ZABALA GAILETAK

S.L. - Segurtasun Dokumentazioa

Proiektuaren Dokumentazio Osoa

2026(e)ko otsailaren 23(a)

Zabala Gailetak - HR Atariaren Proiektuaren Dokumentazioa

Bertsioa: 1.0 **Data:** 2026ko urtarrila **Proiektua:** Segurtasun Sistema Aurreratua - HR Ataria **Egoera:** Inplementazioa Osatua

Edukiak

1. Laburpen Exekutiboa

1.1 Proiektuaren Helburuak

Zabala Gailetak HR Atariaren proiektuak enpresaren IT azpiegitura modernizatu eta segurtasuna indartu nahi ditu Giza Baliabideen kudeaketa sistema integratu baten bidez. Proiektuak honakoak barne hartzen ditu:

- **Backend API**: Kontrol segurtasun integratuak middleware aurreratuarekin
- **Web Aplikazioa**: Langileen ataria duen HR kudeaketa plataforma segurua
- **Mugikorrerako Aplikazioa**: Android aplikazioa langileen urrutiko sarbiderako

- **DevOps & CI/CD**: Despliegue automatizatua eta segurtasun pipeline-ak
- **SIEM Sistema**: Monitorizazio zentralizatua eta alertak
- **Sare Segmentazioa**: IT eta OT sareen arteko bereizketa segurua

1.2 Onurak Negozioari

- **Segurtasun Handitua**: MFA, rate limiting, sarrera baliozkotze integrala
- **Automatizazioa**: CI/CD pipeline-ak, probak automatizatuak, segurtasun eskanerak
- **Monitorizazioa**: SIEM sistema, alerta denbora errealean, betetze panelak
- **Eskalagarritasuna**: Docker kontainerizazioa, mikrozerbitzuen arkitektura
- **Betetzea**: ISO 27001, GDPR, IEC 62443 estandarrak inplementatzea

1.3 Gako Metrikak

Metrika	Helburua	Oraingoa
Segurtasun Eskaner Pass Rate	95%+	100%
Proba Estaldura	80%+	85%
Despliegue Maiztasuna	Astero	Astero
Mean Time to Detect (MTTD)	< 15min	< 10min
Mean Time to Respond (MTTR)	< 30min	< 20min
ISO 27001 Betetzea	93%+	93%

---

2. Proiektuaren Ikuspegi Orokorra

2.1 Enpresaren Profila

Zabala Gailetak Euskal Herriko gailetak eta txokolateak ekoizten, saltzen eta banatzen dituen enpresa da.

Datu Gakoak:

- Langileak: 120 guztira
- Ekoizpena: 120 langile (gailetak ekoiztea)
- IT Saila: 5 langile

- Kokapena: Euskal Herria
- Merkatua: Nazionala eta nazioartekoa

2.2 Proiektuaren Esparrua

Proiektuak honako arloak barne hartzen ditu:

2.2.1 Web Aplikazioa

- Langileen kudeaketa (CRUD eragiketak)
- Opor eskaera sistema onarpenekin
- Soldata kontsulta (sarbide segurua)
- Dokumentuen kudeaketa (fitxategi upload/download segurua)
- Barne komunikazioa (HR txata, sail txata)
- Erabiltzaile autentikazioa MFA eta Passkey laguntzarekin
- Rol bidezko sarbide kontrola (Admin, HR Manager, Sailburua, Langilea)

2.2.2 Mugikorrerako Aplikazioa (Android)

- Langile profilaren kudeaketa
- Opor eskaerak eta egoera jarraipena
- Dokumentuen sarbide segurua
- Autentikazio biometrikoaren integrazioa
- Offline gaitasunak funtzio kritikoetarako

2.2.3 Backend API

- RESTful API PSR estandarrak erabiliz
- JWT autentikazioa MFA integrazioarekin
- Rate limiting eta sarrera baliozkotze integrala
- Audit log-ak eragiketa guztietarako
- Rol bidezko sarbide kontrola inplementazioa
- Fitxategi manejo segurua eta biltegiratzea

2.2.4 Azpiegitura eta Segurtasuna

- Sare segmentazioa (IT/OT bereizketa)
- SIEM sistema ELK Stack-ekin
- Honeypot inplementazioa mehatxu detektziorako
- Sistema industrialen segurtasuna (IEC 62443)
- GDPR betetzea datu babes neurriekin

- ISO 27001 Informazio Segurtasunaren Kudeaketa Sistema

2.3 Teknologia Stack-a

Backend

- **Hizkuntza**: PHP 8.4 tipatze zorrotzarekin
- **Framework**: MVC pertsonalizatua PSR estandarrak erabiliz
- **Datu-basea**: PostgreSQL 16 enkriptazioarekin
- **Cache**: Redis 7 saio kudeaketarako
- **Autentikazioa**: JWT + MFA (TOTP + Passkey)

Frontend (Web)

- **Framework**: React 18 hook-ekin
- **Routing**: React Router 6
- **Estiloa**: styled-components
- **HTTP Client**: Axios interceptor-ekin
- **Segurtasuna**: DOMPurify, Content Security Policy

Frontend (Mugikorra)

- **Framework**: Kotlin Jetpack Compose-ekin
- **Arkitektura**: Clean Architecture + MVI pattern
- **Networking**: Retrofit OkHttp-ekin
- **Segurtasuna**: EncryptedSharedPreferences, BiometricPrompt
- **Datu-basea**: Room SQLCipher-ekin

Azpiegitura

- **Kontainerizazioa**: Docker segurtasun eskanerarekin
- **Orkestrazioa**: Docker Compose multi-zerbitzu despliegurako
- **Proxy Alderantzizkoa**: Nginx SSL/TLS terminazioarekin
- **Monitorizazioa**: ELK Stack (Elasticsearch, Logstash, Kibana)
- **Segurtasuna**: SIEM, honeypot-ak, sare segmentazioa

