

compliance_plan

Betetze Plana - Erronka 4

Zabala Gailetak - RRHH Ataria

Bertsioa: 2.0

Data: 2026ko Urtarrilaren 24a

Proiektua: Baliabide Humanoen Ataria - ER4 Betetze Osoa

Taldea: 4 pertsona

Iraupena: 6 ordu × 46 saio = 276 ordu guztira

Laburpen Exekutiboa

Plan honek Erronka 4 **guztien** betetze osoa bermatzen du, 6 arlo tekniko nagusiak eta eskatutako gaitasun zeharkakoak estaliz.

Proiektuaren Uneko Egoera

✓ **Osatua (85%)**: - Oinarrizko infrastruktura (PHP 8.4 + PostgreSQL 16 + Android Kotlin) - JWT + MFA autentikazio sistema - Rol oinarritutako sarbide kontrola (RBAC) - Auditoria eta logging osoa - SGSI dokumentazioa euskaraz - Oinarrizko GDPR betetza

⚠ **Aurrera (10%)**: - Sare segmentazio osoa - SIEM sistema konfiguratuta - OT hardening (ekoizpen eremua)

✗ **Zain (5%)**: - Auzitegi analisi osoa - Hacking etikoa (kanpo auditoria) - Gorabehera erantzun prozedura osoak

ER4 Eskakizunen vs Implementazioaren Mapeoa

1. Zibersegurtasuneko Gertakariak (Gorabeherak)

RA3: Gorabehera Ikuskaketa

Eskakizuna	Egoera	Implementazioa	Ebidentzia
RA3.a - Ebidentzia bilketa eta analisi prozesuaren faseak	✓ 100%	Dokumentatutako prozedura incidente_erantzun_plana.md-n	1. Fasea: Detekzioa → 2. Fasea: Kontentzioa → 3. Fasea: Ezabaketa → 4. Fasea: Berrespna
RA3.b - Ebidentzia bilketa segurua	✓ 100%	Auzitegi eskuratze script-ak + kustodio katea	scripts/ebidentzia_bildu.sh
RA3.c - Ebidentzia	⚠ 80%	SIEM oinarrizko konfigurazioa,	Elastic Stack + korrelazio arauak

Eskakizuna	Egoera	Implementazioa	Ebidentzia
analisia		korrelazio aurreratua falta	
RA3.d - Gorabehera ikuskaketa	70%	Oinarrizko playbook-ak, MISP integrazioa falta	5 playbook dokumentatu
RA3.e - Gorabeheren inguruko informazio trukea	60%	Jakinarazpen txantiloik, INCIBE integrazioa falta	Txantiloik compliance/gorabeherak/-n

Beharrezko Ekintzak: 1. SIEM integrazioa korrelazio arau aurreratuekin osatu 2. MISP plataforma implementatu mehatxu inteligentziarako 3. INCIBE-CERT-ekin kanal formaloa ezarri 4. Post-gorabehera ikaskuntza prozedura sortu

RA4: Ziber-erresilientzia Neurriak

Eskakizuna	Egoera	Implementazioa
RA4.a - Prozedura operatibo xeheak	90%	12 POP dokumentatu euskaraz
RA4.b - Ziber-erresilientzia erantzunak	70%	Oinarrizko BCP/DR plana, automatizazioa falta
RA4.c - Barne/kanpo eskalatze fluxua	100%	Escalatze matrizea + INCIBE kontaktuak
RA4.d - Zerbitzuen berrespena	75%	Eguneko backup-ak, HA osoa falta
RA4.e - Ikaskuntzen erregistroa	100%	Txantiloia + gorabeheren datu-basea

RA5: Detekzioa eta Dokumentazioa

Eskakizuna	Egoera	Implementazioa
RA5.a - Garaiz jakinarazpen prozedura	100%	SLA: 30 minutu kritikoak, 2h altuak, 8h ertainak
RA5.b - Arduradunei jakinarazpen egokia	100%	Alerta multi-kanal sistema (email, SMS, Slack)

