Zabala Gailetak - AI Agenteen Testuinguru eta Segurtasun Betekuntza Gida Osoa

Gida oso honek **Zabala Gailetak** proiektuarekin interakzioan ari diren AI agente eta garatzaileentzako testuinguru guztia eskaintzen du, arkitektura, lan-fluxuak eta segurtasun/betekuntza eskakizun xeheak barne.

📋 Eduki-taula

---

1. Proiektuaren ikuspegi orokorra

Zabala Gailetak galleta-fabrika batentzako zibersegurtasun eta azpiegitura-modernizazio proiektu integral bat da. Jatorrian e-commerce plataforma gisa kontzeptuatua, HR Atari Seguru bihurtu da langileen bizitza-ziklo osoa kudeatzeko betekuntza eskakizun zorrotzekin.

- **Testuingurua:** “Erronka 4” - Sistema Aurreratuak (Euskadi FP Erronka).
- **Helburu nagusia:** IT/OT azpiegitura modernizatzea segurtasun garrantzi handiarekin (ISO 27001:2022, GDPR, IEC 62443) eta barne-kudeaketa sistema seguru bat eraikitzea.
- **Dokumentazioaren hizkuntza:** Dokumentazio nagusia **gaztelaniaz** eta **euskaraz** dago. Iruzkin teknikoak eta kodea **ingelesaz** daude.
- **Denbora-lerroa:** 2026eko urtarrila - 2026eko abendua.
- **Egoera aktuala (2026 otsaila):** Azpiegitura martxan, autentikazio nukleoa inplementatuta, segurtasun-monitoreo aktiboa.

---

2. Sistema-arkitektura

Sistemak **Zero Trust** arkitektura jarraitzen du IT/OT segmentazio zorrotzarekin eta defentsa-sakon-geruzako segurtasun-geruza.

A. Aplikazio-geruza

- **Backend:** PHP 8.4 REST API garbia (PSR-compliant, framework-rik gabe)
    - **Stack:** Nginx, PostgreSQL 16, Redis 7
    - **Estandarrak:** PSR-1/4 (autoloading), PSR-7 (HTTP), PSR-11 (DI), PSR-15 (middleware)
    - **Segurtasuna:** JWT refresh tokenekin, TOTP MFA, WebAuthn (passkeys), RBAC (5 rol)
    - **Rate Limiting:** Redis-oinarriduna endpointeko mugalaritarekin
    - **Saio-kudeaketa:** Saio-kudeaketa segurua, gailuen hatz-markaketa
- **Web Frontend:** React 18 SPA (`src/web/`)
    - **Build:** Vite 5 (HMR, produkzio-build optimizatuak)
    - **Estiloa:** Styled Components (CSS-in-JS, gai-kontziente)
    - **Egoera:** Context API + hook pertsonalizatuak, SWR zerbitzari-egoerarako
    - **Ezaugarriak:** Langileen CRUD, Oporren Egutegia, Dokumentu-kudeaketa, Txat erreala (WebSocket)
- **Mobile App:** Android natiboa (`android-app/` - momentu honetan plangintzan)
    - **Stack:** Kotlin 2.0, Jetpack Compose, Material 3 Design
    - **DI:** Hilt (konpilazio-denborako dependency injection)
    - **Sarea:** Retrofit + OkHttp ziurtagiri-pinning-arekin
    - **Arkitektura:** Clean Architecture + MVI pattern

B. Azpiegitura-geruza (`infrastructure/`)

- **Sare-segmentazioa:** VLANak firewall arau zorrotzekin
    - VLAN 10: Kudeaketa (sarbide mugatua)
    - VLAN 20: IT/Enpresa aplikazioak
    - VLAN 30: DMZ (publikoari begirako zerbitzuak)
    - VLAN 50: OT/Industriala (airez IT-tik banatua)
- **Karga-orekatzea:** HAProxy osasun-egiaztapenekin eta SSL terminazioarekin

- **Kontainer Orkestrazioa:** Docker Compose (dev), Kubernetes (produkziorako planifikatua)

C. OT (Operational Technology) (`infrastructure/ot/`)

- **Simulazioa:** Galleta-ekoizpen lerroa (demo helburuetarako)
- **Stack:** OpenPLC (Structured Text IEC 61131-3), ScadaBR (HMI), Node-RED
- **Sarea:** VLAN 50 isolatua IEC 62443-compliant segurtasun-guneekin
- **Segurtasuna:** Conpot honeypots, Modbus IDS, norabide-bakarreko data diode
- **Betekuntza:** SL 2 (Security Level 2) SL 3-ra bideratuta sistema kritikoentzako

D. Segurtasun-geruza (`security/`)

- **SIEM:** ELK Stack + Wazuh log agregaziorako eta mehatxu-detekziorako
- **Honeypots:** T-Pot/Cowrie mehatxu-inteligentziarako
- **Forensika:** Toolkit Volatility, Autopsy, YARA araulekin
- **Penetration Testing:** Ebaluazio periodikoak OWASP ZAP, Burp Suite, Metasploit-ekin

