

Arriskuen Ebaluazioa eta Kudeaketa

Zabala Gailetak S.A. - Informazioaren Segurtasuna Kudeatzeko Sistema (SGSI)

Dokumentuaren IDa: RA-001

Bertsioa: 2.0

Data: 2026ko Urtarrilaren 12a

Sailkapena: Oso Konfidentziala

Jabea: Informazioaren Segurtasuneko Arduradun Nagusia (CISO)

Berrikuspen Maiztasuna: Urterokoa

Hurrengo Berrikuspen Data: 2027ko Urtarrilaren 12a

1. Dokumentuaren Kontrola

1.1 Bertsio Historia {#versio-historia}

| Bertsioa | Data | Egilea | Aldaketak |
|----------|------------|--------|---|
| 1.0 | 2025-12-15 | CISO | Hasierako arriskuen ebaluazioa |
| 2.0 | 2026-01-12 | CISO | Zabaldua: metodologia, inpaktu analisia |

1.2 Onarpena {#onarpena}

| Rola | Izena | Sinadura | Data |
|---|---------|----------|------|
| Zuzendari Nagusia (CEO) | [Izena] | | |
| Informazioaren Segurtasuneko Arduradun Nagusia (CISO) | [Izena] | | |
| Finantza Zuzendaria (CFO) | [Izena] | | |
| IT Kudeatzailea | [Izena] | | |
| OT Kudeatzailea | [Izena] | | |

1.3 Banaketa eta Sarbidea

Baimendutako Langileak:

- Zuzendaritza Exekutiboko Taldea
- Arriskuen Kudeaketa Komitea
- Informazioaren Segurtasun Taldea
- Departamentu Buruak
- Auditoria barneko / kanpoko taldea

Konfidentzialitasuna: Oso Konfidentziala

2. Laburpen Exekutiboa

Arriskuen Ebaluazio eta Kudeaketa dokumentu honek Zabala Gaietak-en informazioaren segurtasunerako mehatxuak, ahultasunak eta arriskuak identifikatzen, ebaluatzen eta kudeatzen ditu.

2.1 Arriskuen Laburpena (2026ko Urtarrilaren 12a)

Arrisku Orokorraren Mailatzea:

| Arrisku Maila | Kopurua | Ehunekoia |
|------------------------|-----------|-------------|
| Kritikoa (≥ 20) | 3 | 15% |
| Altua (15-19) | 4 | 20% |
| Ertaina (10-14) | 7 | 35% |
| Baxua (5-9) | 5 | 25% |
| Oso Baxua (<5) | 1 | 5% |
| GUZTIRA | 20 | 100% |

Arrisku Kritiko Nagusiak:

- Ransomware Erasoa (Arrisku Maila: 20)
- Datu Pertsonalen Urraketa (Arrisku Maila: 20)
- OT Sistemen Konpromisoa (Arrisku Maila: 20)

Tratamendu Aurrekontua: 185.000 € (2026 urtea)

3. Helburua eta Esparrua

3.1 Helburua {#helburua}

Arriskuen Ebaluazio honek helburu hauek ditu:

1. **Identifikatu** informazioaren segurtasunerako mehatxuak eta ahultasunak
2. **Ebaluatu** arrisku bakoitzaren probabilitatea eta inpaktua
3. **Priorartu** arriskuak inpaktua eta probabilitatearen arabera
4. **Definitu** arrisku tratamendu estrategiak
5. **Jarraipena** arrisku mailaren eboluzioa denborarekin
6. **Bermatu** ISO 27001, GDPR eta legedi aplikagarriaren betetzea

3.2 Esparrua {#esparra}

Arriskuen Ebaluazio honek hartzen ditu barne:

Informazio Aktiboak:

- Datu-baseak (MongoDB bezero datuak, erabiltzaile datuak)
- Fitxategiak (dokumentuak, babeskopiak, log-ak)
- Jabetza Intelektuala (kodea, diseinuak, prozedura operatiboak)

