POP-014_kriptografia_kontrolak

POP-014: Kriptografia Kontrolen Prozedura

Helburua: Kriptografiaren erabilera egokia eta segurua bermatzea. **Arduraduna:** CISO

1. Algoritmo Onartuak

- **Simetrikoa:** AES-256 (Datuak gordetzeko).
- **Asimetrikoa:** RSA-4096 edo ECC (Gakoen trukerako eta sinadurarako).
- **Hash:** SHA-256 edo handiagoa.
- **Salts:** Ausazkoak eta bakarrak erabiltzaile bakoitzeko.

2. Gakoen Kudeaketa

- **Sorkuntza:** Ausazko zenbaki sortzaile seguruak (CSPRNG) erabili.
- **Biltegiratzea:** HSM edo Key Management Service (KMS) bidez. Inoiz ez kodean (hardcoded).
- **Errotazioa:** Gako simetrikoak urtean behin; Asimetrikoak 2 urtean behin.
- **Ezabatzea:** Suntsipen segurua gakoa iraungitzean.

3. Datuak Trantsitoan

- TLS 1.3 derrigorrezkoa zerbitzu publikoetarako.
- TLS 1.2 minimoa barne zerbitzuetarako.

4. Datuak Atsedenean

- Diskoak zifratuta (BitLocker/LUKS).
- Datu baseak zifratuta (TDE).