---

3. Direktorio-egitura

```
/home/kalista/erronkak/erronka4/
├── Zabala Gailetak/
│   ├── hr-portal/                    # Aplikazio nagusia (PHP)
│   │   ├── src/                      # Backend iturburua (Controllers, Models, Servi
│   │   ├── public/                   # Web erroa (index.php, assets, views)
│   │   │   ├── views/                # PHP SSR templates (auth, dashboard, employees
│   │   │   └── assets/               # CSS, JS, images, vendor libs (Bootstrap)
│   │   ├── config/                   # Aplikazio-konfigurazioa
│   │   ├── migrations/               # SQL datu-base migrazioak
│   │   ├── scripts/                  # CLI scriptak (migrate, seed)
│   │   ├── tests/                    # PHPUnit testak
│   │   ├── storage/                  # Fitxategi-igoerak, cache
│   │   └── logs/                     # Aplikazio-logak
│   ├── android-app/                  # Android app natiboa (Kotlin)
│   ├── tests/                        # Test Suite-ak
│   │   ├── e2e/                      # Playwright end-to-end testak
│   │   └── load/                     # K6 errendimendu testak
│   ├── compliance/                   # Betekuntza Dokumentazioa
│   │   ├── gdpr/                     # GDPR betekuntza docs
│   │   ├── sgsi/                     # ISO 27001 ISMS dokumentazioa
│   │   ├── iec62443/                 # IEC 62443 industrial security
│   │   └── nis2/                     # NIS2 direktiba betekuntza
│   ├── security/                     # Segurtasun Tresnak eta Logak
│   │   ├── siem/                     # ELK Stack + Wazuh konfigurazioak
│   │   ├── honeypot/                 # T-Pot deployment scriptak
```

```
│   │   ├── forensics/              # Tresna forensikoak eta txostenak
│   │   ├── pentesting/             # Penetration test txostenak
│   │   ├── incidents/              # Gertaera-erantzun logak
│   │   └── audits/                 # Segurtasun audit trail-ak
│   ├── infrastructure/             # Azpiegitura kode gisa
│   │   ├── network/                # Sare topologia eta konfigurazioak
│   │   ├── systems/                # Sistema arkitektura diagramak
│   │   └── ot/                     # Operational Technology konfigurazioa
│   │       ├── openplc/            # PLC programak (Structured Text)
│   │       └── simulations/        # HMI eta prozesu simulazioak
│   ├── nginx/                      # Nginx konfigurazioa
│   └── docs/                       # Dokumentazio gehigarria
│       └── network_diagrams/       # Sare topologia bisualak
├── scripts/                        # Utilitate Scriptak
│   └── verify_implementation.sh    # Betekuntza egiaztapen scripta
├── archive/                        # Artxibatutako migrazio docs
├── ER4.md                          # Erronka Akademikoaren Eskakizun Nukleoak
├── API_DOCUMENTATION.md            # REST API Erreferentzia
└── AGENTS.md                       # Fitxategi hau (Gida Osoa)
```

---

4. Garapenaren lan-fluxua

Frontend Garapena (React SPA)

- **Kokapena:** `Zabala Gailetak/src/web/`
- **Komandoak:**
  - `npm install` - Dependentziak instalatu
  - `npm run dev` - Vite dev server abiarazi (HMR gaituta, 5173 portua)
  - `npm run build` - Produkzio-build (minified, tree-shaken)
  - `npm run preview` - Produkzio-build aurreikusi
  - `npm run lint` - ESLint React/segurtasun araulekin
  - `npm run format` - Prettier kode-formatzea

Backend Garapena (PHP API - Garabidean)

- **Kokapena:** `Zabala Gailetak/src/api/` (planifikatua)
- **Egoera aktuala:** Backend legacy egituratik migratzen
- **Etorkizuneko komandoak:**
  - `composer install` - PHP dependentziak instalatu
  - `php artisan serve` edo Nginx konfigurazioa local dev-rako
  - `vendor/bin/phpunit` - Unit testak exekutatu (PHPUnit)
  - `vendor/bin/phpcs` - Kode-estilo egiaztapena (PSR-12)

    - Datu-base migrazioak migrazio sistema pertsonalizatuaren bidez

Testak

- **E2E Testak:** `Zabala Gailetak/tests/e2e/`
    - Playwright testak web fluxuetarako
    - Komandoa: `npx playwright test`
- **Load Testing:** `Zabala Gailetak/tests/load/`
    - K6 errendimendu testak
    - Komandoa: `k6 run load_test.js`

Azpiegitura eta Segurtasuna

- **SIEM:** `security/siem/` - ELK Stack + Wazuh
    - Sarbidea: Kibana dashboard 5601 portuan
- **Honeypot:** `security/honeypot/` - T-Pot/Cowrie
    - DMZ sare segmentu isolatuan deployment-atua
- **OT Simulazioa:** `infrastructure/ot/`
    - OpenPLC runtime 8080 portuan
    - ScadaBR HMI 9090 portuan

---

5. Segurtasun eta Betekuntza Ikuspegi Orokorra

KRITIKOA: Proiektu hau segurtasun ikuskizun integral bat da. Kode, konfigurazio eta dokumentazio guztiak zorrotz bete behar ditu:

A. ISO 27001:2022 - Informazio Segurtasunaren Kudeaketa Sistema (ISMS)

- **Inplementazio tasa:** 87/93 kontrolak (%93 betekuntza)
- **Egoera:** Annex A kontrolak 8. atalean xehetuak
- **Eskakizun garrantzitsuak:**
    - Aktuen inbentarioa eta sailkapena (A.5.9, A.5.12)
    - Sarbide-kontrola eta identitate-kudeaketa (A.5.15-5.18)
    - Gertaera-kudeaketa prozedurak (A.5.24-5.28)
    - Enpresa-jarraibidearen plangintza (A.5.29-5.30)
    - Segurtasun audit eta berrikuspen periodikoak (A.5.35)

B. GDPR (General Data Protection Regulation)

- **Datu-babesaren printzipioak:** Legalitatea, helburu-muga, datu-minimizazioa, zehaztasuna, biltegiratze-muga, osotasuna
- **Oinarri legalak:** Onespena, kontratua, lege-betekuntza, interes legitimoak
- **Datu-subjektuen eskubideak:** Sarbidea, zuzenketa, ezabaketa (“ahazteko eskubidea”), portablezia, aurkaritza
- **Eskakizun garrantzitsuak:**
  - Diseinuko eta lehenetsitako pribatutasuna
  - Datu-babesaren eragin-ebaluazioak (DPIA)
  - 72 orduko haustura-ohartarazpena
  - Prozesamendu-jardueren erregistroak (RoPA)
  - Datu-babeseko arduradunaren (DPO) izendapena

C. IEC 62443 - Industrial Control Systems Security

- **Helburuko segurtasun-maila:** SL 2 (une honetan), SL 3 (sistema kritikoentzako)
- **Gune/Hodi Eredua:** IT eta OT arteko sare-segmentazio zorrotza
- **Eskakizun garrantzitsuak:**
  - Sare-segmentazioa eta firewalling (SR 5.1, SR 5.2)
  - Autentikazioa eta baimentzea (SR 1.1, SR 1.2, SR 2.1)
  - Kode maltzurren babesa (SR 3.1)
  - Audit log eta monitoreoa (SR 6.1, SR 6.2)
  - Garapen-bizitza ziklo segurua (IEC 62443-4-1)

D. OWASP Top 10 (2021)

- A01: Broken Access Control → RBAC inplementazioa 5 rolekin
- A02: Cryptographic Failures → TLS 1.3, AES-256-GCM at rest
- A03: Injection → Parameterized queries, input validation
- A04: Insecure Design → Threat modeling design fasean
- A05: Security Misconfiguration → Automated security scanning (SonarQube)
- A07: Authentication Failures → JWT + TOTP MFA + WebAuthn
- A08: Software/Data Integrity → SRI, dependency scanning (npm audit, Snyk)
- A09: Logging/Monitoring Failures → Centralized SIEM (ELK + Wazuh)

Betekuntza Egiaztapena: Exekutatu `./scripts/verify_implementation.sh` betekuntza egiaztapen automatizatuak egiteko.

