



# Kredentzialen erabilera segurua

## Checklist

- Erabili bigarren autentifikazio-faktore bat.

Sistemak babesten laguntzen du kredentzialen eta nahi ez diren sarbideen konpromisoaren aurka.

- Erabili pasahitz sendoak.

Pasahitzek 12 karaktere izango dituzte gutxienez, eta letra maiuskulak eta minuskulak, zenbakiak eta ikurrak eduki beharko dituzte.

- Ez erabili aurreikusi daitezkeen pasahitzak.

Aurreikusi daitezkeen pasahitzak errazago asmatzen dira.

- Ez erabili lehenetsitako pasahitzak.

Lehenetsitako pasahitzak erraz lortu daitezke.

- Ez berrerabili pasahitzak.

Erabili pasahitz desberdin bat zerbitzu bakoitzerako.

- Eduki zure pasahitza sekretuan.

Ez idatzi eta ez inori esan zure pasahitza.

- Aldatu pasahitza aldian behin.

Pasahitza konprometituta geratzen bada, denbora jakin baten ondoren baztertua izan dadin.

- Begiratu ondo non sartzen duzun pasahitza.

Kontuz zure pasahitza lapurtzeko asmoa besterik ez duten webguneekin. Egiaztatu pasahitz bat sartzen duzunean leku legitimoan egiten ari zarela.

- Kontu handia izan pasahitzak erabiltzean.

Egiaztatu inor ez dagoela begira pasahitz bat idazten duzunean.

- Erabili pasahitzen kudeatzaile bat.

Zerbitzu guztietarako gogoratu behar dugun pasahitz kopuru handia kudeatzeko lagungarriak gerta dakizkizukeen programak daude.

Babesteko moduari buruzko informazio gehiago jakin nahi baduzu, sar tu zaitez webgune honetan: <https://www.zibersegurtasun.eus/>

Aholkularitza profesionala behar baduzu, webgunean eskuragarri duzun Euskadiko ziberseguratsun-hornitzaileen katalogoa kontsultatu dezakezu.