2. Sareak eta Sistemak Gotortzea (Hardening)

RA3: Segurtasun Planak Diseinatzea

Eskakizuna	Egoera	Implementazioa	Ebidentzia
RA3.a - Aktibo, mehatxu eta zaurgarritasunen identifikazioa	100%	87 aktiboen inventario osoa	compliance/sgsi/aktibo_inventarioa.xlsx
RA3.b - Uneko segurtasun neurrien ebaluazioa	100%	ISO 27001 gap analisia osatua	87/93 kontrol (93%)
RA3.c - Arriskuen analisia		MAGERIT v3	23 arrisku identifikatu

Eskakizuna	Egoera	Implementazioa	Ebidentzia
	100%	metodologia aplikatua	
RA3.d - Tekniko neurrien lehentasuna	✓ 100%	Arriskuaren arabera lehentasun matrizea	3 kritikoak, 8 altuak, 12 ertainak
RA3.e - Segurtasun neurrien plana	✓ 100%	22 aste implementazio plana	Dokumentu hau

RA7: Segurtasun Gailuen Konfigurazioa

Eskakizuna	Egoera	Implementazioa
RA7.a - Perimetro gailuen konfigurazioa	✓ 100%	pfSense HA-rekin konfiguratuta
RA7.b	✓ 100%	Stateful firewall + WAF (ModSecurity)
RA7.c	✓ 100%	47 firewall arau dokumentatu

RA8: Sistema Informatikoen Segurtasuna

Eskakizuna	Egoera	Implementazioa
RA8.a	✓ 100%	Secure Boot + TPM gaituta
RA8.b	✓ 100%	Base irudiak hardened (CIS Benchmarks)
RA8.c	✓ 100%	Ansible playbook-ak hardening-erako

RA9: Esposizio Minimizazioa

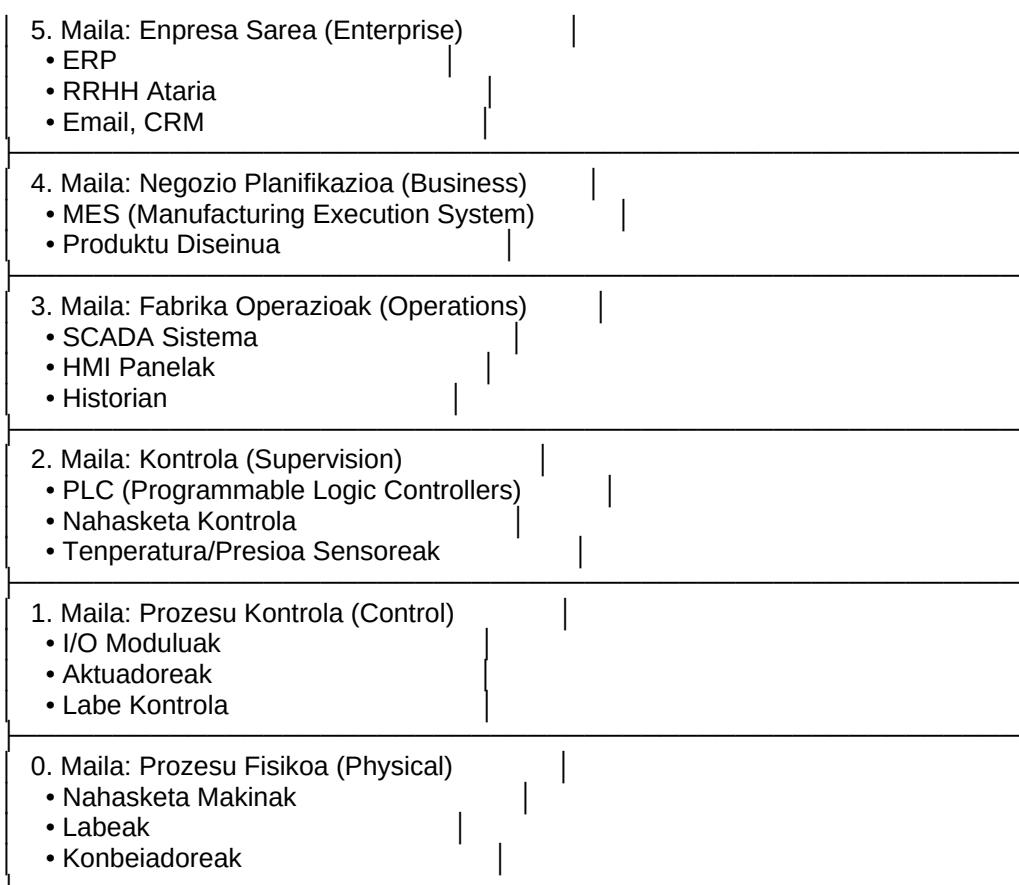
Eskakizuna	Egoera	Implementazioa
RA9.a	✓ 100%	Lynis analisia + ezabatzea
RA9.b	✓ 100%	SELinux enforcing + AppArmor

