

Aplikagarritasun Adierazpena (SOA)

Zabala Gailetak S.L.

ISO/IEC 27001:2022

Bertsioa: 1.0

Data: 2026ko Urtarrilaren 8a

Sailkapena: Barnekoa - Konfidentziala

Dokumentuaren Kontrola

Bertsioa	Data	Egilea	Aldaketak
1.0	2026-01-08	CISO	Hasierako SOA sorrera

Onartua: Informazioaren Segurtasuneko Arduradun Nagusia (CISO)

Berrikuspen Data: 2026-07-08 (6 hilabete)

1. Sarrera

1.1 Helburua

Aplikagarritasun Adierazpen (SOA) honek dokumentatzen du ISO/IEC 27001:2022 A Eranskinetako zein kontrol diren aplikagarriak Zabala Gailetak-en Informazioaren Segurtasuna Kudeatzeko Sistemari (ISMS/SGSI) eta barne hartzeko edo baztertzeko erabakiak justifikatzen ditu.

1.2 Esparrua

ISMS esparruak honako hauek hartzen ditu barne:

- IT Azpiegitura:** Zerbitzariak, sareak, datu-baseak, hodeiko zerbitzuak
- OT Sistemak:** Produkzio kontrol sistemak, SCADA, PLCak
- Aplikazioak:** Web aplikazioak, mugikor aplikazioak, ERP sistemak
- Datuak:** Bezeroen datuak, negozio informazioa, jabetza intelektual
- Langileak:** 120 langile guztiak, kontratistak, hirugarrenak
- Kokapenak:** Donostiako instalazio nagusia eta urruneko langileak

1.3 ISMS Testuingurua

Zabala Gailetak IT eta OT sistema integratuak dituen gaileta fabrikazio enpresa bat da. Gure ISMS-k honako hauek jorratzen ditu:

- Bezeroen datu pertsonalen babesa (GDPR betetzea)
 - Teknologia operatiboaren segurtasuna (produkzio sistemak)
 - Hornidura katearen segurtasuna
 - Zibersegurtasun mehatxuak fabrikazio eragiketetarako
-

2. A Eranskinaren Kontrolen Ebaluazioa

A.5 Antolakuntza Kontrolak (37 kontrol)

A.5.1 Informazioaren segurtasunerako politikak

Egoera:  **Inplementatuta**

Justifikazioa: Informazioaren Segurtasun Politika ezarrita eta zuzendaritzak onartuta.

Ebidentzia: Informazioaren Segurtasun Politika 1.0 bertsioa (betetze pakete honetan dokumentatua)

Inplementazioa: Zuzendaritzak onartutako politika langile guztiei jakinarazia intranet eta onboarding bidez.

A.5.2 Informazioaren segurtasun rolak eta erantzukizunak

Egoera:  **Inplementatuta**

Justifikazioa: Rol definituta, CISO, Segurtasun Taldea, Sistema Administrazioaileak barne.

Ebidentzia: Antolakuntza-karta, lan deskribapenak, erantzukizun matrizea

Inplementazioa: RACI matrizea sortuta, erantzukizunak esleituta eta dokumentatuta.

A.5.3 Eginkizunen bereizketa

Egoera:  **Inplementatuta**

Justifikazioa: Rol kritikoak bereizita iruzurra eta erroreak prebenitzeko.

Ebidentzia: Sarbide kontrol politikak, onarpen lan-fluxuak

Inplementazioa: Garapen, proba eta produkzio inguruneak bereizita. Pertsona bakar batek ezin du kodea hedatu eta aldaketak onartu.

A.5.4 Zuzendaritzaren erantzukizunak

Egoera:  **Inplementatuta**

Justifikazioa: Zuzendaritza konprometituta ISMS-rekin baliabide esleipenarekin.

Ebidentzia: ISMS aurrekontu onarpena, zuzendaritza berrikuspen bilerak

Implementazioa: Hiruhileko kudeaketa berrikuspenak, urteko ISMS aurrekontua.

A.5.5 Agintariekin harremana

Egoera:  **Implementatuta**

Justifikazioa: Kontaktuak ezarrita Datuen Babeserako Espainiako Bulegoarekin (AEPD), tokiko poliziarekin.

Ebidentzia: Kontaktu zerrenda, intzidente erantzun plana

Implementazioa: Larrialdi kontaktuak dokumentatuta, harremanak mantenduta.

A.5.6 Interes talde bereziekin harremana

Egoera:  **Implementatuta**

Justifikazioa: Zibersegurtasun foroetan eta industria taldeetan parte hartzea.

Ebidentzia: Kidetza erregistroak, mehatxu inteligentzia harpidetzak

Implementazioa: Zibersegurtasun Euskal Zentroko kidea, INCIBE alertak harpidetuta.

A.5.7 Mehatxu inteligentzia

Egoera:  **Implementatuta**

Justifikazioa: Mehatxu inteligentzia jarioak SIEM-en integratuta.

Ebidentzia: SIEM konfigurazioa, mehatxu inteligentzia harpidetzak

Implementazioa: MITRE ATT&CK esparrua erabilia, mehatxu jario automatizatuak.