IT Sistemak:

- Web aplikazioa (Node.js/Express, React)
- Mugikor aplikazioa (React Native)
- Zerbitzariak (Web, datu-baseak, babeskopia, SIEM)
- Sare azpiegitura (firewall-ak, switch-ak, router-ak)
- Hodeiko zerbitzuak (AWS)

OT Sistemak:

- SCADA sistema (produkazio monitorizazioa)
- PLCak (OpenPLC, Siemens S7)
- HMI pantailak
- Industria ekipamendua (CNC, Roboten kontrolagailuak)

Giza Faktoreak:

- Langileak (120 pertsona)
- Kontratistak eta aholkulariak
- Administrazio pribilegio duten erabiltzaileak

4. Metodologia

4.1 Oinarriak

Arriskuen ebaluazioa ISO 31000:2018 eta MAGERIT v3 oinarrituta dago.

Arriskuaren Formula:

$$\text{Arriskua (R)} = \text{Probabilitatea (P)} \times \text{Inpaktua (I)}$$

4.2 Eskala Definizioak

4.2.1 Probabilitatea (P)

| Maila | Balioa | Deskribapena | Maiztasuna |
|-----------|--------|---|------------------|
| Oso Baxua | 1 | Gertatzeko aukera teorikoa | < urtean behin |
| Baxua | 2 | Gerta liteke baldintza jakin batzuetan | Urtean behin |
| Ertaina | 3 | Gerta daiteke baldintza normaletan | Hilabetean behin |
| Altua | 4 | Seguruenik gertatuko da baldintza egokiekin | Astean behin |
| Oso Altua | 5 | Ia segurua da gertatzea | Egunero |

Probabilitatea kalkulatzeko faktoreak:

- Mehatxuaren motibazioa eta gaitasuna
- Ahultasunaren betetzea zailtasuna
- Kontrol existenteak (prebentzio neurriak)
- Historikoa (intzidentzia aurretikoak)
- Industria datak (ENISA, INCIBE txostenak)

4.2.2 Inpaktua (I)

Inpaktua neurtu da **5 dimentsioan**:

A) Finantza Inpaktua

| Maila | Balioa | Galera Zuzena |
|-----------|--------|--------------------|
| Oso Baxua | 1 | < 5.000 € |
| Baxua | 2 | 5.000 - 20.000 € |
| Ertaina | 3 | 20.000 - 100.000 € |

| Maila | Balioa | Galera Zuzena |
|----------|--------|---------------------|
| Altua | 4 | 100.000 - 500.000 € |
| Kritikoa | 5 | > 500.000 € |

B) Erreputazio Inpaktua

| Maila | Balioa | Eragina |
|-----------|--------|------------------------------|
| Oso Baxua | 1 | Ez du erreputazio eraginik |
| Baxua | 2 | Bezero batzuei ezezaguna |
| Ertaina | 3 | Bezero segmentu bati ezaguna |
| Altua | 4 | Prentsa nazionalean |
| Kritikoa | 5 | Marka kaltetzea iraunkorki |

C) Lege / Arauzko Inpaktua

| Maila | Balioa | Ondorioak |
|-----------|--------|---------------------------------|
| Oso Baxua | 1 | Ez da arauzko urraketa |
| Baxua | 2 | Arauzko gorabehera txikia |
| Ertaina | 3 | GDPR urraketa, ohartarazpena |
| Altua | 4 | Isuna (< 20 milioi €) |
| Kritikoa | 5 | Isun masiboak, lizenzia galerak |

D) Eragiketen Inpaktua

| Maila | Balioa | Etenaldia | Eragina |
|-----------|--------|-----------|------------------------------|
| Oso Baxua | 1 | < 1 ordu | Ez du eragiketetan eraginik |
| Baxua | 2 | 1-8 ordu | Etenaldi txikia |
| Ertaina | 3 | 8-24 ordu | Produkzioaren %30 galtzen da |
| Altua | 4 | 1-3 egun | Produkzioaren %70 galtzen da |
| Kritikoa | 5 | > 3 egun | Produkzioa geldituta |