---

6. Inplementazioaren Egoera (2026 otsaila)

✅ Bukatua (Produkzio-prest)

- **Azpiegitura:**
  - Sare-segmentazioa (4 VLAN firewall araulekin)
  - Docker kontainerizazioa zerbitzuetarako
  - PostgreSQL 16 datu-base eskema
  - Redis 7 cache eta rate limiting-erako
- **Segurtasun oinarria:**
  - JWT autentikazioa refresh tokenekin
  - RBAC 5 rolekin (ADMIN, RRHH_MGR, JEFE_SECCION, EMPLEADO, AUDITOR)
  - TOTP MFA inplementazioa (RFC 6238 compliant)
  - TLS 1.3 enkriptazioa trafiko guztirako
  - SIEM deployment (ELK + Wazuh)
- **Dokumentazioa:**
  - API dokumentazioa (REST endpoint-ak)
  - Sare topologia diagramak
  - ISO 27001 ISMS dokumentazioa (87/93 kontrol)
  - GDPR betekuntza erregistroak (RoPA)

🚧 Garabidean (Garapen Aktiboa)

- **Aplikazio-ezaugarriak:**
  - Langileen kudeaketa CRUD (%80 bukatua)
  - Oporren eskaera sistema onarpen-workflow-arekin (%60)
  - Dokumentu-kudeaketa enkriptazioarekin (%40)
  - Txat erreala WebSocket bidez (%30)
- **Segurtasun aurreratua:**
  - WebAuthn (passkeys) integrazioa (%70)
  - Forensika analisi toolkit-aren finetzea (%50)
  - Honeypot tuning eta mehatxu-inteligentzia (%60)

📋 Hurrengo pausoak (2026 Q2)

- **Testak eta Baliozkotzea:**

    - Load testing K6-arekin (helburua: 1000 erabiltzaile aldi berean)
    - E2E testing Playwright-ekin (estaldura > %80)
    - Penetration testing (barne-ebaluazioa)
- **OT Integrazioa:**
    - OpenPLC galleta-ekoizpen simulazioa amaitzea
    - Norabide-bakarreko data diode inplementatzea OT telemetriarako
    - Conpot honeypots deployment-atzea OT zonan
- **Betekuntza:**
    - ISO 27001 kontrol geratuei amaiera ematea (6 pendiente)
    - Hirugarrenen audit prestatzea
    - DPIA ezaugarri berrientzako

⏳ Planifikatua (2026 Q3-Q4)

- **Aplikazio Mugikorra:** Android app natiboa biometriko autentikazioarekin
- **Analitika Aurreratua:** Langileen errendimendu dashboard-ak
- **Backup eta DR:** Automatizatutako hondamen-berrespen testak
- **Ziurtagiritzea:** ISO 27001 kanpo-audit

---

7. AI Agenteen Gidalerroak

A. Testuinguru-kudeaketa

- **Egia-iturria:** Dokumentu honek (AGENTS.md) testuinguru arkitektoniko eta segurtasun/betekuntza eskakizun guztiak ditu.
- **API Erreferentzia:** Begiratu `API_DOCUMENTATION.md` REST endpoint especifikazio eta autentikazio fluxuetarako.
- **Migrazio Historia:** `archive/migration/` artxibatutako migrazio docs erreferentziarako soilik.

B. Segurtasun-lehenengo Garapena

- **Inoiz ez Bypass Security:** Ez iradoki autentikazioa, baimentzea edo enkriptazioa zirkulbuitzen duen koderik.
- **Balioztatu Segmentazioa:** Ziurtatu IT/OT banaketa mantentzen dela (konexiorik ez VLAN 20 eta 50 artean).
- **Datu-minimizazioa:** Iradoki soilik beharrezkoak diren datuak biltzea/biltzea ezaugarriarentzako.

- **Input Baliozkotzea:** Balioztatu eta garbitu beti erabiltzailearen inputa (erabili parameterized queries, escaping, type checking).
- **Secure Defaults:** Hobetsi secure-by-default konfigurazioak (adib. HTTPS soilik, strict CSP headers, HttpOnly cookies).

C. Kode-kalitatearen Estandarrak

- **PHP Backend:** PSR-1/PSR-4/PSR-12 betekuntza derrigorrezkoa. Framework-ik gabe (PSR inplementazio pertsonalizatua).
- **PHP Frontend (SSR):** View template garbiak, Bootstrap 5 komponenteak, progresiboa hobetzea.
- **Iruzkinak:** Erabili ingelesa iruzkin teknikoetarako. Gaztelania/euskara soilik erabiltzaileari begirako string-etan.
- **Testak:** Iradoki unit testak (PHPUnit, Jest) eta E2E testak (Playwright) ezaugarri berrientzako.

D. Hizkuntza-bikoteketa eta Kontzientzia Kulturala

- **Hizkuntza nagusiak:** Dokumentazioa gaztelaniaz edo euskaraz egon daiteke. Biak irakurtzeko prest egon.
- **Output Teknikoa:** Esplikazio teknikoak ingelesez eman, bestela esplizituki eskatuta ez bada.
- **Erabiltzaileari begirako edukia:** Errespetatu eskakizun elebidunak (es-ES eta eu-ES) UI string-entzako.
- **Testuinguru kulturala:** Euskal Herriko FP heziketa-profesionaleko proiektua identitate regional sendoarekin.

E. Fitxategi-bideen Zehaztasuna

- **Proiektuaren erroa:** `/home/kalista/erronkak/erronka4/`
- **Kode-base aktiboa:** `Zabala Gailetak/hr-portal/` (PHP aplikazio nagusia)
- **Inoiz ez Suposizioak:** Erabili beti bide absolutuak edo berretsi uneko lan-direktorioa fitxategi eragiketak egin aurretik.

F. Betekuntza Egiaztapena

- **Commit egin aurretik:** Exekutatu `./scripts/verify_implementation.sh` betekuntza egoera egiaztatzeko.
- **Dokumentazioaren Eguneraketak:** Eguneratu dagokion betekuntza docs (SOA, RoPA, risk register) ezaugarriak gehitzean.
- **Audit Trail:** Log egindako aldaketa garrantzitsuak `security/audits/` trazabilitaterako.