A.5.8 Informazioaren segurtasuna proiektu kudeaketan

Egoera:  **Implementatuta**

Justifikazioa: Segurtasun baldintzak proiektuaren bizi-zikloan sartuta.

Ebidentzia: Proiektu txantiloiak, segurtasun kontrol-zerrendak

Implementazioa: Segurtasun berrikuspen atea plangintza, garapen, implementazio faseetan.

A.5.9 Informazioaren eta lotutako beste aktiboen inbentarioa

Egoera:  **Implementatuta**

Justifikazioa: Aktiboen erregistroa mantenduta sailkapenekin.

Ebidentzia: Aktiboen erregistro kalkulu-orria, CMDB

Implementazioa: IT/OT aktibo guztien datu-basea, jabeak esleituta, urteko berrikuspena.

A.5.10 Informazioaren eta lotutako beste aktiboen erabilera onargarria

Egoera:  **Implementatuta**

Justifikazioa: Erabilera Onargarriaren Politika (AUP) definituta.

Ebidentzia: AUP dokumentua (pakete honetan)

Implementazioa: Langile guztiek AUP sinatzen dute onboarding-ean.

A.5.11 Aktiboen itzulketa

Egoera:  **Implementatuta**

Justifikazioa: Amaiera kontrol-zerrendak aktiboen itzulketa ziurtatzen du.

Ebidentzia: HR amaiera prozesua, aktiboen jarraipena

Implementazioa: IT ekipamendua, sarbide txartelak, giltzak azken egunean jasota.

A.5.12 Informazioaren sailkapena

Egoera:  **Partzialki Implementatuta**

Justifikazioa: Oinarrizko sailkapena (Publikoa, Barnekoa, Konfidentziala, Mugatua).

Ebidentzia: Sailkapen politika zirriborroa

Implementazioa: Politika definituta baina ez guztiz hedatuta. Ekintza: Dokumentu guztien sailkapen marka osatu 2026ko 2. hiruhilekorako.

A.5.13 Informazioaren etiketatzea

Egoera:  **Partzialki Implementatuta**

Justifikazioa: Etiketa digitalak sistema batzuetan, etiketa fisikoak falta dira.

Ebidentzia: Email oinak, dokumentu txantiloak

Implementazioa: Email sailkapen etiketak implementatuta. Ekintza: Dokumentu sailkapen ur-markak implementatu.

A.5.14 Informazio transferentzia

Egoera:  **Implementatuta**

Justifikazioa: Fitxategi transferentzia seguru prozedurak ezarrita.

Ebidentzia: Datu transferentzia politika, enkriptatze estandarrak

Implementazioa: SFTP, HTTPS soilik. USB unitateak enkriptatuta. Email enkriptatzea eskuragarri.

A.5.15 Sarbide kontrola

Egoera:  **Implementatuta**

Justifikazioa: Roletan Oinarritutako Sarbide Kontrola (RBAC) implementatuta.

Ebidentzia: Sarbide kontrol politika, Active Directory taldeak

Implementazioa: Pribilegio gutxieneko printzipioa, ohiko sarbide berrikuspenak.

A.5.16 Identitate kudeaketa

Egoera:  **Implementatuta**

Justifikazioa: Identitate kudeaketa zentralizatua Active Directory bidez.

Ebidentzia: Identitate kudeaketa prozedurak

Implementazioa: Kontu bakarrak erabiltzaile guztientzat, zerbitzu kontuak bereizita kudeatuta.

A.5.17 Autentifikazio informazioa

Egoera:  **Implementatuta**

Justifikazioa: Pasahitz politika sendoa, MFA administratzaileentzat.

Ebidentzia: Pasahitz politika (pakete honetan), MFA log-ak

Implementazioa: 12 karaktere gutxienez, konplexutasuna beharrezkoa, MFA derrigorrezkoa admin kontuetarako.

A.5.18 Sarbide eskubideak

Egoera:  **Implementatuta**

Justifikazioa: Sarbide hornikuntza eta deshornikuntza prozesu formala.

Ebidentzia: Sarbide eskaera inprimakiak, onarpen lan-fluxuak

Implementazioa: Kudeatzailearen onarpena beharrezkoa, hiruhileko sarbide berrikuspenak.

A.5.19 Informazioaren segurtasuna hornitzaile harremanetan

Egoera:  **Implementatuta**

Justifikazioa: Hornitzaileen segurtasun ebaluazio prozesua.

Ebidentzia: Hornitzaile kudeaketa SOP (pakete honetan), segurtasun galdetegiak

Implementazioa: Segurtasun baldintzak kontratuetan, urteko hornitzaile berrikuspenak.

A.5.20 Informazioaren segurtasuna hornitzaile akordioetan

Egoera:  **Implementatuta**

Justifikazioa: Segurtasun klausulak hornitzaile kontratu guztietan.

Ebidentzia: Kontratu txantiloak, berrikuspen legala

Implementazioa: NDA, segurtasun estandarrak, auditoretza eskubideak, intzidente jakinarazpen baldintzak.

