password_policy

Pasahitz Politika

Zabala Gailetak S.A

Dokumentuaren IDa: PWD-001
Bertsioa: 1.0
Data: 2026ko Urtarrilaren 8a
Sailkapena: Barne Erabilera
Jabea: Informazioaren Segurtasuneko Arduradun Nagusia (CISO)
Berrikuspen Maiztasuna: Urterokoa
Hurrengo Berrikuspen Data: 2027ko Urtarrilaren 8a

---

1. Dokumentuaren Kontrola

1.1 Bertsio Historia

Bertsioa	Data	Egilea	Aldaketak
1.0	2026-01-08	CISO	Hasierako politikaren sorrera

1.2 Onarpena

Rola	Izena	Sinadura	Data
Zuzendari Nagusia (CEO)	[Izena]		
Informazioaren Segurtasuneko Arduradun Nagusia (CISO)	[Izena]		
IT Kudeatzailea	[Izena]		

---

2. Helburua eta Esparrua

2.1 Helburua

Pasahitz Politika honek Zabala Gailetak-en informazio-sistemetara sartzeko erabiltzen diren pasahitzak sortzeko, kudeatzeko eta babesteko baldintzak ezartzen ditu. Pasahitz praktika sendoak kritikoak dira honakoetarako:

- Baimenik gabeko sarbideak prebenitzea sistemetara eta datuetara
- Bezeroen eta langileen informazioa babestea
- ISO/IEC 27001:2022 eta GDPR betetzen direla ziurtatzea
- Kredentzialen lapurreta eta kontu arriskua murriztea
- Segurtasun baldintza arautzaileak eta kontratuzkoak betetzea

2.2 Esparrua

Politika hau honako hauei aplikatzen zaie:

- **Erabiltzaile Guztiak:** Langileak, kontratistak, aholkulariak, aldi baterako langileak eta hirugarrenak
- **Sistema Guztiak:** IT sistemak (lan-estazioak, zerbitzariak, aplikazioak, hodeiko zerbitzuak) eta OT sistemak (PLCak, SCADA, HMI)
- **Sarbide Metodo Guztiak:** Tokiko saio-hasiera, urruneko sarbidea (VPN), web aplikazioak, gailu mugikorrak, administrazio interfazeak
- **Pasahitz Mota Guztiak:** Erabiltzaile pasahitzak, administrazio pasahitzak, zerbitzu kontuak, API gakoak, enkriptatze gakoak

2.3 Betetzea

Politika hau betetzea derrigorrezkoa da. Urraketek honakoak ekar ditzakete:

- Kontua etetea
- Pasahitza berrezartzea behartzea
- Diziplina ekintzak (Erabilera Onargarriaren Politikaren arabera)
- Enpleguaren edo kontratuaren amaiera

---

3. Pasahitz Baldintzak

3.1 Erabiltzaile Kontu Estandarrak

Gutxieneko Baldintzak:

- **Luzera:** Gutxienez 12 karaktere
- **Konplexutasuna:** Honako lau kategorietatik gutxienez hiru eduki behar ditu:
  - Letra larriak (A-Z)
  - Letra xeheak (a-z)
  - Zenbakiak (0-9)
  - Karaktere bereziak (!@#$%^&*()_+-=|;:,.<>?)
- **Iraungitzea:** 90 egun (180 egun Faktore Anitzeko Autentifikazioa gaituta badago)
- **Historia:** Ezin dira azken 12 pasahitzak berrerabili
- **Blokeoa:** Kontua blokeatu egiten da 5 saio-hasiera okerren ondoren 30 minutuz
- **Aldaketa Baldintzak:** Aurreko pasahitzetik nabarmen desberdina izan behar du (ez zenbakiak gehitzea bakarrik)

Pasahitz Sendoen Adibideak:

- Kafea&Gailetak2026!
- Zabala$Gailetak#456
- NireTxakurrak!MaiteDituGailetak
- Donostia2026@Uda

Gomendatua: Erabili pasaesaldiak (4+ ausazko hitz):

- zaldi-zuzena-bateria-grapagailua
- ElefanteUrdina!DantzanSalsa77
- Pizza$Labea#Okina$2026

3.2 Kontu Pribilegiatuak eta Administratiboak

Baldintza Handituak:

- **Luzera:** Gutxienez 14 karaktere
- **Konplexutasuna:** Lau karaktere kategoriak eduki behar ditu (larria, xehea, zenbakia, berezia)
- **Iraungitzea:** 60 egun (90 egun MFA gaituta badago)
- **Historia:** Ezin dira azken 24 pasahitzak berrerabili
- **Blokeoa:** Kontua blokeatu egiten da 3 saio-hasiera okerren ondoren ordu batez
- **Kontu Bereiziak:** Administratzaileek administrazio kontu bereizia izan behar dute (adib., admin_jgarcia) erabiltzaile kontu arruntetik bereizita (jgarcia)
- **Saio Amaiera:** Saio-amaiera automatikoa 15 minutu inaktibitate ondoren

Esparrua:

- Domeinu Administratzaileak
- Zerbitzari administratzaileak (root, Administrator kontuak)
- Datu-base administratzaileak
- Sare administratzaileak (suebaki, switch, router sarbidea)
- Hodei plataforma administratzaileak (AWS, Azure, M365 Global Admin)
- SCADA/OT sistema administratzaileak
- Segurtasun sistema administratzaileak

3.3 Zerbitzu Kontuak

Baldintzak:

- **Luzera:** Gutxienez 20 karaktere (ausaz sortua)
- **Konplexutasuna:** Ausazkotasun maximoa (karaktere mota guztiak)
- **Iraungitzea:** 365 egun edo inoiz ez (zerbitzuei eragiten badie)
- **Biltegiratzea:** Pasahitz kutxa enkriptatua (HashiCorp Vault, CyberArk, edo baliokidea)
- **Erabilera:** Prozesu automatizatuak soilik (saio-hasiera interaktiborik ez)
- **Monitorizazioa:** Zerbitzu kontuen jarduera erregistratu eta monitorizatzen da
- **Pribilegio Gutxienekoa:** Baimenak eskakizun zehatzetara mugatuta

Adibideak:

- Datu-base zerbitzu kontua aplikazio konexioetarako
- Babeskopia zerbitzu kontua
- Monitorizazio agente kontuak
- API integrazio kontuak

3.4 Partekatutako eta Talde Kontuak

Politika: Partekatutako kontuak **debekatuta** daude teknikoki saihestezina den kasuetan izan ezik.

Salbuespenek Behar Dute:

- CISOren onarpena negozio justifikazioarekin
- Erregistro hobetua (jarraitu zein norbanakok erabili duen kontu partekatua)
- Pasahitz aldaketa baimendutako erabiltzaile bakoitzaren sarbidea amaitzean
- Aldizkako sarbide berrikuspenak (hilero)

Ohiko Salbuespenak:

- Larrialdi “kristala apurtu” administratzaile kontua (gutun-azal zigilatua kutxa gotorrean)

- Tokiko kontsola bakarra duten industria ekipamendu espezifikoak (banakako urruneko sarbidearekin osatua)
- Erabiltzaile anitzeko euskarririk gabeko sistema zaharrak (ordezkatzeko programatuta)

3.5 Aldi Baterako eta Gonbidatu Kontuak

Baldintzak:

- **Pasahitz Lehenetsia:** Ausaz sortua (gutxienez 12 karaktere)
- **Aldaketa Behartu:** Pasahitza aldatu behar da lehen saio-hasieran
- **Iraungitzea:** Kontua automatikoki iraungitzen da epe zehatz baten ondoren (lehenetsia: 30 egun)
- **Onarpena:** Kudeatzailearen eta ITren onarpena behar du
- **Monitorizazioa:** Jarduera erregistratu eta berrikusten da

Erabilera Kasuak:

- Kontratistak eta aholkulariak (epe laburreko proiektuak)
- Aldi baterako langileak
- Auditoreak
- Hornitzaileak (sistema sarbide mugatua)

---

4. Pasahitz Sortze Jarraibideak

4.1 Pasahitz Sendoen Ezaugarriak

EGIN Pasahitzak Honelakoak:

- Luzeak dira (12+ karaktere erabiltzaileentzat, 14+ adminentzat)
- Karaktere mota nahasketa erabiltzen dute (larria, xehea, zenbakia, berezia)
- Zuretzat gogoratzen errazak dira baina besteentzat asmatzen zailak
- Bakarrak dira sistema bakoitzerako (inoiz ez berrerabili pasahitzak)
- Pasaesaldiak erabiltzen dituzte (ausazko hitz anitz)

Pasahitz Sendo Gogangarriak Sortzeko Teknikak:

1. **Pasaesaldi Metodoa:** Ausazko hitz kateak
    - Adibidea: Elefante!Morea$Dantzan#Tangoa
2. **Esaldi Metodoa:** Esaldi baten lehen letrak + aldaketak
    - Esaldia: “Zabala gailetak jatea maite dut arratsaldeko 3etan ostiralero!”
    - Pasahitza: Zgjmd@a3eo!
3. **Karaktere Ordezkapena:** Letrak antzeko karaktereekin ordezkatu
    - Hitza: “Txokolate Txip Gaileta”
    - Pasahitza: Tx0k0l@t3Tx1pG@1l3t@

4.2 Debekatutako Pasahitz Praktikak

EZ EGIN Pasahitzik:

- Hiztegi hitzak dituztenak (hitz bakarrak erraz pitzatzen dira)
- Informazio pertsonala dutenak:
    - Zure izena, erabiltzaile-izena, langile IDa
    - Familiako kideen edo maskoten izenak
    - Jaiotegunak, urteurrenak
    - Telefono zenbakiak, helbideak

- Enpresa informazioa dutenak:
    - Enpresa izena (“Zabala”, “Gailetak”)
    - Departamentu izenak
    - Produktu izenak
- Eredu sinpleak dituztenak:
    - 123456, password, qwerty, abc123
    - Teklatu ereduak (qwertyuiop, asdfghjkl)
    - Sekuentziak (abcdefgh, 12345678)
    - Errepikatutako karaktereak (aaaaaaaa, 11111111)
- Pasahitz zaharren aldaketa txikiak direnak:
    - Zenbakiak gehitzea (Pasahitza1, Pasahitza2, Pasahitza3)
    - Urtaro aldaketak (Uda2025, Udazkena2025, Negua2026)
    - Pasahitz zaharrari ! edo 1 gehitzea soilik

Pasahitz AHULEN Adibideak (Inoiz Ez Erabili):

- Zabala2026 (enpresa izena + urtea)
- Pasahitza123! (hitz arrunta + eredua)
- Gailetak! (enpresa izena + karaktere berezia)
- Admin@123 (rola + eredu sinplea)
- 123456 (sekuentzia)
- qwerty (teklatu eredua)
- JuanGarcia1975 (izena + jaiotze urtea)
- Uda2026! (urtaroa + urtea)

---

5. Pasahitz Kudeaketa

5.1 Pasahitz Babesa

INOIZ EZ:

- Partekatu zure pasahitza inorekin (kudeatzaileak, IT langileak, lankideak barne)
- Idatzi pasahitzak paperean (post-it oharrak, koadernoak, arbelak)
- Gorde pasahitzak enkriptatu gabeko fitxategietan (Word dokumentuak, Excel orriak, testu fitxategiak)
- Bidali pasahitzak posta elektronikoz edo berehalako mezu bidez
- Esan pasahitza ozenki besteek entzun dezaketen lekuan
- Sartu pasahitza norbait begira dagoen bitartean (“shoulder surfing”)
- Erabili pasahitz bera laneko eta kontu pertsonaletarako

BETI:

- Mantendu pasahitzak konfidentzial
- Aldatu pasahitza berehala arriskua susmatzen bada
- Erabili pasahitz desberdinak sistema desberdinetarako
- Itxi saioa lan-estazioa zaintzarik gabe uztean
- Blokeatu pantaila aldentzen zarenean (Windows+L)

5.2 Pasahitz Kudeatzaileak (Onartuak)

Erakundeak Onartutako Pasahitz Kudeatzaileak:

- **1Password Business** (gomendio nagusia)
- **LastPass Enterprise**

- **Dashlane Business**
- **KeePass** (kode irekia, erabilera kasu zehatzetarako)

Abantailak:

- Pasahitz sendoak eta ausazkoak sortu
- Pasahitzak enkriptatuta gorde
- Kredentzialak automatikoki bete (idazteko erroreak murriztu, phishing erresistentzia)
- Pasahitz bakarra kontu bakoitzerako
- Pasahitz partekatze segurua (beharrezkoa denean)
- Auditoretza arrastoa eta txostenak

Erabilera Baldintzak:

- Erabili pasahitz maisu sendoa (gutxienez 16 karaktere)
- Gaitu Faktore Anitzeko Autentifikazioa pasahitz kudeatzailean
- Ez partekatu pasahitz maisua
- Aldizka berrikusi eta eguneratu gordetako pasahitzak
- Kendu kredentzial zaharrak/erabili gabeak

