ZABALA GAILETAK

S.L. - Dokumentazio Akademikoa

Sareak eta Sistemak Gotortzea

2026(e)ko otsailaren 23(a)

MODULUA 1: SAREAK ETA SISTEMAK GOTORTZEA

Zabala Gailetak — Zibersegurtasun Proiektua ER4

Erakundea: Zabala Gailetak S.L. — Gaileta Ekoizle Industriala **Dokumentu Mota:** Azpiegitura Segurtasun Dokumentazio Integrala **Bertsioa:** 2.0 **Data:** 2026-02-22 **Egilea:** Zibersegurtasun Arkitektura Taldea **Sailkapena:** KONFIDENTZIALA — Barne Erabilpenerako Soilik

AURKIBIDEA

1. SARRERA ETA HELBURUAK

1.1 Moduluaren Xedea

Dokumentu honek **Zabala Gailetak S.L.** enpresaren azpiegitura informatiko eta industrialaren segurtasun gogortze neurri guztiak jasotzen ditu. ER4 proiektuaren esparruan garatutako SOP (Standard Operating Procedure), konfigurazio eta inplementazio guztiak biltzen dira hemen, erreferentzia tekniko nagusi gisa.

Zabala Gailetak gaileta ekoizle industrial bat da, eta bere azpiegiturak bi dimentsio kritiko ditu:

- **IT Azpiegitura:** Web aplikazioa (HR Portala), datu-baseak, zerbitzariak eta erabiltzaile-ekipoak.
- **OT Azpiegitura:** Fabrikako kontrol-sistemak — PLCak, SCADA, HMIak eta robot industrialak — elikagaien ekoizpen prozesuak automatizatzen dituztenak.

Bi azpiegitura hauen segurtasunak elkar eragiten du: OT sarearen urraketak ekoizpen-geldialdia, segurtasun-arriskuak eta ospe-kaltea ekar ditzake; IT sarekoak, berriz, langileen datu pertsonalak eta enpresaren sekretismo industrial guztia arriskuan jar dezake.

1.2 Aplikagarriak diren Arauak eta Estandarrak

Araua/Estandarra	Aplikazio-Eremua
IEC 62443	OT/ICS sistemak segurtatzea, Purdue Eredua
ISO/IEC 27001	SGSI — Informazio Segurtasun Kudeaketa Sistema
NIS2 Zuzentaraua	Azpiegitura kritikoen babes-baldintzak
GDPR	Langileen eta bezeroen datu pertsonalen babesa
OWASP Top 10	Web aplikazioen segurtasun estandarrak
CIS Benchmarks	Zerbitzarien eta sistemen gogortze-gidak

1.3 Indar-Eremua

Dokumentu hau aplikatzen zaie:

- ZG-Gateway (Router/Suebaki nagusia)
- ZG-App (Web zerbitzaria — HR Portala)
- ZG-Data (PostgreSQL datu-base zerbitzaria)
- ZG-SecOps (SIEM / Wazuh zerbitzaria)
- ZG-OT (OpenPLC eta SCADA simulazioa)
- Honeypot azpiegitura (DMZ-an isolatuta)

2. SARE TOPOLOGIA ETA INBENTARIOA

2.1 Sare Segmentazioaren Printzipioak

Zabala Gailetak-eko sare-diseinua **segmentazio zorrotzean** oinarritzen da, "defense in depth" (defentsa sakonak) printzipioari jarraituz. IT eta OT sareen arteko bereizketa fisiko eta logikoa da oinarrizko baldintza, IEC 62443 estandarrak eskatzen duen bezala.

Segmentazio Filosofia

```
INTERNET
    |
[FW-PERIM] ← Perimetro Suebakia (Edge)
    |
   DMZ (192.168.2.0/24)
   ├── SRV-WEB (Web Zerbitzaria Publikoa)
   └── HONEYPOT (Mehatxu-erakarle Sistema)
    |
[FW-INT] ← Barne Suebakia (IT/OT Muga)
    |
   ┌──────────────────────────┐
   |     BARNE SAREA (LAN)    |
   ├── Erabiltzaileak (IT): 10.0.20.0/24
   ├── Zerbitzariak (IT):   10.0.10.0/24
   └── Kudeaketa (MGMT):    192.168.200.0/24
    |
[OT SUEBAKIA] ← Isolamendu Zehatza
    |
   OT SAREA (172.16.0.0/16)
   ├── OT Kudeaketa: 172.16.1.0/24
   └── OT Prozesua:  172.16.2.0/24
```

2.2 Sare Gailuen Inbentarioa

Fitxategia: `infrastructure/network/inventory.txt`

ID	Mota	Kokapena	Funtzioa	IP Helbidea
FW-PERIM	Suebaki Perimetrala	Sarrera (Edge)	Interneteko trafikoa iragazi, VPN, DMZ kudeaketa	192.168.1.1
FW-INT	Barne Suebakia	IT/OT Muga	IT eta OT sareen arteko segmentazio zorrotza	10.0.0.1
SW-CORE	Switch Core	CPD	Sare nagusiaren bizkarrezurra	10.0.1.1
SW-ACC-OFF	Switch Sarbidea	Bulegoak	Administrazio eta Ikerketa ekipoak	10.0.2.1
SW-ACC-PROD	Switch Industriala	Fabrika	OT gailuak — gogortua	172.16.1.1
WIFI-AP	Sarbide Puntuak	Bulegoak/Fabrika	Langileen eta gonbidatuen Wi-Fi (VLAN bereiziak)	—

2.3 IT Zerbitzarien Inbentarioa

Hostname	Sistema Eragilea	Funtzioa	IP Helbidea
SRV-DC01	Windows Server	Domeinu Kontrolatzailea (AD), DNS, DHCP	10.0.10.10
SRV-ERP	Linux/Windows	ERP Sistema eta Datu-basea	10.0.10.20
SRV-WEB	Linux (Debian 12)	Webgune publikoa eta HR Portala (DMZ)	192.168.2.10
SRV-APP	Linux (Debian 12)	Mugikorreko App-aren API zerbitzaria	10.0.10.30

Hostname	Sistema Eragilea	Funtzioa	IP Helbidea
SRV-FILE	Windows/Linux	Fitxategi zerbitzaria (Dokumentazioa, Diseinuak)	10.0.10.40
SRV-SIEM	Linux (Debian 12)	Wazuh/ELK SIEM — Log bilketa	10.0.10.50

2.4 OT Kontrolagailuen Inbentarioa

Gailu ID	Mota	Funtzioa	Sarea
PLC-KNEAD-01/02	OpenPLC (simulatua)	Oratzeko makinen kontrola	172.16.2.x
PLC-OVEN-01	OpenPLC (simulatua)	Labe industrialaren kontrola — kritikoa	172.16.2.x
SCADA-SRV	ScadaBR	Ekoizpen datuen zerbitzaria	172.16.1.10
HMI-01	HMI Panel	Operadore interfazea	172.16.1.20

2.5 IP Planifikazioa

VLAN / Segmentua	Sareko Helbidea	Erabilpena
DMZ	192.168.2.0/24	Web zerbitzariak, Honeypot
Erabiltzaileak (IT)	10.0.20.0/24	Bulegoak, Langileen ekipoak
Zerbitzariak (IT)	10.0.10.0/24	Zerbitzari nagusiak
Kudeaketa (MGMT)	192.168.200.0/24	Administrazio-sarbide esklusiboa
OT Kudeaketa	172.16.1.0/24	SCADA, HMI, Jump Host
OT Prozesua	172.16.2.0/24	PLCak, Sentsoreak, Aktuadoreak
Gonbidatuak	192.168.100.0/24	Isolatuta — Internet soilik

2.6 Sare Topologiaren Deskribapena

Fitxategia: `docs/network_diagrams/network_topology.md`

Enpresak sare segmentatu bat ezarri du segurtasuna bermatzeko. Egitura nagusia:

- **DMZ (Gune Desmilitarizatua):** Kanpotik eskuragarri egon behar diren zerbitzuak hartzen ditu (Web zerbitzaria, Honeypot). Suebaki bidez isolatuta dago barne saretik.
- **Barne Sarea (LAN):** Erabiltzaileen ekipoak eta inprimagailuak. Segmentu honetan ez dago Internet sarbide zuzenekik — proxy-aren bidez kontrolatutako sarbidea baino ez.
- **Sistemen Sarea (Server VLAN):** Datu-baseak, Fitxategi zerbitzariak eta Domeinu Kontrolatzailea. Sarbidea oso murriztuta dago — bakarrik beharrezko portuak irekitzen dira.
- **OT Sarea (Industrial):** PLCak (OpenPLC), HMIak, SCADA sistemak eta Node-RED datuen integrazioa. IT saretik guztiz isolatuta, edo "Data Diode" / Suebaki zorrotz baten bidez banatuta.

---

3. SARE SEGMENTAZIO SOP — NFTABLES SUEBAKIA

Fitxategia: `infrastructure/network/network_segmentation_sop.md` **Bertsioa:** 2.0
Rola: ZG-Gateway (Router/Suebakia)

3.1 Interfazen Konfigurazioa

Konfigurazio honek Gateway-a barne azpisare guztien errota-gailu gisa definitzen du.

Fitxategia: `/etc/network/interfaces`

```
# /etc/network/interfaces
# Zabala Gailetak - Gateway Interfaze Konfigurazioa

source /etc/network/interfaces.d/*

auto lo
iface lo inet loopback

# WAN (Eth0) - Internetera konektatua (Isard Bridge)
allow-hotplug eth0
iface eth0 inet dhcp

# LAN (Eth1) - Barne Sarera konektatua
# Interfaze bakarra, VLAN gateway-ekin
allow-hotplug eth1
iface eth1 inet static
    address 192.168.1.1
    netmask 255.255.0.0
    # Gateway Logikoak
    up ip addr add 192.168.10.1/24 dev eth1   # ERABILTZAILE GATEWAY
    up ip addr add 192.168.20.1/24 dev eth1   # ZERBITZARI GATEWAY
    up ip addr add 192.168.50.1/24 dev eth1   # OT GATEWAY
    up ip addr add 192.168.200.1/24 dev eth1  # KUDEAKETA GATEWAY
```

3.2 NFTables Suebaki Arauak

IEC 62443 eta proiektuaren segurtasun-politikak eskatzen duen isolamendu zorrotza betearazten duen arau-multzoa.