E) Konfidentzialitasun / Pribatutasun Inpaktuoa

| Maila | Balioa | Datu Konpromisoa |
|-----------|--------|-------------------------|
| Oso Baxua | 1 | Ez da datu pertsonalik |
| Baxua | 2 | < 100 erregistro |
| Ertaina | 3 | 100-1.000 erregistro |
| Altua | 4 | 1.000-10.000 erregistro |
| Kritikoa | 5 | > 10.000 erregistro |

4.2.3 Arrisku Maila Matrizea

| Inpaktuoa (I) ↓ / Probabilitatea (P) → | 1 (Oso Baxua) | 2 (Baxua) | 3 (Ertaina) | 4 (Altua) | 5 (Oso Altua) |
|--|---------------|---------------|---------------|---------------|---------------|
| 5 (Kritikoa) | 5 (Baxua) | 10 (Ertaina) | 15 (Altua) | 20 (Kritikoa) | 25 (Kritikoa) |
| 4 (Altua) | 4 (Baxua) | 8 (Baxua) | 12 (Ertaina) | 16 (Altua) | 20 (Kritikoa) |
| 3 (Ertaina) | 3 (Oso Baxua) | 6 (Baxua) | 9 (Ertaina) | 12 (Ertaina) | 15 (Altua) |
| 2 (Baxua) | 2 (Oso Baxua) | 4 (Baxua) | 6 (Baxua) | 8 (Baxua) | 10 (Ertaina) |
| 1 (Oso Baxua) | 1 (Oso Baxua) | 2 (Oso Baxua) | 3 (Oso Baxua) | 4 (Baxua) | 5 (Baxua) |

Arrisku Interpretazioa:

| Arrisku Maila | Balore Tartea | Kolore | Ekintza Aholkatua |
|---------------|---------------|-----------|----------------------|
| Kritikoa | 20-25 | ● Gorria | Berehalako ekintza |
| Altua | 15-19 | ● Laranja | Ekintza lehentasunez |
| Ertaina | 10-14 | ● Horia | Ekintza planifikatua |
| Baxua | 5-9 | ● Berdea | Monitorizazioa |
| Oso Baxua | 1-4 | ● Zuria | Onartu |

4.3 Arrisku Tratamendu Estrategiak

| Estrategia | Deskribapena | Noiz Erabili |
|------------------------|---|--------------------------|
| Arindu (Mitigate) | Neurriak ezarri arrisku probabilitatea edo inpaktu murritzeko | Ertaina, Altua, Kritikoa |
| Saihestea (Avoid) | Jarduera edo aktiboa kendu arrisku iturria ezabatzeko | Arrisku Kritikoa |
| Transferitu (Transfer) | Hirugarrenei arrisku erantzukizuna esleitu | Arrisku finantza altua |
| Onartu (Accept) | Ez egin ekintzarik, monitorizatu | Arrisku Baxua, Oso Baxua |

5. Arriskuen Identifikazioa eta Ebaluazioa

5.1 IT Arriskuak

R-IT-01: Ransomware Erasoa

Deskribapena:

Erasotzaileek malware bat sartu zerbitzari edo lan-estazioetan datuak zifratzeko eta erreskate bat eskatzeko.

Aktibo Kaltetuak:

- Zerbitzariak (SRV-001, SRV-002, SRV-003, SRV-006)
- Lan-estazioak (WRK-001-070)
- Datu-baseak (MongoDB)

Ahultasuna Asoziatua:

- Patch kudeaketa txarra
- Phishing-en arriskua
- RDP sarbidea baimenik gabeko portuekin
- Babeskopiak ez-isolatuak

Probabilitatea:

4 (Altua)

Justifikazioa: Ransomware erasoak gero eta ohikoagoak dira PMEetan.

