik_gabekoa.yml
  └── PB-015_supply_chain_konpromisoa.yml
```

2.3.3 Komunikazio Kanal Prest-egitea

```
# Slack kanal konfigurazioa (CSIRT bakarrik)
#csirt-alerta          → Alerta guztiak (bot automatikoa)
#csirt-koordinazioa    → Talde komunikazioa
#csirt-ebidentziak     → Forensika datuak
#csirt-post-mortem     → PIR txostenak

# Signal taldea (P1 larrialdi komunikazio enkriptatua)
# Kideak: CSIRT buru, analistalari senior, IT zuzendaria, CEO

# ServiceNow ticketing
# URL: https://zabala-gailetak.service-now.com
# Automatikoki ticket sortzen du Wazuh-etik
```

2.4 Prestaketa Egiaztapen Zerrenda

- ☐ CSIRT kideak prestakuntza eguneratua dute (≤6 hilabete)
- ☐ Playbook guztiak probatuta daude (≤3 hilabete)
- ☐ Kontaktu zerrenda eguneratua (CEO, DPO, INCIBE, AEPD, aseguratzailea)
- ☐ Zipher disko enkriptatua prestaketa-kitarekin (Kali Linux live USB, forensika tresnak)
- ☐ Out-of-band komunikazioa testeatuta (Signal, telefono satelitea)
- ☐ Segurtasun kopiak egiaztaturik (3-2-1 araua betetzen da)
- ☐ Tabletop simulazioa ≤6 hilabete
- ☐ DR drilla ≤urtean behin

3. Intzidentzien Sailkapena eta Triajea

3.1 Intzidentzia Kategoriak

Kategoria	Deskribapena	Adibideak
CAT-01	Malware/Ransomware	Cryptolocker, Ryuk, APT droppers
CAT-02	Datu Filtrazioa	Datu pertsonalak, IP lapurreta
CAT-03	Sarerako Intrusioa	APT, C2 komunikazioa
CAT-04	DDoS/Erabilgarritasun Galerak	Web down, ERP ezin erabilgarri
CAT-05	Credential Lapurreta	Phishing, brute-force, credential stuffing
CAT-06	OT/ICS Erasoak	PLC manipulazioa, SCADA urruneko sarbidea
CAT-07	Insider Mehatxua	Langile baimenik gabekoa, sabotajea
CAT-08	Supply Chain	Hornitzaile konpromisoa, software bildumakoa
CAT-09	Web Aplikazio Erasoa	SQLi, XSS, OWASP Top 10
CAT-10	Fisikoa	Sarreraldi fisikoa, hardware lapurreta

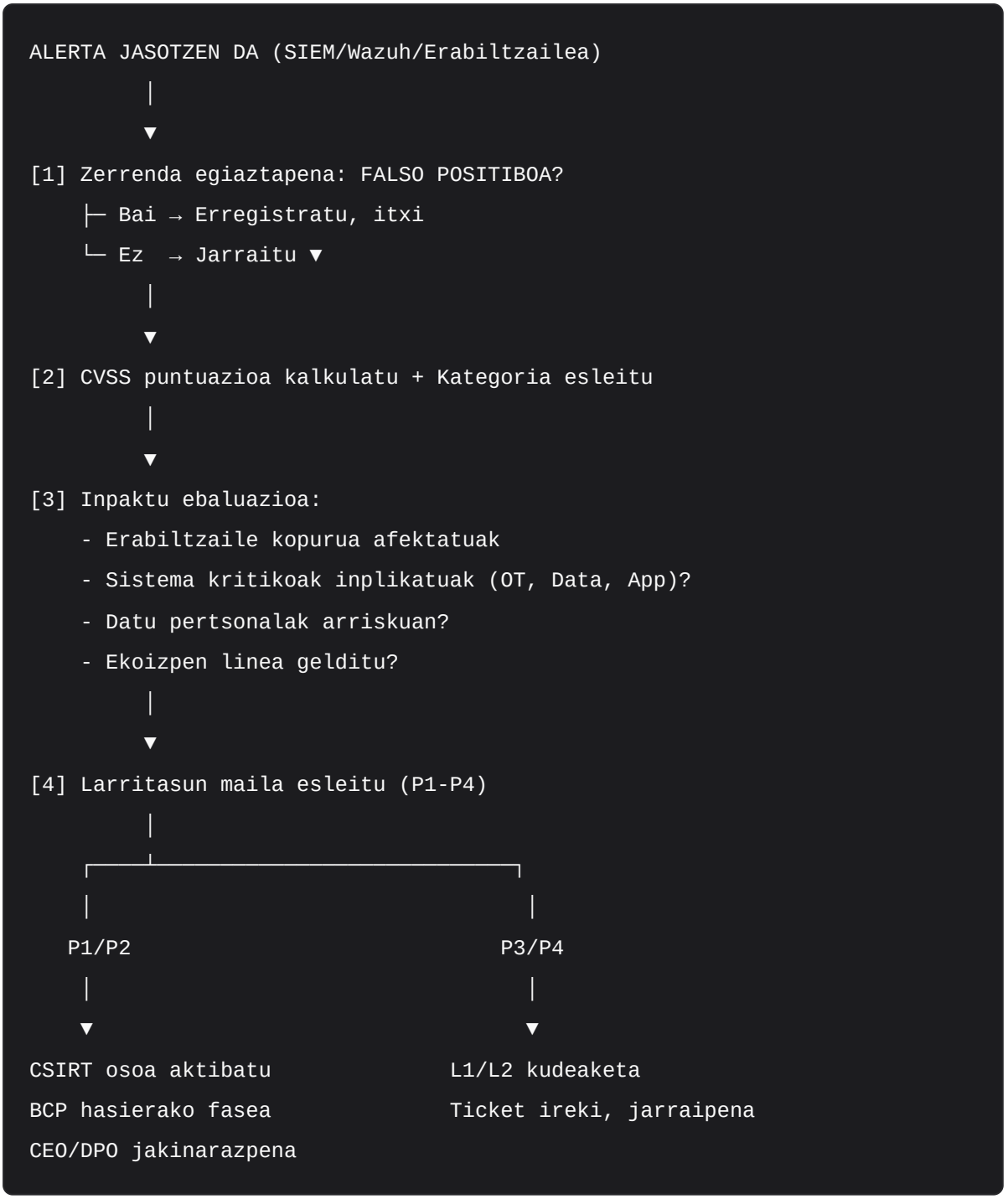
3.2 Larritasun Mailen Definizioa

Maila	Etiketa	CVSS Tartea	Erantzun Denbora	Eskalazio
P1	KRITIKOA	9.0 – 10.0	15 minutu	L3 berehalakoa
P2	ALTUA	7.0 – 8.9	1 ordu	L2 → L3 2h
P3	ERTAINA	4.0 – 6.9	4 ordu	L1 → L2 8h
P4	BAXUA	0.1 – 3.9	24 ordu	L1 kudeaketa

3.3 Inpaktua Ebaluatzeko Matrizea

INPAKTUA	PROBABILITATEA: Baxua	Ertaina	Altua
Altua	P2	P1	P1
Ertai.	P3	P2	P2
Baxua	P4	P4	P3

3.4 Triaje Prozesua — Fluxu Diagrama



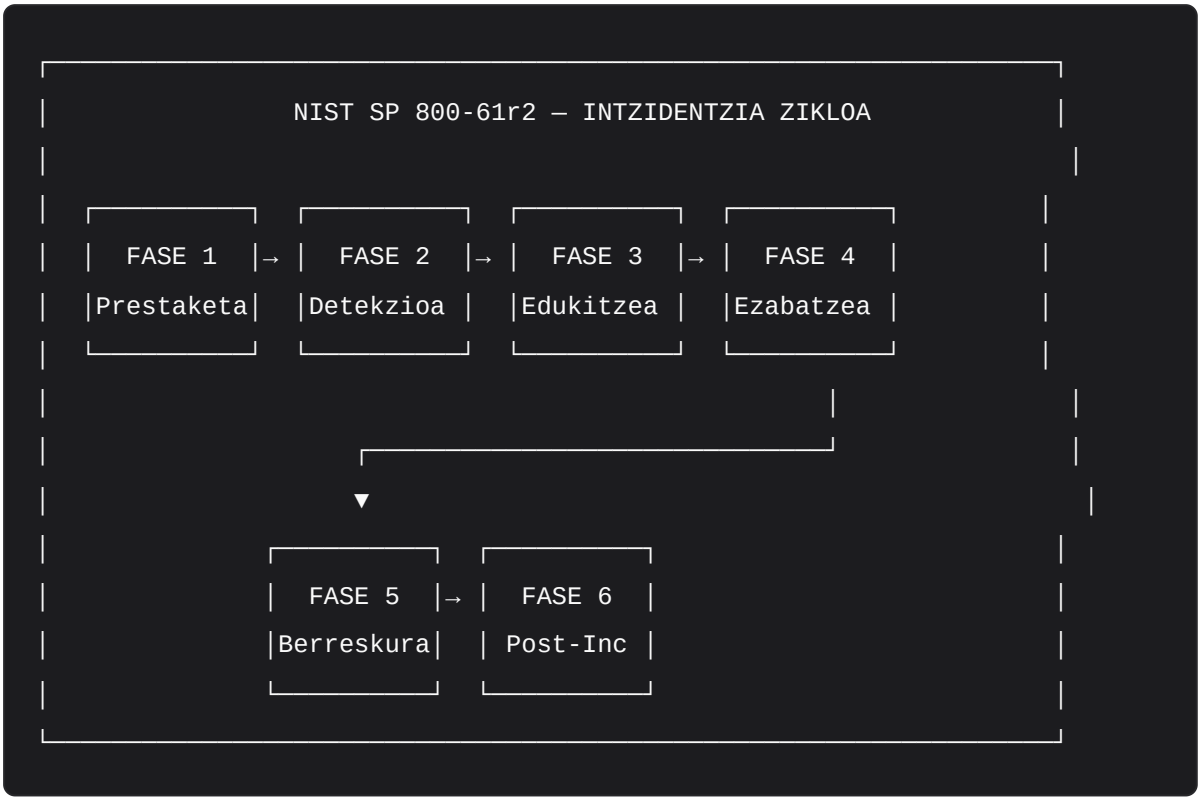
3.5 MITRE ATT&CK Mapaketa

Teknika ID	Izena	Detekzio Adierazlea	Erantzun Playbook
T1566	Phishing	Email gateway alerta	PB-006
T1078	Kontu Baliabideak Baliatu	Saio-hasiera anomalia	PB-010

Teknika ID	Izena	Detekzio Adierazlea	Erantzun Playbook
T1486	Datu Enkriptatzea (Ransomware)	Azkar fitxategi aldaketa	PB-002
T1041	Datu Exfiltazioa C2	DNS anomalia, outbound berria	PB-003
T1190	Aplikazio Publikoa Ustiatu	WAF alerta, SQLi patroiak	PB-011
T1059	Komando-lerroa	PowerShell/bash anomalia	PB-004
T0855	Urruneko OT Komandoa	Modbus TCP anomalia	PB-009
T0828	OT Prozesua Manipulatu	Tenperatura aldaketa PLC	PB-008

4. NIST SP 800-61 — 6 Faseko Erantzun Prozedura

4.1 Faseen Ikuspegi Orokorra



4.2 Fase 1 — Prestaketa (Preparation)

Ikus Atala 2 — CSIRT Taldea eta Prestaketa.

Funtsezko elementuak:

- CSIRT taldea konfiguratua
- Playbook liburutegia osatua (15 playbook)
- Komunikazio kanalak aktibo (Slack, Signal, ServiceNow)
- Tresnak instalaturik (ELK, Wazuh, Velociraptor, TheHive)
- Segurtasun kopiak egiaztaturik (3-2-1 araua)

4.3 Fase 2 — Detekzioa eta Analisia (Detection & Analysis)

4.3.1 Detekzio Iturriak