Fitxategia: `/etc/nftables.conf`

```
#!/usr/sbin/nft -f
# Zabala Gailetak - NFTables Suebaki Arauak
# IEC 62443 eta ISO 27001 arabera

flush ruleset

table ip filter {
    chain input {
        type filter hook input priority 0; policy drop;

        # Loopback-a baimendu
        iifname "lo" accept

        # Ezarritako konexioak baimendu
        ct state established,related accept

        # SSH bakarrik Administrazio Sareetik (MGMT)
        ip saddr 192.168.200.0/24 tcp dport 22 accept

        # ICMP (Ping) diagnostikorako baimendu
        ip protocol icmp accept

        # DHCP eskaerak baimendu LAN-ean
        iifname "eth1" udp dport { 67, 68 } accept
    }

    chain forward {
        type filter hook forward priority 0; policy drop;
        ct state established,related accept

        # --- ACL ARAUAK (Sarbide Kontrol Zerrendak) ---

        # 1. ERABILTZAILEAK -> APP (Web Sarbidea soilik)
        # Erabiltzaileei Web Zerbitzarira sarbidea baimendzen zaie
        ip saddr 192.168.10.0/24 ip daddr 192.168.20.10 tcp dport { 80, 443 }

        # 2. APP -> DATA (Datu-base Sarbidea soilik)
        # Web Zerbitzariari Datu-base eta Redis-era sarbidea
        ip saddr 192.168.20.10 ip daddr 192.168.20.20 tcp dport { 5432, 6379
```

```
        # 3. MGMT -> DENA (Administrazio Osoa)
        # Administrariei dena baimendzen zaie
        ip saddr 192.168.200.0/24 accept

        # 4. OT ISOLAMENDUA
        # OT sarea (192.168.50.0/24) dena blokeatuta dago
        # politika DROP da — ez da arau gehigarririk behar.
        # INOIZ EZ da OT sarea IT sareekin zuzenean konektatu behar.

        # 5. INTERNET SARBIDEA (Irteera)
        # Barne sareak Internetera sar daitezke (NAT bidez)
        iifname "eth1" oifname "eth0" accept
    }

    chain output {
        type filter hook output priority 0; policy accept;
    }
}

table ip nat {
    chain postrouting {
        type nat hook postrouting priority 100; policy accept;

        # NAT (Masquerade) Internet Sarbiderako
        oifname "eth0" masquerade
    }
}
```

3.3 Konfigurazioa Aplikatzea

```
# 1. Sareko konfigurazioa berrabiarazi
systemctl restart networking

# 2. Suebaki arauak aplikatu
nft -f /etc/nftables.conf

# 3. NFTables abiaraztean aktibatu
systemctl enable nftables
systemctl start nftables
```

3.4 Egiaztapena eta Berrespen Komandoak

```
# Bideratzeak egiaztatu
ip route

# Arauak egiaztatu
nft list ruleset

# Interfazeak egiaztatu
ip addr show

# Konexioen egoerak ikusi
ss -tuln

# Firewall erregistroak egiaztatu
dmesg | grep nft
journalctl -u nftables
```

3.5 OT Isolamendua — Arau Kritikoak

> ***SEGURTASUN OHARRA KRITIKOA:*** *OT sarearen eta IT sarearen arteko komunikazio zuzena* ***ERABAT DEBEKATUTA*** *dago. Edozein salbuespen dokumentatu eta CAB-ek onartu behar du aldez aurretik.*

Beharrezko komunikazioa (adibidez, eguneraketak edo datuen eskualdaketa) beti:

1. DMZ Industrialaren bidez igaro behar da.
2. "Jump Host" baten bidez egin behar da.
3. MFA eta VPN erabiliz baino ez da baimenduko.

4. OT MAKINERIA INBENTARIOA — ZABALA GAILETAK

Fitxategia: `infrastructure/ot/machinery_inventory.md`

4.1 Ekoizpen Prozesuaren Deskribapena

Zabala Gailetak-eko fabrikako ekoizpen prozesua automatizatuta dago eta hainbat makina mota erabiltzen ditu. Segurtasun ikuspegitik, gailu hauek **OT Sarean** egon behar dute, IT saretik isolatuta.

4.2 Ekoizpen Lerroa — Faseetan

A. Nahasketa eta Prestaketa Fasea

Gailu Mota	Deskribapena	Konektibitatea
Pisatzeko Sistemak	Lehengaiak (irina, koipea, ura) dosifikatzeko sentsoreak eta kontroladoreak	OT Sarea — SCADA monitorizazioa
Oratzeko Makinak (Kneaders)	PLC bidez kontrolatutako motor industrialak	SCADA sistemara konektatuta

B. Formazioa Fasea

Gailu Mota	Deskribapena	Kontrola
Laminazio Makinak	Orea luzatzeko eta ijezteko arrabol motorizatuak	PLC bidez
Ebaketa Makinak	Orea pieza txikietan zatitzeko trokelak	PLC bidez sinkronizatuta

C. Egostea Fasea — KRITIKOA

Gailu Mota	Kritikotasuna	Sentsoreak	Aktuadoreak
Labe Industrialak	**OSO ALTUA**	Tenperatura, hezetasuna, presioa	Erregailuak, aireztapen sistemak

> ***Arriskuen Ohar:*** *Tenperatura oker batek produktua hondatu edo* ***sute arriskua*** *sor dezake. Labe kontroladoreek redundantzia eta alerta-sistema automatiko bikoiztuak behar dituzte.*

D. Akabera Fasea

Gailu Mota	Deskribapena	Kontrola
Bainatzeko Makinak	Txokolatezko estaldura aplikatzeko	Tenperatura eta fluxua
Enbalatzeko Robotak	Amaitutako produktuak kaxetan sartzeko beso robotikoak	PLC/Robot kontroladore

4.3 OT Kontrol Sistema eta Simulazioa

Proiektu honetan ingurune erreala simulatzeko software espezifikoa erabili da:

Tresna	Funtzioa	Protokoloa
Factory I/O	Makina fisikoak simulatzeko ingurunea birtuala	—
OpenPLC	PLCak (Programmable Logic Controllers) simulatzeko	Modbus TCP / IEC 61131-3
HMI (Human Machine Interface)	Operadoreek makinak maneiatzeko panelak	—
ScadaBR	Fabrika osoaren ikuspegi orokorra eta datuen bilketa	Modbus, DNP3
Node-RED	Datuen integrazioa eta fluxuen kudeaketa	MQTT, HTTP

4.4 OpenPLC Programa — Gaileta Ekoizpena (Structured Text)

Fitxategia: `infrastructure/ot/openplc/programs/cookie_production.st`

```
PROGRAM CookieProduction
  VAR
    (* === SARRERAK (Factory IO edo HMI-tik) === *)
    StartButton     AT %IX0.0 : BOOL;   (* Abiarazte-botoia *)
    StopButton      AT %IX0.1 : BOOL;   (* Geldiarazte-botoia *)
    EmergencyStop   AT %IX0.2 : BOOL;   (* Larrialdi Geldialdia *)
    OvenTempSensor  AT %IW0   : INT;    (* 0-1000 = 0-250°C *)
    WeightSensor    AT %IW1   : INT;    (* Orea pisua gramatan *)

    (* === IRTEERAK === *)
    ConveyorMotor   AT %QX0.0 : BOOL;  (* Zinta garraiatzailea *)
    MixerMotor      AT %QX0.1 : BOOL;  (* Nahasgailua *)
    OvenHeater      AT %QX0.2 : BOOL;  (* Labearen berogailua *)
    AlarmLight      AT %QX0.3 : BOOL;  (* Alarma argia *)
    ExtruderValve   AT %QX0.4 : BOOL;  (* Extrusioa balbula *)

    (* === BARNE ALDAGAIAK === *)
    State         : INT := 0;  (* 0:Geldi, 1:Nahaste, 2:Extrusioa, 3:Egostea
    TargetTemp    : INT := 720; (* ~180°C *)
    TimerMixing   : TON;
    TimerBaking   : TON;
  END_VAR

  (* === LARRIALDI LOGIKA === *)
  IF EmergencyStop THEN
    ConveyorMotor  := FALSE;
    MixerMotor     := FALSE;
    OvenHeater     := FALSE;
    ExtruderValve  := FALSE;
    AlarmLight     := TRUE;
    State          := 0;
    RETURN;
  END_IF;

  (* === GELDIARAZTE LOGIKA === *)
  IF StopButton THEN
    State := 0;
  END_IF;
```

```
(* === ABIARAZTE LOGIKA === *)
IF StartButton AND State = 0 THEN
  State      := 1;
  AlarmLight := FALSE;
END_IF;

(* === EGOERA MAKINA (State Machine) === *)
CASE State OF
  0: (* Geldi / Idle *)
    MixerMotor    := FALSE;
    ExtruderValve := FALSE;
    ConveyorMotor := FALSE;
    OvenHeater    := FALSE;

  1: (* Nahasketa / Mixing — 10 segundo *)
    MixerMotor := TRUE;
    TimerMixing(IN := TRUE, PT := T#10s);
    IF TimerMixing.Q THEN
      TimerMixing(IN := FALSE);
      MixerMotor := FALSE;
      State := 2;
    END_IF;

  2: (* Extrusioa — Orea zintan jaistea *)
    ExtruderValve := TRUE;
    IF WeightSensor > 500 THEN  (* Helburuko pisua lortu *)
      ExtruderValve := FALSE;
      State := 3;
    END_IF;

  3: (* Egostea eta Garraioa — 30 segundo *)
    ConveyorMotor := TRUE;
    (* Tenperatura Kontrola *)
    IF OvenTempSensor < TargetTemp THEN
      OvenHeater := TRUE;
    ELSE
      OvenHeater := FALSE;
    END_IF;
    TimerBaking(IN := TRUE, PT := T#30s);
    IF TimerBaking.Q THEN
```

```
        TimerBaking(IN := FALSE);
        State := 0;  (* Zikloa amaituta *)
      END_IF;
  END_CASE;

END_PROGRAM

CONFIGURATION Config0
  RESOURCE Res0 ON PLC
    TASK TaskMain(INTERVAL := T#50ms, PRIORITY := 0);
    PROGRAM Inst0 WITH TaskMain : CookieProduction;
  END_RESOURCE
END_CONFIGURATION
```

4.5 OT Docker Azpiegitura

Fitxategia: `infrastructure/ot/docker-compose.ot.yml`

```yaml
version: '3.8'

services:
  # === OpenPLC — PLC Simuladorea ===
  openplc:
    image: openplcproject/openplc:v3
    container_name: zabala-openplc
    ports:
      - "8080:8080"  # Web interfazea
      - "502:502"    # Modbus TCP protokoloa
    volumes:
      - ./openplc/programs:/programs
      - openplc_data:/persistent
    networks:
      ot_network:
        ipv4_address: 192.168.50.10
    restart: unless-stopped

  # === ScadaBR — SCADA Sistema ===
  scadabr:
    image: scadabr/scadabr:latest
    container_name: zabala-scadabr
    ports:
      - "9090:8080"  # SCADA Web interfazea
    depends_on:
      - openplc
    networks:
      - ot_network
    restart: unless-stopped

networks:
  ot_network:
    driver: bridge
    internal: true          # ← GARRANTZITSUA: Internet sarbiderik EZ
    ipam:
      config:
        - subnet: 192.168.50.0/24
```

```
volumes:
  openplc_data:
```

> ***Segurtasun Oharra:*** `internal: true` *parametroak OT sarea Internetetik guztiz isolatzen du Docker mailan. Hau ezinbestekoa da IEC 62443 betetzeko.*

---

5. OT SEGURTASUN SOP — PURDUE EREDUA

Fitxategia: `infrastructure/ot/sop_ot_security.md`

5.1 Helburua

Fabrikako kontrol sistemen (ICS/SCADA) segurtasuna bermatzea, ekoizpenaren jarraitutasuna eta langileen segurtasun fisikoa babesteko. Zabala Gailetak-en gaileta-ekoizpen lerroak PLCen bidez kontrolatzen dira; hauen huts-egiteak produktu-galera zuzena edo segurtasun-istripu fisikoak eragin ditzake.