G. Errore-kudeaketa eta Debug

- **Log Xehea:** Iradoki logging egituratua (JSON formatua) larritasun-mailekin.
- **Daturik ez Logetan:** Inoiz ez logeatu pasahitzak, token-ak, PII edo gako kriptografikoak.
- **Degradazio Graziosoa:** Ziurtatu zerbitzuek modu seguruan huts egitea (adib. ukatu sarbidea auth huts egitean, ez eman).

---

8. Betekuntza Eskakizun Xeheak

🔒 Segurtasun eta Betekuntza Eskakizunak

Informazio Segurtasunaren Kudeaketa Sistema (ISO 27001:2022)

SOA (Statement of Applicability) oinarrituz, Zabala Gailetak-ek 93tik 87 ISO 27001:2022 kontrol inplementatzen ditu (%93 betekuntza tasa):

ISMS Osagai Nukleoak:

- **Informazio Segurtasunaren Politikak**: Segurtasun politikak esparru guztietarako
- **Informazio Segurtasunaren Antolaketa**: Rolak, erantzukizunak eta agintariak
- **Giza Baliabideen Segurtasuna**: Langileen azterketa, prestakuntza eta amaiera prozedurak
- **Aktuen Kudeaketa**: Aktuen erregistroa, sailkapena eta kudeaketa prozedurak
- **Sarbide-kontrola**: Enpresa-eskakizunak, erabiltzaile-sarbide kudeaketa, erabiltzaile-erantzukizunak
- **Kriptografia**: Kontrol kriptografikoen erabileraren politika
- **Fisiko eta Ingurumen Segurtasuna**: Eremu seguruak, ekipoen segurtasuna
- **Eragiketa Segurtasuna**: Eragiketa prozedurak, malwarearen aurkako babesa, backup prozedurak
- **Komunikazio Segurtasuna**: Sare-segurtasun kudeaketa, informazio-transferentzia
- **Sistema Erosketa, Garapen eta Mantentzea**: Segurtasun eskakizunak, garapeneko segurtasuna, hornitzaile-harremanak
- **Hornitzaile-harremanak**: Informazio segurtasuna hornitzaile-hitzarmenetan
- **Informazio Segurtasun Gertaeren Kudeaketa**: Txostena, ebaluazioa, erantzuna, ikaskuntza
- **Enpresa-jarraibidearen Informazio Segurtasun Ikuspegiak**: Jarraibide-plangintza, erredundantziak
- **Betekuntza**: Legezko, arauzko eta kontrataziozko eskakizunekin betekuntza

Beharrezko Kontrolak (Annex A) - Inplementazio Egoera:

A.5 Kontrol Organizatiboak (37 kontrol - %100 inplementatua)

- **A.5.1 Information security policies** ✅
- **A.5.2 Information security roles and responsibilities** ✅
- **A.5.3 Segregation of duties** ✅
- **A.5.4 Management responsibilities** ✅
- **A.5.5 Contact with authorities** ✅
- **A.5.6 Contact with special interest groups** ✅
- **A.5.7 Threat intelligence** ✅
- **A.5.8 Information security in project management** ✅
- **A.5.9 Inventory of assets** ✅
- **A.5.10 Acceptable use of information and other associated assets** ✅
- **A.5.11 Return of assets** ✅
- **A.5.12 Classification of information** ⚠️ Partzialki inplementatua
- **A.5.13 Labelling of information** ⚠️ Partzialki inplementatua
- **A.5.14 Information transfer** ✅
- **A.5.15 Access control** ✅
- **A.5.16 Identity management** ✅
- **A.5.17 Authentication information** ✅
- **A.5.18 Access rights** ✅
- **A.5.19 Information security in supplier relationships** ✅
- **A.5.20 Addressing information security within supplier agreements** ✅
- **A.5.21 Managing information security in the ICT supply chain** ✅
- **A.5.22 Monitoring, review and change management of supplier services** ✅
- **A.5.23 Information security for use of cloud services** ✅
- **A.5.24 Information security incident management planning and preparation** ✅
- **A.5.25 Assessment and decision on information security events** ✅
- **A.5.26 Response to information security incidents** ✅
- **A.5.27 Learning from information security incidents** ✅
- **A.5.28 Collection of evidence** ✅
- **A.5.29 Information security during disruption** ✅
- **A.5.30 ICT readiness for business continuity** ✅
- **A.5.31 Legal, statutory, regulatory and contractual requirements** ✅
- **A.5.32 Intellectual property rights** ✅

- **A.5.33 Protection of records ✅**
- **A.5.34 Privacy and protection of PII ✅**
- **A.5.35 Independent review of information security ✅**
- **A.5.36 Compliance with policies and standards of information security ✅**
- **A.5.37 Documented operating procedures ✅**

A.6 Pertsonen Kontrolak (8 kontrol - %100 inplementatua)

- **A.6.1 Screening ✅**
- **A.6.2 Terms and conditions of employment ✅**
- **A.6.3 Information security awareness, education and training ✅**
- **A.6.4 Disciplinary process ✅**
- **A.6.5 Responsibilities after termination or change of employment ✅**
- **A.6.6 Confidentiality or non-disclosure agreements ✅**
- **A.6.7 Remote working ✅**
- **A.6.8 Information security event reporting ✅**

A.7 Kontrol Fisikoak (14 kontrol - %100 inplementatua)

- **A.7.1 Physical security perimeter ✅**
- **A.7.2 Physical entry controls ✅**
- **A.7.3 Securing offices, rooms and facilities ✅**
- **A.7.4 Physical security monitoring ✅**
- **A.7.5 Protecting against physical and environmental threats ✅**
- **A.7.6 Working in secure areas ✅**
- **A.7.7 Clear desk and clear screen policy ⚠️** Partzialki inplementatua
- **A.7.8 Equipment siting and protection ✅**
- **A.7.9 Security of assets off-premises ✅**
- **A.7.10 Storage media ✅**
- **A.7.11 Supporting utilities ✅**
- **A.7.12 Cabling security ✅**
- **A.7.13 Equipment maintenance ✅**
- **A.7.14 Secure disposal or re-use of equipment ✅**

A.8 Kontrol Teknologikoak (34 kontrol - %94 inplementatua)