```
DETEKZIO ITURRIAK (15 arau aktibo — Wazuh + ELK):

Sareko Alertak:
  RULE-001: Portu eskaneatze masiboa (>100 port/min)
  RULE-002: SSH brute-force (>20 saiakera/5min)
  RULE-003: DNS exfiltrazio patroiak (pakete handi >512B)
  RULE-004: Modbus TCP anomalia (irakurketa ez-ohikoa portu 502)
  RULE-005: Baimenik gabeko sareko konexioa OT segmentutik

Sistemen Alertak:
  RULE-006: Root priibilegio eskalazio saiakera
  RULE-007: Segurtasun kopien aldaketa baimenik gabe
  RULE-008: Konfigurazio fitxategi kritikoaren aldaketa
  RULE-009: Zerbitzu geldiarazte saiakera (systemd/service)
  RULE-010: Honeypot konexioa detektatu (T-Pot/Cowrie)

Aplikazio Alertak:
  RULE-011: SQL injekzio patroiak web logetan
  RULE-012: Autentifikazio huts masiboak (>50/min)
  RULE-013: JWT token anomalia (algoritmo aldaketa)
  RULE-014: API rate-limit gainditzea (>1000 dei/min)
  RULE-015: Datu-base baimenik gabeko kontsulta masiboak
```

4.3.2 Analisi Tresnak

```
# 1. Log bilketa eta ikerketa — Elasticsearch
curl -X GET "http://192.168.200.20:9200/wazuh-alerts-*/_search" \
  -H "Content-Type: application/json" \
  -d '{
    "query": {
      "bool": {
        "must": [
          {"range": {"@timestamp": {"gte": "now-1h"}}},
          {"match": {"rule.level": "10"}}
        ]
      }
    },
    "sort": [{"@timestamp": "desc"}]
  }'

# 2. Honeypot alerta aztertu — Cowrie
ssh analyst@192.168.200.20
docker logs cowrie-honeypot --since 1h | grep "New connection"

# 3. Sare konexio aktiboak aztertu — ZG-Gateway
ssh admin@192.168.2.1
netstat -tulpn | grep ESTABLISHED
ss -tlnp | grep -v "127.0.0.1"

# 4. Prozesu anomaliak — Velociraptor
velociraptor -config /etc/velociraptor/client.yml \
  artifacts collect Generic.System.Pstree

# 5. Hash egiaztapena — sistemen osotasuna
sha256sum -c /etc/aide/aide.db
aide --check --config=/etc/aide/aide.conf
```

4.3.3 Ebidentzien Biltze Protokoloa

```
#!/bin/bash
# evidence_collection.sh — Forenzika ebidentzien biltze protokoloa
# GARRANTZITSUA: Read-only modu deskribapen jasotakoa

INCIDENT_ID=$1
TIMESTAMP=$(date +%Y%m%d_%H%M%S)
EVIDENCE_DIR="/mnt/forensics/INC-${INCIDENT_ID}/${TIMESTAMP}"

mkdir -p "$EVIDENCE_DIR"/{memory,network,logs,disk}

echo "[+] Memoriaren dump — RAM bilketa"
# avml edo LiME erabiliz (volatile lehen beti)
avml "$EVIDENCE_DIR/memory/ram_dump.lime"
md5sum "$EVIDENCE_DIR/memory/ram_dump.lime" > "$EVIDENCE_DIR/memory/ram_dump

echo "[+] Sare egoera bilketa"
netstat -tulpn > "$EVIDENCE_DIR/network/netstat.txt"
ss -tlnp >> "$EVIDENCE_DIR/network/ss.txt"
arp -a > "$EVIDENCE_DIR/network/arp.txt"
ip route > "$EVIDENCE_DIR/network/routes.txt"

echo "[+] Prozesu bilketa"
ps auxf > "$EVIDENCE_DIR/logs/processes.txt"
ls -la /proc/*/exe 2>/dev/null > "$EVIDENCE_DIR/logs/proc_exe.txt"

echo "[+] Fitxategi sistema"
find / -newer /tmp/.incident_marker -type f 2>/dev/null | \
  head -1000 > "$EVIDENCE_DIR/logs/recently_modified.txt"

echo "[+] Log sistematikoak kopiatzea"
cp -r /var/log/ "$EVIDENCE_DIR/logs/system_logs/"
journalctl --since "2 hours ago" > "$EVIDENCE_DIR/logs/journal.txt"

echo "[+] Ebidentziak zigilatu SHA-256"
find "$EVIDENCE_DIR" -type f -exec sha256sum {} \; > \
  "$EVIDENCE_DIR/chain_of_custody.sha256"

echo "[✓] Ebidentzia bilketa osatua: $EVIDENCE_DIR"
```

4.4 Fase 3 — Edukitzea (Containment)

4.4.1 Epe Laburreko Edukitzea (0–2 ordu)

```
# OHARRA: Edukitzea ordenak C-EXEC-001 baimenarekin soilik exekutatu

# 1. Sistema konprometitua isolatu — VLAN isolamendu
# ZG-Gateway — pfSense
pfctl -t blocked_hosts -T add 10.0.20.45  # sistema konprometitua
pfctl -e  # arauak aktibatu

# 2. Interfaze sareko blokeo (larrialdietarako)
ssh admin@10.0.10.1
iptables -I FORWARD -s 10.0.20.45 -j DROP
iptables -I FORWARD -d 10.0.20.45 -j DROP
iptables-save > /etc/iptables/rules.v4

# 3. Erabiltzaile kontu izoztea (credential lapurreta kasuan)
# ZG-App zerbitzarian
ssh admin@10.0.10.10
php artisan user:disable --id=45 --reason="Security incident INC-2025-XXX"
# edo datu-basean zuzenean
psql -U hrportal -d hr_production \
  -c "UPDATE employees SET is_active=false, lock_reason='INC-2025-XXX'
      WHERE id=45;"

# 4. VPN konexioak izoztea
ssh admin@192.168.2.1
# OpenVPN — erabiltzaile baten ziurtagiria desgaitu
cd /etc/openvpn/easy-rsa
./easyrsa revoke affected_user
./easyrsa gen-crl
cp pki/crl.pem /etc/openvpn/
systemctl reload openvpn

# 5. DNS blokeo — C2 domeinua (RULE-003 detektatu badu)
echo "0.0.0.0 malicious-c2-domain.xyz" >> /etc/hosts
# Unbound DNS-en ere blokeo
echo 'local-zone: "malicious-c2-domain.xyz" refuse' >> /etc/unbound/unbound.c
systemctl reload unbound
```

4.4.2 Epe Luzeko Edukitzea (2–24 ordu)

```
# Snapshot prestatu — berreskuratze puntua
# IsardVDI / Proxmox
proxmox-snapshot create ZG-App "pre-incident-INC-2025-XXX"
proxmox-snapshot create ZG-Data "pre-incident-INC-2025-XXX"

# Segurtasun kopien osotasuna egiaztatu
# Ikus BCP Atala 8 — berreskuratze prozedura

# Honeytoken hedatu — intrusoaren mugimendua jarraitu
# (Aldez aurretik prestatutako kontu "erakarri" batekin)
# Wazuh-ek kontrolatu badu saio-hasiera alerta sortuko du
```

4.4.3 OT Edukitzea

```
# OT intzidentzian: 3 urratseko isolamendu protokoloa

# URRATS 1: Historian zerbitzaria konektatzetik desgaitu
# ScadaBR — Modbus TCP konexioa eten
# ZG-OT (172.16.0.0/16 segmentua)
iptables -I FORWARD -s 172.16.1.0/24 -d 10.0.10.0/24 -j DROP

# URRATS 2: PLC-ak "local" modura aldatu
# OpenPLC runtime — urruneko sarbidea desgaitu
ssh admin@172.16.1.10
openplc_service stop_remote_access
openplc_service enable_local_only

# URRATS 3: Produkzio supervisorari jakinarazi
# Ekoizpen linea geldiarazi modu seguruan
# (SOP-OT-STOP-001 prozedura jarraitu)
```

4.5 Fase 4 — Ezabatzea (Eradication)

```
# 1. Malware aztarnak ezabatu
# Antivirus eskaneatzea — ClamAV
clamscan -r /var/www/ --remove=yes --log=/tmp/clamav_scan.log
clamscan -r /home/ --remove=yes >> /tmp/clamav_scan.log