A.5.21 Informazioaren segurtasuna kudeatzea IKT hornidura katean

Egoera:  **Implementatuta**

Justifikazioa: Software hornidura katearen segurtasuna kontuan hartuta.

Ebidentzia: Dependentsia eskaneatzea (OWASP Dependency-Check), SBOMak

Implementazioa: Dependentsien ahultasun eskaneatze automatizatua CI/CD pipeline-an.

A.5.22 Hornitzaile zerbitzuen monitorizazioa,

berrikuspena eta aldaketa kudeaketa

Egoera:  **Implementatuta**

Justifikazioa: Hornitzaile errendimendu monitorizazioa.

Ebidentzia: Hornitzaile puntuazio-txartela, hiruhileko berrikuspenak

Implementazioa: SLA monitorizazioa, segurtasun intzidente jarraipena hornitzaile bakoitzeko.

A.5.23 Informazioaren segurtasuna hodeiko zerbitzuen erabilerarako

Egoera:  **Inplementatuta**

Justifikazioa: Hodeiko segurtasun politika AWS/Azure erabilerarako.

Ebidentzia: Hodeiko segurtasun politika, CSA STAR ebaluazioa

Inplementazioa: Enkriptatzea geldirik/trantsitoan, hodei segurtasun jarrera kudeaketa.

A.5.24 Informazioaren segurtasun intzidente kudeaketa plangintza eta

prestaketa

Egoera:  **Inplementatuta**

Justifikazioa: Intzidente erantzun plana dokumentatuta.

Ebidentzia: Intzidente Erantzun Plana (security/incident_response/ karpetan)

Inplementazioa: IR taldea identifikatuta, playbook-ak sortuta, hiruhileko mahai-gaineko ariketak.

A.5.25 Informazioaren segurtasun gertaeren ebaluazioa eta erabakia

Egoera:  **Inplementatuta**

Justifikazioa: Gertaera sailkapen irizpideak definituta.

Ebidentzia: Gertaera sailkapen matrizea, SIEM alerta arauak

Inplementazioa: Gertaera korrelazio automatizatua SIEM-en, larritasun mailak esleitura.

A.5.26 Informazioaren segurtasun intzidenteei erantzuna

Egoera:  **Inplementatuta**

Justifikazioa: Intzidente erantzun prozedurak dokumentatuta.

Ebidentzia: IR playbook-ak, komunikazio txantiloiak

Inplementazioa: Edukiera, ezabapena, berreskuratze prozedurak. Auzitegi-tresneria eskuragarri.

A.5.27 Informazioaren segurtasun intzidenteetatik ikastea

Egoera:  **Inplementatuta**

Justifikazioa: Intzidente osteko berrikuspenak eginda.

Ebidentzia: Intzidente txostenak ikasitako ikasgaiekin

Inplementazioa: Erroko kausa analisisa, ekintza zuzentzaileak jarraituta, ezagutza oinarria eguneratuta.

A.5.28 Ebidentzia bilketa

Egoera:  **Inplementatuta**

Justifikazioa: Ebidentzia biltzeko prozedurak auzitegi-analisirako.

Ebidentzia: Auzitegi SOPak (security/forensics/ karpetan)

Implementazioa: Zaintza-kate inprimakiak, ebidentzia kontserbazio tresnak, hash egiaztapena.

A.5.29 Informazioaren segurtasuna etenaldian zehar

Egoera:  **Implementatuta**

Justifikazioa: Negozioaren Jarraitutasun Planak segurtasuna jorratzen du.

Ebidentzia: BCP (pakete honetan)

Implementazioa: Babeskopia guneak, failover prozedurak, krisi komunikazio plana.

A.5.30 IKT prestutasuna negozio jarraitutasunerako

Egoera:  **Implementatuta**

Justifikazioa: IT hondamendi berreskuratze gaitasunak.

Ebidentzia: DR plana, babeskopia proba log-ak

Implementazioa: Eguneroko babeskopiak, hiruhileko DR probak, RTO/RPO definituta.

A.5.31 Lege, estatutu, erregulazio eta kontratu betekizunak

Egoera:  **Implementatuta**

Justifikazioa: Betetze erregistroa mantenduta.

Ebidentzia: Betetze erregistro kalkulu-orria

Implementazioa: GDPR, LOPD, sektoreko araudiak jarraituta. Lege berrikuspena hiruhilero.

A.5.32 Jabetza intelektualaren eskubideak

Egoera:  **Implementatuta**

Justifikazioa: IP babes neurriak indarrean.

Ebidentzia: Software lizentzia erregistroa, IP politika

Implementazioa: Lizentziadun softwarea jarraituta, kode irekiko lizentziak egiaztatuta.

A.5.33 Erregistroen babesa

Egoera:  **Implementatuta**

Justifikazioa: Erregistro atxikipen politika definituta.

Ebidentzia: Erregistro atxikipen egutegia

Implementazioa: Finantza erregistroak 10 urte, HR 5 urte, log-ak 2 urte GDPRren arabera.

A.5.34 Pribatutasuna eta informazio pertsonalaren babesa

Egoera:  **Implementatuta**

Justifikazioa: GDPR betetze programa.