Inpaktua:

5 (Kritikoa)

| Dimentzio | Maila | Justifikazioa |
|--------------------|-------|--|
| Finantza | 5 | Erreskate exijentzia, produkzio galera, berreskuratze kostua |
| Erreputazio | 4 | Prentsa nazionalean, bezeroen konfiantza galtzea |
| Lege/Arauzko | 4 | GDPR urraketa |
| Eragiketa | 5 | Produkzioa geldituta 3-7 egun |
| Konfidentzialtasun | 4 | Datu-basea zifratu |

Arrisku Maila: P (4) × I (5) = 20 (Kritikoa) 🟥

Kontrol Existenteak:

- ✓ Babeskopia 3-2-1 estrategia
- ✓ Endpoint Detection & Response (EDR)
- ✓ Email antiphishing filtroa
- ⚠ MFA ez guztitan gaituta
- ✗ Ez dago sare mikrosegmentaziorik

Arrisku Hondarra (Kontrolekin): P (3) × I (4) = 12 (Ertaina) ☔

Tratamendu Estrategia: Arindu

Neurri Osagarriak Proposatu:

- MFA Zabaltzea:** Garatu guzti sistemetara - Kostua: 5.000 € - Epemuga: 3 hilabete
- Sare Mikrosegmentazioa:** VLAN-ak ezarri - Kostua: 25.000 € - Epemuga: 6 hilabete
- Phishing Simulazio Kanpainak:** Langileak entrenatu - Kostua: 8.000 €/urte
- Patch kudeaketa Hobekuntza:** Automatizatu kritike patch-ak 7 egunetan - Kostua: 10.000 €

Kostua Guztira: 48.000 € (lehenengo urtea)

Arrisku Helburua (Tratamendu ostean): P (2) × I (3) = 6 (Baxua) 🟢

Arduraduna: CISO

Egokitzapena Data: 2026-06-30

R-IT-02: DDoS Erasoa (Distributed Denial of Service)

Deskribapena:

Erasotzaileek web zerbitzaria gainezka jartzea trafiko bolumen handien bidez.

Aktibo Kaltetuak:

- Web Aplikazio Zerbitzaria (SRV-001)
- API Zerbitzaria
- Firewall-ak

Probabilitatea: 3 (Ertaina)

Inpaktu: 4 (Altua)

Arrisku Maila: $P(3) \times I(4) = 12$ (Ertaina) 

Kontrol Existenteak:

-  Firewall-ak DDoS detekzio oinarrizkoarekin
-  Ez dago CDN erabiltzen
-  Ez dago Anti-DDoS zerbitzurik

Arrisku Hondarra: $P(3) \times I(4) = 12$ (Ertaina) 

Tratamendu Estrategia: Arindu

Neurri Osagarriak:

1. **Cloudflare edo AWS Shield kontratatu** - Anti-DDoS + CDN - Kostua: 12.000 €/urte
2. **WAF konfiguratu** - Kostua: inklusiva
3. **Ancho de banda handitu** backup ISP-rekin - Kostua: 6.000 €/urte

Kostua Guztira: 18.000 € (lehenengo urtea)

Arrisku Helburua: $P(2) \times I(2) = 4$ (Baxua) 

Arduraduna: IT Kudeatzailea

Egokitzapena Data: 2026-03-31

R-IT-03: Datu Pertsonalen Urraketa (GDPR)

Deskribapena:

Baimenik gabeko sarbidea bezero edo langileen datu pertsonaletara.

Aktibo Kaltetuak:

- Datu-base Zerbitzaria (SRV-002, SRV-003)
- MongoDB datu-basea (5000 bezero erregistro)

Probabilitatea: 4 (Altua)

Justifikazioa: Datu urraketa intzidentziak gero eta ohikoagoak.