# 2. Rootkit ikerketa
rkhunter --check --sk --rwo
chkrootkit -q

# 3. Backdoor eta scheduled task ikerketa
crontab -l -u www-data
find / -name "*.php" -newer /tmp/.incident_marker | xargs grep -l "eval\|base
find /tmp /var/tmp /dev/shm -type f -executable

# 4. Pakete eta dependentzia osotasuna
# PHP
composer audit --format=json
# Node.js (React)
npm audit --json

# 5. Pasahitz aldaketa (credential lapurreta bada)
# Erabiltzaile guztien pasahitz berresleitu
php artisan users:force-password-reset --all
# Session guztiak deuseztatu
php artisan session:flush

# 6. Ziurtagirien berritu (SSL/TLS konpromisoa bada)
certbot renew --force-renewal
systemctl reload nginx
```

4.6 Fase 5 — Berreskuratzea (Recovery)

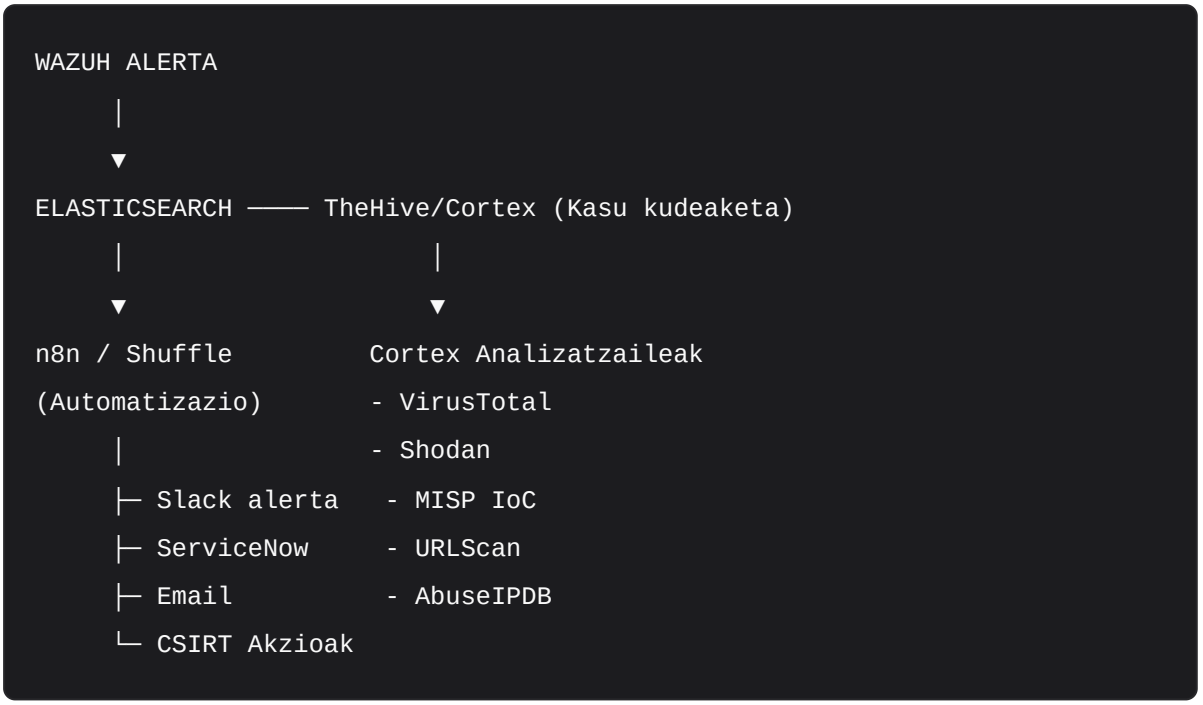
```
# 1. Osasun egiaztapena berreskuratu baino lehen
# Backup-ren osotasuna
sha256sum /backup/latest/hr_database.sql.gpg
sha256sum /backup/latest/webapp_files.tar.gz.gpg

# 2. Segurtasun kopiaren deszifraketa
gpg --batch --passphrase-file /etc/backup/key.gpg \
    --decrypt /backup/latest/hr_database.sql.gpg | \
    psql -U hrportal -d hr_production

# 3. Web aplikazioaren berresleipena (fitxategi garbia)
tar -xzf /backup/latest/webapp_files.tar.gz -C /var/www/html/
chown -R www-data:www-data /var/www/html/
chmod -R 755 /var/www/html/

# 4. Konfigurazio fitxategien berreskurapena
cp /backup/config/nginx.conf /etc/nginx/nginx.conf
cp /backup/config/.env.production /var/www/html/.env
nginx -t && systemctl reload nginx

# 5. Docker zerbitzu berrabiaraztea
docker-compose -f /opt/zabala/docker-compose.yml up -d
docker-compose ps  # Zerbitzu guztiak "Up" egoera egiaztatu

# 6. Osasun egiaztapenak
# HR Atari osasuna
curl -f https://hr.zabala-gailetak.eus/health || echo "HUTSEGITEA"
# API osasuna
curl -f https://api.zabala-gailetak.eus/api/health || echo "HUTSEGITEA"
# Datu-base konexioa
psql -U hrportal -d hr_production -c "SELECT 1;" || echo "DB ARAZOA"

# 7. ELK/Wazuh monitorizazioa birbiztu
systemctl status elasticsearch kibana wazuh-manager
# Berreskuratze ondorengo 24h monitorizazio areagotua
wazuh-logtest <<< "test_post_incident_monitoring"
```

4.7 Fase 6 — Post-Intzidentzia Jarduera

Ikus Atala 9 — Post-Intzidentzia Berrikuspena.

5. SOAR Playbook-ak eta Automatizazioa

5.1 SOAR Arkitektura



5.2 Playbook Zehatza — PB-002 Ransomware Erantzuna

```
# PB-002_ransomware_erantzuna.yml
# TheHive/Cortex SOAR playbook

name: "Ransomware Erantzuna"
version: "2.1"
severity: "KRITIKOA"
mitre_techniques:
  - T1486  # Data Encrypted for Impact
  - T1490  # Inhibit System Recovery
  - T1082  # System Information Discovery

triggers:
  - rule_id: "RULE-007"  # Fitxategi masibo aldaketa
  - ioc_pattern: ".*\\.encrypted|.*\\.locked|.*\\.ransom"
  - process_anomaly: "vssadmin delete shadows"

steps:
  - id: "S01"
    name: "Berehalako Isolamendua"
    automation: true
    timeout: "2m"
    actions:
      - type: "firewall_block"
        target: "{{source_ip}}"
        scope: "all_outbound"
      - type: "network_isolate"
        target: "{{affected_host}}"
        vlan: "quarantine_vlan_999"
      - type: "disable_user"
        target: "{{source_user}}"
        reason: "Ransomware INC-{{incident_id}}"

  - id: "S02"
    name: "Alerta Jakinarazpena"
    automation: true
    timeout: "1m"
    actions:
      - type: "slack_notify"
```

```
      channel: "#csirt-alerta"
      message: |
        🚨 RANSOMWARE DETEKTATU — P1 KRITIKOA
        Intzidentzia: INC-{{incident_id}}
        Sistema: {{affected_host}} ({{affected_ip}})
        Erabiltzailea: {{source_user}}
        Fitxategi aldaketak: {{file_changes_count}}
        Ekintza: Sistema isolatua automatikoki
        CSIRT Akzioa beharrezkoa: Berehalakoa
    - type: "page_oncall"
      team: "csirt-core"
      priority: "P1"
    - type: "servicenow_ticket"
      category: "CAT-01"
      priority: "P1"
      assignee: "csirt-buru"

- id: "S03"
  name: "Backup Osotasun Egiaztapena"
  automation: true
  timeout: "5m"
  actions:
    - type: "verify_backup_integrity"
      targets:
        - "/backup/latest/hr_database.sql.gpg"
        - "/backup/latest/webapp_files.tar.gz.gpg"
      checksum_file: "/backup/checksums.sha256"
    - type: "slack_update"
      message: "Backup egiaztapena: {{backup_status}}"

- id: "S04"
  name: "Forensika Bilketa"
  automation: false  # Gizakiak eskuz gauzatu
  instructions: |
    1. evidence_collection.sh INC-{{incident_id}} exekutatu
    2. RAM dump lehentasunezkoa (volatile datuak)
    3. Prozesu arbola dokumentatu
    4. Sare konexio aktiboak erregistratu
    5. Ransom ohar kopiatu (aldatu gabe)
```

```yaml
  - id: "S05"
    name: "GDPR Balorazioa"
    automation: false
    sla: "2h"
    instructions: |
      DPO-k ebaluatu:
      - Datu pertsonalak afektatuak? (Bai/Ez)
      - Afektatu kopurua estimatua: ___
      - Arrisku maila: Altua / Ertaina / Baxua
      Arrisku altua → AEPD jakinarazpen 72h (GDPR Art. 33)

  - id: "S06"
    name: "Berreskuratze Erabakia"
    automation: false
    approvers: ["csirt-buru", "it-zuzendaria"]
    options:
      - "Backup-etik berreskuratu (RTO: 4h)"
      - "Sistema garbia eraiki (RTO: 8h)"
      - "Pagatu erreskatea (GOMENDATZEN EZ)"
```

5.3 Playbook — PB-009 OT/PLC Manipulazioa

```yaml
# PB-009_plc_manipulazioa.yml

name: "OT/PLC Manipulazio Erantzuna"
version: "1.3"
severity: "P1 KRITIKOA"
mitre_techniques:
  - T0855  # Unauthorized Command Message
  - T0828  # Manipulate IO Image
  - T0826  # Loss of Availability

triggers:
  - rule_id: "RULE-004"  # Modbus TCP anomalia
  - rule_id: "RULE-005"  # Baimenik gabeko OT konexioa
  - ot_alert: "temperature_out_of_range"
  - ot_alert: "unauthorized_modbus_write"

steps:
  - id: "OT-S01"
    name: "OT Espezialista Jakinarazpena"
    automation: true
    timeout: "2m"
    actions:
      - type: "page_oncall"
        team: "ot-specialist"
        message: |
          OT ALERTA P1: Modbus anomalia
          PLC: {{plc_address}}
          Erregistroa: {{modbus_register}}
          Balioa: {{value_before}} → {{value_after}}
          Iturria: {{source_ip}}