Ebidentzia: GDPR dokumentazio paketea, DBO izendatua

Implementazioa: Pribatutasuna diseinuaren bidez, datuen tratamendu akordioak, interesdunen eskubideen prozedurak.

A.5.35 Informazioaren segurtasunaren berrikuspen independentea

Egoera:  **Implementatuta**

Justifikazioa: Urteroko kanpo auditoria planifikatua.

Ebidentzia: Auditoria kontratua, aurreko auditoria txostenak

Implementazioa: Barne auditoriak hiruhilero, kanpo auditoria urtero.

A.5.36 Informazioaren segurtasunerako politika,

arau eta estandarren betetzea

Egoera:  **Implementatuta**

Justifikazioa: Politika betetze monitorizazioa.

Ebidentzia: Betetze auditoria txostenak, politika egiaztagirak

Implementazioa: Urteroko politika berrikuspena, langileen egiaztagiria, betetze egiaztapen automatizatuak.

A.5.37 Dokumentatutako eragiketa prozedurak

Egoera:  **Implementatuta**

Justifikazioa: SOPak dokumentatuta prozesu kritiko guztietarako.

Ebidentzia: SOP liburutegia infrastructure/systems/ karpetan

Implementazioa: 20+ SOP babeskopia, adabaki, erabiltzaile kudeaketa, intzidente erantzuna estaltzen.

A.6 Pertsona Kontrolak (8 kontrol)

A.6.1 Baheketa

Egoera:  **Implementatuta**

Justifikazioa: Aurrekari egiaztapenak langile guztientzat.

Ebidentzia: HR kontratazio prozedurak

Implementazioa: Aurrekari penalen egiaztapena, erreferentzia egiaztapena, enplegu historia.

A.6.2 Enplegu baldintzak

Egoera:  **Implementatuta**

Justifikazioa: Segurtasun erantzukizunak enplegu kontratuetan.

Ebidentzia: Enplegu kontratu txantiloia

Implementazioa: Konfidentzialtasun klausula, segurtasun betebeharrak, erabilera onargarriaren aitorpena.

A.6.3 Informazioaren segurtasun kontzientziakzioa,

hezkuntza eta prestakuntza

Egoera:  **Implementatuta**

Justifikazioa: Segurtasun kontzientziazio programa ezarrita.

Ebidentzia: Prestakuntza materialak, bertaratze erregistroak

Implementazioa: Urteroko derrigorrezko prestakuntza, phishing simulazioak hiruhilero, segurtasun aholkuak hilero.

A.6.4 Diziplina prozesua

Egoera:  **Implementatuta**

Justifikazioa: Diziplina prozedurak segurtasun urraketetarako.

Ebidentzia: HR politika eskuliburua

Implementazioa: Diziplina politika progresiboa, segurtasun urraketak larritasunaren arabera jorratuak.

A.6.5 Erantzukizunak amaitu edo enplegua aldatu ondoren

Egoera:  **Implementatuta**

Justifikazioa: Amaiera kontrol-zerrendak sarbide baliogabetzea ziurtatzen du.

Ebidentzia: Amaiera SOP

Implementazioa: Sarbidea kendu azken egunean, irteera elkarriketa, aktiboen itzulketa egiaztatua.

A.6.6 Konfidentzialtasun edo ez-ezagutarazte akordioak

Egoera:  **Implementatuta**

Justifikazioa: NDAk sinatuta langileek eta hirugarrenek.

Ebidentzia: NDA txantiloiak, sinatutako kopiak

Implementazioa: Langile, kontratista, bisitari guztiek datu sentikorrek erabiltzen dituztenean NDA sinatzen dute.

A.6.7 Urruneko lana

Egoera:  **Implementatuta**

Justifikazioa: Urruneko lan segurtasun politika.

Ebidentzia: Urruneko lan politika, VPN erabilera jarraibideak

Implementazioa: VPN derrigorrezkoa, enkriptatutako eramangarriak, segurtasun kontzientziazioa etxeko langileentzat.

A.6.8 Informazioaren segurtasun gertaeren jakinarazpena

Egoera:  **Implementatuta**

Justifikazioa: Jakinarazpen kanalak ezarrita.

Ebidentzia: Intzidente jakinarazpen prozedura, telefonoa

Implementazioa: Segurtasun intzidente emaila, telefonoa, web inprimakia, erru gabeko kultura sustatuta.

A.7 Segurtasun Fisiko eta Ingurumen Kontrolak (14 kontrol)

A.7.1 Segurtasun fisiko perimetroak

Egoera:  **Implementatuta**

Justifikazioa: Instalazio sarbide kontrolak.

Ebidentzia: Segurtasun fisiko ebaluazioa

Implementazioa: Hesi perimetroa, segurtasun zaindariak, sarbide txartel irakurgailuak.

A.7.2 Sarrera fisikoa

Egoera:  **Implementatuta**

Justifikazioa: Sarrera kontrolatua instalazioetara.

Ebidentzia: Sarbide kontrol log-ak

Implementazioa: Txartel bidezko sarbidea, bisitarien erregistroa, laguntza politika eremu sentikorretarako.