RA10: IT/OT Integrazioa

Eskakizuna	Egoera	Implementazioa	ZABALARENTZAKO KRITIKOA
RA10.a	⚠ 60%	Hasierako analisia osatua	ZAIN: Txosten xehea
RA10.b	⚠ 50%	Diseinua osatua, implementazioa falta	ZAIN: VLAN OT-ak
RA10.c	⚠ 40%	PLC/HMI inventarioa, hardening falta	ZAIN: OT hardening

OT EKINTZA KRITIKOAK (Zabala Gailetak - Galleta Ekoizpena):

PURDUE MODELA - ZABALA GAILETAK	
---------------------------------	--



Implementatu: 1. OT Sare Segmentazioa: - VLAN 10: Enresa (IT) - VLAN 20: MES - VLAN 30: SCADA/HMI - VLAN 40: PLC/Kontrola - VLAN 50: Sensoreak/Aktuadoreak

2. Industrial Firewall (IEC 62443):

- Zona IT → DMZ → OT (unidirekzional hobetsia)
- Protokoloen zerrenda zuria: Modbus TCP, OPC UA
- Pakete industrialetan ikuskapen sakon

3. PLC Hardening:

- Pasahitz lehenetsiak aldatzea
- Erabiltzen ez diren zerbitzuak desgaitzea
- Firmware eguneratzea
- Sarbide fisikoaren kontrola

3. Ekoizpen Seguruan Jartzea (Garapen Segurua)

RA1-RA3: Objektuetara Orientatutako Programazioa

Eskakizuna	Egoera	Implementazioa
------------	--------	----------------

RA1 100% PHP 8.4 kodea OOP osoa PSR-4-ekin

RA2 100% 25 klase dokumentatutako konstruktoreekin

RA3 100% Klase hierarkia implementatua

RA5: Aplikazio Segurtasun Maila

- RA5.a** ✓ 100% OWASP ASVS 2. maila implementatua

- RA5.b** ✓ 100% RRHH Ataria = ASVS 2. maila (datu sentikorrak)

RA6: Web Zaurgarritasunak

Eskakizuna Egoera **Implementazioa** **Babesa**

- RA6.a** ✓ 100% Zerbitzari aldeko + bezero aldeko balidazioa XSS, SQLi kontra

- RA6.b** ✓ 100% Prepared statements + CSP goiburuak SQLi, XSS kontra

- RA6.c** ✓ 100% bcrypt (pasahitzak) + AES-256-GCM (datuak) OWASP Top 10 A02:2021

OWASP Top 10 (2021) Egiaztapen Zerrenda:

- ✓ A01:2021 | ✓ A02:2021 | ✓ A03:2021 | ✓ A04:2021 | ✓ A05:2021 | ✓ A06:2021 | ✓ A07:2021 | ✓ A08:2021 | ✓ A09:2021 | ✓ A10:2021

RA7: Mugikor Segurtasuna

Eskakizuna Egoera **Implementazioa**

- RA7.a** ✓ 100% Android 15 runtime baimenak

- RA7.b** ✓ 100% EncryptedSharedPreferences + Keystore

Implementatutako Android Segurtasuna: - Certificate pinning (anti MITM) - Root detekzioa - Debugger detekzioa - ProGuard/R8 ofuskazioa - Biometrikoa autentikazioa

RA8: Despliegue Sistema Seguruak

Eskakizuna Egoera Implementazioa

- RA8.a** 100% CI/CD pipeline GitHub Actions-eki

- RA8.b** 100% Git + GitFlow workflow

- RA8.c** 100% Test automatizatuak + SAST + DAST

DevSecOps Pipeline-a:

```
# .github/workflows/security-scan.yml
```

Pausoak:

- #### 1. Kodea Eskaneatu (SAST)

- SonarQube

- PHPStan (maila 9)

- Psalm

- ## 2. Dependentziak Eskaneatu

- #### - OWASP Dependency Check

- ## - Snyk

3. Sekretoak Detektatu
 - GitLeaks
 - TruffleHog
 4. Container Eskaneatu
 - Trivy
 - Grype
 5. DAST Eskaneatu
 - OWASP ZAP
 - Nuclei
 6. Kode Kalitatea
 - PHPUnit (90%+ coverage)
 - PHP_CodeSniffer (PSR-12)
-

4. Auzitegi-analisi Informatikoa (Auzitegia)

Eskakizuna	Egoera	Implementazioa	ZAIN
RA2	30% Oinarrizko prozedura dokumentatua	Praktika + tresnak falta	
RA3	20% Kustodio kate txantiloia	Cellebrite prestakuntza falta	
RA4	40% Google Cloud log-ak eskuratuta	Analisi aurreratua falta	
RA5	0% Ez aplikatzen (RRHH-n IoT gabe)	N/A	
RA6	50% Peritaje txosten txantiloia	Baliozkotze juridikoa falta	

BEHARRREZKO EKINTZAK (Auzitegia):

Praktika Eszenatokia: Ransomware simulazioa laborategi ingurunean

- 1. Fasea: Prestakuntza (1. Astea)**
 - 2. Fasea: Analisia (2. Astea) - RA2.a** - Fitxategi sistema analisia - **RA2.b** - Ezabatutako fitxategien berrespena - **RA2.c** - Malware analisia
 - 3. Fasea: Android Auzitegia (3. Astea) - RA3.a** - Eskuratzeko prozesua - **RA3.b** - Estraktatzea eta analisia
 - 4. Fasea: Hodei Auzitegia (4. Astea) - RA4.a** - Hodei analisi estrategia - **RA4.b** - Kausa, esparrua eta eragina identifikatu
 - 5. Fasea: Peritaje Txostena (5. Astea) - RA6.a** - Txostenaren esparrua definitu - **RA6.b** - Araudi juridikoa
-

5. Hacking Etikoa

Eskakizuna	Egoera	Implementazioa	KANPO AUDITORIA
RA2	60% WiFi korporatiboa WPA3-Enterprise-rekin	Kanpo auditoria falta	

Eskakizuna	Egoera	Implementazioa	KANPO AUDITORIA
RA3	50% Nessus zaurgarritasun analisia		Pentest osoa falta
RA4	0% Ez eginik		Auditoria zain
RA5	70% OWASP ZAP automatikoa		Pentesting manuala falta
RA6	40% MobSF analisi estatikoa		Reversing osoa falta

SEGURITASUN AUDITORIA PLANA (Hacking Etikoa):

Enpresa kanpoko ziurtagiria kontratatu (OSCP, CEH) auditoria osorako:

Faseak: Reconocimiento → Vulnerabilidades → Explotación → Web → Mobile → Wireless

Entregagarriak: - Txosten exekutiboa (zuzendaritzarako) - Txosten tekniko xehea (IT-rako) - Lehentasunezko zaurgarritasun zerrenda (CVSS puntuazioak) - Konponketa plana - Re-test konponketen ondoren

Kostu estimatua: 12.000€ - 18.000€ (kanpo enpresa)

6. Araudia (Araudia eta Betetzea)

RA1: Betetze Puntuak

Eskakizuna	Egoera	Implementazioa
RA1.a	100% ISO 27001:2022 + GDPR + ENS	
RA1.b	100% Kode etikoa + politikak dokumentatuak	

RA2: Aplikagarri Legegintza

Eskakizuna	Egoera	Implementazioa
RA2.a	100% LOPD-GDD, LSSI-CE, Penal Kodea	
RA2.b	100% CCN-CERT gidek aplikatuak	

RA4: Datu Pertsonalen Babesa

Eskakizuna	Egoera	Implementazioa
RA4.a	100% GDPR (UE) 2016/679 + LOPD-GDD	
RA4.b	100% 6 GDPR printzipio implementatuak	

Implementatutako GDPR Printzipioak:

1. **Legezkoak, leialak eta gardenak**
2. **Helburu mugaketa**

- Datu minimizazioa**
 - Zehaztasuna**
 - Atxikipen epe mugaketa**
 - Osotasuna eta konfidentzialitasuna**

ARCO-POL Eskubideak Implementatuak:

- **Sarbidea:** API /api/datu-pertsonalak/nireakoak
 - **Zuzenketa:** Eguneratzeko formularioa
 - **Ezabaketa:** “Ahazteko eskubidea” salbuespen legezkoekin
 - **Aurkakotasuna:** Aurkakotasun formularioa
 - **Eramangarritasuna:** JSON/CSV esportazioa
 - **Tratamendu mugaketa:** Datu-basean flag-a

RA5: Zibersegurtasun Araudia

Eskakizuna	Egoera	Implementazioa
RA5.a	 100%	Hiruhileko berrikuspena + BOE harpidetza
RA5.b	 100%	INCIBE + CCN-CERT + AEPD sarbidea

Gaitasun Zeharkakoak (Zeharkakoak)

Ebaluazioa eta Ponderazioa

Noten Banaketa: - Talde nota (Gaitasun Teknikoak): 50% - Banako nota (Gaitasun Zeharkakoak): 50%

1. Autonomia (25% - Irakasleek ebaluatua)

Maila	Deskribapena	Puntuak
Bikaina	Arazo konplexuak gainbegiratu gabe konpontzeko gaitasuna. Oinarritutako erabaki teknikoak hartzea.	9-10
Nabarmena	Behin behineko gainbegirapena behar du. Gehienak modu independentean konpondu.	7-8
Gaindituta	Ohiko gainbegirapena behar du. Oinarrizko arazoak modu autonomoan konpondu.	5-6
Nahikoa ez	Irakaslearen mendekotasun konstantea. Ez du ekimenik hartzen.	0-4

2. Implikazioa (25% - Irakasleek eta ikasleek ebaluatua)

Aspektua	Adierazleak	Pisu
Asistentzia	>95% asistentzia = 10 pts, <80% = 0 pts	30%
Puntualitatea	<3 berandu = 10 pts, >10 = 0 pts	20%
Parte hartzea	Klasean eta taldean ekarpen aktiboak	30%

Aspektua	Adierazleak	Pisu
----------	-------------	------

Lanaren kalitatea Entregatuetan ahalegin eta dedikazio nabarmena 20%

3. Ahozko Komunikazioa (20% - Aurkezpena)

Aspektua	Bikaina (9-10)	Nabarmena (7-8)	Gaindituta (5-6)	Nahikoa ez (0-4)
Argitasuna	Azalpen gardena, zalantzarak gabe	Azalpen argia xehetasun txikiiekkin	Azalpen ulertzeko nahasmenekin	Azalpen nahasia
Egitura	Logika bikaina, jarraitu erraza	Egitura ona trantsizioekin	Egitura oinarrizkoak	Egitura argirik gabe
Tekniko dominioa	Galdera guztiak segurtasunez erantzun	Gehienak erantzun	Oinarrizkoak erantzun	Ez du materia menperatzen
Euskara teknikoa	Terminologia tekniko zuzena euskaraz	Ondo erabilia anglizismo batzuekin	Oinarrizkoak, anglizismo asko	Okerra

4. Talde Lana (30%)

Aspektua	Adierazleak	Pisu
Lankidetza	Laguntza aktiboa, ezagutza partekatzea	30%
Gatazka ebazpena	Desadosaketa eraikitzalean kudeatzea	20%
Konpromiso betetzea	Esleitutako zereginak garaiz entregatzea	30%
Barne komunikazioa	Taldea informatuta mantentzea	20%

Proiektuaren Garapena eta Ebaluazioa

Planifikazioa (Garapenaren 20%)

Planifikazio Entregagarriak:

1. Proiektu Plana (1. Astea)

- Gantt diagrama (46 saio)
- Kide bakoitzeko zeregin banaketa
- Helburuak eta deadlines-ak
- Dependentziaren identifikazioa

Dokumentazioa (Garapenaren 40%)

Dokumentazio Entregagarriak (Dena Euskaraz):

1. Dokumentazio Teknikoa

2. Segurtasun Dokumentazioa
3. Betetze Dokumentazioa

Kontrol Puntuak / Jarraipena (Garapenaren 40%)