  - id: "OT-S02"
    name: "Ekoizpen Geldialdi Segurua"
    automation: false
    responsible: "ot-espezialista + ekoizpen-supervisora"
    instructions: |
      1. Ekoizpen linea modu seguruan geldiarazi (ELS — Emergency Line Stop)
      2. PLC-ak "local" modura aldatu (urruneko sarbidea eten)
```

```
      3. HMI pantailak begizta estali (argazkiak hartu lehen)
      4. Tenperatura/presio erregistroa gorde (paper-based)

  - id: "OT-S03"
    name: "IT-OT Sare Isolamendua"
    automation: true
    timeout: "1m"
    actions:
      - type: "firewall_block"
        interface: "it_to_ot_bridge"
        direction: "both"
        duration: "until_cleared"

  - id: "OT-S04"
    name: "PLC Firmware Egiaztapena"
    automation: false
    instructions: |
      1. OpenPLC bertsioa egiaztatu (itxarondakoa: v3.0.x)
      2. Programa logika backup-arekin alderatu
      3. Aldaketa detektatu bada: firmware berrezarri
      4. Kalibrazioa egiaztatu (tenperatura sentsoreak)

  - id: "OT-S05"
    name: "INCIBE-CERT Jakinarazpena"
    automation: false
    sla: "4h"
    instructions: |
      NIS2 betebehar: INCIBE-CERT-i jakinarazi
      URL: https://www.incibe-cert.es/en/early-warning
      Inprimakia bete: OT sistema industriala inplikatua
```

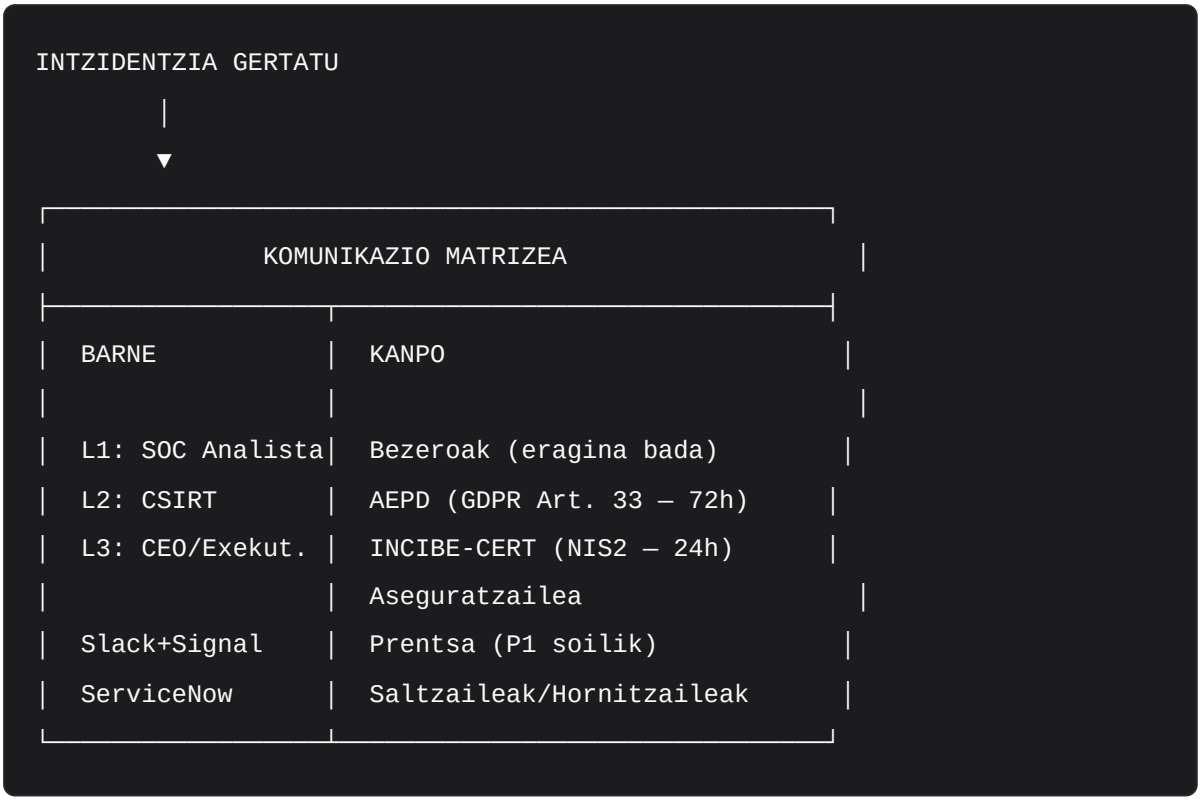
5.4 15 Alerta Arau Automatizatuen Laburpena

#	Arau ID	Izena	Larritasuna	Playbook	Automatizazioa
1	RULE-001	Portu eskaneo masiboa	P3	PB-004	Firewall blokeo auto
2	RULE-002	SSH brute-force	P2	PB-010	IP ban + alerta

#	Arau ID	Izena	Larritasuna	Playbook	Automatizazioa
3	RULE-003	DNS exfiltrazioaren patroiak	P2	PB-003	DNS blokeo + alerta
4	RULE-004	Modbus TCP anomalia	P1	PB-009	OT isolamendu + paginazioa
5	RULE-005	Baimenik gabeko OT konexioa	P1	PB-009	Firewall blokeo + alarma
6	RULE-006	Root priibilegio eskalazio	P2	PB-005	Kontu izoztea + alerta
7	RULE-007	Segurtasun kopien aldaketa	P1	PB-002	Sistema isolamendu + CSIRT
8	RULE-008	Konfigurazio fitxategi aldaketa	P2	PB-007	Alerta + hash egiaztapena
9	RULE-009	Zerbitzu geldiarazte saiakera	P2	PB-007	Alerta + rollback
10	RULE-010	Honeypot konexioa	P3	PB-004	Alerta + log bilketa
11	RULE-011	SQL injekzio patroiak	P2	PB-011	WAF blokeo + alerta
12	RULE-012	Autentifikazio huts masiboa	P2	PB-010	Rate-limit + CAPTCHA
13	RULE-013	JWT token anomalia	P1	PB-010	Session flush + alerta
14	RULE-014	API rate-limit gainditzea	P3	PB-007	Auto throttling
15	RULE-015	DB baimenik gabeko kontsulta	P2	PB-003	Konexio izoztea + alerta

6. Komunikazio Plana

6.1 Komunikazio Arkitektura



6.2 Barne Komunikazio Templateak

6.2.1 L1 — SOC-etik CSIRT-era (Alerta Iniziala)

```
GAIA: [ALERTA P{maiila}] {intzidentzia_mota} — INC-{urtea}-{zenbakia}
HARIA: #csirt-alerta (Slack)

═══════════════════════════════════════════
INTZIDENTZIA ALERTA — P{maila}
═══════════════════════════════════════════
Intzidentzia ID:    INC-{urtea}-{zenbakia}
Detekzio data/ordua: {data} {ordua} (CET)
Detekzio iturria:   {Wazuh/Snort/Erabiltzaile/...}
Kategoria:          CAT-{XX} — {izena}
Larritasuna:        P{1-4} ({KRITIKOA/ALTUA/ERTAINA/BAXUA})

DESKRIBAPENA:
{gertaeraren laburpen teknikoa — 2-3 esaldi}

AFEKTATURIKO SISTEMAK:
- {sistema1} ({IP})
- {sistema2} ({IP})

HASIERAKO EKINTZAK HARTUA:
☑ Alerta egiaztatu (falso positibo ez)
☑ Triajea egina (P{maila} esleitu)
☑ Playbook PB-{XXX} aktibatu
☐ CSIRT Erantzuna beharrezkoa

HURRENGO URRATSA:
CSIRT {maila} erantzuna {denbora} barruan
═══════════════════════════════════════════
```

6.2.2 L2 — CSIRT-etik Exekutiboetara (P1/P2 Kasuan)

```
GAIA: [INTZIDENTZIA P{maila}] {mota} — Egoera Eguneratzea {ordua}
HARIA: Signal taldea (CSIRT buru → CEO, DPO, IT Zuzendaria)

═══════════════════════════════════════════

EXEKUTIBO TXOSTENA — INTZIDENTZIA INC-{urtea}-{ZZZ}
═══════════════════════════════════════════

Data: {data}  Ordua: {ordua}

LABURPENA:
{teknikarik gabe laburpen exekutiboa — 3-4 esaldi}

ERAGINA:
- Sistema/Zerbitzu afektatuak: {zerrenda}
- Langile afektatuak: ~{kopurua}
- Datu pertsonalik arriskuan: BAI/EZ
- Ekoizpen eragina: BAI/EZ

EGUNGO EGOERA:
□ Edukitzea: {OSATUA/PROZESUAN/ZAIN}
□ Ezabatzea: {OSATUA/PROZESUAN/ZAIN}
□ Berreskurapena: {OSATUA/PROZESUAN/ZAIN}
□ Komunikazioak: {OSATUA/PROZESUAN/ZAIN}

BETEBEHAR LEGALAK:
□ GDPR Art. 33 (72h): {BEHARREZKOA/EZ}
□ NIS2 (24h INCIBE): {BEHARREZKOA/EZ}
□ Aseguratzailea: {JAKINARAZPENA EGIN/ZAIN}

HURRENGO TXOSTENA: {data eta ordua}
═══════════════════════════════════════════
```

6.2.3 Langile Komunikazio Orokorra

```
GAIA: IT Sistema Mantentze Lana — {data}

Langile guztiei,

Egun sistema teknikoen mantentze lan batzuk egiten ari gara.
Ondorioz, {zerbitzu/aplikazioa} denboraldi batean erabilgarri
ez egon daiteke.

Iraupena: Gutxi gorabehera {denbora}

Arazoren bat izanez gero: it@zabala-gailetak.eus

Eskerrik asko zuen ulermenarekin.