5.2 Purdue Ereduaren Arkitektura

IEC 62443 estandarrak Purdue Eredua erabiltzen du ICS sistemak maila funtzionaletan antolatzeko:

Arau Nagusia: Komunikazioa soilik maila ezberdineen artean eta **DMZ industrialaren bidez** egon daiteke. Maila 4 eta Maila 3ren arteko komunikazio zuzena **DEBEKATUTA**

dago.

5.3 Segurtasun Arauak

5.3.1 Sare Segmentazioa

Araua	Deskribapena
IT/OT Bereizketa	IT eta OT sareen arteko komunikazio zuzena **erabat debekatuta**
DMZ Industriala	Komunikazio guztia DMZ industrialaren bidez igaro behar da
Suebaki Mailaketa	Suebakiak maila bakoitzaren artean (North-South trafikoa)
Protokolo Kontrola	Modbus, DNP3, S7Comm bakarrik OT sarean baimenduta

5.3.2 Urruneko Sarbide Politika

```
DEBEKATUTA:
  × TeamViewer, AnyDesk edo antzeko tresna zuzenak PLCetara
  × RDP zuzenean OT gailuetara
  × SSH pasahitz bidez OT sistemetan

BAIMENDUTA:
  ✓ VPN seguru bidez → Jump Host → OT gailu
  ✓ MFA (Multi-Factor Authentication) derrigorrezkoa
  ✓ Saio guztiak erregistratuta (audit trail osoa)
  ✓ Saio denbora-muga: gehienez 4 ordu jarraian
```

5.3.3 Gailu Eramangarrien (USB) Politika

Ekintza	Baimena
USB memoria pertsonalak konektatzea OT ekipoetan	**DEBEKATUTA**
Kiosko estazioetan eskaneatutako USBak konektatzea	Baimenduta (eskaneatuta)

Ekintza	Baimena
CD/DVD bidezko eguneraketak	Baimenduta (sinatutako multimedia soilik)

Prozedura:

1. USB dispositiboa Kiosko Estazioari aurkeztu.
2. Malware eskaneoa automatikoki exekutatu (Antivirus + YARA arauak).
3. Emaitza onartu ezean, USBa suntsitu edo zigilatu.
4. Onartu ezean, intzidentea erregistratu.

5.3.4 Eguneraketa Politika

> ***OHARRA KRITIKOA:*** *OT sistemak **inoiz ez** eguneratu automatikoki. Eguneraketa automatikoak ekoizpena eten dezake eta PLCak ezegonkortu.*

Fasea	Deskribapena
1. Laborategia	Adabakia laborategiko ingurunean probatu (Factory I/O simulazio)
2. Mantentze-leiho	Mantentze-leiho planifikatua adostu ekoizpen-buruarekin
3. Atzera-bueltako plana	Aurreko bertsiorako atzera-bueltako plan dokumentatua sortu
4. Aplikazioa	Adabakia aplikatu eta funtzionaltasuna egiaztatu
5. Dokumentazioa	Aldaketa CMDB-an eta aldaketa-erregistroan dokumentatu

---

6. ZERBITZARIEN GOGORTZE SOP (DEBIAN 12)

Fitxategia: `infrastructure/systems/sop_server_hardening.md` **Helmuga:** Zerbitzari Guztiak (App, Data, SecOps, OT) **Erabiltzailea:** Root

6.1 Oinarrizko Sistema Segurtatzea

Komando hauek instalazio berri bakoitzean berehala exekutatu behar dira.

```
# === 1. Sistema Eguneratu eta Tresnak Instalatu ===
apt update && apt upgrade -y
apt install -y ufw fail2ban curl git htop unattended-upgrades auditd

# === 2. Root Ez Den Erabiltzaile Administratiboa Sortu ===
adduser admin
usermod -aG sudo admin

# === 3. Memoria Partekatua Segurtatu ===
echo "tmpfs /run/shm tmpfs defaults,noexec,nosuid 0 0" >> /etc/fstab
mount -o remount /run/shm

# === 4. Kernel Parametroak Segurtatu (sysctl) ===
cat <<EOF >> /etc/sysctl.d/99-zabala-security.conf
# IP Spoofing-aren prebentzioa
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1

# Ping bideak onartu ez
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Source routing desgaitu
net.ipv4.conf.all.accept_source_route = 0
net.ipv6.conf.all.accept_source_route = 0

# SYN Flood babesa
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_max_syn_backlog = 2048

# IP forwarding desgaitu (Gateway ez diren zerbitzarietan)
net.ipv4.ip_forward = 0
EOF
sysctl -p /etc/sysctl.d/99-zabala-security.conf
```

6.2 SSH Gogortze Kritikoa

Konfigurazio honek root saio-hasiera eta pasahitz bidezko indar gordina (brute force) saihesten ditu.

```
# === SSH Gogortze Konfigurazio Fitxategia Sortu (Debian 12 metodoa) ===
cat <<EOF > /etc/ssh/sshd_config.d/99-zabala-hardening.conf
# Zabala Gailetak - SSH Segurtasun Politika
PermitRootLogin no
PasswordAuthentication no
X11Forwarding no
MaxAuthTries 3
LoginGraceTime 20
ClientAliveInterval 300
ClientAliveCountMax 2
AllowUsers admin
Protocol 2
EOF

# === SSH Berrabiarazi ===
systemctl restart sshd

# === SSH Giltzak Egiaztatu ===
ssh-keygen -t ed25519 -C "zabala-gailetak-admin"
```

> ***ABISUA:*** *Pasahitzak desgaitu baino lehen, ziurtatu* `admin` *erabiltzaileak SSH giltza publikoak konfiguratuta dituela!*

6.3 Ostalari Suebakia (UFW) Konfigurazioa

ZG-App (Web Zerbitzaria)

```
ufw default deny incoming
ufw default allow outgoing
ufw allow ssh
ufw allow 80/tcp    # HTTP (301 birbideraketa HTTPS-ra)
ufw allow 443/tcp   # HTTPS
ufw enable
```

ZG-Data (Datu-base Zerbitzaria)

```
ufw default deny incoming
ufw default allow outgoing
ufw allow ssh
# PostgreSQL — App Zerbitzaritik soilik
ufw allow from 192.168.20.10 to any port 5432
# Redis — App Zerbitzaritik soilik
ufw allow from 192.168.20.10 to any port 6379
ufw enable
```

ZG-SecOps (Wazuh / SIEM)

```
ufw default deny incoming
ufw default allow outgoing
ufw allow ssh
ufw allow 443/tcp    # Wazuh Dashboard
ufw allow 1514/tcp   # Agente komunikazioa
ufw allow 1515/tcp   # Agente inskripzioa
ufw allow 5601/tcp   # Kibana Dashboard (MGMT saretik soilik)
ufw enable
```

ZG-OT (Sistema Industriala)

```
ufw default deny incoming
ufw default allow outgoing
ufw allow ssh
ufw allow 8080/tcp   # OpenPLC Web Interfazea
ufw allow 502/tcp    # Modbus TCP protokoloa
ufw enable
```

6.4 Fail2Ban — Brute Force Babesa

SSH indar gordinak babesteko.

```
# === Konfigurazio Lokala Sortu ===
cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local

# === SSH Kartzela Gaitu ===
cat <<EOF >> /etc/fail2ban/jail.local

[sshd]
enabled  = true
port     = ssh
filter   = sshd
logpath  = /var/log/auth.log
maxretry = 3
bantime  = 3600
findtime = 600

[nginx-http-auth]
enabled  = true
filter   = nginx-http-auth
logpath  = /var/log/nginx/error.log
maxretry = 5
bantime  = 1800

[nginx-limit-req]
enabled  = true
filter   = nginx-limit-req
logpath  = /var/log/nginx/error.log
maxretry = 10
bantime  = 600
EOF

systemctl restart fail2ban
systemctl enable fail2ban

# === Egoera Egiaztatu ===
fail2ban-client status
fail2ban-client status sshd
```

6.5 Auditoretza (auditd) Konfigurazioa

```
# === Auditd Gaitu ===
systemctl enable auditd
systemctl start auditd

# === Arau Kritikoak Gehitu ===
cat <<EOF > /etc/audit/rules.d/zabala-security.rules
# Zabala Gailetak - Auditoretza Arauak

# Sarbide Kontrola
-w /etc/passwd -p wa -k user-modify
-w /etc/shadow -p wa -k user-modify
-w /etc/sudoers -p wa -k priv-escalation

# Sistema deiak monitoratu
-a always,exit -F arch=b64 -S execve -k exec
-a always,exit -F arch=b64 -S open -F exit=-EACCES -k access-denied
-a always,exit -F arch=b64 -S open -F exit=-EPERM  -k access-denied

# Sare konfigurazioa
-w /etc/nftables.conf -p wa -k firewall-modify
-w /etc/ufw -p wa -k firewall-modify

# SSH konfigurazioa
-w /etc/ssh/sshd_config -p wa -k ssh-config
EOF

# Arauak kargatu
augenrules --load
```

7. BABESKOPIA ETA BERRESKURATZE SOP

Fitxategia: `infrastructure/systems/sop_backup_recovery.md` **Helmuga:** ZG-Data VM **Erabiltzailea:** Root

7.1 Babeskopia Estrategia

Zabala Gailetak-ek **3-2-1 Babeskopia Estrategia** jarraitzen du:

- **3** kopia: datu guztien 3 kopia independente.
- **2** euskarri: bi mota ezberdineko euskarrietan (disko lokala + hodeian).
- **1** kanpoko: kopia bat fisikoki kanpoko lekuan.