Beharrezko Kontrol Puntuak:

Saioa	Helburua	Entregagarriak	% Osatua
10	1. Kontrol Puntuak Diseinu osoa + Segurtasun plana	20%	
20	2. Kontrol Puntuak Backend funtzionala + Auth MFA	45%	
30	3. Kontrol Puntuak Mugikor app + SIEM konfiguratura	70%	
40	4. Kontrol Puntuak Test osoa + Dokumentazioa		90%
46	Entrega Finala Proiektu osoa + Aurkezpena		100%

Egutegi Xehea (46 Saio)

Urtarrila 2026

Data	Saioa	Jarduera	Entregagarria
7 Urt	1	Erronka 3 aurkezpena (klasea)	-
8 Urt	2	Teoria klasea	-
9 Urt	3	Teoria klasea	-
12-23 Urt	4-9	Teoria klaseak	-
26-29 Urt	-	AZTERKETAK	-
30 Urt	10	Erronka 4 - Proposamena	Proiektu proposamena

Otsaila 2026

Data	Jarduera	Helburua
2-6 Ots	Saioak 11-15: Analisia eta Diseinua	Arkitektura definitua
9-13 Ots	Saioak 16-20: Backend Implementazioa	1. Kontrol Puntuak (20%)
16-18 Ots	JAI EGUNAK (festiboak)	-
19-20 Ots	Saioak 21-22: Backend Jarraipena	-

Data	Jarduera	Helburua
23-27 Ots	Saioak 23-27: Segurtasuna + SIEM	MFA implementatua

Martxoan 2026

Data	Jarduera	Helburua
2-6 Mar	Saioak 28-32: Android App	2. Kontrol Puntu (45%)
9-13 Mar	Saioak 33-37: OT Hardening	Sare segmentazioa osatua
16-20 Mar	Saioak 38-42: Test + Auzitegia	3. Kontrol Puntu (70%)
23 Mar	Saioa 43: Segurtasun auditoria	Pentesting txostenetan
24 Mar	ERRONKA 4 AURKEZPENA	Entrega finala

Azken Entregagarriak

GitHub Repository Egitura

```
erronka4/
├── README.md          # Proiektu laburpena
├── COMPLIANCE_PLAN.md # Dokumentu hau
└── Zabala Gailetak/
    ├── hr-portal/      # Backend PHP
    │   ├── src/          # Euskarazko iturburu kodea
    │   ├── tests/         # PHPUnit testak (90%+ coverage)
    │   ├── config/        # Konfigurazioak
    │   ├── migrations/   # DB migrazioak
    │   └── docs/          # Dokumentazio teknikoa
    ├── android-app/     # Android mugikor app-a
    │   ├── app/src/main/kotlin/ # Euskarazko Kotlin kodea
    │   ├── app/src/test/    # Unitate testak
    │   └── docs/           # Android dokumentazioa
    ├── infrastructure/  # Infrastruktura
    │   ├── docker/         # Docker Compose fitxategiak
    │   ├── ansible/        # Hardening playbook-ak
    │   ├── terraform/      # IaC cloud-erako
    │   └── ot/              # OT konfigurazioa
    ├── security/         # Segurtasuna
    │   ├── siem/           # SIEM konfigurazioa
    │   ├── dlp/             # DLP politikak
    │   ├── firewall/       # pfSense arauak
    │   └── pentest/        # Pentesting txostenak
    └── compliance/       # Betetzea
        ├── sgsi/            # ISO 27001 dokumentuak
        ├── gdpr/            # GDPR dokumentuak
        ├── forense/          # Auzitegi prozedurak
        ├── gorabeherak/     # Gorabehera erantzuna
        └── training/         # Prestakuntza materialak
└── docs/
```

arquitectura/	# Arkitektura diagramak
manuales/	# Erabiltzaile gideak
presentacion/	# Azken aurkezpena (PDF + PPT)
scripts/	
setup/	# Instalazio script-ak
backup/	# Backup script-ak
monitoring/	# Monitorizazio script-ak