IT Saila — Zabala Gailetak S.L.
```

Oharra: Ez aipatu "zibersegurtasun intzidentzia" barne komunikazioetan, ikerketa arriskuan ez jartzeko.

6.3 Kanpo Komunikazio Templateak

6.3.1 GDPR Art. 33 — AEPD Jakinarazpena (72h Barruan)

```
HARTZAILE: AEPD (Agencia Española de Protección de Datos)
BIDEA: https://sedeagpd.gob.es/sede-electronica-web/vistas/formNotificacionV
EPEA: Ezagutarazte unetik 72 orduko barruan

═══════════════════════════════════════════

DATU URRAKETA JAKINARAZPENA — GDPR 33. ARTIKULUA
═══════════════════════════════════════════

Erakundea:        Zabala Gailetak S.L.
IFZ/NIF:          {NIF}
DPO Kontaktua:    {DPO izena} — dpo@zabala-gailetak.eus
Helbidea:         {helbidea}, Euskal Herria

Gertaera Data:    {data eta ordua}
Jakinarazpen Data: {data} (ezagutarazte unetik {XX} ordu)

URRAKETA MOTA:
☑/□ Konfidentzialtasun urraketa (datuetara sarbide baimenik gabe)
☑/□ Osotasun urraketa (datuak aldatu edo ezabatu)
☑/□ Erabilgarritasun urraketa (datuak ez eskuragarri)

AFEKTATURIKO DATU KATEGORIAK:
- {langileen datu pertsonalak, osasun datuak, finantza datuak...}
Afektatu kopurua (gutxi gorabeherako): ~{kopurua} pertsona

DESKRIBAPENA:
{gertaeraren deskribapen teknikoa, nola gertatu zen, zer sistema
inplikatu ziren, zenbat denboran iraun zuen}

ONDORIOAK ETA ARRISKUA:
{afektatuentzako arrisku probablea — identitate-lapurreta,
finantza kalte, diskriminazioa...}

HARTUTAKO NEURRIAK:
1. {kontainmendu neurria}
2. {ezabatzea neurria}
3. {berreskuratze neurria}
4. {prebentzio neurria etorkizunerako}

AFEKTATUEI JAKINARAZPENA (Art. 34):
```

```
☑/□ Jakinarazpena bidali: {data}
☑/□ Arrisku altua ez — ez da jakinarazpen berezirik behar
Arrazoia: {justifikazioa}
═══════════════════════════════════════════
```

6.3.2 NIS2 — INCIBE-CERT Jakinarazpena (24h Barruan)

```
HARTZAILE: INCIBE-CERT
BIDEA: https://www.incibe-cert.es/en/early-warning
EPEA: Ezagutarazte unetik 24 orduko barruan

═══════════════════════════════════════════
NIS2 INTZIDENTZIA JAKINARAZPENA
═══════════════════════════════════════════
Erakundea:     Zabala Gailetak S.L.
Sektore:       Elikadura industria / Fabrikazioa
NIS2 Kategoria: Garrantzitsua / Ezinbestekoa
Kontaktua:     csirt-buru@zabala-gailetak.eus / {telefono}

Gertaera Laburpena:
{teknikaren laburpen eta eragina — 5-10 esaldi}

Larritasun Maila: P{1-4}
Afektaturiko Sistemak: {IT/OT/Biak}
Erabilgarritasun Eragina: {ehunekoa edo deskribapena}
Kalte Ekonomiko Estimatua: {EUR edo "Oraindik kalkulatu gabe"}

Ikerketa Egoera: {Abian/Osatua}
═══════════════════════════════════════════
```

6.3.3 Bezero Komunikazioa (Zerbitzu Eragina Bada)

```
GAIA: Zabala Gailetak — Zerbitzu Aldi Baterako Etena

Estimatua bezero/bazkide,

Zabala Gailetak-ek jakinarazi nahi dizu gure {zerbitzu mota}
zerbitzu teknikoen arazo baten ondorioz aldi baterako etena
egon dela {data} eta {ordua} artean.

Zure {pedido/eskaera/entrega} honi eragina egin ahal dio:
{espezifikoa bada, aipatu; orokorra bada, ez}.

Hartutako neurriak:
- Arazoaren kausa identifikatu eta konpondu dugu
- Zure datuak eta eskariak seguru daude
- {beste neurri espezifikoak}

Galderarik baldin baduzu: {kontaktu}

Barkamena eskatzen dugu eragozpenak direla eta.

Harreman komertzialerako,
Zabala Gailetak S.L.
```

6.3.4 Prentsa Oharra (P1 — Publiko Jakintza Bada Soilik)

PRENTSA OHARRA

Zabala Gailetak S.L. — Zibersegurtasun Gertaerari Buruzko Adierazpena

{Herria}, {data}

Zabala Gailetak S.L.-k jakinarazi nahi du {data eta orduan} zibersegurtasun gertaera bat identifikatu zuela bere sistema informatikoekin lotuta.

Gure segurtasun taldeak berehalako neurriak hartu zituen gertaera kontrolpean jartzeko eta gure eragiketak egunerokotasunean jarraitu ahal izateko.

Araketaren arabera, {datu pertsonalak afektatuak/ez} ziren. {Afektatua bada: Pertsona afektatuei zuzenean jakinarazi diegu.}

Zabala Gailetak-ek bere sistema eta datuen segurtasunari garrantzi handia ematen dio eta bere zibersegurtasun neurriak etengabe hobetzen ditu.

Informazio gehiago: komunikazioa@zabala-gailetak.eus

6.4 Komunikazio Kudeaketa Taldea (CMT) — Bilera Gidoia

```
CMT BILERA GIDOIA — P1/P2 Intzidentziak

PARTAIDEAK: CEO, IT Zuzendaria, DPO, CSIRT Buru, Ekoizpen Burua
MAIZTASUNA: Lehen 4 ordutan: orduero | Ondoren: 4 ordutik behin

AGENDA (30 minutu max):
═══════════════════════

1. [5 min] Egungo egoera txostena (CSIRT Buru)
   - Zer gertatu zen?
   - Zer sistema afektatuak?
   - Egungo egoera (edukitzea/ezabatzea/berreskurapena)?

2. [5 min] Eragina ebaluazioa
   - Datu pertsonalen eragina (DPO)
   - Ekoizpen eragina (Ekoizpen Burua)
   - Bezero eragina (CEO)

3. [10 min] Komunikazio erabakiak
   - AEPD jakinarazpena beharrezkoa? (DPO)
   - INCIBE-CERT jakinarazpena? (CSIRT Buru)
   - Bezero komunikazioa? (CEO)
   - Barneko jakinarazpena? (IT Zuzendaria)

4. [5 min] Berreskuratze lehentasunak
   - Hurrengo 2 orduko helburuak
   - Baliabide beharrak

5. [5 min] Hurrengo bilera antolatu
═══════════════════════

ERABAKIAK DOKUMENTATU ServiceNow-en
```

6.5 Komunikazio KPIak

KPI	Helburua	Neurria	Maiztasuna
Alerta-CSIRT denbora	< 15 min (P1)	Wazuh alerta → Slack alerta	Intzidentzia bakoitzean
AEPD jakinarazpen denbora	< 72 ordu	Detekzioa → Inprimakia bidali	Intzidentzia bakoitzean
INCIBE jakinarazpen denbora	< 24 ordu	Detekzioa → Jakinarazpena	Intzidentzia bakoitzean
Bezero komunikazio denbora	< 4 ordu (P1)	Intzidentzia → Email	Intzidentzia bakoitzean
Falso positibo tasa	< 10%	FP/(FP+TP)	Hilabetekoa

7. OT Intzidentzia Simulazioa

7.1 Simulazioaren Deskribapena

Data: 2025ko martxoa **Mota:** Red Team / Blue Team tabletop + teknikoa **Iraupena:** 4 ordu **Eszenarioa:** Dual-homed PC bidezko OT sarea arriskuan jartzea

7.2 Ingurunea eta Arkitektura

```
Simulazioaren ingurunea:

  [IT SAREA]          [DUAL-HOMED PC]         [OT SAREA]
  10.0.20.0/24  ──►  eth0: 10.0.20.99    eth1: 172.16.1.99  ──►  [OpenPLC]
                ◄──  Aurkitua             Exploitatu            172.16.1.1(
                     RULE-005              ◄──                   Modbus 502

  Bide:
  1. Red Team → IT sare eskaneo
  2. Dual-homed PC aurkitu (2 NIC-ekin)
  3. Pivot OT sareetara
  4. Modbus TCP → PLC erregistro aldaketa
  5. Tenperatura setpoint manipulatu (70°C → 110°C)
```

7.3 Erasoaren Kronologia

Ordua	Ekintza	Teknika (MITRE)	Blue Team Detekzioa
T+00:00	Nmap eskaneo IT sarearen	T1046	RULE-001 (ez, azpi-ataria)
T+05:23	Dual-homed PC identifikatu (10.0.20.99)	T1018	Ez detektatu
T+12:41	SSH brute-force PC-ra (admin/admin123)	T1110	RULE-002 alerta P2
T+15:18	OT sareko sarbidea pivot bidez	T1021	RULE-005 alerta P1 🔴

Ordua	Ekintza	Teknika (MITRE)	Blue Team Detekzioa
T+16:02	Modbus TCP irakurketa (portu 502, erregistroak)	T0861	RULE-004 alerta P1
T+18:45	Modbus TCP idazketa — setpoint aldatu	T0855	RULE-004 alerta P1 🔴
T+19:30	Blue Team detekzioa — CSIRT aktibatu	—	Detekzio berria
T+22:15	IT-OT firewall arau aktibatu (isolamendu)	—	Edukitzea
T+28:33	PLC local modura aldatu	—	OT bakartua
T+34:51	Setpoint berrezkuratu (70°C)	—	Ekoizpen normalizatu

Erantzun denbora totala: 15 minutu 21 segundu (RULE-005 alerta → edukitzea osatua)

7.4 Exploit Xehetasunak (Dokumentazio Helburuetarako)

```
#!/usr/bin/env python3
# OHARRA: Honek soilik dokumentazio helburuetarako da.
# Simulazioa baimentzaileko ingurunean egin zen (IsardVDI,
# ekoizpenetik isolatuta).