Debekatuta:

- Nabigatzailean integratutako pasahitz kudeatzaileak (Chrome, Firefox “Gorde Pasahitza”) laneko kontuetarako
- Pasahitz kudeatzaile pertsonalak/kontsumo mailakoak laneko pasahitzetarako
- Enkriptatu gabeko pasahitz biltegiratzea (testu fitxategiak, kalkulu orriak)

5.3 Pasahitz Aldaketak

Errutina Aldaketak:

- Erabiltzaile estandarrak: 90 egunero (iraungitze automatikoa)
- Administratzaileak: 60 egunero
- Zerbitzu kontuak: 365 egunero (edo bideragarria denean)
- MFA duten erabiltzaileak: 180 egunero (luzatua MFA babesagatik)

Behartutako Aldaketak Beharrezkoak Dira:

- Hasierako/aldi baterako pasahitza (lehen saio-hasiera)
- IT-k pasahitza berrezartzea
- Arriskua susmatzen edo baieztatzen denean
- Sarbide partekatua/eskuordetua duen pertsona baten irteera
- Autentifikazio sistemari eragiten dion segurtasun intzidentea
- Baimen luze baten ondoren (>90 egun)

Aldaketa Prozesua:

- Erabiltzaileei jakinarazten zaie iraungitze data baino 14 egun lehenago (eguneroko oroigarriak azken 3 egunetan)
- Auto-zerbitzu pasahitz aldaketa atariaren bidez edo Ctrl+Alt+Del → Aldatu Pasahitza
- Helpdesk laguntza eskuragarri arazoetarako
- Ezin dira azken 12 pasahitzak berrerabili (azken 24 administratzaileentzat)

5.4 Pasahitz Berrezartzeak

Auto-Zerbitzu Berrezarpena:

- Eskuragarri hemen: https://password.zabalagailetak.com
- Faktore anitzeko autentifikazioa behar du:
    - Segurtasun galderak (kontu sorreran ezarriak)
    - Email egiaztapena (erregistratutako emailera)
    - SMS kodea (erregistratutako mugikorrera)

Helpdesk Berrezarpena:

- Kontaktatu IT helpdesk: helpdesk@zabalagailetak.com | +34 XXX XXX XXX
- Identitate egiaztapena beharrezkoa:
    - Langile IDa
    - Informazio pertsonalaren egiaztapena
    - Kudeatzailearen berrespena (urrunekoa bada)
- Aldi baterako pasahitza ematen da (lehen saio-hasieran aldatu behar da)
- Berrezarpena erregistratu eta monitorizatzen da

Segurtasun Neurriak:

- Pasahitz berrezartze estekak ordu 1 igaro ondoren iraungitzen dira
- Berrezartze esteka erabilera bakarrekoa da
- Kontu blokeoaren berrezarpenak onarpena behar du (errepikatutako saio-hasiera okerren ondoren)
- Administratzaile pasahitz berrezarpenak CISOren onarpena behar du

---

6. Faktore Anitzeko Autentifikazioa (MFA)

6.1 MFA Baldintzak

MFA Derrigorrezkoa da:

- Urruneko sarbiderako (VPN)
- Administrazio eta pribilegiatutako kontuetarako
- Oso Konfidentziala den datuak dituzten sistemetarako sarbidea:
    - Bezero datu-baseak
    - Finantza sistemak
    - HR sistemak
- Hodeiko zerbitzuetarako:
    - Microsoft 365 admin kontuak
    - AWS root eta administrazio kontuak
    - GitHub admin kontuak
- Barne sistemetarako kanpo sarbidea

MFA Gomendagarria da:

- Erabiltzaile kontu guztietarako (lan-estazio estandarrak)
- Enpresako emailerako gailu mugikorren sarbidea
- Bezero edo langile PIIra sartzen den edozein sistema

MFA Abantailak:

- Pasahitzak bakarrik zaurgarriak dira (phishing, lapurreta, asmatzea)
- MFAk bigarren egiaztapen faktorea gehitzen du (duzun zerbait)
- Kontu arriskua %99,9 murrizten du
- Pasahitz iraungitze luzeagoa ahalbidetzen du (aldaketa gutxiago)

6.2 MFA Metodoak

Onartutako MFA Metodoak (lehentasun ordenan):

