

Dokumentazio Beharrrezkoen Auditoria

ISO 27001:2022 + GDPR + IEC 62443

Data: 2026ko Urtarrilaren 24a

Proiektua: Zabala Gaietak - RRHH Ataria

Helburua: Ziurtatu betetze GUZTIA ziurtagitzarako

Laburpen Exekutiboa

Estandar ofizialak eta auditoria eskakizunak berrikusi ondoren, **GAPS KRITIKOAK** identifikatu ditut dokumentazioan ziurtagiria eskatu aurretik **OSATU** behar direnak:

Dokumentazioaren Egoera Uneko

Ziurtagiria	Dok. Beharrrezkoak	Implementatuak	Faltan	% Osatua
ISO 27001:2022	13 + 25 Annex A	30/38	8	79%
GDPR	12 beharrezko	8/12	4	67%
IEC 62443	8 (OT-rako)	3/8	5	38%

⚠ KRITIKOA: Uneko dokumentazioarekin, **EZ ZENUKE** ziurtagiri auditoria bat gaindituko.

1. ZATIA: ISO 27001:2022 - Dokumentazio Beharrrezkoak

A Atala: 4-10 Klauzelak (Gorputz Nagusia) - 13 DOKUMENTU BEHARRREZKOAK

#	Klausula	Dokumentu Beharrrezkoa	Egoera	Uneko Kokapena	FALTAN
1	4.3	SGSI Esparrua (SGSI-ren Irismena)	✓	compliance/sgsi/sgsi_esparra.md	-
2	5.1 & 5.2	Informazio Segurtasun Politika	✓	compliance/sgsi/informazio_segurtasun_politika.md	-
3	6.1.2	Arrisku Ebaluazio Prozedura	✓	compliance/sgsi/arrisku_ebaluazio_prozedura.md	-
4	6.1.3(d)	Aplikagarritasun Adierazpena (SoA)	✓	compliance/sgsi/aplikagarritasun_adierazpena.md	-

#	Klausula	Dokumentu Beharrrezkoa	Egoera	Uneko Kokapena	FALTAN
5	6.1.3	Arrisku Tratamendu Prozedura	✓	compliance/sgsi/arrisku_tratamendu_prozedura.md	-
6	6.2	Informazio Segurtasun Helburuak	✓	compliance/sgsi/segurtasun_helburuak.md	-
7	7.2	Langileen Erregistroak (Gaitasun ebidentzia)	⚠ PARTZIALA	HR fitxategi sakabanatuak	✗ Erregistro formal zentralizatua
8	8.1	SGSI Eragiketa Informazioa (Prozedura operatiboak)	⚠ PARTZIALA	12 POP dokumentatuak	✗ 5 POP kritiko falta
9	8.2	Arrisku Ebaluazio Txostenak	✓	compliance/sgsi/arrisku_txostenak/	-
10	8.3	Arrisku Tratamendu Plana	✓	compliance/sgsi/arrisku_tratamendu_plana.md	-
11	9.1	Segurtasun Metrikak (KPI-ak)	✗	-	✗ OSOA FALTA
12	9.2.2	Barne Auditoria Programa eta Txostenak	⚠ PARTZIALA	Txantiloia sortua	✗ Auditoria programa + txostenak falta
13	9.3.3	Zuzendaritzaren Berrikuspen Txostenak	✗	-	✗ OSOA FALTA

DOKUMENTU KRITIKO FALTAN (Gorputz Nagusia):

1. Langileen Gaitasun Erregistroak (KI. 7.2) - BEHARRREZKOA

Ikusi compliance/sgsi/langileen_gaitasun_erregistroa.md

EKINTZA: Sortu compliance/sgsi/langileen_gaitasun_erregistroa.xlsx

2. Segurtasun Metrikak / KPI-ak (KI. 9.1) - BEHARRREZKOA

Ikusi compliance/sgsi/segurtasun_metrikak.md

EKINTZA: Sortu compliance/sgsi/segurtasun_metrikak.md + Dashboard automatizatua

3. Barne Auditoria Programa (KI. 9.2.2) - BEHARRREZKOA

Ikusi compliance/sgsi/barne_auditoria_programa.md

EKINTZA: Sortu compliance/sgsi/barne_auditoria_programa.md

4. Zuzendaritzaren Berrikuspen Txostenak (KI. 9.3.3) - BEHARRREZKOA

Ikusi compliance/sgsi/zuzendaritzaren_berrikusketa_txostenak/2025_Q4.md

EKINTZA: Sortu compliance/sgsi/zuzendaritzaren_berrikusketa_txostenak/2025_Q4.md

5. Faltako POP-ak (KI. 8.1) - BEHARRREZKOAK

12 POP dituzu baina 5 kritiko falta dira:

- ✗ POP-013: Aldaketa Kudeaketa Procedura
- ✗ POP-014: Kriptografiko Kontrolen Procedura
- ✗ POP-015: Garapen Seguruaren Bizitza Zikloa (SDLC)
- ✗ POP-016: Sarbide Fisikoaren Kontrola
- ✗ POP-017: Informazio Sailkapena eta Maneiua