- **A.8.1 User endpoint devices ✅**
- **A.8.2 Privileged access rights ✅**

- **A.8.3 Information access restriction** ✅
- **A.8.4 Access to source code** ✅
- **A.8.5 Secure authentication** ✅
- **A.8.6 Capacity management** ✅
- **A.8.7 Protection against malware** ✅
- **A.8.8 Management of technical vulnerabilities** ✅
- **A.8.9 Configuration management** ✅
- **A.8.10 Information deletion** ✅
- **A.8.11 Data masking** ⚠️ Partzialki inplementatua
- **A.8.12 Data leakage prevention** ⚠️ Partzialki inplementatua
- **A.8.13 Information backup** ✅
- **A.8.14 Redundancy of information processing facilities** ⚠️ Partzialki inplementatua
- **A.8.15 Logging** ✅
- **A.8.16 Monitoring activities** ✅
- **A.8.17 Clock synchronization** ✅
- **A.8.18 Use of privileged utility programs** ✅
- **A.8.19 Installation of software on operational systems** ✅
- **A.8.20 Network security** ✅
- **A.8.21 Security of network services** ✅
- **A.8.22 Segregation of networks** ✅
- **A.8.23 Web filtering** ✅
- **A.8.24 Use of cryptography** ✅
- **A.8.25 Secure development lifecycle** ✅
- **A.8.26 Application security requirements** ✅
- **A.8.27 Secure system engineering principles** ✅
- **A.8.28 Secure coding** ✅
- **A.8.29 Security testing in development and acceptance** ✅
- **A.8.30 Outsourced development** ✅
- **A.8.31 Separation of development, test and production environments** ✅
- **A.8.32 Change management** ✅
- **A.8.33 Test information** ✅
- **A.8.34 Protection of information systems during audit testing** ✅

Datuen Babeserako Araudi Orokorraren (GDPR) Betekuntza

Datu-babesaren Printzipioak:

- **Legalitatea, Zuzenketa eta Gardentasuna**: Prozesamendua legala, zuzena eta gardena izan behar da
- **Helburu-muga**: Zehaztutako, esplizitu eta legitimo helburuetarako bildua
- **Datu-minimizazioa**: Egokia, garrantzitsua eta beharrezkoarekin mugatua
- **Zehaztasuna**: Zehatza eta eguneratua
- **Biltegiratze-muga**: Identifikaziorako aukera ematen duen forman soilik beharrezko den bitartean mantentzen da
- **Osotasuna eta Konfidentzialtasuna**: Behar bezala babestuta prozesatzen da
- **Erantzukizuna**: Kontroladorea betekuntzarekin erantzulea eta betekuntza frogatzeko gaitasuna

Prozesamendurako Oinarri Legalak:

- **Onespena**: Norbanakoak onespen argia eman du
- **Kontratua**: Kontratuaren betearritzea beharrezkoa den prozesamendua
- **Lege-betekuntza**: Lege-betekuntzarekin betearritzea beharrezkoa den prozesamendua
- **Interes Vitalak**: Interes vitalak babestea beharrezkoa den prozesamendua
- **Zeregin Publikoa**: Interes publikoko zeregina betearritzea beharrezkoa den prozesamendua
- **Interes Legitimoak**: Interes legitimoak beharrezkoa den prozesamendua (gainidatzi ez bada)

Datu-subjektuen Eskubideak:

- **Informazio-eskubidea**: Prozesamenduari buruzko informazio gardena
- **Sarbide-eskubidea**: Datu pertsonalak prozesatzen diren baieztapena, datuetarako sarbidea
- **Zuzenketa-eskubidea**: Datu pertsonal zehatzagabeen zuzenketa
- **Ezabaketa-eskubidea (“ahazteko eskubidea”)**: Zirkunstantzia jakin batzuetan datu pertsonalen ezabaketa
- **Prozesamendu-mugaketa-eskubidea**: Zirkunstantzia jakin batzuetan prozesamenduaren mugaketa
- **Portabletasun-eskubidea**: Datu pertsonalak jasotzea eta zerbitzuen artean berrerabiltzea
- **Aurkaritza-eskubidea**: Interes legitimoetan edo marketin zuzenan oinarritutako prozesamenduari aurka egitea
- **Erabaki Automatizatuei Buruzko Eskubideak**: Eragin nabarmenak dituzten erabaki automatizatuei ez azaldua izatea

Datu-babesaren Eragin-ebaluazioa (DPIA):

- Prozesamendu jarduera arriskutsuentzako beharrezkoa
- Prozesatu aurretik egin behar da
- Beharraren eta proportzioaren ebaluazioa
- Eskubide eta askatasunen aurkako arriskuak kontuan hartu
- Arriskuak tratatzeko neurriak identifikatu
- Behar izanez gara agintasun gainbegiratzailearekin kontsultatu

Datu-hausteraren Ohartarazpena:

- 72 orduetan ohartarazi agintasun gainbegiratzaileri hausturaren berri izan ondoren
- Eskubide eta askatasunen aurkako arriskua dagoenean norbanakoei komunikatu
- Dokumentatu haustura guztiak hausturarekin lotutako datuekin, efektuak, hartutako ekintza zuzentzaileak
- Mantendu hausturen erregistroa

Datu-babeseko Arduraduna (DPO):

- Eskubide eta askatasunen aurkako arrisku handia sortuko duen prozesamenduan izendatua
- Datu-babesaren lege eta praktiketan aditua
- Datu-babesarekin lotutako gai guztietan parte hartzen du
- Zuzenean kudeaketa-maila altuenari txostenak egiten dizkio
- Agintasun gainbegiratzaileren eta datu-subjektuen kontaktu-puntua

Prozesamendu-jardueren Erregistroak:

- Kontroladore eta prozesadore guztiek mantentzen dute
- Prozesamenduaren helburuak, datu-subjektuen kategoriak eta datu pertsonalak barne
- Hartzaileak edo hartzaileen kategoriak
- Hirugarren herrialdeetara transferentziak eta babes-neurriak
- Retentzio-epeAK
- Neurri tekniko eta antolakuntzako segurtasun-neurriak

Diseinuko eta Lehenetsitako Datu-babesa:

- Datu-babesaren printzipioak prozesamenduan integratuta
- Bideen zehaztapeneko eta prozesamenduko denboran
- Neurri tekniko eta antolakuntzako egokiak inplementatuta
- Helburu jakin bakoitzeko beharrezkoak diren datu pertsonalak soilik prozesatzen dira
- Datu-babesa bizitza-ziklo osoan zehar

Prozesamendu-jarduerak (Prozesamendu-erregistroetatik):