7.2 Datu-base Babeskopia Scripta

```
# Script sortu
cat <<'EOF' > /usr/local/bin/backup-db.sh
#!/bin/bash
# Zabala Gailetak - PostgreSQL Babeskopia Scripta
# Egunero 02:00etan exekutatzen da (cron bidez)

# === KONFIGURAZIOA ===
BACKUP_DIR="/backups/postgres"
CONTAINER_NAME="zabala-postgres"
DB_USER="zabala_user"
DB_NAME="zabala_db"
RETENTION_DAYS=7
LOG_FILE="/var/log/db-backup.log"

# === EXEKUZIOA ===
mkdir -p $BACKUP_DIR
TIMESTAMP=$(date +%Y%m%d_%H%M%S)
FILENAME="db_${TIMESTAMP}.sql.gz"

echo "[$(date)] Babeskopia hasitzen..." >> $LOG_FILE

# Datu-basea exportatu eta konprimitu
docker exec $CONTAINER_NAME pg_dump -U $DB_USER $DB_NAME | gzip > "${BACKUP_D

if [ $? -eq 0 ]; then
  echo "[$(date)] Babeskopia Arrakastatsua: $FILENAME" >> $LOG_FILE
  # Fitxategiaren tamaina erregistratu
  SIZE=$(du -sh "${BACKUP_DIR}/${FILENAME}" | cut -f1)
  echo "[$(date)] Tamaina: $SIZE" >> $LOG_FILE
else
  echo "[$(date)] BABESKOPIA HUTS EGIN DU — BEREHALA IKERTZEN HASI!" >> $LOG_
  # Segurtasun taldeari jakinarazi
  mail -s "[ZABALA GAILETAK] Babeskopia HUTS" security@zabala-gailetak.com <
  exit 1
fi

# Zaharkitutako babeskopiak garbitu (7 egun baino zaharragoak)
```

```
find $BACKUP_DIR -name "db_*.sql.gz" -mtime +$RETENTION_DAYS -delete
echo "[$(date)] Garbiketea osatuta — ${RETENTION_DAYS} egun baino zaharragoal
EOF

# Exekutagarri egin
chmod +x /usr/local/bin/backup-db.sh
```

7.3 Egunero Babeskopia Programatu (Cron)

```
# Crontab-era gehitu (egunero 02:00etan)
(crontab -l 2>/dev/null; echo "0 2 * * * /usr/local/bin/backup-db.sh >> /var/

# Cron egiaztatu
crontab -l
```

7.4 Berreskuratze Scripta

Fitxategi espezifiko batetik datu-basea berrezartzeko.

```
cat <<'EOF' > /usr/local/bin/restore-db.sh
#!/bin/bash
# Zabala Gailetak - Datu-base Berreskuratze Scripta
# KONTUZ: Eragiketa honek datu-basea gainidazten du!

if [ -z "$1" ]; then
  echo "Erabilpena: $0 <babeskopia_fitxategia.sql.gz>"
  exit 1
fi

BACKUP_FILE=$1
CONTAINER_NAME="zabala-postgres"
DB_USER="zabala_user"
DB_NAME="zabala_db"

echo "ABISUA: Honek ${DB_NAME} datu-basea GAINIDATZIKO du."
echo "Ziur zaude? (y/n)"
read confirm
if [ "$confirm" != "y" ]; then
  echo "Berrezartzea bertan behera utzi."
  exit 0
fi

echo "[$(date)] ${BACKUP_FILE}-tik berrezartzen..."
gunzip -c $BACKUP_FILE | docker exec -i $CONTAINER_NAME psql -U $DB_USER -d $

if [ $? -eq 0 ]; then
  echo "[$(date)] Berreskuratzea arrakastatsua."
else
  echo "[$(date)] BERRESKURATZE ERROREA — IT taldea kontaktatu."
  exit 1
fi
EOF

chmod +x /usr/local/bin/restore-db.sh
```

7.5 MongoDB Babeskopia (Scripta)

Fitxategia: `scripts/backup-mongodb.sh`

```
# MongoDB babeskopia scripta
# Helmuga: MongoDB zerbitzariak

#!/bin/bash
TIMESTAMP=$(date +%Y%m%d_%H%M%S)
BACKUP_DIR="/backups/mongodb"

mkdir -p $BACKUP_DIR

mongodump \
  --out "${BACKUP_DIR}/dump_${TIMESTAMP}" \
  --gzip \
  --oplog

find $BACKUP_DIR -mtime +7 -delete
echo "MongoDB babeskopia osatuta: dump_${TIMESTAMP}"
```

7.6 Babeskopien Egiaztapen Prozedura

Babeskopiak hilabetean behin EGIAZTATU behar dira:

```
# 1. Babeskopia fitxategiaren osotasuna egiaztatu
gzip -t /backups/postgres/db_*.sql.gz && echo "Osotasuna: OK"

# 2. Proba ingurunean berreskuratu
docker run --rm \
  -e POSTGRES_PASSWORD=test \
  -e POSTGRES_USER=zabala_user \
  -e POSTGRES_DB=zabala_db \
  postgres:14 &

sleep 5

gunzip -c /backups/postgres/db_latest.sql.gz | \
  psql -h localhost -U zabala_user zabala_db

# 3. Datu lagin bat egiaztatu
psql -h localhost -U zabala_user zabala_db -c "SELECT COUNT(*) FROM employees
```

8. ALDAKETA KUDEAKETA SOP

Fitxategia: `infrastructure/systems/sop_change_management.md`

8.1 Helburua

Sistema eta azpiegitura aldaketa guztiak modu kontrolatuan kudeatzen direla bermatzea, ezusteko etenenak eta segurtasun-intzidenteak saihesteko.

8.2 Aldaketa Eskaera Prozesua

```
┌─────────────────────────────────────────────────────────┐
│  1. RFC Aurkeztu (Request for Change)                   │
│     → Txartel-sisteman (ticketing system) bidez         │
├─────────────────────────────────────────────────────────┤
│  2. CAB Berrikusketa (Change Advisory Board)            │
│     → Astekako bilera (arruntean)                       │
│     → Ebaluazioa: eragina, arriskua, atzera-bueltako plana │
├─────────────────────────────────────────────────────────┤
│  3. Aldaketa-leiho Planifikatu                          │
│     → Produkzioko ordu apalenak (asteburuak, gauak)     │
│     → Langile arduraduna izendatu                       │
├─────────────────────────────────────────────────────────┤
│  4. Inplementazioa: Dev → Staging → Produkzioa          │
│     → Probak fase bakoitzean                            │
├─────────────────────────────────────────────────────────┤
│  5. Ondorengo Berrikusketa (Post-Implementation Review) │
│     → 24-72 orduren buruan                              │
│     → CMDB eguneratu                                    │
└─────────────────────────────────────────────────────────┘
```

8.3 Aldaketa Klasifikazioa

Mota	Deskribapena	CAB Onarpena	Denbora-muga
Estandar	Prozedura ezaguna, arrisku baxua	Ez beharrezkoa	Aurrez onartuta
Arrunta	Arrisku ertaineko aldaketa	Beharrezkoa	7 egun
Larrialdi	Segurtasun-patch kritikoa	24h barruan	Berehala

8.4 Larrialdi Aldaketak

- CAB prozedura arruntetik salbuetsita daude.
- **24 orduren barruan** dokumentatu behar dira.
- **72 orduren barruan** ondorengo berrikusketa egin behar da.
- CISO eta IT Zuzendaria berehala jakinarazi behar dira.

8.5 OT Aldaketa Berezitasunak

OT sistemetako aldaketak baldintza gehigarriak betetzen dituzte:

Baldintza	Deskribapena
Laborategiko Proba	Aldaketa OT simulazio-ingurunean probatu behar da lehenik
Ekoizpen Koordinazioa	Ekoizpen buruaren onarpena lortu behar da
Mantentze-leiho	Aldaketa ekoizpen-geldialdi planifikatuan egin
Atzera-bueltako Plana	PLC programa aurreko bertsioaren kopia gorde

9. ADABAKI KUDEAKETA SOP

Fitxategia: `infrastructure/systems/sop_patch_management.md`

9.1 Ahultasun Eskaneoa

```
# OpenVAS astekako eskaneoa
# ZG-SecOps zerbitzaritik exekutatu

# Omp tresna erabiliz (OpenVAS CLI)
omp -u admin -w PASSWORD -h localhost \
    --xml='<create_task><name>Zabala Weekly Scan</name>
    <target id="TARGET_ID"/><config id="CONFIG_ID"/>
    </create_task>'

# Txostena sortu
omp -u admin -w PASSWORD -h localhost \
    --xml='<get_reports format_id="FORMAT_PDF"/>'
```

9.2 Adabakien Sailkapena eta Erantzun Denborak

Larritasuna	CVSS Puntuazioa	Erantzun Denbora	Prozedura
Kritikoa	9.0 – 10.0	**72 ordu**	Berehala eskalatu CISO-ra
Altua	7.0 – 8.9	**7 egun**	CAB larrialdi gisa tratatu
Ertaina	4.0 – 6.9	**30 egun**	Hurrengo aldaketa-leihoan
Baxua	0.1 – 3.9	**90 egun**	Ohiko adabaki-zikloan

9.3 Inplementazio Prozesua

```
1. PROBA INGURUNEA
   └── Adabakia garapen/proba zerbitzarian aplikatu
   └── Funtzionalitate probak gainditu behar ditu
   └── Segurtasun probak (erregresio) gainditu behar ditu

2. STAGING INGURUNEA
   └── Produkzio konfigurazio berdinean probatu
   └── 24-48 ordu monitorizatu

3. PRODUKZIOA
   └── Aldaketa-leiho planifikatua (larunbatetan 02:00-06:00)
   └── Atzera-bueltako plana prest egon behar da
   └── Aplikatu eta berehala egiaztatu

4. DOKUMENTAZIOA
   └── CMDB eguneratu
   └── Aldaketa-erregistroa bete
   └── Ahultasun-erregistroa itxi
```

9.4 IT vs OT Adabaki Estrategia

Ezaugarria	IT Sistemak	OT Sistemak
Eguneraketa Automatikoak	Baimenduta (unattended-upgrades)	**DEBEKATUTA**
Proba Ingurunea	Staging zerbitzaria	OT laborategia (Factory I/O)
Ekoizpenean Eragina	Minimoa (berrabio bizkorra)	Kritikoa (plangintza zehatza)
Atzera-bueltako Denbora	Minutuak	Orduak

9.5 Eguneraketa Automatikoa (IT Zerbitzariak)

```
# unattended-upgrades konfiguratu (Debian 12)
cat <<EOF > /etc/apt/apt.conf.d/50unattended-upgrades
Unattended-Upgrade::Allowed-Origins {
    "${distro_id}:${distro_codename}-security";
};
Unattended-Upgrade::Remove-Unused-Dependencies "true";
Unattended-Upgrade::Mail "security@zabala-gailetak.com";
Unattended-Upgrade::MailReport "on-change";
EOF

# Aktibatu
systemctl enable unattended-upgrades
systemctl start unattended-upgrades
```

10. ERABILTZAILE SARBIDE KUDEAKETA SOP

Fitxategia: `infrastructure/systems/sop_user_access.md`

10.1 Erabiltzaile Hornidura Prozesua

```
1. Eskaera jaso → Zuzendariak idatziz eskatu
2. Nortasuna egiaztatu → NAN edo pasaporte bidez
3. Kontua sortu → Gutxieneko pribilegioetan (least privilege)
4. Segurtasun kontzientziatze prestakuntza → Onboarding sesio derrigorrezkoa
5. Sarbide Erregistroan dokumentatu → CMDB eta Access Log eguneratu
```

10.2 Sarbide Berrikusketa Egutegia

Berrikusketa Mota	Maiztasuna	Arduraduna
Kontu Arrunten Berrikusketa	Hiruhilabetero	IT Arduraduna
Kontu Pribilegiodun Berrikusketa	Hilabetero	CISO
Ezohiko Sarbideak	Berehala intzidenterakoan	IT + CISO
Langileak alde egitean	Berehala	IT Arduraduna

10.3 Rol Oinarritutako Sarbide Kontrola (RBAC)

Rola	Baimendutako Eragiketak	Sistema Sarbidea
Erabiltzaile	Norberaren datuak irakurri, eskaerak egin	HR Portala soilik
Kudeatzaile	Taldeko datuak irakurri, eskaerak onartu	HR Portala + Txostenak
Admin	Sistema sarbide osoa	Dena
Auditorea	Irakurketa soilik (dena)	Log sistema + Txostenak