# Simulatutako Modbus TCP irakurketa (diagnostikoa)
# IEC 61131-3 / OpenPLC — Coil/Register irakurtzea

from pymodbus.client.sync import ModbusTcpClient

# Konexioa (simulazio ingurunea soilik — 172.16.1.10)
client = ModbusTcpClient('172.16.1.10', port=502)
client.connect()

# Tenperatura setpoint irakurri (Holding Register 0)
result = client.read_holding_registers(address=0, count=1, unit=1)
print(f"Egungo setpoint: {result.registers[0] / 10.0}°C")
# Emaitza: Egungo setpoint: 70.0°C

# ⚠️ SIMULAZIOA: Setpoint idazketa (manipulazioa erakusteko)
# EKOIZPEN SISTEMAN SEKULA EZ EGIN
client.write_register(address=0, value=1100, unit=1)  # 110.0°C
print("⚠️ SIMULAZIO: Setpoint aldatu → 110.0°C")

client.close()
```

7.5 Blue Team Erantzuna

7.5.1 Detekzio Fasea (T+15:18 – T+19:30)

```
# Wazuh alerta jaso (RULE-005): Baimenik gabeko OT konexioa
# Log: 172.16.1.99 → 172.16.1.10:502 (Modbus TCP)

# Analista: ELK Stack Kibana dashboard
# Query: source_ip: "172.16.1.99" AND destination_port: 502
# Emaitza: 23 konexio azken 5 minututan (ohikoa: 0)

# IP jatorria ikertzen:
ip route get 172.16.1.99
# → 10.0.20.99 (IT saretik biratzen ari da)

# Dual-homed PC konfirmatu:
nmap -sn 10.0.20.99
# Emaitza: 2 NIC interfaze (eth0: 10.0.20.99, eth1: 172.16.1.99)
```

7.5.2 Edukitzea (T+19:30 – T+22:15)

```
# Firewall araua BEREHALAKOA — ZG-Gateway
iptables -I FORWARD -s 10.0.20.99 -d 172.16.0.0/16 -j DROP -m comment \
  --comment "OT_INCIDENT_INC-2025-031"
iptables -I FORWARD -s 172.16.0.0/16 -d 10.0.20.0/24 -j DROP -m comment \
  --comment "OT_INCIDENT_INC-2025-031"

# Egiaztatu
iptables -L FORWARD | grep OT_INCIDENT

# PC dual-homed konexioa eten
ssh admin@10.0.20.99
shutdown -h now  # larrialdian; normalean izolatu VLAN bidez
```

7.5.3 Berreskurapena (T+22:15 – T+34:51)

```
# PLC setpoint berrezkuratu modu lokalean
# OpenPLC interfazean:
# 1. Runtime gelditu
# 2. Holding Register 0 → 700 (70.0°C)
# 3. Runtime berrabiarazi
# 4. Kalibrazioa egiaztatu sentsoreetan

# Egiaztapena (monitorizazio terminaltik)
python3 -c "
from pymodbus.client.sync import ModbusTcpClient
c = ModbusTcpClient('172.16.1.10', port=502)
c.connect()
r = c.read_holding_registers(0, 1, unit=1)
print(f'Setpoint: {r.registers[0]/10}°C')
c.close()
"
# Emaitza: Setpoint: 70.0°C ✓
```

7.6 Aurkikuntzak eta Hobekuntzak

#	Aurkikuntza	Larritasuna	Egoera
OT-F01	Dual-homed PC-ak IT-OT segmentazio politika hausten du	KRITIKOA	**Konponduta**
OT-F02	Modbus TCP baimenik gabe idazketa posible zen	KRITIKOA	**Konponduta**
OT-F03	OpenPLC administrazioa pasahitz ahularekin babestua	ALTUA	**Konponduta**
OT-F04	RULE-001 ataria baxuegi (eskaneo detektatu gabe)	ERTAINA	**Konponduta**
OT-F05	OT sare isolamendu gida eskuz baino ez	BAXUA	**Konponduta**

Hobekuntza neurriak:

```
OT-F01 → Dual-homed PC kendu; IT-OT juntura unidireccional diodo bidez
OT-F02 → Modbus TCP → Modbus TLS (OpenPLC v3.1+) edo VPN tunnel
OT-F03 → Pasahitz politika OT-ra hedatu (min 16 karaktere, MFA)
OT-F04 → RULE-001 ataria: >20 port/min (ez 100)
OT-F05 → PB-009 playbook automatizatu (SOAR)
```

8. Negozio Jarraitutasun Plana (BCP)

8.1 BCP Laburpen Exekutiboa

Parametro	Balioa	Deskribapena
RTO	4 ordu	Zerbitzu itzultzeko gehieneko denbora
RPO	1 ordu	Datu galera onartua (azken backup-etik)
MTPD	24 ordu	Eragiketa eten gehieneko iraupena
Backup Araua	3-2-1	3 kopia, 2 euskarri, 1 kanpoan
RTO Faseak	4 fase	Lehentasuna, IT, OT, Ekoizpen

8.2 Business Impact Analysis (BIA)

Funtzio Kritikoa	RTO	RPO	Eten Kostua/Ordu	Prioritatea
Ekoizpen linea (PLC/SCADA)	2 ordu	30 min	~15.000€	P1
HR Ataria (langile datuak)	4 ordu	1 ordu	500€	P2
Logistika/Stock sistema	4 ordu	1 ordu	2.000€	P2
Android bezero aplikazioa	8 ordu	4 ordu	300€	P3
Email/Komunikazioa	8 ordu	4 ordu	200€	P3
Web erakusleiho	24 ordu	24 ordu	100€	P4

8.3 Segurtasun Kopien Estrategia (3-2-1 Araua)

```
3-2-1 BACKUP ARAUA — ZABALA GAILETAK

KOPIA 1 (Live): Ekoizpen sistema (ZG-Data, ZG-App)
KOPIA 2 (Local): NAS aparatua (bulegoko sare isolatua)
KOPIA 3 (Kanpo): Hodeiko backup (Hetzner S3 / Backblaze B2)

MAIZTASUNA:
┌──────────────────────────────────────────────────────┐
│  Datu-basea:          Orduro (incremental)           │
│                        Egunero (full) — 02:00 CET    │
│  Fitxategi sistema:   Egunero (differential)         │
│  Konfigurazio:        Aldaketa bakoitzean (git + backup) │
│  OT konfig (PLC):     Astero (manual export)         │
│  Docker irudiak:      Astero (GHCR/Docker Hub)       │
└──────────────────────────────────────────────────────┘

ENKRIPTATZEA:
  - AES-256-GCM enkriptatzea backup guztietan
  - GPG giltza: /etc/backup/master.gpg (HSM-an gordea)
  - Backup fitxategi giltza: /etc/backup/key.gpg (bananduta)

EGIAZTAPENA:
  - Astero: Backup osotasun egiaztapena (SHA-256)
  - Hilabetero: Berreskuratze testa (sandbox ingurunean)
  - Urtero: DR simulazio osoa
```

8.4 IT Berreskuratze Prozedura — Lehentasun Ordena

```
FASE 0 — LARRIALDI HASIERA (0 - 30 min)
═══════════════════════════════════════
☐ CMT aktibatu (CEO, IT Zuzendaria, CSIRT Buru)
☐ BCP aktibazio erabakia (CEO + IT Zuzendaria)
☐ Aseguratzaileari jakinarazpena (tel: {aseguratze tel})
☐ Out-of-band komunikazioa aktibatu (Signal)

FASE 1 — AZPIEGITURA KRITIKOA (30 min - 2 ordu)
═══════════════════════════════════════════════
Sistema lehentasuna:
  1. ZG-Gateway (sarea + firewall — IsardVDI berrabiarazi)
  2. ZG-Data (PostgreSQL + Redis — datu-base zerbitzaria)
  3. ZG-SecOps (ELK + Wazuh — monitorizazioa)

VM berreskuratze aginduak (Proxmox/IsardVDI):
  proxmox-vm start ZG-Gateway
  proxmox-vm start ZG-Data
  proxmox-vm start ZG-SecOps

  # Backup-etik berreskuratu (beharrezkoa bada)
  proxmox-backup restore ZG-Data "pre-incident-snapshot"

FASE 2 — APLIKAZIOAK (2 - 3 ordu)
═════════════════════════════════
  4. ZG-App (HR Ataria — PHP + Nginx + Docker)
  5. ZG-Client (React Frontend)

  # Docker zerbitzu berrabiarazi
  ssh admin@10.0.10.10
  docker-compose -f /opt/zabala/docker-compose.hrportal.yml up -d
  docker-compose ps

  # Datu-base berreskuratu backup-etik (beharrezkoa bada)
  gpg --decrypt /backup/latest/hr_database.sql.gpg | \
    psql -U hrportal -d hr_production

FASE 3 — OT SISTEMA (paralelo bada)
═══════════════════════════════════
```

```
  6. ZG-OT (ScadaBR + OpenPLC)

  # OT berreskuratze protokola (ikus 8.5)

FASE 4 — EGIAZTAPEN ETA MONITORIZAZIOA (3 – 4 ordu)
═══════════════════════════════════════════════════

☐ Zerbitzu guztiak osasuntsu
☐ Datu osotasuna egiaztatu
☐ ELK alertak berrezarri (15 arauak aktibo)
☐ Erantzun 24h monitorizazio areagotua aktibatu
☐ Lagundutako berpizte dokumentatu (INC ticket eguneratu)
```

8.5 OT Berreskuratze Prozedura

```
OT BERRESKURATZE PROTOKOLA
═══════════════════════════════════════════════════════

AUKERA A: Software berreskurapena (konfigurazioa soilik)
─────────────────────────────────────────────────────
1. OpenPLC programa backup-etik berrezarri
   cp /backup/ot/plc_program_latest.st /opt/openplc/program.st
   openplc_service restart

2. ScadaBR proiektua inportatu
   # ScadaBR web UI: http://172.16.1.20:8080
   # → Import → JSON proiektua kargatu

3. Kalibrazioa egiaztatu
   - Tenperatura sentsoreak: ±1°C tolerantzia
   - Presioa sentsoreak: ±0.5 bar tolerantzia

4. Ekoizpen linea gradualkiago berrabiarazi
   - Labean lehenik tenperatura egiaztatu
   - Ekoizpen supervisoraren onespena eskatu