EKINTZA: Sortu 5 POP hauek compliance/sgsi/prozedura_operatiboak/

B Atala: Annex A Kontrolak - 25 DOKUMENTU BEHARRREZKO GEHIAGO

#	Kontrola	Dokumentu Beharrezkoan	Egoera	FALTAN
1	A.5.1	Informazio segurtasun politika (goian estalita)	✓	-
2	A.5.7	Mehatxu inteligentzia politika	✗	✗ FALTA
3	A.5.10	Acceptable Use Policy (AUP)	✓	-
4	A.5.14	Informazio transferentzia politika	⚠	✗ Oso orokorra
5	A.5.23	Hodei zerbitzu segurtasun politika	✗	✗ FALTA
6	A.5.30	ICT prestutasuna negozio jarraitasunerako	⚠	✗ Test dokumentazioa falta
7	A.5.31	Legezko eskakizunen identifikazioa	⚠	✗ Erregistro osoa falta
8	A.5.32	Jabetza intelektual eskubideen prozedura	✗	✗ FALTA
9	A.5.37	Eragiketa prozeduren dokumentazioa	⚠	✗ 5 POP falta
10	A.6.1	Hautaketa prozedura (enplegua)	✗	✗ FALTA
11	A.6.2	Enplegu baldintzak (segurtasuna)	⚠	✗ Klauzula espezifikoak falta
12	A.6.4	Diziplina prozesua (segurtasun urraketak)	✗	✗ FALTA
13	A.6.5	Konfidentzialitasun/NDA txantiloia	✓	-
14	A.6.7	Urrutiko lan politika	⚠	✗ BYOD eguneratu falta
15	A.6.8	Informazio segurtasun gertakizunen jakinarazpen prozedura	✓	-

#	Kontrola	Dokumentu Beharrrezkoak	Egoera	FALTAN
16	A.7.4	Segurtasun fisikoko monitorizazioa	⚠	✗ Procedura formal falta
17	A.7.7	Mahai garbi eta pantaila garbi politika	✓	-
18	A.8.9	Konfigurazio kudeaketa dokumentazioa	⚠	✗ Baseline-ak falta
19	A.8.10	Informazio ezabatze politika	✗	✗ FALTA
20	A.8.11	Datu maskarazte politika	⚠	✗ Procedurak falta
21	A.8.12	Datu isuri prebentzio (DLP) politika	⚠	✗ Implementazioa falta
22	A.8.15	Logging politika	✓	-
23	A.8.19	Software instalazio politika	✗	✗ FALTA
24	A.8.23	Web iragazketa politika	✗	✗ FALTA
25	A.8.28	Kodifikazio seguruko gidaliburuak	⚠	✗ OWASP erreferentzia, barne dokumentua falta

2. ZATIA: GDPR - Dokumentazio Beharrrezkoak

12 DOKUMENTU BEHARRREZKOAK GDPR

#	Artikulua	Dokumentu Beharrrezkoak	Egoera	Kokapena	FALTAN
1	Art. 13-14	Pribatutasun Oharra / Pribatutasun Politika	✓	compliance/gdpr/pribatutasun_oharra.md	-
2	Art. 30	Tratamendu Jardueren Erregistroa (RAT)	✓	compliance/gdpr/tratamendu_erregistroa.xlsx	-
3	Art. 32	Segurtasun Neurrien Dokumentazioa	✓	ISO dokumentu anitz	-
4	Art. 33-34	Datu Haustura Jakinarazpen Prozedura	✓	compliance/gdpr/datu_haustura_prozedura.md	-
5	Art. 35	Datu Babesaren Eragin Ebaluazioa (EIPD)	✓	compliance/gdpr/eipd_portal_rrhh.md	-
6	Art. 28	Datu Tratamendu Akordioak (DPA)	⚠ PARTZIALA	Txantiloia existitzen da	✗ Hornitzaire guztiekin sinatu falta