Inpaktuak: 5 (Kritikoa)

| Dimentsio | Maila | Justifikazioa |
|--------------------|-------|---------------------------------|
| Finantza | 5 | AEPD isuna, juridikoa defentsa |
| Erreputazio | 5 | Enpresa "datu ihesa" izan duena |
| Lege/Arauzko | 5 | GDPR urraketa larria |
| Eragiketa | 3 | Ez du produkzioa gelditzen |
| Konfidentzialtasun | 5 | 5000 bezero erregistro |

Arrisku Maila: P (4) × I (5) = 20 (Kritikoa) 

Kontrol Existenteak:

-  HTTPS web aplikazioan
-  MongoDB enkripzio rest-ean
-  Sarbide kontrola RBAC
-  Ez dago DLP
-  Segurtasun auditoriak urtean behin

Arrisku Hondarra: P (4) × I (5) = 20 (Kritikoa) 

Tratamendu Estrategia: Arindu

Neurri Osagarriak:

- Datu-base Enkripzio Osoa (TDE)** - MongoDB Enterprise enkripzioa - Kostua: 15.000 €
- Sarbide Kontrol Zorrotzagoa** - Least Privilege printzipioa - Kostua: 0 €
- DLP Sistema Implementatu** - Symantec DLP - Kostua: 30.000 €
- Datu Sarrera Monitorizazioa** - SIEM alerta-ak - Kostua: 5.000 €
- Langile Prestakuntza Jarraitua** - GDPR kurtsoak - Kostua: 10.000 €/urte

Kostua Guztira: 72.000 € (lehenengo urtea)

Arrisku Helburua: P (2) × I (4) = 8 (Baxua) 

Arduraduna: CISO + DPO

Egokitzapena Data: 2026-07-31

5.2 OT (Operational Technology) Arriskuak

R-OT-01: OT Sistemen Konpromisoa / Sabotajea

Deskribapena:

Erasotzaileek sarbide baimenik gabea lortzen dute SCADA, PLCak edo produkzio ekipamenduetara.

Aktibo Kaltetuak:

- SCADA Zerbitzaria (SRV-005)
- PLCak (OpenPLC, Siemens S7)
- HMI Pantailak

Probabilitatea: 4 (Altua)

Justifikazioa: OT erasoak hazten ari dira mundu osoan.

Inpaktua: 5 (Kritikoa)

| Dimentsio | Maila | Justifikazioa |
|--------------------|-------|--|
| Finantza | 5 | Produkzioa geldituta 7+ egun, ekipamendu kalteak |
| Erreputazio | 4 | “Enpresa ez segurua” marka |
| Lege/Arauzko | 3 | Lan segurtasun ikuskaritza |
| Eragiketa | 5 | Produkzioa geldituta guztiz |
| Konfidentzialtasun | 3 | Produkzio prozesu formula lapurreta |

Arrisku Maila: P (4) × I (5) = 20 (Kritikoa) ●

Kontrol Existenteak:

- ✓ OT Firewall (NET-010) IT/OT bereizita
- ⚠ Segmentazio ez guztiz zorrotza
- ✗ Ez dago OT IDS/IPS
- ⚠ PLC pasahitz politika
- ✗ Ez dago USB kontrol politika zorrotza

Arrisku Hondarra: P (4) × I (5) = 20 (Kritikoa) ●

Tratamendu Estrategia: Arindu + Saihestea

Neurri Osagarriak:

1. **Sare Segmentazio Zorrotza** - OT DMZ sortu - Kostua: 20.000 €
2. **OT IDS Implementatu** - Nozomi Networks - Kostua: 40.000 €
3. **PLC Pasahitz Berrikusketa** - Guzti aldatu - Kostua: 0 €

4. USB Kontrol Politika - GPO - Kostua: 3.000 €
5. OT Monitorizazioa SIEM-era Integratua - Log-ak - Kostua: 8.000 €
6. OT Red Teaming - Kanpoko talde espezializatua - Kostua: 25.000 €