A.7.3 Bulegoak, gelak eta instalazioak ziurtatzea

Egoera:  **Implementatuta**

Justifikazioa: Zerbitzari gela eta sare armairuak ziurtatuta.

Ebidentzia: Segurtasun ikuskapen txostenak

Implementazioa: Blokeatutako zerbitzari gela, giltza txartel sarbidea, CCTV monitorizazioa.

A.7.4 Segurtasun fisiko monitorizazioa

Egoera:  **Implementatuta**

Justifikazioa: CCTV zaintza sistema.

Ebidentzia: CCTV sistema dokumentazioa

Implementazioa: 24 kamera sarrera puntuak eta eremu sentikorrak estaltzen, 30 eguneko atxikipena.

A.7.5 Mehatxu fisiko eta ingurumenekoen aurkako babesa

Egoera:  **Implementatuta**

Justifikazioa: Ingurumen kontrolak datu zentroan.

Ebidentzia: Instalazio kudeaketa prozedurak

Implementazioa: Sute itzaltzea, HVAC monitorizazioa, UPS potentzia, ur detekzioa.

A.7.6 Eremu seguruetan lan egitea

Egoera:  **Inplementatuta**

Justifikazioa: Mahai garbia politika eremu sentikorretarako.

Ebidentzia: Segurtasun politika, aldizkako auditoriak

Inplementazioa: Mahai garbia behartuta zerbitzari gelan, produkzio solairu sarbidea kontrolatua.

A.7.7 Mahai garbia eta pantaila garbia

Egoera:  **Partzialki Inplementatuta**

Justifikazioa: Politika badago baina betetzea aldatu egiten da.

Ebidentzia: Mahai garbia politika

Inplementazioa: Pantaila blokeo denbora-mugak behartuta (10 min). Ekintza: Betetzea hobetu auditorien bidez.

A.7.8 Ekipamendu kokapena eta babesa

Egoera:  **Inplementatuta**

Justifikazioa: Ekipamendua baimenik gabeko sarbidea prebenitzeko kokatuta.

Ebidentzia: Ekipamendu diseinu diagramak

Inplementazioa: Zerbitzariak blokeatutako gelan, sare ekipamendua armairu seguruetan.

A.7.9 Aktiboen segurtasuna instalazioetatik kanpo

Egoera:  **Inplementatuta**

Justifikazioa: Ordenagailu eramangarri enkriptatzea, gailu mugikorren kudeaketa.

Ebidentzia: MDM politika, enkriptatze egiaztapena

Inplementazioa: Disko enkriptatze osoa derrigorrezkoa, urruneko garbiketa gaitasuna.

A.7.10 Biltegitratze euskarriak

Egoera:  **Inplementatuta**

Justifikazioa: Euskarri kudeaketa eta ezabaketa prozedurak.

Ebidentzia: Euskarri kudeaketa SOP

Inplementazioa: USB unitateak enkriptatuta, babeskopia zintak segurtasunez gordeta, euskarri saneamendua bota aurretik.

A.7.11 Laguntza utilitateak

Egoera:  **Inplementatuta**

Justifikazioa: Potentzia eta hozte erredundantea.

Ebidentzia: UPS mantentze log-ak, sorgailu probak

Inplementazioa: UPS sistema kritikoetarako, diesel sorgailua, hileroko sorgailu probak.

A.7.12 Kableatu segurtasuna

Egoera:  **Inplementatuta**

Justifikazioa: Sare kableatua babestuta.

Ebidentzia: Sare diagramak, kable kudeaketa

Inplementazioa: Kableak hodietan edo goiko erretiluetan, etiketatuta, zuntz optikoa lotura sentikorretarako.

A.7.13 Ekipamendu mantentzea

Egoera:  **Inplementatuta**

Justifikazioa: Mantentze prebentibo egutegia.

Ebidentzia: Mantentze kontratuak, zerbitzu log-ak

Inplementazioa: Urteroko hardware mantentzea, firmware eguneraketak, hornitzaile laguntza akordioak.

A.7.14 Ekipamenduaren ezabaketa edo berrerabilpen segurua

Egoera:  **Inplementatuta**

Justifikazioa: Saneamendua ezabatu/berrerabili aurretik.

Ebidentzia: Aktibo ezabaketa erregistroak

Inplementazioa: NIST 800-88 betetzen duen datu saneamendua, suntsipen ziurtagiriak.

A.8 Kontrol Teknologikoak (34 kontrol)

A.8.1 Erabiltzaile endpoint gailuak

Egoera:  **Inplementatuta**

Justifikazioa: Endpoint segurtasun estandarrak.

Ebidentzia: Endpoint segurtasun politika

Inplementazioa: Antibirusa derrigorrezkoa, endpoint detekzio eta erantzuna (EDR) hedatuta, adabaki kudeaketa.

A.8.2 Pribilegiatutako sarbide eskubideak

Egoera:  **Inplementatuta**

Justifikazioa: Kontu pribilegiatuak bereizita kudeatuta.

