ZIBERSEGURTASUN AHOLKULARITZA

Zabala Gailetak

Digital Segurtatuta

Proiektuaren Entrega Exekutiboa

2026ko Otsaila · Zuzendaritza Batzordeari Aurkezpena

PROIEKTU LABURPENA

6
Modulu Seguritate

14
Zerbitzari VM

0
Arazo Kritiko

93%
ISO 27001 Betetzea

Zabala Gailetak eta Industria 4.0: Transformazioaren Argia eta Itzala

01

Ekoizpen Tradizionala

Fabrika isolatua, makineria analogikoa, paper-erregistroak eta prozesu manuala

02

Digitalizazio Hasiera

OpenPLC kontrolagailua, SCADA HMI sistema eta bulegoko sare konektatu berria

03

Industria 4.0 Gaur

Cloud zerbitzuak, app mugikorra, RRHH portala eta denbora errealeko datu-elkartrukea

ZABALA GAILETAK EN DATUAK

120	3
Langile	Txanda / Egun
5	6
VLAN Sare	VM Zerbitzari

IT eta OT Konektatzen Direnean: Arrisku Kritikoa

BULEGOA — IT SAREA

- Posta elektronikoa (phishing bektore #1)
- Langile-estazio pertsonalak (100+)
- Internet sarbidea zuzenekoa
- Cloud zerbitzuak: ERP, Office 365

!

FABRIKA — OT/SCADA SAREA

- OpenPLC kontrolagailua (ekoizpen-lerro osoa)
- SCADA HMI sistema (ScadaBR, port 9090)
- Tenperatura-sentsoreak (Modbus TCP 502)
- **PORT 502 / OPC-UA: INTERNETI IREKITA!**

Auditorian aurkitutako arrisku kritikoa: OT sistemak Interneti zuzenean irekita zeuden. Ekoizpen-lerro osoa urrunetik geldiarazi zitekeen.

"Ez Fidatu, Beti Egiaztatu" Zero Trust Segurtasun Arkitektura

Emaitza: Erasotzaileak sare barnera sartu arren, ezin du mugitu lateralki sistema batetik bestera. Datu kritikoak babestuta daude.

1

Inoiz Ez Fidatu

Sare barnekoa izanda ere, erabiltzaile eta gailu oro susmagarri jotzen da autentifikazio arrakastatsu baten arte

2

Beti Egiaztatu

MFA, JWT tokenak eta RBAC (5 rol) erabiliz, sarbide bakoitza indibidualizatuta egiaztatzen da banan-banan

3

Pribilegio Minimoa

Langile bakoitzak beharrezko datutara soilik du sarbidea. Ez gehiago, ez gutxiago. Kalte posiblea mugatzen da

Sare Segmentazioa: Etxe Bakoitza Bere Aterekin (VLAN Arkitektura)

VLAN	IZENA	IP TARTEA	HELBURUA / OHARRA
VLAN 10	Bulegoa / Kudeaketa	192.168.10.0/24	Langile-estazioak (100+)
VLAN 20	IT / Zerbitzariak	192.168.20.0/24	Web, PHP 8.4, PostgreSQL 16, Redis
VLAN 30	DMZ (Ingurune Desmilitarizatua)	192.168.30.0/24	Internet zerbitzuak: web, posta
VLAN 40	**OT / SCADA (ISOLATUA)**	192.168.40.0/24	**OpenPLC + ScadaBR — Data Diode bidez soilik**
VLAN 99	Honeypot Sarea	172.16.99.0/24	Erasotzaileak erakartzeko tranpa aktibo

VLAN 40 (OT/SCADA) erabat isolatua dago. Bulegotik ezin da zuzenean komunikatu. Datuen elkartrukea Data Diode baten bidez bakarrik, norabide bakarrean (fabrikatik bulegora).

Azpiegitura Adimentsua: Proxmox, Ansible eta IsardVDI

ZG-Gateway

Router / Suebaki

1 vCPU · 1 GB RAM

ZG-App

PHP 8.4 · Nginx · Redis

2 vCPU · 4 GB RAM

ZG-Data

PostgreSQL 16 BBDD

2 vCPU · 4 GB RAM

ZG-SecOps

Wazuh SIEM · Honeypot

4 vCPU · 8 GB RAM

ZG-OT

OpenPLC · ScadaBR

1 vCPU · 2 GB RAM

ZG-Client

Langile-Estazioa (IsardVDI)

2 vCPU · 4 GB RAM

Ansible bidez automatizatutako konfigurazioa · Proxmox hiperbisorearen gainean · IsardVDI ikasgela birtual gisa erabilita

Langile-Tresnak: RRHH Portala eta App Mugikorra

RRHH WEB PORTALA

Autentifikazio Anizkoitza (3 geruza)

JWT + TOTP MFA (RFC 6238) + WebAuthn pasahitz fisikoak — Erasotzailearentzat hiru hormak