Rola	Baimendutako Eragiketak	Sistema Sarbidea
OT Operadorea	HMI eta SCADA operazioak	OT Sarea soilik

10.4 Kontu Pribilegioduen Kontrol Gehigarriak

```
# Sudo erabileraren erregistroa egiaztatu
grep sudo /var/log/auth.log

# Erabiltzaile aktiboen zerrenda
cut -d: -f1,3 /etc/passwd | awk -F: '$2 >= 1000'

# Admin taldeko kideen zerrenda
getent group sudo
getent group admin

# Azkeneko saio-hasierak ikusi
last -n 20
```

10.5 Kontu Blokeatzea — Alde Egiteko Prozedura

```
# 1. Kontua berehala desgaitu
usermod -L username
passwd -l username

# 2. SSH giltza ezabatu
rm -f /home/username/.ssh/authorized_keys

# 3. Iraungo saio guztiak amaitu
pkill -u username

# 4. Cron lanak ezabatu
crontab -r -u username

# 5. Sarbide Erregistroa eguneratu (data, arrazoia)
echo "$(date): username - Lanpostua utzi - Kontua desgaitu" \
  >> /var/log/zabala-access-terminations.log
```

11. NGINX WEB ZERBITZARIA GOGORTZE KONFIGURAZIOA

11.1 Nginx Nagusia — API/Web Zerbitzaria

Fitxategia: `nginx/nginx.conf`

```
# Zabala Gailetak - Nginx API Proxy Konfigurazioa
# TLS 1.2/1.3, HSTS, Tasa Mugaketa eta Segurtasun Goiburuak

events {
    worker_connections 1024;
}

http {
    # === Upstream Backend ===
    upstream api {
        server api:3000;
    }

    # === Tasa Mugaketa (Rate Limiting) ===
    # API orokorra: 10 eskaera/segundo IP bakoitzeko
    limit_req_zone $binary_remote_addr zone=api_limit:10m rate=10r/s;

    # === HTTP → HTTPS Birbideraketa (301 Iraunkorra) ===
    server {
        listen 80;
        server_name zabala-gailetak.com www.zabala-gailetak.com;
        return 301 https://$server_name$request_uri;
    }

    # === HTTPS Zerbitzaria ===
    server {
        listen 443 ssl http2;
        server_name zabala-gailetak.com www.zabala-gailetak.com;

        # === TLS Konfigurazioa ===
        ssl_certificate     /etc/nginx/ssl/cert.pem;
        ssl_certificate_key /etc/nginx/ssl/key.pem;
        ssl_protocols       TLSv1.2 TLSv1.3;
        ssl_ciphers         HIGH:!aNULL:!MD5;
        ssl_prefer_server_ciphers on;
        ssl_session_cache   shared:SSL:10m;
        ssl_session_timeout 10m;

        # === Segurtasun Goiburuak ===
```

```
        add_header Strict-Transport-Security "max-age=31536000; includeSubDor
        add_header X-Frame-Options           "SAMEORIGIN" always;
        add_header X-Content-Type-Options    "nosniff" always;
        add_header X-XSS-Protection          "1; mode=block" always;
        add_header Referrer-Policy           "strict-origin-when-cross-origi

        client_max_body_size 10M;

        # === Proxy Konfigurazioa ===
        location / {
            limit_req zone=api_limit burst=20 nodelay;
            proxy_pass         http://api;
            proxy_http_version 1.1;
            proxy_set_header   Upgrade $http_upgrade;
            proxy_set_header   Connection 'upgrade';
            proxy_set_header   Host $host;
            proxy_set_header   X-Real-IP $remote_addr;
            proxy_set_header   X-Forwarded-For $proxy_add_x_forwarded_for;
            proxy_set_header   X-Forwarded-Proto $scheme;
            proxy_cache_bypass $http_upgrade;
            proxy_connect_timeout 60s;
            proxy_send_timeout    60s;
            proxy_read_timeout    60s;
        }

        # === Osasun Egiaztapena ===
        location /health {
            access_log off;
            proxy_pass http://api/api/health;
        }
    }
}
```

11.2 Nginx HR Portal — PHP-FPM Konfigurazioa

Fitxategia: `nginx/nginx-hrportal.conf`

```
# Zabala Gailetak - HR Portal Nginx Konfigurazioa
# PHP-FPM, Segurtasun Goiburuak, Tasa Mugaketa

user nginx;
worker_processes auto;
error_log /var/log/nginx/error.log warn;
pid /var/run/nginx.pid;

events {
    worker_connections 1024;
    use epoll;
}

http {
    include      /etc/nginx/mime.types;
    default_type application/octet-stream;

    # === Erregistro Formatua ===
    log_format main '$remote_addr - $remote_user [$time_local] "$request" '
                    '$status $body_bytes_sent "$http_referer" '
                    '"$http_user_agent" "$http_x_forwarded_for"';

    access_log /var/log/nginx/access.log main;

    # === Oinarrizko Optimizazioa ===
    sendfile        on;
    tcp_nopush      on;
    tcp_nodelay     on;
    keepalive_timeout 65;

    # === Gzip Konpresioa ===
    gzip             on;
    gzip_vary        on;
    gzip_proxied     any;
    gzip_comp_level  6;
    gzip_types text/plain text/css text/xml text/javascript
               application/json application/javascript application/xml+rss;

    # === Segurtasun Goiburuak (Globalak) ===
```

```
    add_header X-Frame-Options        "SAMEORIGIN" always;
    add_header X-Content-Type-Options "nosniff" always;
    add_header X-XSS-Protection       "1; mode=block" always;
    add_header Referrer-Policy        "strict-origin-when-cross-origin" alway

    # === Tasa Mugaketa Eremuak ===
    limit_req_zone $binary_remote_addr zone=api_limit:10m   rate=10r/s;
    limit_req_zone $binary_remote_addr zone=login_limit:10m rate=5r/m;

    upstream php_backend {
        server php:9000;
    }

    server {
        listen 80;
        server_name localhost;
        root  /var/www/html/public;
        index index.php index.html;

        # Zerbitzari Tokena Ezkutatu
        server_tokens off;

        access_log /var/log/nginx/hr_portal_access.log main;
        error_log  /var/log/nginx/hr_portal_error.log warn;

        # === Kokapen Nagusia ===
        location / {
            try_files $uri $uri/ /index.php?$query_string;
        }

        # === PHP-FPM Prozesatzea ===
        location ~ \.php$ {
            try_files $uri =404;
            fastcgi_split_path_info ^(.+\.php)(/.+)$;
            fastcgi_pass       php_backend;
            fastcgi_index      index.php;
            include            fastcgi_params;
            fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
            fastcgi_param PATH_INFO       $fastcgi_path_info;
            fastcgi_buffering  off;
```

```
        fastcgi_read_timeout 300;
    }

    # === API Endpoint-ak — Tasa Mugaketa ===
    location /api/ {
        limit_req zone=api_limit burst=20 nodelay;
        try_files $uri $uri/ /index.php?$query_string;
    }

    # === Login Endpoint — Tasa Mugaketa Zorrotzagoa ===
    location /api/auth/login {
        limit_req zone=login_limit burst=3 nodelay;
        try_files $uri /index.php?$query_string;
    }

    # === Fitxategi Ezkutuak Ukatu ===
    location ~ /\. {
        deny all;
        access_log off;
        log_not_found off;
    }

    # === Fitxategi Sentikor Ukatu ===
    location ~ (composer\.json|composer\.lock|\.env)$ {
        deny all;
        access_log off;
        log_not_found off;
    }

    # === Fitxategi Estatikoak Katxea ===
    location ~* \.(jpg|jpeg|png|gif|ico|css|js|svg|woff|woff2|ttf|eot)$ {
        expires 1y;
        add_header Cache-Control "public, immutable";
        access_log off;
    }

    # === Osasun Egiaztapen Endpoint-a ===
    location /health {
        access_log off;
        return 200 "OK\n";
```

```
            add_header Content-Type text/plain;
        }
    }

    include /etc/nginx/conf.d/*.conf;
}
```

12. WEB APLIKAZIO SEGURTASUN GOGORTZE SOP

Fitxategia: `security/web_hardening_sop.md` **Helburua:** Web aplikazioa OWASP Top 10 arauak kontuan hartuta segurtatzea

12.1 Segurtasun Goiburuen Konfigurazioa (Node.js / Helmet)

```
// Zabala Gailetak - Helmet Middleware Konfigurazioa
const helmet = require('helmet');

// === Content Security Policy (CSP) ===
app.use(helmet.contentSecurityPolicy({
  directives: {
    defaultSrc:  ["'self'"],
    styleSrc:    ["'self'", "'unsafe-inline'"],
    scriptSrc:   ["'self'"],
    imgSrc:      ["'self'", "data:"],
    connectSrc:  ["'self'"],
    fontSrc:     ["'self'"],
    objectSrc:   ["'none'"],
    mediaSrc:    ["'self'"],
    frameSrc:    ["'none'"],
  },
}));

// === HSTS (HTTP Strict Transport Security) ===
app.use(helmet.hsts({
  maxAge:            31536000,   // 1 urtea segundotan
  includeSubDomains: true,
  preload:           true
}));
```

12.2 Sarrera Balidazioa — SQL Injection Prebentzioa

```
// Express-Validator bidezko sarrera balidazioa
const { body, validationResult } = require('express-validator');

app.post('/api/employees', [
  body('name').trim().isLength({ min: 2, max: 100 }).escape(),
  body('email').isEmail().normalizeEmail(),
  body('salary').isFloat({ min: 0 }).toFloat(),
  body('department').trim().isLength({ max: 50 }).escape()
], (req, res) => {
  const errors = validationResult(req);
  if (!errors.isEmpty()) {
    return res.status(400).json({ errors: errors.array() });
  }
  // Prozesatu langilea...
});
```

SQL Injection prebentzioa — Arau absolutuak:

- Beti parameterized queries erabili.
- Ez eraiki SQL kateak dinamikoki katetatuz.
- ORM seguruak erabili (Sequelize, TypeORM, Mongoose).

12.3 Sesio Kudeaketa Segurua

```
// Cookie eta Sesio Konfigurazio Segurua
app.use(session({
  secret:            process.env.SESSION_SECRET,
  resave:            false,
  saveUninitialized: false,
  cookie: {
    secure:   true,      // HTTPS soilik
    httpOnly: true,      // JavaScript bidez ezin da atzitu
    sameSite: 'strict',  // CSRF prebentzioa
    maxAge:   3600000    // 1 ordu (millisekundo)
  }
}));
```

12.4 CSRF Babesa

```
// CSRF Token Babesa
const csrf = require('csurf');
const csrfProtection = csrf({ cookie: true });

// Formulario GET
app.get('/form', csrfProtection, (req, res) => {
  res.render('send', { csrfToken: req.csrfToken() });
});

// Formulario POST — CSRF token egiaztatu
app.post('/form', csrfProtection, (req, res) => {
  // Token automatikoki egiaztatzen da — ez da kode gehigarririk behar
  // Prozesatu eskaera...
});
```

12.5 Pasahitz Politika eta Hashing

```
// Bcrypt bidezko pasahitz hashing-a
const bcrypt = require('bcryptjs');

// Pasahitza gordetzea (salt rounds = 10)
const hashPassword = async (password) => {
  return await bcrypt.hash(password, 10);
};

// Pasahitza egiaztatzea
const verifyPassword = async (password, hash) => {
  return await bcrypt.compare(password, hash);
};
```

Pasahitz Politika Arauak:

- Gutxienez **8 karaktere** (gomendatua: 12+).
- **Maiuskula** eta **minuskula** gutxienez bat.
- **Zenbaki** bat gutxienez.
- **Karaktere berezia** bat gutxienez (!, @, #, $...).
- **5 saiakera oker** ondoren: kontua automatikoki blokeatu.