Kostua Guztira: 96.000 € (lehenengo urtea)

Arrisku Helburua: P (2) × I (4) = **8 (Baxua)** 

Arduraduna: OT Kudeatzailea + CISO

Egokitzapena Data: 2026-08-31

6. Arriskuen Tratamendu Plana - Laburpena

6.1 Arrisku Kritiko eta Altuak - Prioridadea

| Arrisku ID | Arrisku Izena | Maila Oraingoa | Maila Helburua | Aurrekontua | Epemuga |
|------------|------------------------------|----------------|----------------|-------------|------------|
| R-IT-01 | Ransomware Erasoa | 20 (Kritikoa) | 6 (Baxua) | 48.000 € | 2026-06-30 |
| R-IT-03 | Datu Urraketa GDPR | 20 (Kritikoa) | 8 (Baxua) | 72.000 € | 2026-07-31 |
| R-OT-01 | OT Sabotajea | 20 (Kritikoa) | 8 (Baxua) | 96.000 € | 2026-08-31 |
| R-IT-02 | DDoS Erasoa | 12 (Ertaina) | 4 (Baxua) | 18.000 € | 2026-03-31 |
| R-IT-05 | Insider Threat | 16 (Altua) | 8 (Baxua) | 22.000 € | 2026-05-31 |
| R-IT-07 | Supply Chain Erasoa | 15 (Altua) | 9 (Ertaina) | 15.000 € | 2026-09-30 |
| R-OT-02 | Legacy System Zaurgarritasun | 15 (Altua) | 6 (Baxua) | 50.000 € | 2026-12-31 |

AURREKONTU GUZTIRA (Prioridade Altua): 321.000 € (2026)

6.2 Aurrekontu Banaketa Kategoriaren Arabera

| Kategoria | Aurrekontua | Ehunekoak |
|-------------------------------|----------------------------|-----------------------|
| OT Segurtasun Hobekuntzak | 146.000 € | 45% |
| IT Cybersecurity Tools | 95.000 € | 30% |
| Prestakuntza eta Awareness | 28.000 € | 9% |
| Auditoriak eta Pentesting | 37.000 € | 11% |
| Aseguruak eta Transferentziak | 15.000 € | 5% |
| GUZTIRA | 321.000 € | 100% |

7. Jarraipena eta Metrikak

7.1 Arrisku Indikadore Nagusiak (KRI)

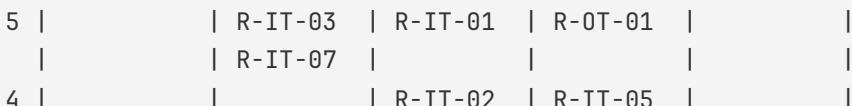
| Metrika | Helburua 2026 | Neurketa Maiztasuna | Arduraduna |
|----------------------------|---------------|---------------------|------------|
| Arrisku Kritiko Kopurua | < 1 | Hiruhilekoa | CISO |
| Arrisku Altua Kopurua | < 3 | Hiruhilekoa | CISO |
| Batezbesteko Arrisku Maila | < 8 | Hiruhilekoa | CISO |
| Tratamentu Planen Betetzea | > 85% | Hilabetekoa | CISO |