#	Artikulua	Dokumentu Beharrrezkoa	Egoera	Kokapena	FALTAN
7	Art. 37-39	DBA Izendapen Gutuna		-	OSOA FALTA
8	Art. 15-22	Datu Subjektu Eskubideen Procedurak	PARTZIALA	Oinarrizko prozedurak	Formularioak + workflow-ak falta
9	Art. 17	Datu Atxikipen Politika	PARTZIALA	Dokumentazio partziala	Atxikipen egutegi osoa falta
10	Art. 25	Data Protection by Design Dokumentazioa		-	FALTA
11	Art. 46	Nazioarteko Transferentzia Mekanismoak (SCCs)		-	FALTA (US zerbitzuak erabiltzen badira)
12	Art. 7-8	Baimen Kudeaketa Erregistroak		-	FALTA

DOKUMENTU KRITIKO FALTAN (GDPR):

1. DBA Izendapen Gutuna (Art. 37) - BEHARRREZKOA

Ikusi compliance/gdpr/dpo_izendapena.md

EKINTZA: Sortu compliance/gdpr/dpo_izendapena.pdf

2. Datu Subjektu Eskubideen Workflow-ak (Art. 15-22) - BEHARRREZKOA

Prozedurak + formularioak behar dira eskubide bakoitzeko:

Ikusi compliance/gdpr/eskubide_prozedurak.md

EKINTZA: Sortu compliance/gdpr/eskubide_prozedurak.md + Formularioak

3. Datu Atxikipen Egutegia (Art. 17) - BEHARRREZKOA

Ikusi compliance/gdpr/datu_atxikipen_egutegia.md

EKINTZA: Sortu compliance/gdpr/datu_atxikipen_egutegia.md

4. Datu Tratamendu Akordioak (Hornitzairen guztiekin sinatu) - BEHARRREZKOA

DPAs sinatu behar dira datuak tratatzen dituzten HORNITZAILE GUZTIEKIN:

Hornitzalea	Zerbitzua	Datu Motak	DPA Egoera
Google Workspace	Email, Drive	Langileak, dokumentuak	✗ SINATU GABE
AWS	Hosting	Datu guztiak	✗ SINATU GABE
Twilio	SMS (MFA)	Telefono zenbakiak	✗ SINATU GABE
SendGrid	Email transakzionala	Langileen emailak	✗ SINATU GABE
Stripe (erabiltzen bada)	Ordainketak	N/A (ez du RRHH-ri aplikatzen)	N/A

EKINTZA: Sinatu DPAs-ak hornitzairen guztiekin ziurtagiriaren aurretik

5. Baimen Kudeaketa Sistema Dokumentazioa - BEHARRREZKO marketina bada

Ikusi [compliance/gdpr/baimen_sistema_ez_aplikagarria.md](#)

EKINTZA: Marketinik EZ bada, dokumentatu ez dela aplikatzen
[compliance/gdpr/baimen_sistema_ez_aplikagarria.md-N](#)

6. Data Protection by Design Dokumentazioa (Art. 25) - BEHARRREZKO

Ikusi [compliance/gdpr/privacy_by_design.md](#)

EKINTZA: Sortu [compliance/gdpr/privacy_by_design.md](#)

3. ZATIA: IEC 62443 - Dokumentazio Beharrrezkoak (OT/Industrial)

8 DOKUMENTU BEHARRREZKOAK IEC 62443

#	Atala	Dokumentu Beharruzkoa	Egoera	FALTAN
1	2-1	IACSentzako Segurtasun Programa	⚠	✗ Programa osoa falta
2	3-2	Segurtasun Arrisku Ebaluazioa (OT espezifikoan)	⚠	✗ OT assessment falta
3	3-3	Sistema Segurtasun Eskakizunen Espezifikazioa	✗	✗ FALTA
4	4-1	Garapen Seguruaren Bizitza Zikloa	✗	✗ FALTA (OT software garapena baduzu)
5	4-2	Segurtasun Tekniko Eskakizunak	⚠	✗ Partziala ISO dokumentuetan
6	Zonak	Sare Segmentazio Dokumentazioa (Purdue Model)	⚠	✗ Fisiko implementazioa falta
7	Zonak	Konduitu Dokumentazioa (zona arteko komunikazioa)	✗	✗ FALTA
8	Patch	OT Patch Kudeaketa Prozedura	✗	✗ FALTA

DOKUMENTU KRITIKO FALTAN (IEC 62443):

1. OT Segurtasun Arrisku Ebaluazioa - BEHARRREZKO

Ikusi compliance/iec62443/ot_arrisku_ebaluazioa.md

Justifikazioa: Produktu kontsumoa (osasuna), erreputazioa