RBAC 5 Rolen Sistema

ADMIN, RRHH_MGR, JEFE_SECCION, EMPLEADO, AUDITOR — Pribilegio minimoa bermatu

Funtzionalitateak

Oporrak, nomina ikustea, dokumentu zifratu deskargak, txat WebSocket denbora errealekoa

Segurtasun-goiburuak (OWASP)

HSTS, CSP, X-Frame-Options, TLS 1.3 — OWASP Top 10 zerrenda osoa kontuan hartuta

APP MUGIKORRA (ANDROID)

Kotlin 2.0 + Jetpack Compose

Material 3 diseinua, Clean Architecture + MVI eredua, Hilt dependency injection

Certificate Pinning aktibo

TLS ziurtagiriak aplikazioan kodetuta — Man-in-the-Middle erasoak ezinezko

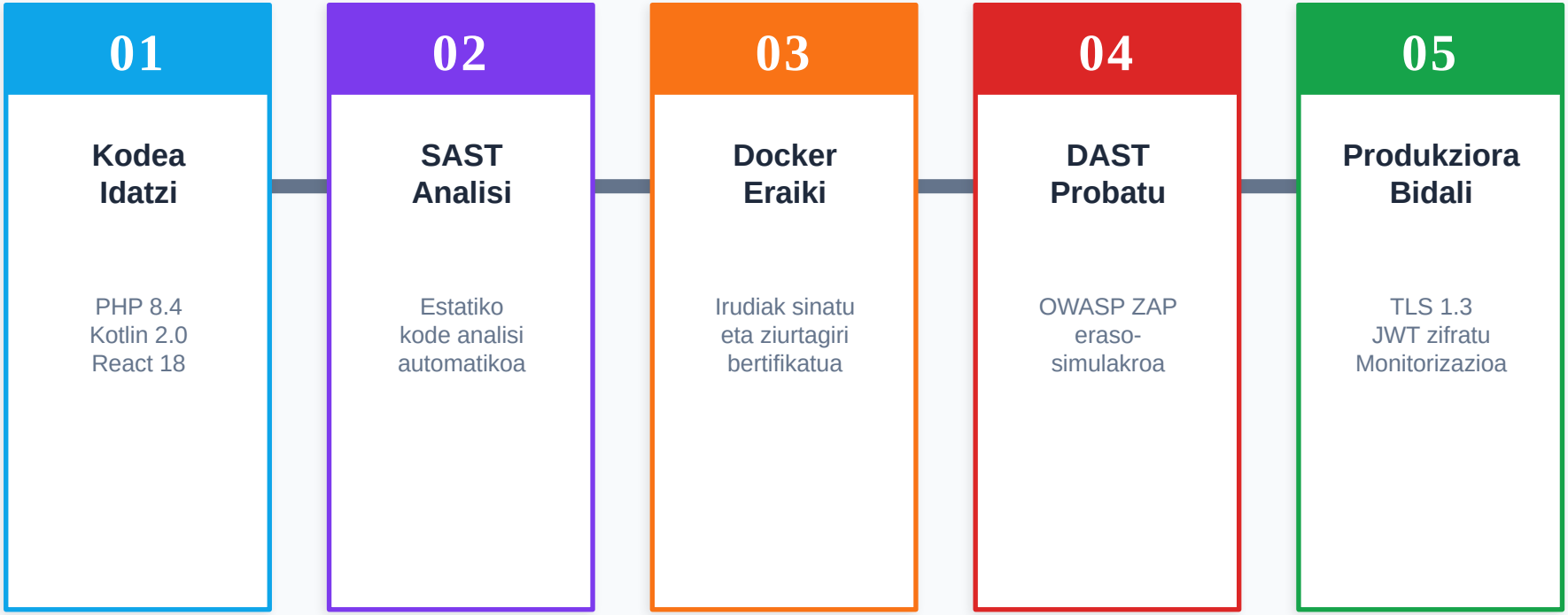
CI/CD automatikoa

GitHub Actions bidez eraikia eta sinatua — SHA-256 egiaztatzapena banatzerakoan

App Transport Security (HTTPS)

Cleartext konexiorik ez baimentzen da inoiz — Sare guztiak enkriptatuta

Segurtasuna Hasieratik: DevSecOps Pipeline eta Edukiontzi Estrategia



"Shift Left" printzipioa: segurtasun-arazoak kodean aurkitzea produkzioan konpontzea baino 100x merkeagoa da.

Gure Defentsak Probatu Ditugu: Pentesting eta WiFi Auditoriaren Emaitzak

0 — Arazo Kritiko

CVSS 9.0+ — Sektorearen gailurrean

2 — Arazo Garrantzitsu

CVSS 7.5-7.8 — Biok konponduta

4 — Arazo Ertain

CVSS 5.3-6.5 — Guztiak kontrolpean

3 — Arazo Txiki

CVSS 3.1-4.3 — Dokumentatuta

WiFi Auditoria (PTES metodologia): 4 eszénario probatu (WPA2-PSK, WPA3-SAE, Open, Hidden SSID). Gomendio nagusia: WPA3-Enterprise + 802.1X + RADIUS zerbitzaria.

