

Hodei Zerbitzuen Segurtasun Politika

Helburua: Hodeiko zerbitzuen (SaaS, PaaS, IaaS) erabilera segurua arautzea.

1. Hornitzaleen Ebaluazioa

- Hornitzaleek segurtasun ziurtagiriak izan behar dituzte (ISO 27001, SOC 2).
- Datuak EBn kokatu behar dira edo GDPR betetzen duten mekanismoak izan.

2. Erantzukizun Partekatua

- IaaS (AWS/Azure): Guk kudeatzen dugu OS, aplikazio eta datuen segurtasuna.
- SaaS (Google Workspace): Guk kudeatzen dugu identitatea eta sarbidea (IAM).

3. Segurtasun Neurriak

- MFA: Derrigorrezkoa hodeiko kontu administratibo guztieta.
- Zifratzea: Datuak zifratuta egon behar dira hornitzalearen biltegian.
- Backup: Ez fidatu bakarrik hornitzalearen backup-ean; eduki kopia propioa.

4. Onarpena

- IT Sailak onartu behar du hodeiko edozein zerbitzu berri (“Shadow IT” debekatua).