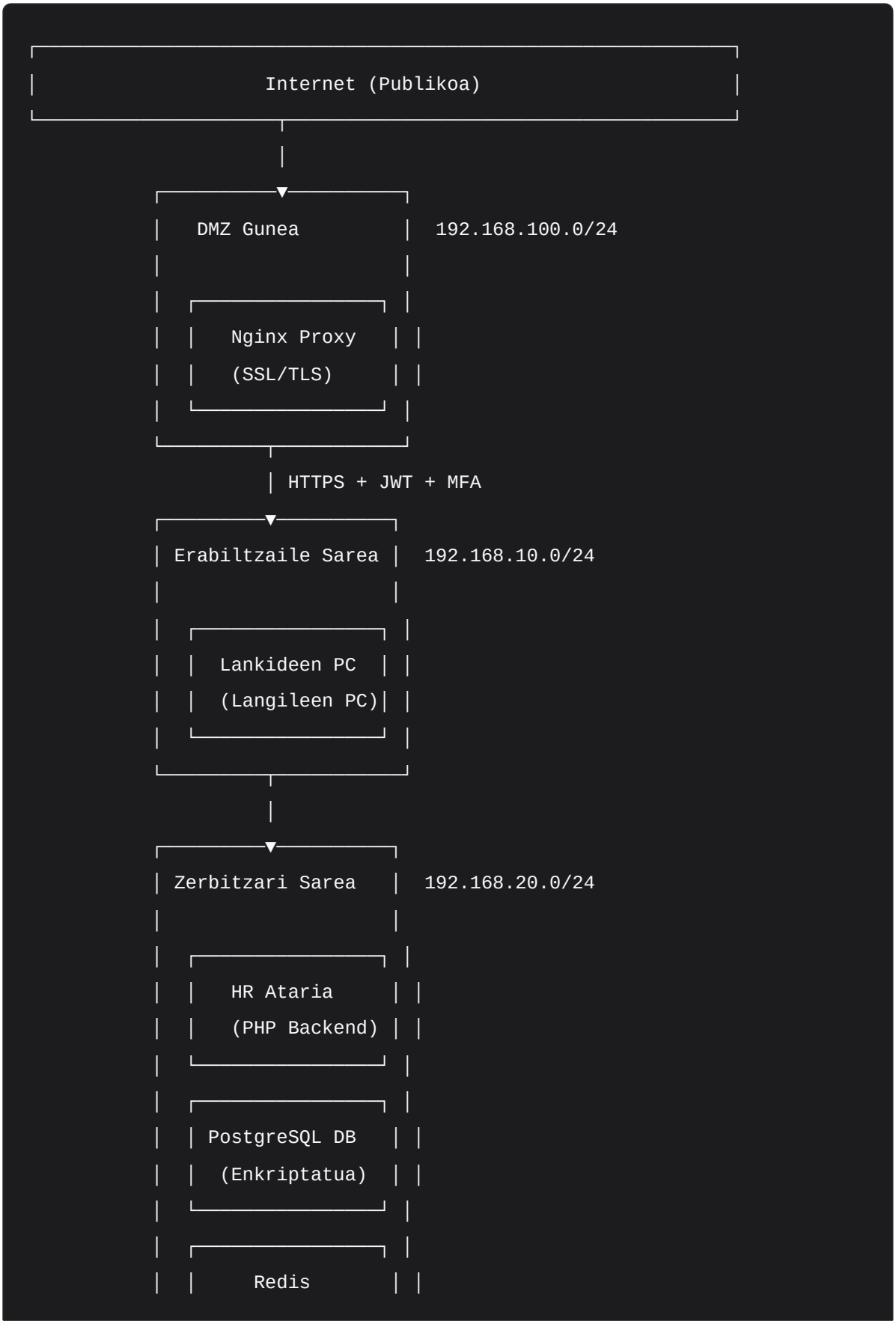
DevOps eta Segurtasuna

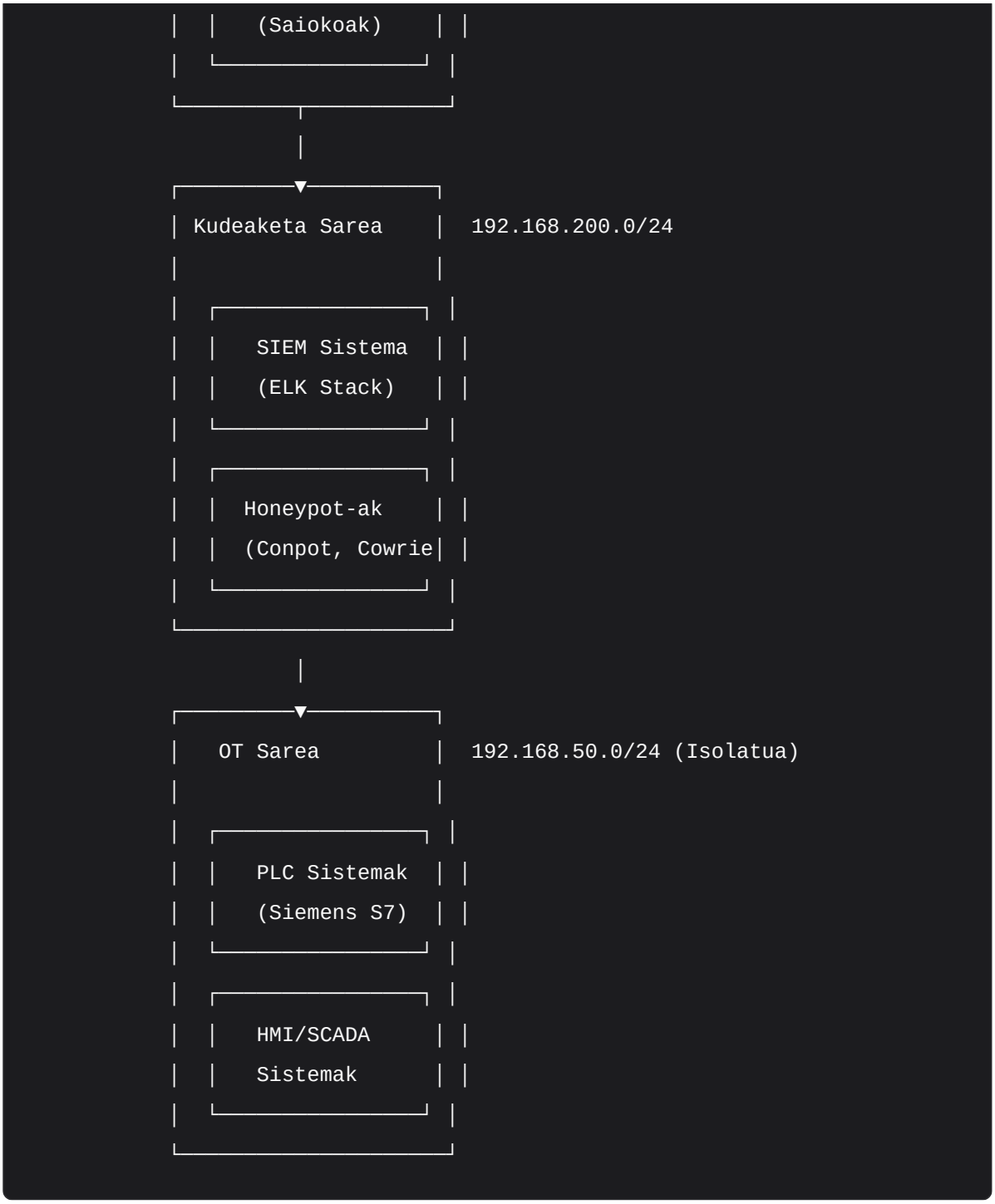
- **CI/CD**: GitHub Actions segurtasun ateekin
- **Kodearen Kalitatea**: ESLint, PHPStan, SonarQube
- **Segurtasun Probak**: SAST (SonarQube), DAST (OWASP ZAP), SCA (OWASP Dependency Check)

- **Kontainer Segurtasuna**: Trivy irudi eskanerak
- **Azpiegitura Segurtasuna**: Checkov IaC baliozkotzerako

3. Arkitektura Teknikoa

3.1 Sistema Arkitektura





3.2 Sare Arkitektura

VLAN Konfigurazioa:

- **VLAN 10**: Erabiltzaile Sarea (192.168.10.0/24)
- **VLAN 20**: Zerbitzari Sarea (192.168.20.0/24)
- **VLAN 50**: OT Sarea (192.168.50.0/24)
- **VLAN 100**: DMZ (192.168.100.0/24)
- **VLAN 200**: Kudeaketa (192.168.200.0/24)