12.6 Tasa Mugaketa API-rako

```
const rateLimit = require('express-rate-limit');

// API orokorra
const apiLimiter = rateLimit({
  windowMs: 15 * 60 * 1000, // 15 minutu
  max:      100,              // Gehienez 100 eskaera
  message:  'Eskaera gehiegi. Saiatu 15 minutu barru.',
  standardHeaders: true
});

// Login endpoint-a — askoz zorrotzagoa
const loginLimiter = rateLimit({
  windowMs: 15 * 60 * 1000,
  max:      5,                // Gehienez 5 saiakera
  message:  'Saiakera gehiegi. Saiatu 15 minutu barru.'
});

app.use('/api/', apiLimiter);
app.use('/api/auth/login', loginLimiter);
```

12.7 HTTPS Ziurtagiria — Let's Encrypt

```
# Let's Encrypt ziurtagiria lortu
sudo apt install certbot python3-certbot-nginx
sudo certbot --nginx \
  -d zabala-gailetak.com \
  -d www.zabala-gailetak.com

# Auto-berritze proba
sudo certbot renew --dry-run

# Cron bidez automatikoki berritu (bi aldiz egunean)
0 12 * * * /usr/bin/certbot renew --quiet
```

12.8 Segurtasun Erregistroak

```
const logger = require('winston');

// Login saiakera arrakastatsua
logger.info('Login arrakastatsua', {
  userId:    user.id,
  ip:        req.ip,
  userAgent: req.headers['user-agent'],
  timestamp: new Date().toISOString()
});

// Login saiakera huts
logger.warn('Login saiakera huts', {
  username:  req.body.username,
  ip:        req.ip,
  timestamp: new Date().toISOString()
});

// Segurtasun urraketa
logger.error('Segurtasun urraketa', {
  type:      'SQL Injection saiakera',
  ip:        req.ip,
  payload:   req.body,
  timestamp: new Date().toISOString()
});
```

13. SIEM ESTRATEGIA ETA INPLEMENTAZIOA

Fitxategia: `security/siem/siem_strategy.md`

13.1 Helburua

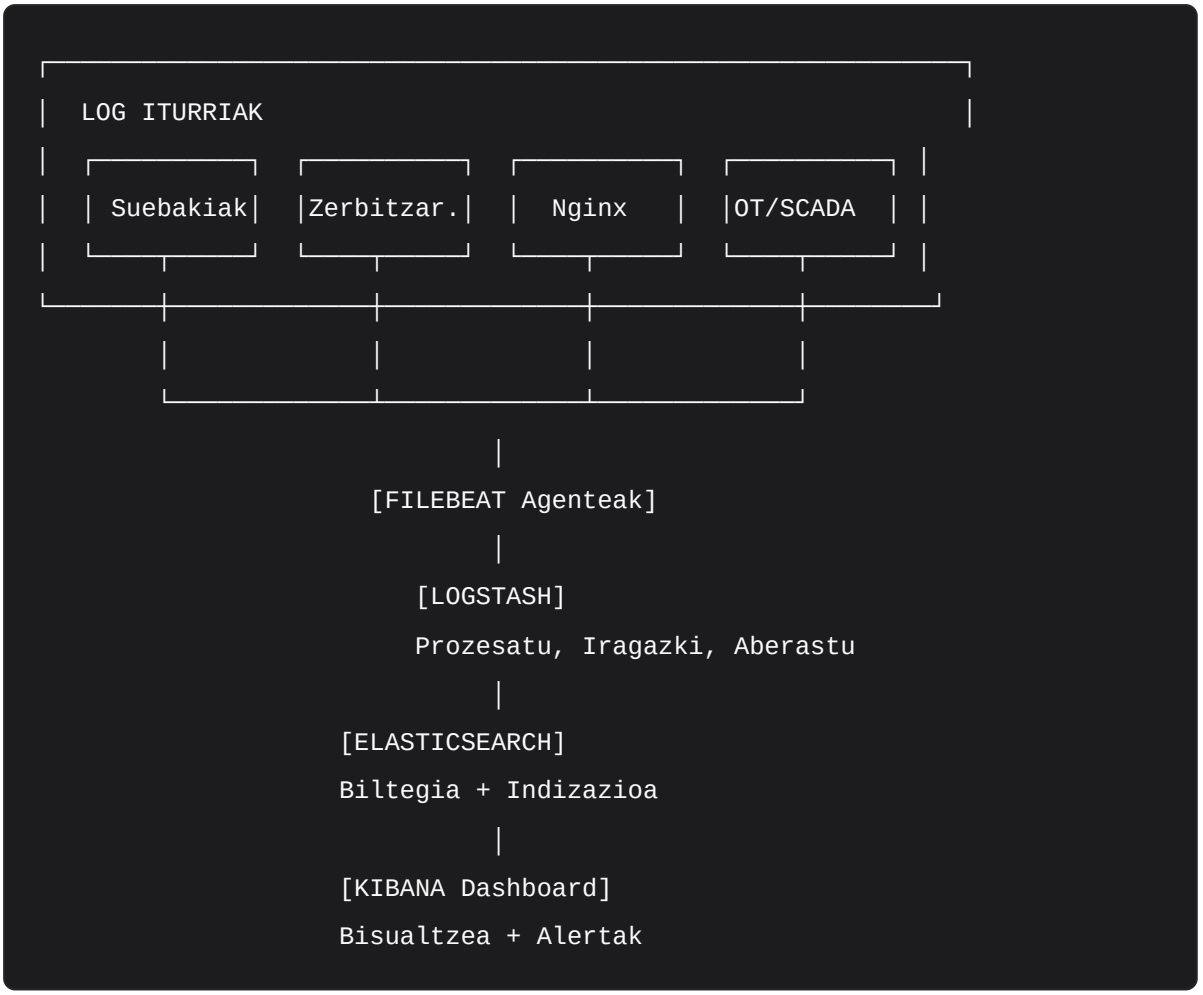
Zabala Gailetak-eko azpiegituran gertatzen diren segurtasun gertaerak **zentralizatu**, **korrelatu** eta **aztertzea**, mehatxuak denbora errealean detektatzeko.

13.2 Aukeratutako Soluzioa — ELK Stack + Wazuh

Osagaia	Bertsioa	Funtzioa
Elasticsearch	8.11.0	Datu-biltegia eta bilaketa motorra
Logstash	8.11.0	Log prozesatzea eta filtrazioa
Kibana	8.11.0	Bisualtzea eta Dashboard-ak
Filebeat	8.11.0	Log bidalketa agentea
Wazuh	—	EDR, HIDS, FIM (File Integrity Monitoring)

Arrazoia: Kostu-eraginkorra (open source), funtzionalitate zabalak (EDR, log analisia, GDPR betetzea), eta komunitate aktiboa.

13.3 SIEM Arkitektura



13.4 Log Iturriak

Iturria	Log Mota	Garrantzia
Suebakiak (NFTables)	Sarrera/Irteera trafikoa, blokeatutako konexioak	Kritikoa
Zerbitzariak (Linux)	Autentikazioak, pribilegio-igoerak, sistema-aldaketak	Kritikoa
Web Zerbitzaria (Nginx)	Access logs (SQLi, XSS saiakerak), Error logs	Altua
OT Sareko Pasabideak	PLC sarrerak, Modbus konexioak	Altua
Honeypot-ak	Eraso-saiakerak, teknikak, malware laginak	Ertaina
HR Portala	Login saiakerak, datu-sarbideak, CSRF saiakerak	Altua

13.5 SIEM Docker Inplementazioa

Fitxategia: `security/siem/docker-compose.siem.yml`

```
version: '3.8'

services:
  # === Elasticsearch — Datu-biltegia ===
  elasticsearch:
    image: docker.elastic.co/elasticsearch/elasticsearch:8.11.0
    container_name: zabala-siem-elasticsearch
    environment:
      - discovery.type=single-node
      - "ES_JAVA_OPTS=-Xms512m -Xmx512m"
      - xpack.security.enabled=true
      - ELASTIC_PASSWORD=${ELASTIC_PASSWORD}
    ports:
      - "9200:9200"
    volumes:
      - es-data:/usr/share/elasticsearch/data
    networks:
      - siem-network
    healthcheck:
      test: ["CMD-SHELL", "curl -u elastic:${ELASTIC_PASSWORD} -s http://loca
      interval: 30s
      timeout: 10s
      retries: 5

  # === Logstash — Log Prozesatzea ===
  logstash:
    image: docker.elastic.co/logstash/logstash:8.11.0
    container_name: zabala-siem-logstash
    volumes:
      - ./security/siem/logstash.conf:/usr/share/logstash/pipeline/logstash.c
      - /var/log/zabala-gailetak:/var/log/zabala-gailetak:ro
      - /var/log/nginx:/var/log/nginx:ro
    ports:
      - "5044:5044"
    depends_on:
      - elasticsearch
    networks:
      - siem-network
    environment:
```

```
      - ELASTIC_PASSWORD=${ELASTIC_PASSWORD}

  # === Kibana — Bisualtzea ===
  kibana:
    image: docker.elastic.co/kibana/kibana:8.11.0
    container_name: zabala-siem-kibana
    environment:
      - ELASTICSEARCH_HOSTS=http://elasticsearch:9200
      - ELASTICSEARCH_USERNAME=elastic
      - ELASTICSEARCH_PASSWORD=${ELASTIC_PASSWORD}
    ports:
      - "5601:5601"
    depends_on:
      - elasticsearch
    networks:
      - siem-network

networks:
  siem-network:
    driver: bridge

volumes:
  es-data:
    driver: local
```