1. **Bezeroen Kudeaketa**: Eskaerak prozesatzea, fakturazioa, bidalketa, lealtasun-programak
2. **Giza Baliabideak**: Nomina, kontratuak, laneko osasuna
3. **Bideokontrola**: Instalazioen segurtasun-monitoreoa

IEC 62443 Industria Automatizazio eta Kontrol-sistemen Segurtasuna

Segurtasun-mailak:

- **SL 0**: Segurtasun eskakizun espezifikorik gabe
- **SL 1**: Hutsegite akatsen edo nahigabeko urraketen prebentzioa
- **SL 2**: Baliabide baxuko modu sinpleekin urraketa nahita egitearen prebentzioa
- **SL 3**: Baliabide moderatuko modu sofistikatuak erabiliz urraketa nahita egitearen prebentzioa
- **SL 4**: Baliabide hedatuko modu sofistikatuak erabiliz urraketa nahita egitearen prebentzioa

IEC 62443-3-3: Sistema Segurtasun Eskakizunak eta Segurtasun-mailak:

- **SR 1.1: Identification and Authentication Control (IAC)**: Erabiltzaile gizakien identifikazioa eta autentikazioa
- **SR 1.2: Identification and Authentication Control (IAC)**: Software prozesu eta gailuen identifikazioa eta autentikazioa
- **SR 2.1: Use Control (UC)**: Baimen betearpena
- **SR 2.2: Use Control (UC)**: Wireless erabilera kontrola
- **SR 2.3: Use Control (UC)**: Gune-mugen babesa
- **SR 2.4: Use Control (UC)**: Gailu-baliabdeen babesa
- **SR 3.1: System Integrity (SI)**: Kode maltzurren babesa
- **SR 3.2: System Integrity (SI)**: Memoriaren babesa
- **SR 3.3: System Integrity (SI)**: Serializing
- **SR 3.4: System Integrity (SI)**: Domeinu-isolamendua
- **SR 3.5: System Integrity (SI)**: Sarbide-puntuen babesa
- **SR 4.1: Data Confidentiality (DC)**: Datuen konfidentzialtasuna
- **SR 4.2: Data Confidentiality (DC)**: Gako kriptografikoen kudeaketa
- **SR 4.3: Data Confidentiality (DC)**: Komunikazioen konfidentzialtasuna
- **SR 5.1: Restricted Data Flow (RDF)**: Sare-segmentazioa
- **SR 5.2: Restricted Data Flow (RDF)**: Gune-segmentazioa
- **SR 5.3: Restricted Data Flow (RDF)**: Zereginen bereizketa
- **SR 6.1: Timely Response to Events (TRE)**: Audit log eskuragarritasuna

- **SR 6.2: Timely Response to Events (TRE)**: Auditan jarraipen etengabea
- **SR 7.1: Resource Availability (RA)**: Zerbitzu-ukapenaren babesa

IEC 62443-4-1: Garapen-bizitza Ziklo Seguruaren Eskakizunak:

- **SDLC Eskakizunak**: Sistema-garapenean segurtasun-kudeaketa
- **Patch Kudeaketa**: Segurtasun patch-ak denboran aplikatzea
- **Ahultasunen Kudeaketa**: Ahultasunen identifikazioa eta konponketa
- **Segurtasun Eguneraketak**: Segurtasun eguneraketa eta patch periodikoak
- **Aldaketa-kudeaketa**: Sistema industrialen aldaketa kontrolatuak
- **Konfigurazio-kudeaketa**: Sistema industrialen konfigurazio segurua

Gune eta Hodi Eredua:

- **Guneak**: Segurtasun eskakizun komunak dituzten aktibo logikoki lotutako taldea
- **Hodiak**: Guneen artean komunikazio kontrolatua eskaintzen duten mekanismoak
- **Segurtasun-mailak**: Gune desberdinetarako segurtasun-maila eskakizun desberdinak
- **Azpi-guneak**: Kontrol segurtasun gehigarrirako guneen barruan zatiketa gehiago

Industrial Control System (ICS) Eskakizun Espezifikoak:

- **Eskuragarritasuna**: Sistema kritikoek eskuragarritasuna mantendu behar dute (%99,9+ uptime)
- **Errealitate-denborako Eragiketak**: Segurtasun kontrolek ez dute errealitate-denborako errendimenduan eragin behar
- **Sistema Legatuak**: Sistema industrial legatuen integrazio segurua
- **Operational Technology (OT) Segurtasuna**: OT ingurunetarako segurtasun espezializatua
- **Hornidura-katearen Segurtasuna**: Hornitzaile industrialentzako segurtasun eskakizunak

Sarbide-kontrola eta Autentikazioa

Multi-Factor Authentication (MFA):

- Sarbide urrutiko eta kontu pribilegiatu guztientzako beharrezkoa
- TOTP (Time-based One-Time Password) inplementazioa RFC 6238 betekuntzarekin
- Berrespen-kodeak eta backup autentikazio metodoak
- MFA bypass prebentzioa eta monitoreoa
- Direktorio-zerbitzuekin integrazioa (LDAP/Active Directory)

Role-Based Access Control (RBAC):

- **ADMIN**: Sistema-sarbide osoa, konfigurazio-kudeaketa, erabiltzaile-administrazioa

- **RRHH MGR**: Langileen kudeaketa, onarpenak, txostenak, HR datu-sarbidea
- **JEFE SECCIÓN**: Sailaren talde-kudeaketa, sailaren txostenak
- **EMPLEADO**: Datu pertsonalen sarbidea soilik, auto-zerbitzu funtzioak
- **AUDITOR**: Audit log eta betekuntza txostenak irakurtzeko soilik

Pribilegiatuen Sarbide-kudeaketa:

- Just-in-time sarbidea funtzio administratiboetarako
- Saio-grabazioa eta monitoreoa saio pribilegiatuetarako
- Sarbide-eskubideen deprovisioning automatizatua
- Pribilegio-igoerarako onarpen-workflow-ak
- Denboran oinarritutako sarbide-mugaketak

Datu-sailkapena eta Kudeaketa

Sailkapen-mailak:

- **Publikoa**: Marketin materialak, enpresa informazio orokorra
- **Barnekoa**: Sentikortasunik gabeko enpresa-datuak, barne-komunikazioak
- **Konfidentziala**: Langileen datu pertsonalak, informazio finantzarioa, enpresa-planak
- **Segurua**: Sekretu komertzialak, datu segurtasun kritikoak, PII, erregistro finantzarioak

Datu-kudeaketa Prozedurak:

- **Etiketatzea**: Datu guztiak sailkapenaren arabera etiketatu behar dira
- **Biltegiratzea**: Sailkapenaren arabera biltegiratze-midia egokia
- **Transmisioa**: Transmisio metodo seguruak (enkriptazioa, protokolo seguruak)
- **Suntsipena**: Suntsipen metodo seguruak (enkriptazio-ezabaketa, suntsipen fisikoa)
- **Backup**: Enkriptatutako backup-ak retentzio politikarekin
- **Artxibatzea**: Integritate-babesarekin artxibatze luzea

Enkriptazio Eskakizunak:

- **At Rest**: AES-256-GCM datu sentikor guztien biltegiratzeko
- **In Transit**: TLS 1.3 gutxienez ziurtagiri-oinarridun autentikazioarekin
- **Pasahitzak**: bcrypt cost factor 12+ edo Argon2
- **Gako-kudeaketa**: Hardware Security Modules (HSM) gako kritikoentzako
- **Gako-igorpena**: Enkriptazio-gakoen igorpen automatizatua

Gertaera-erantzuna eta Kudeaketa

Gertaera-erantzun Plana:

1. **Prestakuntza**: Gertaera-erantzun taldea, tresnak, komunikazio-planak
2. **Identifikazioa**: Monitoreo eta txostenaren bidez gertaera-detekzioa
3. **Mugatzea**: Epe laburreko eta luzeko mugatze estrategiak
4. **Desagerraraztea**: Erro-erroa kendu eta errepikapena saihestu
5. **Berrespena**: Sistemak berresartu eta integritatea balioztatu
6. **Ikaskuntzak**: Gertaera-osteko berrikuspena eta prozesu-hobekuntza

Gertaera-sailkapena:

- **Kritikoa**: Sistema osoko kompromisoa, >100 norbanakori eragiten dion datu-haustura
- **Altua**: Sistemaren eten nabarmena, <100 norbanakori eragiten dion datu-haustura
- **Ertaina**: Sistemaren eragin mugatua, segurtasun ahultasun potentziala
- **Baxua**: Segurtasun gertaera txikiak, positibo faltsuak

Erantzun-denborak (ISO 27001 arabera):

- **Kritikoa**: Erantzuna 15 minututan, konponketa 4 orduetan
- **Altua**: Erantzuna ordubeteetan, konponketa 24 orduetan
- **Ertaina**: Erantzuna 4 orduetan, konponketa 72 orduetan
- **Baxua**: Erantzuna 24 orduetan, konponketa aste betean

Evidencia-bilketa eta Jabetza-katea:

- **Evidencia Digitala**: Memoria bolatilak, disko irudiak, sare-logak
- **Dokumentazioa**: Gertaera-kronologia, hartutako ekintzak, bildutako evidencia
- **Jabetza-katea**: Dokumentatu evidencia bildu, manipulatu edo analizatu duena
- **Tresna Forensikoak**: Evidencia bilketa eta analisirako ziurtatutako tresnak

Garapen-bizitza Ziklo Segurua (SSDLC)

Segurtasun Ateak:

1. **Plangintza**: Threat modeling, segurtasun eskakizunen definizioa, arrisku-ebaluazioa
2. **Diseinua**: Arkitektura seguruaren berrikuspena, threat modeling baliozkotzea, segurtasun diseinu pattern-ak
3. **Kodea**: SAST scanning, coding seguruaren praktikak
4. **Testak**: DAST scanning, penetration testing, dependentzia egiaztapenak
5. **Deployment**: Segurtasun konfigurazio baliozkotzea
6. **Eragiketak**: Monitoreo jarraia, ahultasunen kudeaketa, segurtasun eguneraketak

Beharrezko Segurtasun Testak:

- **SAST (Static Application Security Testing)**: SonarQube, Checkmarx, edo baliokidea
- **DAST (Dynamic Application Security Testing)**: OWASP ZAP, Burp Suite
- **SCA (Software Composition Analysis)**: OWASP Dependency Check, Snyk
- **Penetration Testing**: Urteroko kanpo ebaluazioak, hiruhilekotako barne testak
- **Kontainer Segurtasuna**: Irudi scanning Trivy edo Clair-ekin
- **Azpiegitura Kode Gisa Segurtasuna**: Checkov edo Terrascan

Kode-berrikuspen Eskakizunak:

- **Egiaztapen Automatizatuak**: ESLint segurtasun arauak, SonarQube quality gates
- **Eskuzko Berrikuspena**: Segurtasun-fokuko kode-berrikuspen zerrenda
- **Berdinen Berrikuspena**: Aldaketa guztiak garatzaile batek gutxienez berrikusten ditu
- **Segurtasun Txapeldunak**: Aldaketa konplexuetarako segurtasun berrikusle izendatuak

Fisiko eta Ingurumen Segurtasuna

Eremu Seguruak:

- **Datu Zentroak**: Biometriko sarbidea, CCTV zaintza, ingurumen-kontrolak
- **Zerbitzari-gelak**: Sarbide murriztua, su-itzalketa, etenik gabeko energia-hornidura
- **Laneko Estazioak**: Mahai garbiaren politika, pantaila blokeoak, birziklapen prozedura seguruak

Ingurumen-kontrolak:

- **Tenperatura eta Hezetasuna**: Egoera optimoetarako monitoreoa eta alertak
- **Su-detekzioa eta Itzalketa**: FM-200 edo baliokide agente garbiko sistemak
- **Energiaren Babesa**: UPS sistemak fail-over automatikoarekin
- **Erredundantzia**: Backup energia-sorgailuak eta hozketa sistemak erredundanteak

Aktuen Kudeaketa:

- **Aktuen Erregistroa**: Informazio-aktibo guztien inbentorio osoa
- **Aktuen Sailkapena**: Segurtasun sailkapena eta kudeaketa eskakizunak
- **Aktuen Jarraipena**: Mugimendu-jarraipena eta birziklapen prozedura seguruak
- **Gailu Mugikorren Kudeaketa**: MDM politikak enpresa-gailuetarako

Hornitzaile eta Hirugarrenen Arrisku-kudeaketa

Hornitzaile-ebaluazioa:

- **Segurtasun Galdetegiak**: Estandarizatutako segurtasun ebaluazio galdetegiak
- **Egoera-auditak**: Hornitzaile kritikoentzako segurtasun fisiko eta prozesu auditak

- **Kontratazio-eskakizunak**: Segurtasun klauza kontratu guztietan
- **Monitoreo Jarraia**: Hornitzailearen errendimenduaren segurtasun-monitoreo etengabea