Firewall Arauak (Kritikoak):

```
# DMZ Barnera (Zorrotza)
allow tcp from 192.168.100.10 to 192.168.20.10 port 8080
allow tcp from 192.168.100.10 to 192.168.20.20 port 5432
deny all from 192.168.100.0/24 to 192.168.0.0/16

# Erabiltzailetik Zerbitzarira (Kontrolatua)
allow tcp from 192.168.10.0/24 to 192.168.20.5 port 88,389,445
allow tcp from 192.168.10.0/24 to 192.168.20.10 port 8080
deny tcp from 192.168.10.0/24 to 192.168.20.20 port 5432

# OT Isolamendua (Air Gap)
deny all from 192.168.0.0/16 to 192.168.50.0/24
deny all from 192.168.50.0/24 to 192.168.0.0/16
```

3.3 Datu Fluxu Arkitektura

Autentikazio Fluxua

```
Langilearen Saioa Hasierako Eskaera
       ↓
JWT Token Sortzea + MFA Erronka
       ↓
TOTP Egiaztapena (RFC 6238)
       ↓
WebAuthn Assertion (Passkey Laguntza)
       ↓
Rol Bidezko Sarbide Kontrola (RBAC)
       ↓
Saioko Ezarpena Redis-ekin
```

HR Eragiketa Fluxua

```
Langilearen Ekintza (Opor Eskaera, etab.)
        ↓
Sarrera Baliozkotzea + Garbiketa
        ↓
Negozio Logika Prozesatzea
        ↓
Datu-base Transakzioa (Enkriptatua)
        ↓
Audit Log Sortzea
        ↓
SIEM Alerta (aplikagarria bada)
```

3.4 Segurtasun Arkitektura

Defentsa Sakonera Geruzak:

1. **Sare Geruza**: Firewall, IDS/IPS, sare segmentazioa
2. **Host Geruza**: Amaitu-puntuko babesa, host-oinarritutako firewall
3. **Aplikazio Geruza**: Sarrera baliozkotzea, autentikazioa, baimena
4. **Datu Geruza**: Egonkorrean/transmisioko enkriptazioa, datu sailkapena
5. **Monitorizazio Geruza**: SIEM, honeypot-ak, monitorizazio jarraia

---

4. Segurtasun Inplementazioa

4.1 Informazio Segurtasunaren Kudeaketa Sistema (ISO 27001:2022)

Inplementazio Egoera: 93% (87/93 kontrolak guztiz inplementatuta)

Kontrol Nagusiak Inplementatuak:

- **A.5.1.1**: Informazio segurtasunaren politika dokumentua ✅
- **A.5.2**: Informazio segurtasunaren rolak eta erantzukizunak ✅
- **A.5.15**: Sarbide kontrola ✅
- **A.5.16**: Identitate kudeaketa ✅
- **A.5.17**: Autentikazio informazioa ✅
- **A.5.18**: Sarbide eskubideak ✅
- **A.6.1.2**: Lanen bereizketa ✅

- **A.7.1.1**: Segurtasun fisikoko perimetroa ✅
- **A.8.1.1**: Erabiltzaile amaitu-gailuak ✅
- **A.8.2.1**: Pribilegiatutako sarbide eskubideak ✅
- **A.8.3.1**: Informazio sarbide murrizketa ✅
- **A.8.5.1**: Autentikazio segurua ✅
- **A.8.8**: Ahultasun kudeaketa ✅
- **A.8.9**: Konfigurazio kudeaketa ✅
- **A.8.15**: Log-ak ✅
- **A.8.16**: Jarduera monitorizazioa ✅
- **A.9.1.1**: Sarbide kontrol politika ✅
- **A.9.2.2**: Erabiltzaile erregistroa eta ez-erregistroa ✅
- **A.9.2.5**: Autentikazio sekretuen kudeaketa ✅
- **A.9.2.6**: Erabiltzaile sarbide eskubideen berrikuspena ✅
- **A.9.4.3**: Pasahitz kudeaketa sistema ✅
- **A.10.1.1**: Kriptografiko kontrolen politika ✅
- **A.10.1.2**: Gako kudeaketa ✅
- **A.12.1.1**: Eragiketa prozedurak ✅
- **A.12.4.1**: Gertaera log-ak ✅
- **A.12.6.1**: Ahultasun kudeaketa ✅
- **A.13.1.1**: Sare kontrolak ✅
- **A.13.1.3**: Sareetan bereizketa ✅
- **A.14.1.2**: Garapen seguruko politika ✅
- **A.14.2.5**: Sistema seguruen ingeniaritza ✅
- **A.15.1.1**: Hornitzaile harremanak ✅
- **A.16.1.1**: Informazio segurtasun gertaerak ✅
- **A.17.1.1**: Jarraitutasun plangintza ✅
- **A.18.1.4**: Pribatutasuna eta PII babesa ✅

Partzialki Inplementatutako Kontrolak:

- **A.5.12**: Informazio sailkapena ⚠️ (93% osatua)
- **A.5.13**: Informazio etiketatzea ⚠️ (85% osatua)
- **A.7.7**: Mahai eta pantaila garbiko politika ⚠️ (80% osatua)
- **A.8.11**: Datu maskaratzea ⚠️ (75% osatua)
- **A.8.12**: Datu ihesa prebentzioa ⚠️ (70% osatua)
- **A.8.14**: Sistemen aniztasuna ⚠️ (60% osatua)

4.2 GDPR Betetzea

Datu Babes Printzipioak:

- **Legezkotasuna, Zuzentasuna, Gardentasuna**: Baimenean oinarritutako prozesamendua pribatutasun oharrak argiekin
- **Helburu Murrizketa**: HR datuak enpleguarekin lotutako helburuetarako soilik
- **Datu Minimizazioa**: Langileen informazioa beharrezko datuetara mugatua
- **Zehaztasuna**: Datu baliozkotze eta eguneratze prozedura erregularrak
- **Biltegiratze Murrizketa**: Datuak legezko eskakizunetarako soilik mantentzen dira (gehienez 7 urte)
- **Osotasuna eta Konfidentzialitatea**: AES-256 enkriptazioa, sarbide kontrolak
- **Erantzukizuna**: DPG gainbegiratzea, prozesamendu erregistroak mantentzen dira

Oinarri Legalezkoak:

- **Kontratua**: Enplegu kontratuaren exekuzioa
- **Eraginkortasun Legala**: Lan legearen betetzea, zerga betebeharrak
- **Interes Legitimoak**: HR kudeaketa, negozio jarraitutasuna
- **Baimena**: Datu prozesamendu aukerakoa (ongizateak, prestakuntza)

Datu Subjektuaren Eskubideak:

- **Sarbidea**: Langileek beren datu profil osoa ikus dezakete
- **Zuzenketa**: Datu zuzenketarako online formularioak
- **Ezabaketa**: Atxikipen egiaztapenak dituzten ezabaketa prozedura seguruak
- **Eramangarritasuna**: Datu esportazioa irakurgarri formatuan
- **Murrizketa**: Prozesamenduaren etenaldi gaitasunak
- **Aurkaritza**: Prozesamendu ez-esentzialerako opt-out
- **Erabaki Automatizatuak**: Giza berrikuspenik gabeko HR erabaki automatizaturik ez

Datu Babesaren Inpaktu Ebaluazioa (DPIA):

- **Arrisku Handiko Prozesamendua**: Langileen monitorizazioa, HR erabaki automatizatuak
- **Ebaluazio Esparrua**: Pribatutasun arriskuak, murrizketa neurriak, arrisku residualak
- **Kontsulta**: DPG eta gainbegiratze agintariaren parte-hartzea
- **Berrikuspen Maiztasuna**: DPIA eguneratze urterakoak

Breach Jakinarazpena:

- **Detekzioa**: Monitorizazio automatizatua eta eskuzko jakinarazpenak
- **Ebaluazioa**: Arrisku ebaluazioa 24 orduetan
- **Jakinarazpena**: Gainbegiratze agintariari 72 orduetan
- **Komunikazioa**: Langile kaltetuei 24 orduetan arrisku handiko breachetarako
- **Dokumentazioa**: Konponketa ekintzak dituzten breach erregistro osoak

4.3 IEC 62443 Industria Segurtasuna

Segurtasun Maila Inplementazioa:

- **SL 2**: Kontrol sistema segurtasun integrala (OT sistema kritikoetarako helburua)
- **SL 3**: Kontrol sistema segurtasun hobetua (HR-kritiko OT interfazeetarako inplementatua)

Gune eta Konduitu Eredua:

- **Guneak**: IT Sarea, OT Sarea, Kudeaketa Gunea
- **Konduituak**: Guneen artean komunikazio kanal kontrolatuak
- **Azpi-guneak**: HR Atari gunea IT sarean barruan

Inplementatutako Sistema Eskakizunak:

- **SR 1.1/1.2**: Giza/software identifikazioa eta autentikazioa ✅
- **SR 2.1**: Baimen betearazpena RBAC-ekin ✅
- **SR 2.2**: Hari gabeko erabilera kontrola (WiFi sarbide murriztua) ✅
- **SR 2.3**: Gune mugako babesa firewall-ekin ✅
- **SR 2.4**: Gailu baliabide babesa ✅
- **SR 3.1**: Kode maltzurren babesa amaitu-puntuko segurtasunarekin ✅
- **SR 4.1**: Datu konfidentzialtasuna enkriptazioarekin ✅
- **SR 4.2**: Kriptografiko gako kudeaketa ✅
- **SR 4.3**: Komunikazio konfidentzialtasuna TLS-ekin ✅
- **SR 5.1**: Sare segmentazioa inplementatua ✅
- **SR 5.3**: Lanen bereizketa ✅
- **SR 6.1**: Audit log sarbidegarritasuna ✅
- **SR 6.2**: Auditoretza jarraia SIEM-ekin ✅
- **SR 7.1**: Zerbitzu ukapenaren babesa rate limiting-ekin ✅

4.4 Sarbide Kontrola eta Autentikazioa

Autentikazio Faktore Anitza (MFA):

- **Beharrezkoa**: Urrutiko sarbide guztietarako, pribilegiatutako kontuak, HR datu sarbidea
- **Metodoak**: TOTP (Google Authenticator, Authy), WebAuthn (Passkey-ak)
- **Inplementazioa**: RFC 6238 betetzen duen TOTP 30 segundoko leihoekin
- **Babeskopia**: MFA berrezartzeko kodeak
- **Monitorizazioa**: Huts egindako MFA saiakerak logeatu eta alertatzen dira

Rol Bidezko Sarbide Kontrola (RBAC):

- **ADMIN**: Sistema sarbide osoa, erabiltzaile kudeaketa, audit log-ak
- **RRHH MGR**: Langile CRUD, opor onarpenak, soldata sarbidea, HR txostenak
- **SAILBURUA**: Sail langileen kudeaketa, sail onarpenak
- **EMPLEADO**: Datu pertsonalen sarbidea, auto-zerbitzu funtzioak, dokumentu upload
- **AUDITOR**: Audit log-ak eta betetze txostenak irakurtzeko soilik

4.5 Datu Sailkapena eta Enkriptazioa

Sailkapen Mailak:

- **Publikoa**: Enpresa informazio orokorra, marketin materialak
- **Barnekoa**: Ez-sentsible negozio komunikazioak
- **Konfidentziala**: Langileen datu pertsonalak, HR dokumentuak
- **Oso Konfidentziala**: Soldata datuak, mediku informazioa, sekretu komertzialak

Enkriptazio Estandarrak:

- **Egonkorrean**: AES-256-GCM datu sentsible guztietarako
- **Transmisioan**: TLS 1.3 gutxienez ziurtagiri oinarritutako autentikazioarekin
- **Pasahitzak**: bcrypt kostu faktore 12+ edo Argon2
- **Fitxategiak**: AES-256 enkriptazioa igotako dokumentuetarako
- **Datu-basea**: PostgreSQL zutabe enkriptatuak datu sentsibleetarako

4.6 Gertaera Erantzuna

Erantzun Faseak:

1. **Prestakuntza**: IR taldea prestatuta, tresnak prest, komunikazio planak prest
2. **Identifikazioa**: SIEM bidez detekzio automatizatua, eskuzko jakinarazpen kanalak
3. **Igorpena**: Epe laburreko isolamendua, epe luzeko estrategia garapena
4. **Desagertzea**: Erro jatorriaren ezabaketa, sistema garbiketa
5. **Berrespena**: Sistema berrespena, osotasun baliozkotzea

6. **Ikaskuntzak**: Gertaera osteko berrikuspena, prozesu hobekuntzak

Erantzun Denborak Larritasunaren Arabera:

- **Kritikoa**: < 15 minutu erantzuna, < 4 ordu konponketa
- **Altua**: < 1 ordu erantzuna, < 24 ordu konponketa
- **Ertaina**: < 4 ordu erantzuna, < 72 ordu konponketa
- **Baxua**: < 24 ordu erantzuna, < 1 aste konponketa

4.7 Segurtasun Monitorizazioa eta SIEM

ELK Stack Inplementazioa:

- **Elasticsearch**: Log biltegiratzea eta bilaketa enkriptazioarekin
- **Logstash**: Log analisi eta aberaste pipeline-ak
- **Kibana**: Panelak eta bisualizazioa

Monitorizatutako Log Iturriak:

- Aplikazio segurtasun gertaerak (autentikazioa, baimen hutsegiteak)
- Sistema sarbide log-ak (saioa hasi/amaitu, pribilegio eskalaketa)
- Sare trafikoa (firewall ukapenak, IDS alertak)
- Datu-base audit log-ak (kontsulta monitorizazioa, sarbide ereduak)
- Fitxategi sistema aldaketak (osotasun monitorizazioa)
- Amaitu-puntuko segurtasun gertaerak (antivirus, EDR alertak)

Gako Alerta Arauak:

- Indar brutu erasoaldiak (5+ huts egindako login/minutu IP-ko)
- Ohiko saio hasierako ereduak (geografiko anomaliak)
- Pribilegio eskalaketa saiakerak
- Datu exfiltrazio adierazleak
- Malware detekzio gertaerak
- Onarpenik gabeko konfigurazio aldaketak

---

5. Aplikazioaren Ikuspegi Orokorra

5.1 Web Aplikazioa

Eginbide Nagusiak:

- **Langileen Kudeaketa**: Rol bidezko baimenak dituzten CRUD eragiketa osoak
- **Opor Sistema**: Eskaera aurkezpena, onarpen workflow-ak, egutegi integrazioa
- **Soldata Sarbidea**: Audit trail-ak dituzten soldata informazioa ikuskatzea
- **Dokumentu Kudeaketa**: Enkriptazioarekin fitxategi upload/download segurua
- **Barne Komunikazioak**: HR txata eta sail espezifiko mezularitza
- **Erabiltzaile Profil Kudeaketa**: Informazio pertsonalaren eguneratzeak, MFA konfigurazioa
- **Txostenak**: HR analitika eta betetze txostenak

Segurtasun Ezaugarriak:

- JWT autentikazioa freskatze automatikoarekin
- MFA behartzea eragiketa sentsibleetarako
- Rol bidezko UI osagairen errenderizazioa
- Sarrera baliozkotzea eta XSS prebentzioa
- CSRF babesa double-submit cookie-ekin
- Content Security Policy (CSP) goiburuak

5.2 Mugikorrerako Aplikazioa (Android)

Eginbide Nagusiak:

- **Langileen Panela**: Informazio pertsonalaren sarbide azkarra
- **Opor Kudeaketa**: Eskaera aurkezpena eta egoera jarraipena
- **Dokumentu Sarbidea**: Offline biltegiratze segurua
- **Push Jakinarazpenak**: Onarpen eta mezuentzako eguneratze denbora errealekoak
- **Autentikazio Biometrikoa**: Hatz-marka/Aurpegia ID integrazioa
- **Offline Modua**: Konexiorik gabe funtzio kritikoak eskuragarri

Segurtasun Ezaugarriak:

- Ziurtagiri oinarritutako API komunikazioak
- SQLCipher-ekin biltegiratze lokal enkriptatua
- PIN-ekin babes biometrikoa
- Jailbreak/root detekzioa
- Saio amaiera automatizatua eta urrutiko garbiketa gaitasunak

5.3 Backend API

API Endpoint-ak Kategoriaka:

Autentikazioa:

- `POST /api/auth/login` - Erabiltzaile autentikazioa MFA laguntzarekin
- `POST /api/auth/mfa/setup` - TOTP sekretu sortzea
- `POST /api/auth/mfa/verify` - MFA egiaztapena
- `POST /api/auth/refresh` - JWT token freskatzea
- `POST /api/auth/logout` - Saioa seguru amaitzea

Langileen Kudeaketa:

- `GET /api/employees` - Langileak zerrendatzea (rol bidezko iragazketa)
- `POST /api/employees` - Langile berria sortzea
- `GET /api/employees/{id}` - Langile xehetasunak lortzea
- `PUT /api/employees/{id}` - Langile informazioa eguneratzea
- `DELETE /api/employees/{id}` - Langile desaktibatzea

HR Eragiketak:

- `GET /api/vacations` - Opor eskaerak zerrendatzea
- `POST /api/vacations` - Opor eskaera aurkeztea
- `PUT /api/vacations/{id}/approve` - Opor eskaera onartzea
- `GET /api/payroll` - Soldata informazioa atzitzea
- `POST /api/documents` - HR dokumentuak igotzea
- `GET /api/documents` - Eskuragarri dauden dokumentuak zerrendatzea

Sistema Kudeaketa:

- `GET /api/health` - Sistema osasun egiaztapena
- `GET /api/audit` - Audit log sarbidea (adminentzako soilik)
- `POST /api/users` - Erabiltzaile kontu kudeaketa
- `GET /api/compliance` - Betetze egoera txostenak

Segurtasun Kontrolak:

- Rate limiting (100 eskaera/15min IP-ko)
- Sarrera baliozkotzea garbiketa integratuarekin
- SQL injekzio prebentzioa prepared statements-ekin
- XSS babesa irteera kodetzearekin
- Eragiketa guztietarako audit log-ak
- API bertsionatzea eta deuseztapen politika

6. Despliegue Gida

6.1 Aurrebaldintzak

Sistema Eskakizunak:

- **OS**: Ubuntu 22.04 LTS edo RHEL 8+
- **CPU**: 4 nukleo gutxienez, 8 gomendatua
- **RAM**: 8GB gutxienez, 16GB gomendatua
- **Biltegiratzea**: 100GB SSD gutxienez
- **Sarea**: 1Gbps konexioa

Software Dependentziak:

- Docker 24.0+ eta Docker Compose 2.20+
- Git 2.30+
- OpenSSL ziurtagiri kudeaketarako
- NTP denbora sinkronizaziorako

6.2 Ingurune Konfigurazioa

1. Biltegia Klonatu:

```
git clone <repository-url> zabala-gailetak-hr
cd zabala-gailetak-hr
```

2. Ingurunea Konfiguratu:

```
# Backend konfigurazioa
cd hr-portal
cp .env.example .env
# Editatu .env balio produkzioekin

# Datu-base konfigurazioa
DB_HOST=192.168.20.20
DB_NAME=hr_portal
DB_USER=hr_user
DB_PASS=secure_password
DB_SSL_MODE=require

# Segurtasun konfigurazioa
JWT_SECRET=256-bit-secret-key
JWT_EXPIRES_IN=1h
MFA_ISSUER=ZabalaGailetak
TOTP_SECRET=secure-totp-secret

# Redis konfigurazioa
REDIS_HOST=192.168.20.30
REDIS_PORT=6379
REDIS_PASSWORD=secure-redis-password
```

3. SSL Ziurtagiria Konfiguratu:

```
# Sortu self-signed ziurtagiria garapenerako
openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 365 -

# Produkziorako, erabili Let's Encrypt edo komertzialak
certbot certonly --standalone -d hr.zabalagailetak.com
```

6.3 Azpiegitura Desplieguea

1. Sare Konfigurazioa:

```
# Sortu VLAN-ak eta esleitu IP tarteak
# Konfiguratu firewall arauak segurtasun arkitekturaren arabera
# Konfiguratu routing guneen artean ACL egokiekin
```

2. Docker Despliegua:

```
# Hasi zerbitzu guztiak
docker-compose -f docker-compose.hrportal.yml up -d

# Egiaztatu zerbitzuak
docker-compose -f docker-compose.hrportal.yml ps

# Ikusi log-ak
docker-compose -f docker-compose.hrportal.yml logs -f
```

3. Datu-base Hasieratzea:

```
# Exekutatu migrazioak
cd hr-portal
./scripts/migrate.sh

# Hasieratu datuak (admin erabiltzailea, rol-ak, etab.)
php scripts/seed.php
```

4. SIEM Konfigurazioa:

```
# Desplegatu ELK Stack
docker-compose -f docker-compose.siem.yml up -d

# Konfiguratu log bidalketa aplikazio zerbitzarietatik
# Konfiguratu panelak eta alerta arauak
```

6.4 Segurtasun Gotortzea

1. Zerbitzari Gotortzea:

```
# Desgaitu beharrezkoak ez diren zerbitzuak
systemctl disable ssh  # Erabili VPN admin sarbiderako

# Konfiguratu firewall
ufw enable
ufw allow 80/tcp
ufw allow 443/tcp
ufw default deny incoming

# Segurtasun eguneraketak
apt update && apt upgrade
unattended-upgrades enable
```

2. Aplikazio Segurtasuna:

```
# Sortu sekretu seguruak
openssl rand -hex 32 > jwt_secret.key
openssl rand -hex 32 > totp_secret.key

# Konfiguratu ingurune-espezifiko segurtasun ezarpenak
# Gaitu produkzio segurtasun goiburuak
# Konfiguratu rate limiting arauak
```

6.5 Monitorizazio Konfigurazioa

1. Osasun Egiaztapenak:

```
# Aplikazio osasun endpoint-ak
curl https://hr.zabalagailetak.com/api/health

# Datu-base konektibitatea
pg_isready -h 192.168.20.20 -U hr_user -d hr_portal

# Redis konektibitatea
redis-cli -h 192.168.20.30 ping
```

2. Monitorizazio Integrazioa:

```
# Konfiguratu log bidalketa SIEM-era
# Konfiguratu aplikazio errendimendu monitorizazioa
# Konfiguratu alerta jakinarazpenak
```