13.6 Logstash Konfigurazioa — Segurtasun Detekzioa

Fitxategia: `security/siem/logstash-enhanced.conf`

```
# Zabala Gailetak - Logstash Segurtasun Detekzio Konfigurazioa

input {
  # Filebeat agenteengandik
  beats { port => 5044; codec => json; type => "beats" }

  # Nginx access logak
  file {
    path  => "/var/log/nginx/access.log"
    type  => "nginx-access"
    tags  => ["nginx", "access"]
  }

  # Suebaki logak
  tcp { port => 5514; type => "firewall"; tags => ["firewall"] }

  # Aplikazio audit logak
  http { port => 8080; codec => json; type => "audit"; tags => ["audit"] }
}

filter {
  # === Autentikazio Huts Detekzioa ===
  if [event] == "auth.login.failed" {
    mutate {
      add_field => { "alert_type" => "failed_login" }
      add_field => { "severity"   => "medium" }
      add_tag   => [ "security", "auth_failure" ]
    }
    # IP beretik 5 saiakeraren ondoren: brute force
    aggregate {
      task_id => "%{client_ip}"
      code    => "
        map['failed_attempts'] ||= 0
        map['failed_attempts'] += 1
        event.set('failed_attempts', map['failed_attempts'])
      "
      timeout => 300
    }
  }
```

```
# === SQL Injection Detekzioa ===
if [request_body] =~ /(\bUNION\b|\bSELECT\b|\bINSERT\b|\bDROP\b|--|')/i {
  mutate {
    add_field => { "alert_type" => "sql_injection_attempt" }
    add_field => { "severity"   => "critical" }
    add_tag   => [ "security", "sql_injection", "attack" ]
  }
}

# === XSS Detekzioa ===
if [request_body] =~ /<script|javascript:|onerror=|onload=/i {
  mutate {
    add_field => { "alert_type" => "xss_attempt" }
    add_field => { "severity"   => "high" }
    add_tag   => [ "security", "xss", "attack" ]
  }
}

# === Path Traversal Detekzioa ===
if [request_uri] =~ /\.\.\//|\.\.\\|%2e%2e/i {
  mutate {
    add_field => { "alert_type" => "path_traversal_attempt" }
    add_field => { "severity"   => "high" }
    add_tag   => [ "security", "path_traversal" ]
  }
}

# === Komando Injekzio Detekzioa ===
if [request_body] =~ /;|\||&|`|\$\(|\$\{/i {
  mutate {
    add_field => { "alert_type" => "command_injection_attempt" }
    add_field => { "severity"   => "critical" }
    add_tag   => [ "security", "command_injection" ]
  }
}

# === GeoIP Aberastea ===
if [client_ip] and [client_ip] !~ /^(10\.|172\.(1[6-9]|2[0-9]|3[0-1])\.|192
  geoip {
```

```
      source => "client_ip"
      target => "geoip"
      fields => ["city_name", "country_name", "country_code2", "location"]
    }
  }

  # === Eraso Tresna Detekzioa (User-Agent) ===
  if [user_agent] =~ /sqlmap|nikto|nmap|masscan|metasploit|burp|owasp|zap/i {
    mutate {
      add_field => { "alert_type" => "security_scanner_detected" }
      add_field => { "severity"   => "high" }
      add_tag   => [ "security", "scanner", "attack_tool" ]
    }
  }

  # === Metadatu Gehitu ===
  mutate {
    add_field => {
      "organization" => "Zabala Gailetak"
      "environment"  => "${ENVIRONMENT:production}"
    }
  }
}

output {
  # Elasticsearch-era bidali
  elasticsearch {
    hosts    => ["http://elasticsearch:9200"]
    index    => "zabala-%{+YYYY.MM.dd}"
    user     => "elastic"
    password => "${ELASTIC_PASSWORD}"
  }

  # Alerta kritikoak indize bereizira
  if [severity] == "critical" or "attack" in [tags] {
    elasticsearch {
      hosts    => ["http://elasticsearch:9200"]
      index    => "zabala-alerts-%{+YYYY.MM.dd}"
      user     => "elastic"
      password => "${ELASTIC_PASSWORD}"
```

```
    }
  }

  # Alerta kritikoak posta elektronikoz bidali
  if [severity] == "critical" {
    email {
      to      => "security@zabala-gailetak.com"
      from    => "siem@zabala-gailetak.com"
      subject => "[ALERTA KRITIKOA] %{alert_type}"
      body    => "Alerta Mota: %{alert_type}\nLarritasuna: %{severity}\nIP: %
    }
  }
}
```

13.7 Filebeat Log Bidalketa Konfigurazioa

Fitxategia: `security/siem/filebeat.yml`

```
# Zabala Gailetak - Filebeat Konfigurazioa

filebeat.inputs:
  # Aplikazio logak
  - type: log
    enabled: true
    paths:
      - /var/log/zabala-gailetak/*.log
      - /app/logs/*.log
    fields:
      type: application
      organization: zabala-gailetak
    fields_under_root: true
    json.keys_under_root: true

  # Nginx access logak
  - type: log
    enabled: true
    paths: [/var/log/nginx/access.log]
    fields:
      type: nginx-access
      log_type: web_server
    fields_under_root: true

  # Nginx error logak
  - type: log
    enabled: true
    paths: [/var/log/nginx/error.log]
    fields:
      type: nginx-error
      severity: error
    fields_under_root: true

  # Audit logak
  - type: log
    enabled: true
    paths: [/var/log/zabala-gailetak/audit/*.log]
    fields:
      type: audit
```

```
      log_type: security
    fields_under_root: true
    json.keys_under_root: true

# Prozesadore gehigarriak
processors:
  - add_host_metadata: ~
  - add_docker_metadata: ~

  # Datu sentikorrak ezabatu log-etatik
  - drop_fields:
      fields: ["password", "token", "secret", "api_key"]
      ignore_missing: true

  # Metadatu gehitu
  - add_fields:
      target: ''
      fields:
        organization: Zabala Gailetak
        data_classification: internal

# Logstash-era bidali
output.logstash:
  hosts: ["logstash:5044"]
  loadbalance: true
  compression_level: 3
  bulk_max_size: 2048

# ILM (Index Lifecycle Management)
setup.ilm.enabled: true
setup.ilm.rollover_alias: "zabala-filebeat"
```

13.8 Alerta Arauak

Fitxategia: `security/siem/alert-rules.json` (laburpena)

Arau ID	Izena	Larritasuna	MITRE ATT&CK	Ekintza
auth-001	Login Saiakera Anizkoitz Huts	Altua	T1110.001, T1110.003	Alerta + Intzidentea sortu
sqli-001	SQL Injection Saiakera	Kritikoa	T1190	Alerta + IP blokeatu + Intzidentea
xss-001	XSS Saiakera	Altua	T1189	Alerta + Intzidentea
cmdi-001	Komando Injekzio	Kritikoa	T1059	Alerta + IP blokeatu + CISO jakinarazi
scan-001	Segurtasun Eskaneatzailea	Altua	T1595	Alerta + IP blokeatu
scan-002	Direktorio Enumerazioa	Ertaina	T1083	Alerta + Tasa mugatu
geo-001	Arrisku Handiko Herrialde Sarbidea	Ertaina	T1078	Alerta + MFA behartu
geo-002	Ezinezko Bidaia (Impossible Travel)	Altua	T1078.004	Alerta + Kontua eten
data-001	Datu Esfiltrazio Handia	Kritikoa	T1567	Alerta + Erabiltzailea blokeatu + DPO
mfa-001	MFA Saihesteko Saiakera	Kritikoa	T1556	Alerta + Saioa ezeztu + CISO
gdpr-001	Datu Pertsonalak Baimenik Gabe	Kritikoa	—	DPO + Juridikoa + GDPR erregistroa

13.9 Elasticsearch Indize Txantiloia

Fitxategia: `security/siem/elasticsearch-template.json`

```
{
  "index_patterns": ["zabala-gailetak-*"],
  "template": {
    "settings": {
      "number_of_shards": 1,
      "number_of_replicas": 0,
      "index.lifecycle.name": "zabala-gailetak-policy",
      "index.lifecycle.rollover_alias": "zabala-gailetak"
    },
    "mappings": {
      "properties": {
        "timestamp":  { "type": "date" },
        "level":      { "type": "keyword" },
        "msg":        { "type": "text" },
        "host":       { "type": "keyword" },
        "type":       { "type": "keyword" },
        "tags":       { "type": "keyword" },
        "response":   { "type": "integer" },
        "request":    { "type": "text" }
      }
    }
  }
}
```

14. HONEYPOT SISTEMA INPLEMENTAZIOA

14.1 Helburua eta Estrategia

Fitxategia: `security/honeypot/honeypot_plan.md`

Irudizko sistema zaurgarri bat (Honeypot) ezartzea Interneten, erasotzaileen teknikak, jatorria eta helburuak aztertzeko — gure ekoizpen sistemak arriskuan jarri gabe. Zabala Gailetak industria-honeypot bat abiarazi du (OT ingurunea simulatzen duena), benetako PLCak eta SCADA sistemak babesteko.

14.2 Honeypot Arkitektura

```
DMZ ISOLATUA (172.30.0.0/24)
├── COWRIE (SSH/Telnet Honeypot)      → 2222/tcp
├── CONPOT (ICS/SCADA Honeypot)       → 502/tcp (Modbus), 102/tcp (S7Comm)
├── DIONAEA (Malware Honeypot)        → 21, 445, 3306/tcp
├── ELASTICPOT (Elasticsearch HP)     → 9200/tcp
├── HERALDING (Kredentzial HP)        → 23, 25, 3389/tcp
└── LOGSTASH (Log Biltzailea)         → SIEM nagusira bidalita

SIEM SAREA (172.31.0.0/24)
└── ELK Stack nagusiarekin komunikazioa
```

14.3 Honeypot Motak — Justifikazioa

Honeypot	Mota	Zergatik Zabala Gailetak-entzat
T-Pot	Plataforma integrala	Honeypot multzo osoa batera kudeatzeko
Cowrie	SSH/Telnet	Administrazio-sarbide erasoak antzemateko
Conpot	ICS/SCADA (Modbus, S7Comm)	**Industria-erasotzaileak erakartzeko** — gaileta-fabrika babesteko

Honeypot	Mota	Zergatik Zabala Gailetak-entzat
Dionaea	Malware bilketa	Ransomware eta worm laginak biltzeko
Heralding	Kredentzial harrapaketa	Phishing eta credential stuffing antzemateko