AUKERA B: Hardware ordezkatzea (PLC fisikoa hondatu)
─────────────────────────────────────────────────────
RTO aukera honekin: 6-8 ordu (hardware erabilgarritasun arabera)

1. Ordezko PLC eskuratu (stock: 1 unitate gordeta)
   Kokapena: Biltegia, A4 kabinetea

2. OpenPLC instalatu hardware berrian
   # Raspbian OS + OpenPLC erabiliz
   wget -O install.sh https://github.com/thiagoralves/OpenPLC_v3/raw/master/
   chmod +x install.sh && ./install.sh rpi

3. Programa eta konfigurazioa berrezarri (Aukera A bezala)

AUKERA C: Manual operazio modua (larrialdi ekoizpena)
─────────────────────────────────────────────────────
RTO: Berehalakoa (produkzio ahalmen murriztua — %40)
```

```
1. PLC-a bypass egin — operadore manuala pantailan
2. Tenperatura kontrola: operadore fisikoa, termometro digitala
3. Ekoizpen abiadura murriztu %60-ra (manual jarraipen posible)
4. Lan berria: Manual kontrol fitxa betetzea (30 minutu/ekoizpen)
5. IT sistema berreskuratu bitartean jarraitu

EKOIZPEN BERRESKURATZE FASEAK:
  0 – 2h: Manual operazio modua (%40 ahalmen)
  2 – 4h: Ekoizpen linea 1 berrabiarazi (laborategia + labean)
  4 – 6h: Ekoizpen linea 2 berrabiarazi (txokolatekia)
  6h+: Ekoizpen normal (%100)
```

8.6 Hodeiko Failover (Contingentzia)

```
# Hodeiko failover aktibatu — IT guztiz galdua bada
# Hetzner Cloud zerbitzaria (pre-konfigurazioa)

# 1. Hetzner zerbitzaria aktibatu (Terraform)
cd /backup/terraform/hetzner-failover/
terraform init
terraform apply -var="incident_id=INC-2025-XXX" -auto-approve

# 2. DNS eguneratu (Cloudflare API)
curl -X PATCH \
  "https://api.cloudflare.com/client/v4/zones/{ZONE_ID}/dns_records/{RECORD_I
  -H "Authorization: Bearer ${CF_API_TOKEN}" \
  -H "Content-Type: application/json" \
  --data '{
    "type": "A",
    "name": "hr.zabala-gailetak.eus",
    "content": "HETZNER_FAILOVER_IP",
    "ttl": 60
  }'

# 3. Backup deszifraketa eta zabaltzea hodeian
gpg --decrypt /backup/latest/hr_database.sql.gpg | \
  ssh admin@hetzner-failover "psql -U hrportal -d hr_production"

gpg --decrypt /backup/latest/webapp_files.tar.gz.gpg | \
  ssh admin@hetzner-failover "tar -xzf - -C /var/www/html/"

# 4. Osasun egiaztapena
curl -f https://hr.zabala-gailetak.eus/health
echo "Failover egoera: $?"
```

8.7 BCP Testa eta Drilla Egutegia

Testa Mota	Maiztasuna	Azken Data	Hurrengo Data	Arduradunak
Backup osotasun egiaztapena	Astero	2025-03-01	2025-03-08	SecOps teknikaria
Berreskuratze testa (sandbox)	Hilabetero	2025-03-15	2025-04-15	IT taldea
Tabletop simulazioa	6 hilabetero	2025-01-20	2025-07-20	CSIRT + CMT
DR drilla (ekoizpena eten)	Urtero	2024-11-15	2025-11-15	CSIRT + Ekoizpen
OT failover testa	Urtero	2025-02-01	2026-02-01	OT espezialista

9. Post-Intzidentzia Berrikuspena eta PDCA

9.1 PIR (Post-Incident Review) Prozesua

Post-Intzidentzia Berrikuspena intzidentziaren amaieratik **5 lan-egun** barruan egin behar da. Helburua "blame-free" kultura bati jarraituz hobekuntzak identifikatzea da.

9.1.1 PIR Txosten Egitura

POST-INTZIDENTZIA BERRIKUSPENA (PIR) — INC-{URTEA}-{ZZZ}

Data: {PIR bilera data}

Partaideak: {CSIRT taldea + eragin izandako sailak}

Moderatzailea: CSIRT Buru

1. INTZIDENTZIAREN LABURPENA

   Zer gertatu zen?: {kronologia laburtuta}

   Iraupena: {denbora}

   Eragina: {afektaturiko sistemak, erabiltzaileak, ekoizpena}

   CVSS puntuazioa: {XX.X}

2. KRONOLOGIA ZEHATZA (denbora-lerroa)

   {data/ordua} → {ekintza}

   {data/ordua} → {ekintza}

   ...

3. KAUSA ANALISIA — 5 ZERGATIAK

   Gertaera: {izena}

   Zergatia 1: {azpiko kausa 1}

   Zergatia 2: {azpiko kausa 2}

   ...

   Erro-kausa: {funtsezko kausa}

4. ZER FUNTZIONATU ZUEN ONDO?

   ✓ {detekzio tresnak erantzun dute ondo}

   ✓ {komunikazioak argi egon dira}

   ✓ {BCP prozedura eraginkorra}

5. ZER HOBETU DAITEKE?

   × {atal hobegarria 1}

   × {atal hobegarria 2}

6. EKINTZA PLANA

```
   ──────────────
   | Ekintza | Arduraduна | Epea | Egoera |
   |---------|-----------|------|--------|
   | {ekintza} | {pertsona} | {data} | Irekia |

7. METRIKAK
   ─────────
   MTTD (Detekzio denbora): {X minutu}
   MTTC (Edukitzea denbora): {X minutu}
   MTTR (Berreskuratze denbora): {X minutu}
   SLA betetze: {Bai/Ez}
═══════════════════════════════════════════════════════════
```

9.2 KPI Metrikak — Intzidentzia Kudeaketa

Metrika	Akronimoa	Definizioa	Helburua
Mean Time to Detect	MTTD	Intzidentziatik detekziora	< 15 min (P1)
Mean Time to Contain	MTTC	Detekziotik edukitzera	< 2 ordu (P1)
Mean Time to Recover	MTTR	Detekziotik berreskuratzera	< RTO (4h)
Mean Time Between Incidents	MTBI	Intzidentzien arteko bataz besteko	> 90 egun
False Positive Rate	FPR	FP/(FP+TP)	< 10%
PIR Completion Rate	—	PIR osatu 5 egunetan	100%
Playbook Coverage	—	Detektatutako moten % playbook-ekin	> 90%

9.3 PDCA Hobekuntza Zikloa

```
PDCA — INTZIDENTZIA KUDEAKETA ETENGABEKO HOBEKUNTZA

PLAN (Plangintza):
  → PIR ekintza plana osatu
  → Segurtasun neurri berriak diseinatu
  → Playbook-ak eguneratu (detekzio hutsuneak bada)
  → Prestakuntza beharrak identifikatu

DO (Egitea):
  → Ekintza plana inplementatu (arduradunak + epeak)
  → Playbook-ak eguneratu eta probatu
  → Prestakuntza saioak antolatu
  → Tresna berriak konfiguratu

CHECK (Egiaztapena):
  → KPI metrikak neurtu (hilabetero)
  → Tabletop simulazio eguneratu eszenarioekin
  → Alerta arauak berrikusi (FPR helburua bete?)
  → Backup testak egiaztatu

ACT (Jardutea):
  → SGSI politikak eguneratu (ISO 27001 A.16)
  → CSIRT prozedurak berrikusi
  → Gobernu txostena (CEO + DPO)
  → Auditoretzarako dokumentatu


    ┌──────────────────────────────────────────┐
    │                                          │
    ▼                                          │
  PLAN → DO → CHECK → ACT ─────────────────────┘
   (etengabeko hobekuntza zikloa)
```

9.4 Intzidentzia Erregistro Joera Analisia

```
# Elasticsearch bilaketa — intzidentzia joera analisia
# ELK Kibana Dashboard: "CSIRT Metrics"

# Hilabeteko intzidentzia laburpena
curl -X GET "http://192.168.200.20:9200/incidents-*/_search" \
  -H "Content-Type: application/json" \
  -d '{
    "size": 0,
    "aggs": {
      "by_month": {
        "date_histogram": {
          "field": "created_date",
          "calendar_interval": "month"
        },
        "aggs": {
          "by_severity": {
            "terms": {"field": "severity.keyword"},
            "aggs": {
              "avg_mttr": {
                "avg": {"field": "mttr_minutes"}
              }
            }
          }
        }
      }
    }
  }'

# KPI txostena sortu (hilabetero)
python3 /opt/csirt/scripts/generate_kpi_report.py \
  --month 2025-03 \
  --output /reports/kpi_2025_03.pdf
```

10. Intzidentzia Erregistro Txantiloiak

10.1 Intzidentzia Erregistro Formularioa

```
═══════════════════════════════════════════════════════════════

INTZIDENTZIA ERREGISTROA — ZABALA GAILETAK S.L.