Ebidentzia: PAM irtenbide konfigurazioa

Inplementazioa: Admin kontuak erabiltzaile kontuetatik bereizita, MFA beharrezkoa, saio grabaketa.

A.8.3 Informazio sarbide murrizketa

Egoera:  **Inplementatuta**

Justifikazioa: Jakiteko beharraren arabera sarbide kontrola.

Ebidentzia: Sarbide kontrol zerrendak, baimen matrizea

Implementazioa: RBAC inplementatuta, pribilegio gutxienekoa, ohiko sarbide berrikuspenak.

A.8.4 Iturburu koderako sarbidea

Egoera:  Inplementatuta

Justifikazioa: Iturburu kode biltegirako sarbidea kontrolatua.

Ebidentzia: Git sarbide log-ak, garatzaile kontuak

Implementazioa: GitHub adar babesarekin, kode berrikuspena beharrezkoa, sinatutako commit-ak.

A.8.5 Autentifikazio segurua

Egoera:  Inplementatuta

Justifikazioa: Autentifikazio mekanismo sendoak.

Ebidentzia: Autentifikazio politika, MFA hedapena

Implementazioa: Pasahitz konplexutasuna, MFA admin eta urruneko sarbide guztietarako, SSO ahal denean.

A.8.6 Gaitasun kudeaketa

Egoera:  Inplementatuta

Justifikazioa: Baliabide monitorizazioa eta plangintza.

Ebidentzia: Monitorizazio panelak, gaitasun txostenak

Implementazioa: Prometheus/Grafana monitorizazioa, hiruhileko gaitasun berrikuspenak, eskalatze planak.

A.8.7 Malwarearen aurkako babesa

Egoera:  Inplementatuta

Justifikazioa: Antimalware hedatuta sistema osoan.

Ebidentzia: Antibirus hedapen txostenak

Implementazioa: Endpoint AV, email pasabide iragazketa, web iragazketa, definizioak automatikoki eguneratuta.

A.8.8 Ahultasun teknikoen kudeaketa

Egoera:  Inplementatuta

Justifikazioa: Ahultasun kudeaketa programa.

Ebidentzia: Ahultasun kudeaketa SOP, eskaneatze txostenak

Implementazioa: Asteko ahultasun eskaneatzea, 7 eguneko adabaki kritikoetarako, arriskuan oinarritutako lehentasuna.

A.8.9 Konfigurazio kudeaketa

Egoera:  **Inplementatuta**

Justifikazioa: Konfigurazio oinarriak eta aldaketa kontrola.

Ebidentzia: Konfigurazio kudeaketa datu-basea (CMDB)

Inplementazioa: Azpiegitura Kode gisa, Ansible playbook-ak, aldaketa onarpen prozesua.

A.8.10 Informazio ezabaketa

Egoera:  **Inplementatuta**

Justifikazioa: Ezabaketa seguru prozedurak.

Ebidentzia: Datu ezabaketa SOP

Inplementazioa: Pasaldi anitzeko gainidazketa, ezabaketa kriptografikoa, egiaztapena, GDPR ezabatze eskubide prozesua.

A.8.11 Datu maskaratzea

Egoera:  **Partzialki Inplementatuta**

Justifikazioa: Produkzio datuak maskaratuta proba inguruneetan.

Ebidentzia: Proba datu kudeaketa prozedurak

Inplementazioa: Datu-base anonimizazioa probetarako. Ekintza: Maskaratzea hedatu ez-prod ingurune guztietara 2026ko 2. hiruhilekorako.

A.8.12 Datu galera prebentzioa (DLP)

Egoera:  **Partzialki Inplementatuta**

Justifikazioa: Oinarrizko kontrolak indarrean.

Ebidentzia: Email pasabide arauak, USB politikak

Inplementazioa: Email DLP arauak, USB atakak desgaituta PC gehienetan. Ekintza: DLP irtenbide osoa hedatu.

A.8.13 Informazio babeskopia

Egoera:  **Inplementatuta**

Justifikazioa: Babeskopia estrategia integrala.

Ebidentzia: Babeskopia politika, berreskuratze proba log-ak

Inplementazioa: Eguneroko inkrementala, asteko osoa, gunetik kanpoko erreplikazioa, hiruhileko berreskuratze probak.

A.8.14 Informazioa prozesatzeko instalazioen erredundantzia

Egoera:  **Partzialki Inplementatuta**

Justifikazioa: Erredundantzia batzuk indarrean.

Ebidentzia: Eskuragarritasun handiko konfigurazioa

Inplementazioa: Datu-base clustering, karga banatzaileak, hodei failover. Ekintza: Erredundantzia geografiko osoa inplementatu 2026ko 4. hiruhilekorako.

A.8.15 Erregistroa (Logging)

Egoera:  **Implementatuta**

Justifikazioa: Erregistro zentralizatua SIEM bidez.

Ebidentzia: SIEM konfigurazioa, log atxikipen politika

Implementazioa: Sistema guztiek log-ak bidaltzen dituzte ELK stack-era, 2 urteko atxikipena, manipulazioen aurkakoa.