14.4 Docker Inplementazioa

Fitxategia: `security/honeypot/docker-compose.honeypot.yml`

```yaml
version: '3.8'

services:
  # === T-Pot — Honeypot Plataforma Integrala ===
  tpot:
    image: telekom-security/tpotce:latest
    container_name: zabala-tpot
    hostname: zabala-tpot
    restart: unless-stopped
    network_mode: host
    deploy:
      resources:
        limits:   { cpus: '2.0', memory: 4G }
        reservations: { cpus: '1.0', memory: 2G }
    volumes:
      - tpot_data:/data
      - tpot_log:/var/log/tpot
      - ./config/tpot/tpot.yml:/opt/tpot/etc/tpot.yml:ro
    environment:
      - WEB_USER=admin
      - WEB_PASS=SecurePassword123!   # ← ALDATU produkzioan!
      - TZ=Europe/Madrid
      - HONEYPOTS=cowrie,dionaea,conpot,elasticpot,heralding
      - ELK_ENABLED=true
      - LOGSTASH_HOST=logstash
      - LOGSTASH_PORT=5044
    labels:
      - "com.zabala.service=honeypot"
      - "com.zabala.environment=dmz"

  # === Cowrie — SSH/Telnet Honeypot ===
  cowrie:
    image: cowrie/cowrie:latest
    container_name: zabala-cowrie
    hostname: zabalagailetak-ssh-server   # ← Benetakoa simulatzen du
    restart: unless-stopped
    ports:
      - "2222:2222"  # SSH
      - "2223:2223"  # Telnet
```

```
    deploy:
      resources:
        limits: { cpus: '0.5', memory: 512M }
    volumes:
      - cowrie_log:/cowrie/cowrie-git/var/log/cowrie
      - cowrie_downloads:/cowrie/cowrie-git/var/lib/cowrie/downloads
      - ./config/cowrie/cowrie.cfg:/cowrie/cowrie-git/etc/cowrie.cfg:ro
    environment:
      - TZ=Europe/Madrid
      - COWRIE_JSON_ENABLED=true
    networks:
      - honeypot-net
    labels:
      - "com.zabala.component=cowrie"
      - "com.zabala.protocol=ssh"

  # === Conpot — ICS/SCADA Honeypot (INDUSTRIA KRITIKOA) ===
  conpot:
    image: honeynet/conpot:latest
    container_name: zabala-conpot
    hostname: zabalagailetak-plc-01   # ← PLC benetakoa simulatzen du
    restart: unless-stopped
    ports:
      - "80:8080"     # HTTP (PLC Web Interfazea)
      - "102:102"     # S7Comm (Siemens PLC)
      - "502:502"     # Modbus TCP
      - "161:161/udp" # SNMP
      - "47808:47808" # BACnet
      - "44818:44818" # EtherNet/IP
    deploy:
      resources:
        limits: { cpus: '1.0', memory: 1G }
    volumes:
      - conpot_log:/var/log/conpot
      - ./config/conpot/template.xml:/usr/src/conpot/conpot/templates/default
    environment:
      - TZ=Europe/Madrid
      - CONPOT_DEVICE_NAME=Zabala Gailetak PLC-01
      - CONPOT_JSON=true
    command: ["--template", "default", "--logfile", "/var/log/conpot/conpot.
```

```
    networks:
      - honeypot-net
    labels:
      - "com.zabala.component=conpot"
      - "com.zabala.protocol=ics-scada"

  # === Dionaea — Malware Bilketa Honeypot ===
  dionaea:
    image: dinotools/dionaea:latest
    container_name: zabala-dionaea
    hostname: zabalagailetak-file-server
    restart: unless-stopped
    ports:
      - "21:21"     # FTP
      - "445:445"   # SMB
      - "1433:1433" # MSSQL
      - "3306:3306" # MySQL
    deploy:
      resources:
        limits: { cpus: '1.0', memory: 1G }
    volumes:
      - dionaea_log:/opt/dionaea/var/log
      - dionaea_downloads:/opt/dionaea/var/dionaea/binaries
    networks:
      - honeypot-net
    labels:
      - "com.zabala.component=dionaea"
      - "com.zabala.purpose=malware-collection"

  # === Logstash — Log Bilketa eta SIEM-era Bidaltzea ===
  logstash:
    image: docker.elastic.co/logstash/logstash:8.11.0
    container_name: zabala-honeypot-logstash
    restart: unless-stopped
    ports:
      - "5044:5044"   # Beats sarrera
      - "5000:5000/udp" # Syslog sarrera
    deploy:
      resources:
        limits: { cpus: '1.0', memory: 2G }
```

```
    volumes:
      - ./config/logstash/pipelines:/usr/share/logstash/pipeline:ro
    environment:
      - TZ=Europe/Madrid
      - ELASTICSEARCH_HOSTS=http://elasticsearch:9200
    networks:
      - honeypot-net
      - siem-net
    depends_on: [cowrie, conpot, dionaea]

networks:
  honeypot-net:
    driver: bridge
    ipam:
      config:
        - subnet: 172.30.0.0/24
          gateway: 172.30.0.1
    labels:
      - "com.zabala.network=honeypot"
      - "com.zabala.isolation=true"
  siem-net:
    driver: bridge
    ipam:
      config:
        - subnet: 172.31.0.0/24

volumes:
  tpot_data:    { driver: local }
  tpot_log:     { driver: local }
  cowrie_log:   { driver: local, labels: { "com.zabala.backup": "daily" } }
  cowrie_downloads: { driver: local, labels: { "com.zabala.scan": "malware"
  conpot_log:   { driver: local, labels: { "com.zabala.backup": "daily" } }
  dionaea_log:  { driver: local, labels: { "com.zabala.backup": "daily" } }
  dionaea_downloads: { driver: local, labels: { "com.zabala.scan": "malware"
```

14.5 Conpot Konfigurazioa — Zabala Gailetak PLC Simulazioa

Fitxategia: `security/honeypot/honeypot_implementation_sop.md` (laburpena)

```
<!-- Conpot Template - Zabala Gailetak PLC Simulazioa -->
<template>
    <host>
        <name>Zabala Gailetak PLC</name>
        <mac>00:0C:29:12:34:56</mac>
        <ip>192.168.50.10</ip>
    </host>

    <services>
        <!-- Modbus TCP — Gaileta Ekoizpen Erregistroak (Simulatua) -->
        <modbus port="502">
            <port>502</port>
            <unit_id>1</unit_id>
            <registers>
                <register address="40001" value="100"/>  <!-- Labe Tenperatu
                <register address="40002" value="200"/>  <!-- Orea Pisua -->
            </registers>
        </modbus>

        <!-- S7Comm — Siemens PLC Simulazioa -->
        <s7comm port="102">
            <port>102</port>
            <module_type>CPU 315-2 DP</module_type>
        </s7comm>

        <!-- HTTP — PLC Web Interfaze Faltsua -->
        <http port="8080">
            <port>8080</port>
            <body>
                <html>
                <body>
                <h1>Zabala Gailetak - PLC Interface</h1>
                <p>Unauthorized access is prohibited and logged.</p>
                </body>
                </html>
            </body>
        </http>
    </services>
</template>
```

14.6 Logstash — Honeypot Logak SIEM-era Integratzea

```
# Honeypot Logstash Pipeline
input {
  file {
    path => "/var/log/honeypot/*.log"
    type => "honeypot"
    start_position => "beginning"
  }
}

filter {
  if [type] == "honeypot" {
    grok {
      match => {
        "message" => "%{TIMESTAMP_ISO8601:timestamp} %{LOGLEVEL:level} %{GREE
      }
    }
    # GeoIP bidez erasotzailearen kokapena gehitu
    geoip {
      source => "[src_ip]"
    }
  }
}

output {
  elasticsearch {
    hosts => ["http://elasticsearch:9200"]
    index => "honeypot-%{+YYYY.MM.dd}"
  }
}
```

14.7 Alerta Logika — Python

```
# Honeypot Alerta Sisteman — Elasticsearch bidez

import elasticsearch

es = elasticsearch.Elasticsearch(['http://elasticsearch:9200'])

def check_threshold():
    """Azken orduan 100 eraso baino gehiago badaude, alerta bidali."""
    query = {
        "query": {
            "range": {
                "@timestamp": {
                    "gte": "now-1h"
                }
            }
        }
    }

    result = es.search(index="honeypot-*", body=query)

    if result['hits']['total']['value'] > 100:
        send_alert("Eraso bolumen altua honeypot-ean detektatu da")

def generate_daily_report():
    """Eguneroko txostena sortu."""
    report = {
        "data":           datetime.now().strftime("%Y-%m-%d"),
        "eraso_kopurua":  count_total_attacks(),
        "eraso_motak":    count_by_type(),
        "iturri_nagusiak": get_top_sources(),
        "malware":        get_malware_samples()
    }
    save_report(report)
```

14.8 Segurtasun Neurriak eta Lege-betetzea

Neurria	Deskribapena
Sare Isolazioa	Honeypot-a sare isolatu bereizian (DMZ berezi) — inoiz ez produkzioan
Irteera Trafiko Muga	Irteerako konexioak mugatuta — ez dago lateraleko mugimendurik
Sandbox Izaera	Erasotzaileak ezin du honeypot-etik barne sistemetara saltatu
Dokumentazioa	Honeypot-aren erabilpena eta helburua dokumentatuta
GDPR Betetzea	Honeypot-an bildutako datuak pribatutasun legeen arabera tratatzen dira

14.9 Log Rotazioa eta Babeskopiak

```
# Log Rotazioa (logrotate)
/var/log/honeypot/*.log {
    daily
    rotate 30
    compress
    delaycompress
    missingok
    notifempty
    create 0640 honeypot honeypot
}

# Honeypot Babeskopia
tar -czf honeypot-backup-$(date +%Y%m%d).tar.gz /opt/honeypot/

# SIEM-an gordetako malware laginak berrikusketa forentzikora bidali
docker stats conpot cowrie dionaea
```

ERANSKINA A: KONTROL MATRIX — ISO 27001 / IEC 62443

Kontrol ID	Kontrol Izena	Inplementazio Tresna	Egiaztapen Metodoa	Egoera
A.8.1	Aktiboen Inbentarioa	inventory.txt, machinery_inventory.md	Hilabeteko berrikusketa	✅ Osatuta
A.9.1	Sarbide Kontrola Politika	sop_user_access.md, RBAC	Hiruhilabeteko auditoria	✅ Osatuta
A.9.4	Pribilegio Kudeaketa	UFW, Fail2Ban, auditd	Log analisia	✅ Osatuta
A.10.1	Kriptografia	TLS 1.2/1.3, bcrypt, JWT	Pentesting	✅ Osatuta
A.12.1	Aldaketa Kudeaketa	sop_change_management.md	CAB erregistroak	✅ Osatuta
A.12.3	Babeskopiak	backup-db.sh, 3-2-1 estrategia	Hilabeteko proba	✅ Osatuta
A.12.4	Erregistro eta Monitorizazioa	ELK Stack, Filebeat, Wazuh	SIEM Dashboard	✅ Osatuta
A.12.6	Ahultasun Kudeaketa	sop_patch_management.md, OpenVAS	Astekako eskaneoa	✅ Osatuta
A.13.1	Sare Segurtasuna	NFTables, VLAN, DMZ	Penetration Testing	✅ Osatuta
A.14.2	Garapen Seguruaren Printzipioak	SSDLC, OWASP Top 10	Code Review	✅ Osatuta
IEC 62443-3-3	OT Segurtasun Arkitektura	Purdue Eredua, OT Isolazioa	Sare analisia	✅ Osatuta

ERANSKINA B: SEGURTASUN KONTAKTUAK

Rola	Izena	Helbide Elektronikoa	Telefonoa
CISO	—	ciso@zabala-gailetak.com	+34-XXX-XXX-XXX
DPO	—	dpo@zabala-gailetak.com	—
Segurtasun Taldea	—	security@zabala-gailetak.com	#security-alerts (Slack)
IT Arduraduna	—	it@zabala-gailetak.com	—
OT Arduraduna	—	ot@zabala-gailetak.com	—

Dokumentua sortua: 2026-02-22 Hurrengo berrikusketa: 2026-08-22 Zabala Gailetak S.L. — Zibersegurtasun Arkitektura Taldea Dokumentu hau KONFIDENTZIALA da eta barne erabilpenerako soilik da.