Begiak Beti Irekita: Wazuh SIEM eta Denbora Errealeko Monitorizazioa

SIEM SISTEMAREN BALIOA

1. **Denbora errealeko monitorizazioa**
   Suebakia, zerbitzariak, web-aplikazioa eta OT gailuak aldi berean ikusten ditu

2. **Alerta automatikoak**
   5 saiakera huts / minutu: blokeo automatikoa. Eskaner berria: jakinarazpen berehalakoa

3. **FIM (File Integrity Monitoring)**
   Edozein fitxategi kritikoren aldaketa detektatzen eta jakinarazten du segundotan

4. **Kibana panel bisuala (port 5601)**
   Incidenteak kolore bidez sailkatuta, joerak grafikoetan, erantzuteko pista argiak

ALERTA ARAUAK (ADIBIDEAK)

KRITIKOA
Pribilegioaren eskalada detektatua

ALTUA
Brute-force erasoa (5 huts. / minutu)

ERTAINA
Eskaner berria OT sarean detektatua

BAXUA
Port-eskanerrak kanpotik detektatuta

Tranpak Erasotzaileentzat eta Plan Aktiboa Erantzuteko

HONEYPOT ESTRATEGIA

Cowrie	SSH/Telnet tranpa. Saiakera guztiak grabatu, erabiltzaile+pasahitz patroiak analizatu
Conpot	OT/ICS simulakroa. Modbus TCP baimendua. Industria-erasotzaileak erakarri eta detektatu
T-Pot	Plataforma orokor. GeoIP jatorria, malware-laginen bilketa eta analisi automatikoa

Sare isolatua: 172.16.99.0/24 | Produktioan eraginik ez

INCIDENT RESPONSE PLANA

0-24 h

Detekzioa eta lehenengo albistea

24-72 h

Analisi zehatza + NIS2 txosten ofiziala

72 h+

Konponketa eta sistema-berreskurapena

Post

Forentse-analisia + Ikaskuntzak dokumentatu

Forentse-analisia: log-ak, memoria-argazkiak eta artefaktuen azterketa

Lege-Betetzea: NIS2 Direktiba, RGPD eta IEC 62443

NIS2 DIREKTIBA

60% · Helburua: 2026ko Urria

- Enpresa 'GARRANTZITSUA' gisa sailkatua (Art. 3)
- 24 h: Lehenengo jakinarazpena autoritate eskudunari
- 72 h: Txosten osoa incidente larriari buruz
- Hornidura-kate segurtasuna (Art. 21.2.e)
- Q4 2026: Betetze osoa planifikatua

RGPD / GDPR

100% · Beteta

- DPIA ebaluazioak (RRHH portala + OT sistemak)
- Datu-tratamendu erregistroa (RoPA) osatuta
- Eskubide-prozedurak dokumentatuta (ARCO+)
- Datuen babesa diseinutik bertatik (Privacy by Design)
- Cookie politika eta uko egiteko aukerak aktibo

IEC 62443

70% · SL2 Lortuta

- Purdue Eredua (0-5 mailak) ezarrita OT sisteman
- Zona / Konduit segmentazioa (IT/OT bereiztea)
- SL 2 lortua: autentifikazioa + auditoria aktibo
- Data Diode: telemetria uni-norabidekoa
- SL 3 bidea (sistema kritikoak): Q3 2026

ISO 27001:2022 — 87 / 93 kontrol aktibo (93% betetzea) · OWASP Top 10 — A01-A09 mitigazioak dokumentatuta

Balio Ekonomikoa eta Etorkizunerako Bide-orria

ZERGATIK MEREZI DU INBERTSIO HONEK?

10M€+
NIS2 zigor posibla (%2 fakturazioa)

24/7
SIEM monitorizazioa aktibo

100%
RGPD betetzea — isun-arriskua zero

0
Arazo kritiko aurkitua pentesting-ean

BIDE-ORRIA 2026

V **Q1 2026**
Gap analisia (done) · MFA %100 · NIS2 hasiera

2 **Q2 2026**
EDR zabalkundea · SIEM 24/7 · CSIRT taldea · Vendors

3 **Q3 2026**
IEC 62443 SL3 · BCP probak · Pentest urtekoa

4 **Q4 2026**
NIS2 BETETZE OSOA (Urria 17) · ISO 27001 auditoria

06 · ONDORIOAK ETA GALDERAK

Zabala Gailetak, Seguru eta Etorkizunerako Prest

- Zero Trust + 5 VLAN segmentazio → OT sarea erabat babestuta
- Pentesting: 0 arazo kritiko — Aurkikuntzak guztiak konponduta
- Wazuh SIEM + Honeypots: Monitorizazioa 24/7, incidenteekiko prest
- RGPD %100 · ISO 27001 %93 · NIS2 bidean (2026ko Urria)

GALDERAK ?

Zuzendaritza Batzordeak eta CEO jaunak nahi dituzten galderak jasotzeko prest gaude.