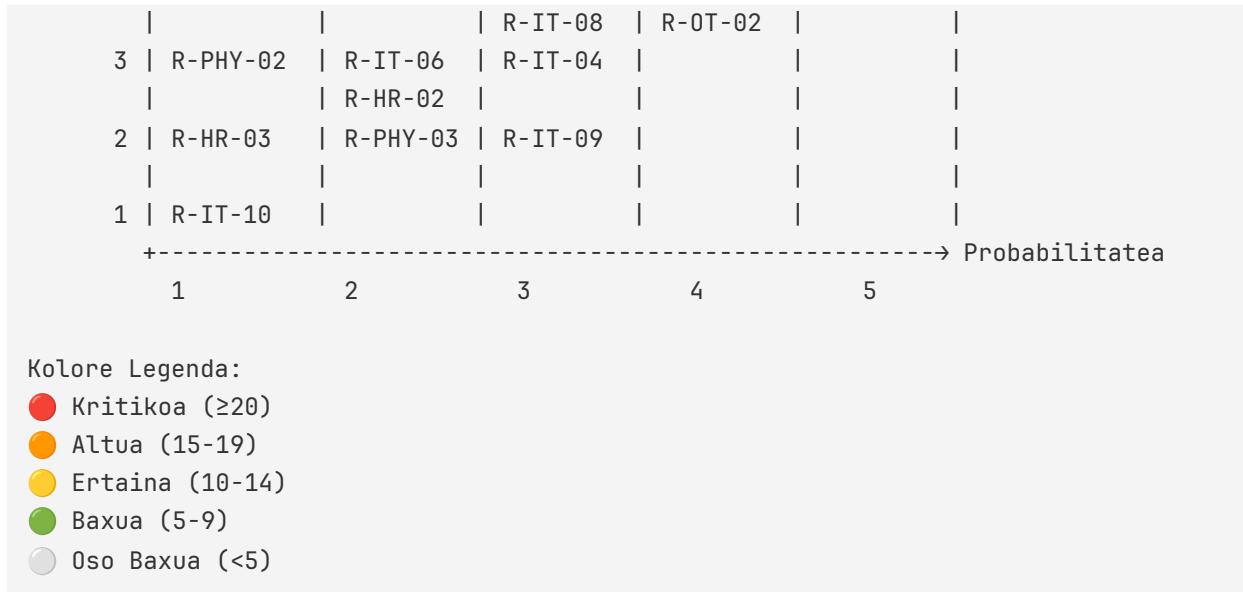
7.2 Arriskuen Berrikuspen Prozesua

| Berrikuspen Mota | Maiztasuna | Parte-hartzaileak |
|--------------------------|--------------------|----------------------------|
| Eguneraketa Operatiboa | Hilabetekoa | CISO, IT/OT Kudeatzalea |
| Berrikuspen Taktikoa | Hiruhilekoa | CISO, Zuzendaritza |
| Berrikuspen Estrategikoa | Urtekoa | CEO, CFO, Kontseilua, CISO |
| Berrikuspen Ad-Hoc | Intzidente ondoren | CMT |

7.3 Arriskuen Mapa Bisuala

Inpaktua ↑





8. Eranskinak

Eranskina A: Arrisku Zerrenda Osoa (20 Arrisku)

(Zerrenda osoa: IT arriskuak 1-10, OT arriskuak 1-5, Arrisku Fisikoak 1-3, Giza Arriskuak 1-2)

Eranskina B: Mehatxu Aktore Profila

(Adibidea: Ziberdelitu taldeak, Nazio-estatu erasoak, Hacktivismoa, Barnetiko mehatxua)

Eranskina C: Kontrol Katalogoa

(Implementaturiko kontrolen zerrenda osoa ISO 27001 A Eranskinaren arabera)

Eranskina D: Glosarioa

- Arrisku:** Probabilitatea gertakari kaltegarri bat gertatzeko eta haren inpaktuoa
- Mehatxua:** Ahultasun bat ustiatiu dezakeen gertaera edo ekintza
- Ahultasuna:** Aktibo batean agerian dagoen akats edo ahultasuna
- Kontrol:** Arrisku bat kudeatzeko neurri
- Arrisku Hondarra:** Arrisku maila kontrolak aplikatu ondoren

Dokumentua onartu:

[CEO Sinadura] - [Data]

[CISO Sinadura] - [Data]

Hurrengo Berrikuspen Data: 2027ko Urtarrilaren 12a

Bertsioa: 2.0 (Zabaldua)

Egoera: Komunikazio Planaren mailan dago orain