A.8.16 Monitorizazio jarduerak

Egoera:  **Implementatuta**

Justifikazioa: Segurtasun monitorizazioa SIEM bidez.

Ebidentzia: SIEM panelak, alerta arauak

Implementazioa: Denbora errealeko monitorizazioa, 15+ alerta arau, 24/7 alerta guardia taldeari.

A.8.17 Erloju sinkronizazioa

Egoera:  **Implementatuta**

Justifikazioa: NTP ordu sinkronizazioa.

Ebidentzia: NTP zerbitzari konfigurazioa

Implementazioa: Sistema guztiek barne NTP zerbitzarietara sinkronizatzen dute, NTP zerbitzariak stratum 1 iturrietara sinkronizatzen dira.

A.8.18 Pribilegiatutako utilitate programen erabilera

Egoera:  **Implementatuta**

Justifikazioa: Admin tresnak kontrolatu eta erregistratu.

Ebidentzia: Sarbide pribilegiatu log-ak

Implementazioa: Admin tresnak mugatuta, erabilera erregistratuta, saio grabaketa arrisku handiko ekintzetarako.

A.8.19 Software instalazioa sistema operatiboetan

Egoera:  **Implementatuta**

Justifikazioa: Software instalazioa kontrolatua.

Ebidentzia: Aldaketa kudeaketa erregistroak

Implementazioa: Erabiltzaile kontu estandarrek ezin dute softwarerik instalatu, zerrenda zuria ikuspegia, aldaketa eskaerak.

A.8.20 Sare segurtasuna

Egoera:  **Implementatuta**

Justifikazioa: Sare segmentazioa eta segurtasun kontrolak.

Ebidentzia: Sare arkitektura diagramak, suebaki arauak

Implementazioa: VLANak (erabiltzailea, zerbitzaria, OT, DMZ, kudeaketa), suebakiak segmentuen artean, IDS/IPS.

A.8.21 Sare zerbitzuen segurtasuna

Egoera:  **Implementatuta**

Justifikazioa: Sare zerbitzuak gogortuta.

Ebidentzia: Sare segurtasun politika, gogortze kontrol-zerrendak

Implementazioa: Beharrezkoak ez diren zerbitzuak desgaituta, protokolo seguruak soilik (SSH ez Telnet), aldizkako berrikuspenak.

A.8.22 Sareen bereizketa

Egoera:  **Implementatuta**

Justifikazioa: Sare segmentazioa implementatuta.

Ebidentzia: Sare diagramak VLANak erakusten

Implementazioa: 5 VLAN: Erabiltzailea (10), Zerbitzaria (20), OT (50), DMZ (100), Kudeaketa (200).

A.8.23 Web iragazketa

Egoera:  **Implementatuta**

Justifikazioa: Web proxy eduki iragazketarekin.

Ebidentzia: Proxy log-ak, blokeatutako gune txostenak

Implementazioa: Squid proxy, kategoria bidezko blokeoa, malware/phishing babesa.

A.8.24 Kriptografiaren erabilera

Egoera:  **Implementatuta**

Justifikazioa: Enkriptatze politika definituta.

Ebidentzia: Kriptografia politika, gako kudeaketa prozedurak

Implementazioa: TLS 1.3 webgunerako, AES-256 datuak geldirik, SSH urruneko sarbiderako.

A.8.25 Garapen bizi-ziklo segurua

Egoera:  **Implementatuta**

Justifikazioa: Segurtasuna SDLCn integratuta.

Ebidentzia: SDLC dokumentazioa, segurtasun atea

Implementazioa: Mehatxu modelaketa, kodeketa seguru prestakuntza, SAST/DAST CI/CDn, kode berrikuspena.

A.8.26 Aplikazio segurtasun baldintzak

Egoera:  **Inplementatuta**

Justifikazioa: Segurtasun baldintzak definituta aplikazioetarako.

Ebidentzia: Segurtasun baldintza kontrol-zerrenda

Inplementazioa: OWASP Top 10 jorratuta, sarrera balidazioa, irteera kodetzea, autentifikazioa/baimena.

A.8.27 Sistema arkitektura eta ingeniari-tza printzipio seguruak

Egoera:  **Inplementatuta**

Justifikazioa: Defentsa sakonean, pribilegio gutxienekoa.

Ebidentzia: Arkitektura dokumentazioa

Inplementazioa: Geruzatutako segurtasuna, fail secure, eginkizunen bereizketa, segurtasuna diseinuaren bidez.

A.8.28 Kodeketa seguruak

Egoera:  **Inplementatuta**

Justifikazioa: Kodeketa seguru praktikak behartuta.

Ebidentzia: Kodeketa estandarrak, linting arauak

Inplementazioa: ESLint segurtasun arauak, kode berrikuspen kontrol-zerrenda, OWASP jarraibideak jarraituta.

A.8.29 Segurtasun probak garapenean eta onarpenean

Egoera:  **Inplementatuta**

Justifikazioa: Segurtasun probak derrigorrezkoak produkzio aurretik.

Ebidentzia: CI/CD pipeline konfigurazioa, proba txostenak

Inplementazioa: SAST (SonarQube, Semgrep), DAST (OWASP ZAP), dependentsia eskaneatzea, penetrazio probak.

