

Zabala Gaietak - Segurtasun Plana

1. Testuingurua eta Irismena

Dokumentu honek Zabala Gaietak enpresaren Segurtasun Plana definitzen du. **Jarduera:** Gaietak eta txokolateak ekoiztea, saltza eta banatzea. **Langileak:** 120 (6 Gerentzia, 10 Admin, 5 IKT, 12 Ikerketa, ~87 Ekoizpena). **Kokapena:** Euskal Herria.

2. Aktiboen Inbentarioa

2.1 Informazioa

- Bezeroen Datuak:** Izenak, helbideak, erosketa historiala, profilak (Web eta App).
- Langileen Datuak:** Nominak, kontratuak, datu pertsonalak.
- Jabetza Intelektuala:** Errezetak (formulazioak), ekoizpen prozesuen xehetasunak.
- Finantza Datuak:** Salmentak, erosketak, banku datuak.

2.2 Softwarea

- ERP:** Ekoizpena, inbentarioa eta finantzak kudeatzeko.
- Webgunea:** E-commerce plataforma (B2B eta B2C) bezeroen profilekin.
- Mugikorretako Aplikazioa:** Bezeroentzako app-a.
- SCADA/HMI:** Fabrikako makineria kontrolatzeko softwarea.

2.3 Hardwarea (IT & OT)

- Zerbitzariak (Web, Datu-baseak, ERP).
- Ordenagailu korporatiboak (Admin, Ikerketa, Gerentzia).
- Sare gailuak (Suebakiak, Switch-ak, Router-ak).
- OT Gailuak:** PLC-ak, Sentsoreak, Robotika (Labeak, Amasadorak).

3. Arriskuen Analisia (Zabala Gaietak)

Mehatxua	Deskribapena	Inpaktua	Probabilitatea
Ransomware	Produkzioa gelditzea eta datuak zifratzea.	Oso Altua (Fabrika gelditzea)	Altua

Mehatxua	Deskribapena	Inpaktua	Probabilitatea
Datu Ihesa	Bezeroen datu pertsonalak (GDPR) lapurtzea.	Altua (Isunak, Ospea)	Ertaina
Espioitza Industriala	Errezetak edo prozesuak lehiakideek eskuratzeari.	Altua (Lehiakortasuna galdu)	Ertaina
IoT/OT Erasoak	Labeen tenperatura aldatzea, nahasketak saboteatzeari.	Oso Altua (Segurtasun fisikoa, Kalitatea)	Ertaina
Zerbitzu Ukapena (DDoS)	Webgunea edo eskaera sistema blokeatzeari.	Ertaina (Salmenta galerak)	Ertaina

4. Segurtasun Politikak eta Estrategiak

- Sare Segmentazioa:** IT sarea eta OT (Fabrika) sarea guztiz bereiztea DMZ eta suebakien bidez.
- Sarbide Kontrola:** MFA (Multi-Factor Authentication) ezartzea sistema kritiko guztieta eta VPN sarbideetan.
- Ekoizpen Segurua:** Web eta App garapenean segurtasuna diseinutik txertatzea (SSDLC).
- Jarraipena:** SIEM sistema bat erabiltzea log-ak zentralizatzeko eta anomaliak detektatzeko.
- Honeypot:** Sistema bat jartzea erasoak erakartzeko eta aztertzeko.

5. Araudia

- GDPR:** Bezero eta langileen datuen tratamendua.
- NIS Zuzentaraaua:** Zerbitzu digitalen eta funtsezkoen segurtasuna.