Hirugarrenen Sarbidea:

- **Sarbide-berrikuspenak**: Hirugarrenen sarbide-eskubideen berrikuspen periodikoa
- **Monitoreoa**: Hirugarrenen jardueren log eta monitoreoa
- **Amaiera-prozedurak**: Kontratu-amaieran sarbide segurua kentzea
- **Atzeko plano-egiaztapenak**: Sarbide pribilegiatua duten pertsonalentzako segurtasun-klaratzea

Enpresa-jarraibidea eta Hondamen-berrespena

Enpresa-eraginaren Analisia (BIA):

- **Funtzio Enpresarial Kritikoak**: Enpresa-prozesu garrantzitsuen identifikazioa
- **Etete Toleragarriaren Epe Maximoa (MTPD)**: Onartzen den etete maximoa
- **Berrespen-denbora Helburuak (RTO)**: Funtzio kritikoak berresartzeko denbora
- **Berrespen-puntu Helburuak (RPO)**: Onartzen den datu-galera maximoa

Enpresa-jarraibide Plana:

- **Larrialdi-erantzuna**: Hainbat hondamen eszenariorako erantzun prozedura berehalakoak
- **Laneko Antolamendu Alternatiboak**: Lan urrutiko gaitasunak eta prozedurak
- **Komunikazio-plana**: Barne eta kanpo komunikazio prozedurak
- **Plana testatzea**: Jarraibide-planen test eta eguneraketa periodikoa

Hondamen-berrespen Plana:

- **Backup Prozedurak**: Backup periodikoak enkriptazioarekin eta biltegiratze urrunarekin
- **Berrespen Prozedurak**: Sistema berrespeneko urrats-urrats prozedurak
- **Fail-over Sistemak**: Sistema erredundanteak eta fail-over gaitasun automatikoak
- **Testak**: Hondamen-berrespen test eta baliozkotze periodikoa

Betekuntza Monitoreoa eta Txostena

Betekuntza Jarraipen etengabea:

- **Kontrol Automatizatuak**: Kontrol teknikoak etengabe monitoreatzen dira
- **Kontrol Eskuzkoak**: Egiaztapen eta test eskuzko periodikoak
- **Salbuespen-kudeaketa**: Kontrol salbuespenak kudeatzeko prozesua
- **Ekintza Zuzentzaileak**: Betekuntza hutsuneen denboran konponketa

Betekuntza Txostena:

- **Barne-txostena**: Kudeaketa eta batzordeari txosten periodikoak
- **Kanpo-txostena**: Arauz eskatutako erregulazio-txostenak
- **Audit prestatzea**: Kanpo auditetarako dokumentazioa eta evidencia
- **Betekuntza Dashboard**: Betekuntza egoera monitoreo erreala

Audit Independenteak:

- **Audit Barneak**: Hiruhilekotako barne betekuntza ebaluazioak
- **Audit Kanpeak**: Urteroko ISO 27001 ziurtagiri auditak
- **Audit Erregulazioak**: Arau zehatzek eskatutako audita
- **Penetration Testing**: Urteroko kanpo penetration testing

Prestakuntza eta Kontzientziazioa

Segurtasun Kontzientziazio Prestakuntza:

- **Langile Berrien Prestakuntza**: Segurtasun oinarriak onboarding-ean
- **Urteroko Prestakuntza Berrigorria**: Segurtasun kontzientziazio integrala urtero
- **Rol-espezifikoko Prestakuntza**: Segurtasun rolentzako prestakuntza espezializatua
- **Gertaera-erantzun Prestakuntza**: Gertaera-erantzun taldearentzako prestakuntza praktikoa

Prestakuntzaren Efektibitatea:

- **Ezagutza Ebaluazioak**: Prestakuntza aurretiko eta osteeko ebaluazioak
- **Phishing Simulazioak**: Phishing kontzientziazio kanpaina periodikoak
- **Metriken Jarraipena**: Prestakuntza osatze-tasak eta efektibitate neurriak
- **Hobekuntza Jarraia**: Gertaera eta mehatxuetan oinarritutako prestakuntza programa eguneraketak

Arrisku-kudeaketa

Arrisku-ebaluazioaren Metodologia:

- **Aktuen Identifikazioa**: Aktuen inbentorio integrala
- **Mehatxu-identifikazioa**: Uneko eta emergente diren mehatxuak
- **Ahultasunen Ebaluazioa**: Ahultasun tekniko eta antolakuntzakoak
- **Eraginaren Ebaluazioa**: Segurtasun gertaeren eragin enpresariala
- **Arrisku-kalkulua**: Arrisku kuantitatiboaren puntuazioa (Probabilidadea × Eragina)

Arrisku-tratamendua:

- **Arrisku-onarpena**: Arrisku residualen dokumentatutako onarpena
- **Arrisku-mitigazioa**: Arriskua murrizteko kontrolen inplementazioa
- **Arrisku-transferentzia**: Aseguru edo kontrataziozko arrisku-transferentzia
- **Arrisku-saihestea**: Jarduera arriskutsuen ezabatzea

Arrisku-monitoreoa:

- **Arrisku Gako-adierazleak (KRIs)**: Arrisku-mailak monitoreatzeko metrikak
- **Arrisku-txostena**: Kudeaketari arrisku-txosten periodikoak
- **Arrisku-gogaitasuna**: Definitutako arrisku tolerantzia mailak
- **Arrisku-erregistroa**: Arrisku jarraipen eta kudeaketa integrala

---

9. Erreferentzia Azkarra

```
# Aplikazio Garapena
cd "Zabala Gailetak/hr-portal"
composer install                      # PHP dependentziak instalatu
php -S localhost:8080 -t public/      # Dev server lokal abiarazi
vendor/bin/phpunit                    # Unit testak exekutatu
vendor/bin/phpcs                      # Kode-estilo egiaztapena

# Testak
cd "Zabala Gailetak/tests/e2e"
npx playwright test                 # E2E testak exekutatu

cd "Zabala Gailetak/tests/load"
k6 run load_test.js                 # Load testak exekutatu

# Betekuntza Egiaztapena
./scripts/verify_implementation.sh   # ISO 27001 betekuntza egiaztatu

# Segurtasun Zerbitzuak
# SIEM: http://localhost:5601 (Kibana)
# OpenPLC: http://localhost:8080
# ScadaBR: http://localhost:9090
```

Azken eguneraketa: 2026-02-06 | **Bertsioa:** 3.0 (Garbitua eta Kontsolidatua)