A.8.30 Azpikontratututako garapena

Egoera:  **Inplementatuta**

Justifikazioa: Hirugarrenen garapen gainbegiratzea.

Ebidentzia: Hornitzaile kontratuak, kode berrikuspenak

Inplementazioa: Segurtasun baldintzak kontratuetan, kode fidantza (escrow), segurtasun ebaluazioak, kode berrikuspena.

A.8.31 Garapen, proba eta produkzio inguruneen bereizketa

Egoera:  **Inplementatuta**

Justifikazioa: Hiru mailako ingurune ereduak.

Ebidentzia: Ingurune dokumentazioa, sare diagramak

Inplementazioa: Dev, staging, produkzioa guztiz bereizita. Produkzio daturik ez dev/test-ean.

A.8.32 Aldaketa kudeaketa

Egoera:  **Inplementatuta**

Justifikazioa: Aldaketa kontrol prozesu formala.

Ebidentzia: Aldaketa kudeaketa SOP, aldaketa tiketak

Inplementazioa: RFC beharrezkoa produkzio aldatetarako, CAB onarpena, inplementazio automatizatuak, atzera egiteko planak.

A.8.33 Proba informazioa

Egoera:  **Inplementatuta**

Justifikazioa: Proba datuak babestuta edo anonimizatuta.

Ebidentzia: Proba datu kudeaketa politika

Inplementazioa: Produkzio datuak anonimizatuta probetarako, datu sintetikoen sorrera, proba datuak garbituta proben ondoren.

A.8.34 Informazio sistemen babesa auditoretza probetan




Egoera:  **Inplementatuta**

Justifikazioa: Auditoretza probak kontrolatuta etenaldiak prebenitzeko.

Ebidentzia: Auditoretza politika, auditoretza egutegiak

Inplementazioa: Irakurketa soileko sarbidea auditoreentzat, probak ez-produkzioan ahal denean, aldaketa izoztea auditoretzetan.

3. Laburpen Estatistikak

Egoera	Kopurua	Ehunekoa
 Inplementatuta	87	%93
 Partzialki Inplementatuta	6	%7
 Ez Inplementatuta	0	%0
N/A Ez Aplikagarria	0	%0
Kontrolak Guztira	93	%100

4. Inplementazio Partzialaren Arriskuan Oinarritutako Justifikazioa

Partzialki Inplementatutako Kontrolak

1. A.5.12 & A.5.13 (Sailkapena & Etiketatzea)

- **Arriskua:** Ertaina - Datu kudeaketa okerreko potentziala
- **Arintzea:** Oinarrizko sailkapena indarrean, datu sentikorrak identifikatuta
- **Ekintza Plana:** Inplementazio osoa 2026ko 2. hiruhilekorako

2. A.7.7 (Mahai eta pantaila garbia)

- **Arriskua:** Baxua - Segurtasun fisikoa jada sendoa
- **Arintzea:** Pantaila blokeoak behartuta, aldizkako auditoriak
- **Ekintza Plana:** Auditoria maiztasuna handitu, kontzientziazio kanpainak

3. A.8.11 (Datu maskaratzea)

- **Arriskua:** Ertaina - Proba datuen esposizioa
- **Arintzea:** Datu-base anonimizazioa indarrean
- **Ekintza Plana:** Ez-prod ingurune guztietara hedatu 2026ko 2. hiruhilekorako

4. A.8.12 (Datu galera prebentzioa)

- **Arriskua:** Ertaina - Datu exfiltrazio potentziala
- **Arintzea:** Email arauak, USB kontrolak, monitorizazioa
- **Ekintza Plana:** DLP irtenbide osoa hedatu 2026ko 3. hiruhilekorako

5. A.8.14 (Erredundantzia)

- **Arriskua:** Ertaina - Hutsegite puntu bakarra
- **Arintzea:** Tokiko erredundantzia, hodei babeskopia
- **Ekintza Plana:** Geo-erredundantzia failover inplementatu 2026ko 4. hiruhilekorako

5. Etengabeko Hobekuntza Plana

2026 2. Hiruhilekoa

- Datu sailkapen hedapena osatu
- Datu maskaratze integrala inplementatu
- Mahai garbia politika betetzea hobetu

2026 3. Hiruhilekoa

- DLP irtenbide osoa hedatu
- ISO 27001 aurre-ebaluazio auditoria egin

2026 4. Hiruhilekoa

- Erredundantzia geografikoa inplementatu
 - ISO 27001 ziurtagiri auditoria osatu
-

6. Onarpena

Prestatua: CISO, Zabala Gailetak

Berrikusia: IT Zuzendaria, Aholkulari Juridikoa, DBO

Onartua: Zuzendari Nagusia (CEO)

Sinadura: _____

Data: 2026ko Urtarrilaren 8a

Hurrengo Berrikuspena: 2026ko Uztailaren 8a

Dokumentu hau Zabala Gailetak S.L.-ren konfidentziala eta jabetzakoa da. Baimenik gabeko banaketa debekatuta dago.