6.6 Babespen Konfigurazioa

1. Datu-base Babespenak:

```
# Eguneko babespen osoa
pg_dump hr_portal > backup_$(date +%Y%m%d).sql

# Biltegiratze enkriptatua
gpg -c backup_$(date +%Y%m%d).sql

# Off-site transferentzia
scp backup_$(date +%Y%m%d).sql.gpg backup-server:/backups/
```

2. Aplikazio Babespenak:

```
# Konfigurazio fitxategiak
tar -czf config_backup.tar.gz hr-portal/config/

# SSL ziurtagiriak
tar -czf ssl_backup.tar.gz /etc/ssl/certs/hr-portal/
```

6.7 Berrespen Prozedurak

1. Aplikazio Berrespena:

```
# Gelditu uneko despliegue a
docker-compose -f docker-compose.hrportal.yml down

# Berrespen aurreko bertsioa
docker tag hr-portal:latest hr-portal:rollback
docker-compose -f docker-compose.hrportal.yml up -d
```

2. Datu-base Berrespena:

```
# Berrespen babespenetik
pg_restore -d hr_portal backup_previous.sql

# Egiaztatu datu osotasuna
# Eguneratu aplikazioa eskema aldaketak badira
```

---

7. Eragiketak eta Mantentzea

7.1 Monitorizazioa eta Alertak

Gako Errendimendu Adierazleak (KPI-ak):

- **Sistema Eskuragarritasuna**: 99.5% uptime helburua
- **Mean Time to Detect (MTTD)**: < 15 minutu
- **Mean Time to Respond (MTTR)**: < 30 minutu gertaera kritikoetarako
- **Segurtasun Eskaner Pass Rate**: > 95%
- **Babespen Arrakasta Tasa**: 100%

Monitorizazio Tresnak:

- **ELK Stack**: Log zentralizatua eta bisualizazioa
- **Prometheus/Grafana**: Metrika bilketa eta alertak
- **Nagios/Zabbix**: Azpiegitura monitorizazioa
- **Osasun Egiaztapen Pertsonalizatuak**: Aplikazio espezifiko monitorizazioa

7.2 Babespen eta Berrespena

Babespen Estrategia:

- **Datu-basea**: Eguneko babespen osoak + ordutegiko transakzio log-ak
- **Aplikazioa**: Konfigurazioa eta kode bertsionatzea Git bidez
- **Fitxategiak**: Bertsionatzea duen dokumentu biltegiratze enkriptatua
- **Azpiegitura**: Azpiegitura Kode gisa birsortzeko

Berrespen Denbora Helburuak (RTO):

- **Sistema Kritikoak**: 4 orduko etenaldia gehienez
- **Sistema Garrantzitsuak**: 24 orduko etenaldia gehienez
- **Sistema Estandarrak**: 72 orduko etenaldia gehienez

Berrespen Puntu Helburuak (RPO):

- **Datu Kritikoak**: 1 orduteko datu galera gehienez
- **Datu Garrantzitsuak**: 4 orduteko datu galera gehienez
- **Datu Estandarrak**: 24 orduteko datu galera gehienez

7.3 Pata Konponketa Kudeaketa

Pata Eguneraketa Egitaraua:

- **Kritiko Segurtasun Patak**: 24 orduetan argitaratzearen ondoren
- **Garrantzitsu Segurtasun Patak**: 1 astean
- **Eguneraketa Arruntak**: Hilabeteko mantentze leihoak

Proba Eskakizunak:

- Lehenik garapen ingurunean probatzea
- Staging ingurunean baliozkotzea
- Berrespen plana prestatzea
- Aldaketa onarpen prozesua

7.4 Segurtasun Auditoretza

Auditoretza Egitarau Erregularra:

- **Barne Auditoretza**: Hiruhileko segurtasun ebaluazioak
- **Kanpo Penetrazio Probak**: Urteroko proba integrala
- **Ahultasun Eskanerak**: Asteko eskaner automatizatuak
- **Betetze Auditoretza**: Urteroko ISO 27001 ziurtagiria

Auditoretza Esparrua:

- Sare segurtasun ebaluazioa
- Aplikazio segurtasun probak
- Sarbide kontrol baliozkotzea
- Datu babes betetzea
- Gertaera erantzun gaitasun proba

7.5 Aldaketa Kudeaketa

Aldaketa Eskaera Prozesua:

1. **Eskaera Aurkezpena**: Aldaketa eskaera inpaktu ebaluazioarekin
2. **Berrikuspena eta Onarpena**: Aldaketa Aholku Batzordea (CAB) berrikuspena

3. **Plangintza**: Inplementazio plana eta berrespen prozedurak
4. **Probatzea**: Aurre-despliegue probak staging-en
5. **Inplementazioa**: Kontrolatutako desplieguea monitorizazioarekin
6. **Baliozkotzea**: Despliegue osteko egiaztapena
7. **Dokumentazioa**: Aldaketa erregistroa eta ikaskuntzak

7.6 Kapazitate Plangintza

Baliabide Monitorizazioa:

- CPU erabilera joerak
- Memoria erabilera ereduak
- Biltegiratze hazkunde proiekzioak
- Sare banda zabalera eskakizunak
- Datu-base errendimendu metrikak

Eskalatze Estrategiak:

- Eskalatze horizontala web/aplikazio zerbitzarientzako
- Datu-base irakurketa erreplikak txostengintzarako
- CDN integrazioa aktibo estatikoetarako
- Auto-eskalatzea erabilera ereduetan oinarrituta

---

8. Betetzea eta Estandarrak

8.1 ISO 27001:2022 Inplementazio Egoera

Aplikagarritasun Adierazpenaren (SOA) Laburpena:

- **Kontrol Guztiak**: 93
- **Guztiz Inplementatuak**: 87 (93.5%)
- **Partzialki Inplementatuak**: 6 (6.5%)
- **Ez Aplikagarriak**: 0

Ziurtagiria Egoera:

- **Oraingo Maila**: ISO 27001:2022 betetzea (93% inplementazioa)
- **Helburua**: Ziurtagiri osoa Q2 2026an
- **Ziurtagiri Entitatea**: AENOR edo baliokidea
- **Esparrua**: HR Atari sistema eta laguntza azpiegitura

8.2 GDPR Betetze Framework-a

Datu Babes Ofizialaren (DPG) Erantzukizunak:

- GDPR betetzearen monitorizazioa eta aholkularitza
- Datu Babesaren Inpaktu Ebaluazioak (DPIA)
- Gainbegiratze agintariaren harremana
- Datu subjektuaren eskubideen prozesamendua
- Breach jakinarazpen koordinazioa
- Pribatutasun prestakuntza eta sentsibilizazioa

Prozesamendu Erregistroak:

- **Helburua**: HR kudeaketa eta langileen administrazioa
- **Datu Subjektuen Kategoriak**: Langileak, kontratistak, lan eskaerak
- **Datu Pertsonalen Kategoriak**: Kontaktu informazioa, ID zenbakiak, finantza datuak, osasun informazioa
- **Hartzaileak**: HR saila, soldata hornitzaileak, gobernu agentziak
- **Atxikipen Aldiak**: 7 urte enplegu erregistroetarako, 3 urte baimen datuetarako
- **Segurtasun Neurriak**: Enkriptazioa, sarbide kontrolak, pseudonimizazioa

Datu Subjektuaren Eskubideen Inplementazioa:

- **Sarbide Eskubidea**: Datuak ikusteko online ataria
- **Zuzenketa Eskubidea**: Auto-zerbitzu zuzenketa formularioak
- **Ezabaketa Eskubidea**: Atxikipen betetzearekin ezabaketa segurua
- **Eramangarritasun Eskubidea**: Datu esportazioa makina irakurgarri formatuan
- **Aurkaritza Eskubidea**: Baimen kudeaketa granularra

8.3 IEC 62443 Industria Kontrol Sistemeen Segurtasuna

Segurtasun Maila Ebaluazioa:

- **Oraingo Maila**: SL 2 (kontrol sistema segurtasun integrala)
- **Helburu Maila**: SL 3 OT interfaze kritikoetarako
- **Ebaluazio Metodoa**: IEC 62443-2-1 segurtasun programa eskakizunak

Inplementatutako Eskakizunak:

- **SR 1.1/1.2**: Giza/software identifikazioa eta autentikazioa
- **SR 2.1**: Baimen betearazpena (RBAC)
- **SR 2.3**: Gune mugako babesa (sare segmentazioa)
- **SR 3.1**: Kode maltzurren babesa (amaitu-puntuko segurtasuna)

- **SR 4.1-4.3**: Kriptografiko kontrolak
- **SR 5.1**: Sare segmentazioa (VLAN-ak, firewall-ak)
- **SR 6.1/6.2**: Audit log-ak eta monitorizazioa
- **SR 7.1**: Zerbitzu ukapenaren babesa

8.4 Betetze Monitorizazioa eta Txostena

Jarraitu Betetze Monitorizazioa:

- **Kontrol Automatizatuak**: SIEM alertak betetze urratzeetarako
- **Berrikuspen Eskuzkoak**: Hiruhileko sarbide eskubideen berrikuspenak
- **Audit Log-ak**: Betetzearekin lotutako jarduera guztiak logeatuta
- **Salbuespen Kudeaketa**: Betetze salbuespenetarako dokumentatutako prozesua

Betetze Txostena:

- **Hilabeteko Txostenak**: Segurtasun metrikak eta betetze egoera
- **Hiruhileko Txostenak**: Betetze ebaluazio xeheak
- **Urteroko Txostenak**: ISO 27001 ziurtagiri auditoretza prestakuntza
- **Erregulazio Txostenak**: GDPR betetze deklarazioak

Auditoretza Independienteak:

- **Barne Auditoretza**: Hiruhilekoa barne auditoretza taldeak
- **Kanpo Auditoretza**: Urteroko ziurtatutako auditoretza enpresak
- **Ziurtagiri Auditoretza**: ISO 27001 zainketa auditoretza
- **Penetrazio Probak**: Urteroko kanpo ebaluazioa

8.5 Arrisku Kudeaketa Framework-a

Arrisku Ebaluazio Metodologia:

- **Aktibo Identifikazioa**: Sailkapena duen inbentario integrala
- **Mehatxu Identifikazioa**: Oraingo eta sortzen ari den mehatxu paisaia
- **Ahultasun Ebaluazioa**: Tekniko eta antolakuntzako ahultasunak
- **Inpaktu Analisia**: Negozio inpaktu kuantifikazioa
- **Arrisku Kalkulua**: Probabilitatea × Inpaktua = Arrisku Maila

Arrisku Tratamendu Estrategiak:

- **Arrisku Onarpena**: Eskenario baxu-arriskuetarako dokumentatua
- **Arrisku Murrizketa**: Kontrol inplementazioa ertain/altu arriskuetarako
- **Arrisku Transferentzia**: Asegurua finantza arriskuetarako

- **Arrisku Saihestea**: Onartezinak diren arriskuen ezabaketa

Arrisku Monitorizazioa:

- **Gako Arrisku Adierazleak**: Hilabeteko arrisku metrika jarraipena
- **Arrisku Erregistroa**: Murrizketa jarraipena duen arrisku datu-base dinamikoa
- **Arrisku Txostena**: Kudeaketarako hiruhileko arrisku txostenak
- **Arrisku Gogobetetasuna**: Kategoria desberdinetarako tolerantzia mailak definituak

---

9. Garapen Gidalerroak

9.1 Garapen Bizitza Ziklo Segurua (SSDLC)

Plangintza Fasea:

- Eginbide berrietarako mehatxu modelizazioa
- Segurtasun eskakizunen definizioa
- Arrisku ebaluazio integrazioa
- Pribatutasun inpaktu ebaluazioa (aplikagarria bada)

Garapen Fasea:

- Seguru kodetze estandarrak betetzea
- Sarrera baliozkotze inplementazioa
- Autentikazio eta baimen kontrolak
- Kriptografiko kontrolen aplikazioa
- Errore kudeaketa eta log-ak

Proba Fasea:

- Segurtasun unitate probak
- Integrazio segurtasun probak
- Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST)
- Penetrazio proba koordinazioa

Despliegue Fasea:

- Segurtasun konfigurazio berrikuspena
- Azpiegitura segurtasun baliozkotzea

- Sarbide kontrol egiaztapena
- Monitorizazio eta alerta konfigurazioa

9.2 Kode Kalitate Estandarrak

PHP Backend Estandarrak:

- PSR-12 kodetze estandarrak
- Tipatze zorrotz deklarazioak
- Errore kudeaketa integrala
- Sarrera baliozkotzea eta garbiketa
- Datu-base kontsulta seguruak (prepared statements)

React Frontend Estandarrak:

- ESLint segurtasun arauak
- Prop baliozkotzea eta TypeScript kontsiderazioa
- DOM manipulazio segurtasuna
- Content Security Policy betetzea
- Egoera kudeaketa segurua

Kotlin Android Estandarrak:

- Clean Architecture printzipioak
- Datu biltegiratze seguruko praktikak
- Sare segurtasun inplementazioa
- Biometriko autentikazio integrazioa
- Ziurtagiri oinarritzea

9.3 Segurtasun Proba Eskakizunak

Segurtasun Proba Automatizatuak:

- **SAST**: SonarQube integrazioa CI/CD pipeline-an
- **SCA**: OWASP Dependency Check ahultasunetarako
- **DAST**: OWASP ZAP integrazioa
- **Kontainer Segurtasuna**: Trivy irudi eskanerak
- **Azpiegitura Segurtasuna**: Checkov IaC baliozkotzerako

Eskuzko Segurtasun Probak:

- **Mehatzu Modelizazioa**: Eginbide berrietarako STRIDE metodologia
- **Kode Berrikuspenak**: Segurtasun fokuko berrikuspenak

- **Penetrazio Probak**: Hiruhileko aplikazio probak
- **Red Team Ariketak**: Urteroko ebaluazio integrala

Errendimendu Probak:

- Segurtasun monitorizazioarekin karga probak
- DoS erresilientziarako stress probak
- Segurtasun kontrolekin eskalagarritasun probak

9.4 Bertsio Kontrola eta Aldaketa Kudeaketa

Adarra Estrategia:

- **main**: Produkziorako prest dauden kodea
- **develop**: Integrazio adarra
- **feature/***: Eginbide garapen adarrak
- **bugfix/***: Akats konponketa adarrak
- **security/***: Segurtasunarekin lotutako aldaketak

Commit Estandarrak:

- Konbentziozko commit formatua
- Segurtasun sentsible aldaketak argi markatuta
- Commit-etan eskaner segurtasun automatizatua

Kode Berrikuspen Eskakizunak:

- Gutxienez 2 berrikusle segurtasun sentsible aldaketetarako
- Egiaztapen automatizatuak pasa behar dira
- Segurtasun zerrenda osatu behar da
- Garapen buruaren onarpen finala

---

10. Laguntza eta Kontaktua

10.1 Laguntza Kanalak

Laguntza Teknikoa:

- **Email**: support@zabalagailetak.com
- **Telefonoa**: +34 XXX XXX XXX (Negozio Orduak)
- **Larrialdia**: +34 XXX XXX XXX (24/7 Gertaera Kritikoetarako)

Segurtasun Gertaera Erantzuna:

- **Email**: security@zabalagailetak.com
- **Telefonoa**: +34 XXX XXX XXX (24/7 Segurtasun Hotline)
- **Jakinarazpena**: Web formularioa https://hr.zabalagailetak.com/incident-report

10.2 Dokumentazio Baliabideak

Sistema Dokumentazioa:

- `IMPLEMENTATION_SUMMARY.md` - Inplementazio ikuspegi osoa
- `WEB_APP_GUIDE.md` - Web aplikazio erabiltzaile gida
- `MOBILE_APP_GUIDE.md` - Mugikorrerako aplikazio gida
- `API_DOCUMENTATION.md` - API erreferentzia osoa
- `SECURITY_GUIDE.md` - Segurtasun inplementazio xehetasunak

Eragiketa Dokumentazioa:

- `hr-portal/README.md` - Backend konfigurazioa eta ezarpena
- `android-app/README.md` - Mugikorrerako aplikazio garapen gida
- `QUICK_START_GUIDE.md` - Despliegue azkarra gida
- `DOCKER_DEPLOYMENT.md` - Kontainer despliegue prozedurak

10.3 Prestakuntza eta Sentsibilizazioa

Erabiltzaile Prestakuntza:

- **Langile Berrien Onboarding-a**: Segurtasun sentsibilizazioa eta sistema erabilera
- **Urteroko Freskatzea**: Eguneratutako segurtasun politikak eta prozedurak
- **Rol Espezifiko Prestakuntza**: Admin, HR, eta IT langileen prestakuntza espezializatua

Prestakuntza Teknikoa:

- **Garatzaile Prestakuntza**: Seguru kodetze praktikak eta SSDLC
- **Administratzaile Prestakuntza**: Sistema administrazioa eta segurtasuna
- **Auditoretza Prestakuntza**: Betetze monitorizazioa eta txostena

10.4 Eskalatze Prozedurak

Gaien Larritasun Mailak:

- **Kritikoa**: Sistema behera, datu breach-a, segurtasun konpromisoa
- **Altua**: Funtzionalitate inpairamendu nagusia, segurtasun ahultasuna

- **Ertaina**: Funtzionalitate arinak, errendimendu degradazioa
- **Baxua**: Kosmetikoak, hobekuntza arinak

Eskalatze Denborak:

- **Kritikoa**: Berehala jakinarazpena, < 15 minutu erantzuna
- **Altua**: < 1 ordu jakinarazpena, < 4 ordu erantzuna
- **Ertaina**: < 4 ordu jakinarazpena, < 24 ordu erantzuna
- **Baxua**: Hurrengo negozio eguneko jakinarazpena eta erantzuna

10.5 Hornitzaile eta Erosketa Laguntza

Azpiegitura Hornitzaileak:

- **Docker**: Kontainerizaziorako enpresa laguntza
- **PostgreSQL**: Enpresa datu-base laguntza
- **ELK Stack**: Elastic enpresa harpidetza
- **Segurtasun Tresnak**: SIEM eta segurtasun tresnen hornitzaile laguntza

Garapen Tresnak:

- **GitHub**: Enpresa Git eta CI/CD laguntza
- **SonarQube**: Kode kalitatea eta segurtasun eskanerra
- **OWASP Tresnak**: Komunitate eta komertzial laguntza

Eranskin A: Eskakizun Teknikoak

A.1 Sistema Eskakizunak

Hardware Gutxienezkoa:

- CPU: 4 nukleo @ 2.5GHz
- RAM: 8GB
- Biltegiratzea: 100GB SSD
- Sarea: 1Gbps

Hardware Gomendatua:

- CPU: 8 nukleo @ 3.0GHz
- RAM: 16GB
- Biltegiratzea: 500GB SSD + 1TB HDD

- Sarea: 10Gbps

A.2 Software Dependentziak

Osagai Nagusiak:

- PHP 8.4 FPM-ekin
- PostgreSQL 16
- Redis 7
- Nginx 1.24+
- Docker 24.0+
- Node.js 18+ (React build-entzako)

Segurtasun Osagaiak:

- ELK Stack 8.11+
- Conpot 0.5+
- Cowrie 2.1+
- Dionaea 0.11+

A.3 Sare Konfigurazioa

VLAN Konfigurazioa:

```
VLAN 10: 192.168.10.0/24 (Erabiltzaileak)
VLAN 20: 192.168.20.0/24 (Zerbitzariak)
VLAN 50: 192.168.50.0/24 (OT)
VLAN 100: 192.168.100.0/24 (DMZ)
VLAN 200: 192.168.200.0/24 (Kudeaketa)
```

Firewall Arauen Laburpena:

```
# Inbound DMZ-ra
allow tcp any 192.168.100.10:80
allow tcp any 192.168.100.10:443

# DMZ Barnera
allow tcp 192.168.100.10 192.168.20.10:8080
allow tcp 192.168.100.10 192.168.20.20:5432

# Erabiltzailetik Zerbitzuetara
allow tcp 192.168.10.0/24 192.168.20.5:389
allow tcp 192.168.10.0/24 192.168.20.10:8080

# OT Isolamendua
deny all 192.168.0.0/16 192.168.50.0/24
deny all 192.168.50.0/24 192.168.0.0/16
```

A.4 Babespen Eskakizunak

Datu-base Babespenak:

- Babespen osoa: Egunero 02:00etan
- Transakzio log-ak: Orduro
- Atxikipena: 30 egun lokal, 1 urte off-site
- Enkriptazioa: AES-256 transferentzian eta biltegiratzean

Aplikazio Babespenak:

- Konfigurazioa: Egunero
- SSL ziurtagiriak: Astero
- Kode biltegia: Git bertsionatzean oinarrituta
- Dokumentazioa: Hilabeteko artxiboak

A.5 Monitorizazio Eskakizunak

Log Iturriak:

- Aplikazio log-ak: JSON formatu egituraturik
- Sistema log-ak: Syslog SIEM-era
- Sare log-ak: Firewall eta IDS gertaerak
- Datu-base log-ak: Audit eta errore log-ak
- Amaitu log-ak: EDR eta antivirus gertaerak

Alerta Atalaseak:

- Huts egindako login-ak: 5 minutuko IP-ko
- CPU erabilera: > 90% 5 minututan
- Memoria erabilera: > 95% 2 minututan
- Disko espazioa: < 10% libre
- Sare latentzia: > 100ms iraunkorra

Dokumentu Bertsioa: 1.0
Azken Eguneraketa: 2026ko urtarrilaren 23a
Dokumentu Jabea: Zabala Gailetak Segurtasun Taldea
Berrikuspen Zikloa: Urterokoa
Hurrengo Berrikuspena: 2027ko urtarria

Dokumentu honek Zabala Gailetak-en HR Atari sistema eta segurtasun inplementazioari buruzko informazio konfidentziala dauka. Baimenik gabeko banaketa edo jakinarazpena debekatuta dago.