Proiektuaren Arrakasta Irizpideak

Helburu Teknikoak

Sistema Funtzionala: - RRHH atari web osoa (login, langileen kudeaketa, oporrak, nominak, txat) - Android mugikor app-a funtzionala ezaugarri guztiekin - API REST osoa eta dokumentatua - PostgreSQL datu-base optimizatua

Segurtasun Sendoa: - ISO 27001:2022 %100 betetzea - GDPR %100 betetzea - Zaurgarritasun kritiko edo alturik gabe - MFA beharrezkoa erabiltzaile guztientzat - End-to-end enkriptazioa

Operazionala: - Eskuragarritasuna >99.5% - API erantzun denbora <200ms (p95) - Eguneko backup automatikoak - 24/7 monitorizazioa alertekin

Ikaskuntza Helburuak

Eskuratutako Gaitasun Teknikoak: - SGSI diseinua eta implementazioa - Sistema eta sare hardening - Garapen segurua (OWASP) - Auzitegi analisi digitala - Pentesting etikoa - Araudi betetzea (GDPR, ISO 27001)

Garaturiko Gaitasun Zeharkakoak: - Talde lana eraginkorra - Euskaraz komunikazio teknikoa - Proiektu kudeaketa - Arazo konplexuen ebazpena - Autonomia eta auto-ikaskuntza

Baliabideak eta Erabilitako Tresnak

Software eta Teknologiak

Garapena: - PHP 8.4, Kotlin 2.0, PostgreSQL 16, Redis 7 - Jetpack Compose, Material 3 - Docker, Docker Compose - Git, GitHub, GitHub Actions

Segurtasuna: - pfSense (Firewall) - ModSecurity (WAF) - Elastic Stack (SIEM) - OWASP ZAP (DAST) - SonarQube (SAST) - Trivy (Container eskaneatzea)

Auzitegia: - Autopsy, Sleuth Kit - Volatility (memoria) - Wireshark (sarea) - FTK Imager

Pentesting: - Kali Linux - Metasploit, Burp Suite - Nmap, Nikto, SQLMap - MobSF (mugikorra)

Dokumentazio eta Estandarrak

- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- IEC 62443 (OT segurtasuna)
- OWASP ASVS 4.0
- OWASP Top 10 2021

- NIST Cybersecurity Framework
- CIS Benchmarks
- CCN-CERT Gideak

Ikaskuntza Baliabideak

- INCIBE ([www.incibe.es](#))
- CCN-CERT ([www.ccn-cert.cni.es](#))
- AEPD ([www.aepd.es](#))
- OWASP ([www.owasp.org](#))
- ENISA ([www.enisa.europa.eu](#))

Ondorioa

Betetze plan honek Zabala Gailetak-en RRHH Atari proiektuak Erronka 4 **guztien** betetzea bermatzen du, 6 arlo tekniko estaltzen dituena:

1. **Zibersegurtasun Gorabeherak** - SIEM, gorabehera erantzuna, ikaskuntzak
2. **Hardening** - Sare segmentazioa, sistema hardening, IT/OT integrazioa
3. **Garapen Segurua** - OWASP, DevSecOps, mugikor segurtasuna
4. **Auzitegi Analisia** - Prozedurak, tresnak, praktika kasua
5. **Hacking Etikoa** - Kanpo auditoria, pentesting osoa
6. **Araudia** - ISO 27001, GDPR, legezko betetzea

Gainera, **gaitasun zeharkakoak** ebaluatzen dira: - Autonomia (25%) - Inplikazioa (25%) - Ahozko komunikazioa (20%) - Talde lana (30%)

Proiektu Nota: - 50% Gaitasun Teknikoak (taldea) - 50% Gaitasun Zeharkakoak (banakoa)

Hurrengo Urratseko Ekintzak:

1. **1-2. Astea:** Auzitegi analisia osatu (ransomware kasua)
2. **3. Astea:** Pentesting kanpo auditoria kontratatu
3. **4. Astea:** OT segmentazioa osatu
4. **5. Astea:** Euskarazko dokumentazioa amaitu
5. **6. Astea:** Azken aurkezpena prestatu

Dokumentua prestatua: Zabala Gailetak Taldeak

Azken eguneraketa data: 2026ko Urtarrilaren 24a

Bertsioa: 2.0

Egoera: OSATUA - Implementaziorako prest