═══════════════════════════════════════════════════════════════

[IDENTIFIKAZIOA]
Intzidentzia ID:        INC-{URTEA}-{ZENBAKIA (3 digitio)}
Data / Ordua (Hasiera): ___/___/______  ___:___ (CET)
Data / Ordua (Amaiera): ___/___/______  ___:___ (CET)
Iraupena (minutu):      _______
Ticket ID (ServiceNow): INC{zenbakia}

[DETEKZIOA]
Detekzio Iturria:
  □ Wazuh/ELK alerta (Arau ID: _______)
  □ Erabiltzaile jakinarazpena (Izena: _____________)
  □ Sare monitorizazioa
  □ Honeypot (T-Pot/Cowrie)
  □ Kanpoko jakinarazpena (INCIBE/bezero)
  □ Beste: _____________________________

Detekzio Ordua:         ___:___ (CET)
Alerta → Triaje Denbora: _______ minutu

[SAILKAPENA]
Kategoria:
  □ CAT-01 Malware/Ransomware   □ CAT-06 OT/ICS
  □ CAT-02 Datu Filtrazioa      □ CAT-07 Insider Mehatxua
  □ CAT-03 Intrusioa            □ CAT-08 Supply Chain
  □ CAT-04 DDoS/Eragingabetasun □ CAT-09 Web Erasoa
  □ CAT-05 Credential Lapurreta □ CAT-10 Fisikoa

Larritasuna:  □ P1 KRITIKOA  □ P2 ALTUA  □ P3 ERTAINA  □ P4 BAXUA
CVSS Puntuazioa: _______ (kalkulatu: cvss.js.org)
MITRE Teknika:  T___________ / T___________
```

[ERAGINA]
Afektaturiko Sistemak:
  □ ZG-Gateway   □ ZG-App   □ ZG-Data
  □ ZG-SecOps   □ ZG-OT   □ ZG-Client
  □ Kanpoko zerbitzua (zehaztu): _____

Afektaturiko Erabiltzaile Kopurua: _____
Datu Pertsonalak Arriskuan: □ BAI (kopurua: _____) □ EZ
Ekoizpen Eragina: □ BAI (%_____ galera) □ EZ
Finantza Kalte Estimatua: €_____

[ARDURADUNAK]
L1 Analista: _____ | Eginkizuna: _____:___ (CET)
L2 CSIRT Analistal: _____ | Eginkizuna: _____:___ (CET)
L3 CSIRT Buru: _____ | Eginkizuna: _____:___ (CET)
DPO/Legea: _____ | Eginkizuna: _____:___ (CET)
OT Espezialista: _____ | Eginkizuna: _____:___ (CET)

[PLAYBOOK ERABILIA]
□ PB-001 □ PB-002 □ PB-003 □ PB-004 □ PB-005
□ PB-006 □ PB-007 □ PB-008 □ PB-009 □ PB-010
□ PB-011 □ PB-012 □ PB-013 □ PB-014 □ PB-015
□ Beste (deskribatu): _____

[ERANTZUN FASEAK]
Edukitzea Ordua: ___:___ (CET) MTTC: _____ min
Ezabatzea Ordua: ___:___ (CET)
Berreskuratze Ordua: ___:___ (CET) MTTR: _____ min
SLA Betetzea: □ BAI □ EZ (arrazoiak: _____)

[KOMUNIKAZIOAK]
Barne Komunikazioa:
  □ L1→L2 eskalazio (ordua: ___:___)
  □ L2→L3 eskalazio (ordua: ___:___)
  □ CEO/Exekutiboa jakinarazpena (ordua: ___:___)
  □ Langile komunikazio orokorra (ordua: ___:___)
Kanpo Komunikazioa:
  □ AEPD (GDPR 33) — bidali: ___/___/_____ ___:___ (epea: +72h)
  □ INCIBE-CERT (NIS2) — bidali: ___/___/_____ ___:___ (epea: +24h)

```
  □ Aseguratzailea — bidali: ___/___/______ ___:___
  □ Bezeroak — bidali: ___/___/______ ___:___
  □ Prentsa oharra — bidali: ___/___/______ ___:___

[EBIDENTZIAK]
Ebidentzia fitxategiak: /mnt/forensics/INC-{URTEA}-{ZZZ}/
SHA-256 Zigilua: _________________________________________________
Ebidentzia Kateko Arduraduna: _____________________________

[BERRESKURAPENA]
Backup-etik berreskuratu: □ BAI  □ EZ
Backup data erabilia: ___/___/______ ___:___
BCP aktibatu: □ BAI  □ EZ

[POST-INTZIDENTZIA]
PIR Bilera Data:  ___/___/______
PIR Txostena:     /docs/pir/INC-{URTEA}-{ZZZ}_PIR.md
Ekintza Plana:    □ Osatua  □ Zain
SGSI Eguneratzea: □ Beharrezkoa  □ Ez

[ITXIERA]
Itxiera Data:     ___/___/______ ___:___ (CET)
Itxi arduradunа:  _____________________________
Itxiera Arrazoia: □ Konpondu  □ Baliogabetu (FP)  □ Beste: _____

═══════════════════════════════════════════════════════════════════
```

10.2 Intzidentzia Txosten Laburtua (Exekutiboa)

```
═══════════════════════════════════════════════════
INTZIDENTZIA LABURPEN EXEKUTIBOA — INC-{URTEA}-{ZZZ}
═══════════════════════════════════════════════════

Data:          {data}
Larritasuna:   P{1-4} — {KRITIKOA/ALTUA/ERTAINA/BAXUA}
MTTR:          {X} ordu {X} minutu

LABURPENA:
{3-5 esaldi teknikarik gabe}

ERAGINA:
• Sistema afektatuak: {zerrenda}
• Langile afektatuak: ~{kopurua}
• Datu pertsonalak: {BAI/EZ}
• Ekoizpen etetea: {denbora edo EZ}
• Kalte ekonomiko estimatua: €{zenbakia}

KAUSA NAGUSIA:
{1-2 esaldi}

HARTUTAKO NEURRIAK:
1. {neurria 1}
2. {neurria 2}
3. {neurria 3}

PREBENTZIO NEURRIAK ETORKIZUNERAKO:
1. {neurria 1}
2. {neurria 2}

BETEBEHAR JURIDIKOAK:
□ AEPD jakinarazpena: {BIDALI/BEHAR EZ}
□ INCIBE-CERT: {BIDALI/BEHAR EZ}
═══════════════════════════════════════════════════
```

10.3 Intzidentzia Erregistro Adibidea — INC-2025-031

```
═══════════════════════════════════════════════════════
INTZIDENTZIA ERREGISTROA — ADIBIDEA (OT Simulazioa)
═══════════════════════════════════════════════════════

Intzidentzia ID:  INC-2025-031
Data/Ordua:       2025-03-15  14:32 CET
Iraupena:         35 minutu
Kategoria:        CAT-06 — OT/ICS Erasoa
Larritasuna:      P1 — KRITIKOA
CVSS:             9.1 (AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)
MITRE:            T0855 (Unauthorized Command), T0828 (IO Manipulate)

DESKRIBAPENA:
Red Team-ek dual-homed PC (10.0.20.99/172.16.1.99) bidez OT
sarean sartu eta Modbus TCP bidez OpenPLC-ko tenperatura
setpoint 70°C-tik 110°C-ra aldatu zuen. Wazuh RULE-005 alertak
15 minututan detektatu zuen.

AFEKTATURIKO SISTEMAK:
- ZG-OT (172.16.1.10 — OpenPLC)
- Dual-homed PC (10.0.20.99)

ERANTZUN DENBORA:
MTTD: 15 minutu 18 segundo
MTTC: 22 minutu 15 segundo
MTTR: 34 minutu 51 segundo

KOMUNIKAZIOAK:
☑ L1→L2 eskalazio: 14:47 CET
☑ L2→L3 eskalazio: 14:48 CET
☑ Ekoizpen supervisora jakinarazpena: 14:50 CET
☐ AEPD — Ez beharrezkoa (datu pertsonalik ez)
☐ INCIBE — Ez beharrezkoa (simulazioa)

KONPONBIDEA:
1. Dual-homed PC kendu (IT-OT segmentazioa berreskuratu)
2. Modbus TCP → Modbus TLS ezarri
3. RULE-001 ataria doitu
```

```
4. PB-009 playbook eguneratu


PIR Data: 2025-03-20
═══════════════════════════════════════════════════════════
```

Laburpena eta Ondorioak

Moduluaren Emaitzen Laburpena

Atala	Helburua	Egoera
CSIRT Taldea	5 kideko taldea, erantzukizunak definituta	✅ Osatua
Intzidentzia Sailkapena	10 kategoria, P1-P4 larritasun mailak	✅ Osatua
NIST 6 Faseak	Fase guztiak dokumentatuta + aginduak	✅ Osatua
SOAR Playbook-ak	15 playbook, 2 xeheki dokumentatuta	✅ Osatua
Komunikazio Plana	Barne/kanpo template guztiak	✅ Osatua
OT Simulazioa	15 min detekzioa, 35 min berreskurapena	✅ Osatua
BCP (RTO=4h, RPO=1h)	3-2-1 backup, 4 fase, hodeiko failover	✅ Osatua
Post-Intzidentzia (PDCA)	PIR txostena, KPI metrikak, PDCA zikloa	✅ Osatua
Erregistro Txantiloiak	Erregistro osoa + exekutibo laburpena	✅ Osatua

KPI Emaitzak (OT Simulazioa)

KPI	Helburua	Lortutakoa	Egoera
MTTD (P1)	< 15 min	15 min 18 seg	⚠️ la bete
MTTC (P1)	< 2 ordu	22 min 15 seg	✅ Gainditu
MTTR (P1)	< 4 ordu (RTO)	34 min 51 seg	✅ Gainditu
Backup Test	Hilabetero	Egina	✅
Playbook Coverage	> 90%	15/15 (100%)	✅

Hobekuntzarako Proposamenak

1. **MTTD < 15 min lortzeko:** RULE-001 ataria doitu (100 → 20 port/min) eta ML-oinarritutako anomalia detekzioa hedatu (ELK ML modulua)

2. **OT segurtasuna:** Modbus TLS inplementatu (OpenPLC v3.1+) eta unidireccional IT-OT diodo instalatu
3. **SOAR automatizazioa:** n8n/Shuffle plataformarekin hedatu playbook automatizazioa (oraindik PB batzuk eskuzkoak)
4. **Prestakuntza:** CSIRT taldeko kide guztiei SANS FOR508/SEC504 ziurtagiria lortzeko aukera eskaintzea
5. **Tabletop maiztasuna:** 6 hilabetetik 3 hilabeteko maiztasunera pasatu (NIS2 gomendioa)

Dokumentua: MODULUA_04_ZIBERSEGURTASUN_GORABEHERAK.md **Bertsioa:** 1.0 **Egoera:** Osatua ✅ **Azken Eguneraketa:** 2025 **Arauak:** NIST SP 800-61r2 | ISO/IEC 27035 | GDPR Art. 33/34 | NIS2 | IEC 62443-2-4 | ISO 22301