1. **Autentifikatzaile Aplikazioa (TOTP - Denboran Oinarritutako Erabilera Bakarreko Pasahitza):**
    - Gomendatua: Microsoft Authenticator, Google Authenticator, Authy
    - 6 digituko kodea sortzen du 30 segundoro
    - Lineaz kanpo funtzionatzen du
    - Eguneroko erabilerarako seguruena
2. **Hardware Tokena (FIDO2/U2F):**
    - YubiKey, Titan Security Key
    - USB portuan sartzen den edo NFC bidez ukitzen den gailu fisikoa
    - Segurtasun handiena (phishing erresistentea)
    - Pribilegio handieneko kontuetarako derrigorrezkoa (domeinu adminak, root)
3. **Push Jakinarazpena:**
    - Microsoft Authenticator, Duo Push
    - Onartu saio-hasiera eskaera gailu mugikorrean
    - Erosoa baina internet konexioa behar du
    - Egiaztatu saio-hasiera xehetasunak onartu aurretik (zenbaki parekatzea)
4. **SMS Kodea (Gutxien Hobetsia):**
    - Testu mezu bidez bidalitako 6 digituko kodea
    - Beste metodoak ez badaude eskuragarri soilik erabili
    - SIM swapping erasoen aurrean zaurgarria
    - Ez onartua administrazio kontuetarako

Debekatutako MFA Metodoak:

- Email bidezko kodeak (autentifikazio nagusiaren kanal berean)
- Ahots deiak (gizarte ingeniaritza arriskua)
- Egiaztatu gabeko mugikor aplikazioak

6.3 MFA Konfigurazioa eta Babeskopia

Hasierako Konfigurazioa:

- Erabiltzaile guztiek MFAn izena eman behar dute kontua sortu eta 7 eguneko epean
- IT-k konfigurazio argibideak eta laguntza ematen ditu
- Probatu MFA saio-hasiera ordezko sarbidea desgaitu aurretik

Babeskopia Metodoak:

- Eman izena gutxienez bi MFA gailutan (nagusia eta babeskopia)
- Adibideak: Autentifikatzaile aplikazioa telefonoan + YubiKey
- Gorde babeskopia kodeak leku seguruan (pasahitz kudeatzailea)
- Erregistratu babeskopia telefono zenbakia

Galdutako edo Lapurtutako MFA Gailua:

- Jakinarazi berehala IT helpdesk-ari
- Erabili babeskopia MFA metodoa kontuetara sartzeko
- IT-k aldi baterako MFA desgaitu dezake kontua berreskuratzeko (egiaztapenarekin)
- Gailu berrian izena eman 24 orduko epean

---

7. Kontu Blokeoa eta Segurtasuna

7.1 Kontu Blokeo Politika

Kontu Estandarrak:

- **Huts Egindako Saio-hasiera Muga:** 5 saiakera oker
- **Blokeo Iraupena:** 30 minutu (desblokeo automatikoa)
- **Eskuzko Desblokeoa:** IT helpdesk (identitate egiaztapenarekin)

Administrazio Kontuak:

- **Huts Egindako Saio-hasiera Muga:** 3 saiakera oker
- **Blokeo Iraupena:** 1 ordu (desblokeo automatikoa)
- **Eskuzko Desblokeoa:** CISOren onarpena beharrezkoa

Arrazoibidea:

- Indar gordin bidezko pasahitz asmatzea prebenitzen du
- Segurtasuna eta erabilgarritasuna orekatzen ditu
- Blokeo gertaera guztiak erregistratzen ditu monitorizaziorako

Blokeatuta Bada:

1. Itxaron desblokeo automatikoa (30 edo 60 minutu)
2. EDO jarri harremanetan IT helpdesk-arekin identitate egiaztapenerako eta eskuzko desblokeorako
3. Egiaztatu erabiltzaile-izen eta pasahitz zuzena erabiltzen ari zarela
4. Egiaztatu Maiuskula Blokeoa, teklatuaren konfigurazioa (EN vs ES)
5. Errepikatutako blokeoak badaude, aldatu pasahitza (arriskuan egon daiteke)

7.2 Pasahitz Erasoak eta Detekzioa

Ohiko Pasahitz Eraso Motak:

- **Indar Gordina (Brute Force):** Konbinazio posible guztiak probatzea (konplexutasuna + blokeoa bidez arinduta)
- **Hiztegi Erasoa:** Hitz eta pasahitz arruntak probatzea (konplexutasuna bidez arinduta)
- **Kredentzial Stuffing-a:** Beste urraketa batzuetatik filtratutako pasahitzak erabiltzea (pasahitz bakarrak + MFA bidez arinduta)
- **Phishing-a:** Erabiltzaileak engainatzea pasahitzak eman ditzaten (prestakuntza + MFA bidez arinduta)
- **Keylogging-a:** Tekla sakatzeak harrapatzen dituen malwarea (endpoint babesa + MFA bidez arinduta)
- **Gizarte Ingeniaritza:** Erabiltzaileak manipulatzea pasahitzak parteka ditzaten (prestakuntza + “inoiz ez partekatu” politika bidez arinduta)

Detekzioa eta Erantzuna:

- SIEM-ek honako hauek monitorizatzen ditu:
    - Huts egindako saio-hasiera saiakera anitz
    - Ezinezko bidaia (distantzia luzeko kokapenetatik denbora laburrean saioa hastea)
    - Ezohiko IP helbide edo herrialdeetatik saioa hastea
    - Ordu arruntez kanpoko saio-hasiera (erabiltzaile zehatzentzat)
    - Kontu blokeo anitz
- Segurtasun taldeari alerta automatizatuak
- Erantzun automatizatua: IP helbidea blokeatu, pasahitza berrezartzea behartu, kontua eten

- Erabiltzaileari jakinarazpena jarduera susmagarriaz

---

8. Erabilera Kasu Bereziak

8.1 OT Sistemak (PLCak, SCADA, HMI)

Erronkak:

- Pasahitz gaitasun mugatuak dituzten sistema zaharrak
- Erraz berrabiarazi ezin diren sistemak (produkzio eragina)
- Tokiko kontsola sarbidea soilik (sare autentifikaziorik ez)

Baldintzak:

- **Gutxieneko Luzera:** 12 karaktere (sistemak onartzen badu)
- **Konplexutasuna:** Ahalik eta handiena sistemaren mugen barruan
- **Aldaketa Maiztasuna:** 180 egun (edo saltzailearen gomendioen arabera)
- **Dokumentazioa:** Pasahitza kutxa enkriptatuan gordeta
- **Sarbide Kontrola:** OT eremura sarbide fisikoa mugatuta
- **Babeskopia Autentifikazioa:** Urruneko sarbide bereizia MFArekin ahal denean
- **Monitorizazioa:** OT autentifikazio guztiak erregistratuta

Prozedura:

- OT pasahitz aldaketak mantentze leihoekin koordinatuta
- Bi langile baimendu aldaketetarako (kontrol bikoitza)
- Probatu autentifikazioa aldaketen aurretik eta ondoren
- Eguneratu pasahitz kutxa berehala
- Dokumentatu aldaketa aldaketa kudeaketa sisteman

8.2 Larrialdi Sarbidea (“Kristala Apurtu”)

Helburua:

- Larrialdiko administratzaile sarbidea autentifikazio nagusia erabilgarri ez dagoenean
- Azken aukera hondamendi berreskuratze edo intzidente larri batean

Kontrolak:

- Pasahitza gutun-azal batean zigilatuta, kutxa gotor fisiko batean gordeta
- Kutxa gotorrak bi giltza behar ditu (CEO eta CISO)
- Gutun-azalaren zigilua dokumentatutako larrialdian bakarrik hausten da
- Pasahitza berehala aldatzen da erabili ondoren
- Ekintza guztiak erregistratu eta berrikusten dira
- Intzidente txostena beharrezkoa da erabilera azaltzeko

“Kristala Apurtu” Eszenatokiak:

- Autentifikazio sistema nagusiaren hutsegitea (Active Directory erorita)
- Administratzaile kontu blokeoa intzidente kritikoan zehar
- Hondamendi berreskuratzea (administratzaile guztiak ez daude eskuragarri)
- Ransomware-ak autentifikazio sistemei eragiten die

8.3 API Gakoak eta Aplikazio Sekretuak

Ez Dira Pasahitz Tradizionalak Baina Antzeko Babesa Behar Dute:

- **API Gakoak:** Aplikazioen arteko komunikaziorako kredentzialak
- **Datu-base Konexio Kateak:** Erabiltzaile-izena/pasahitza barne
- **Enkriptatze Gakoak:** Enkriptatutako datuak babesteko
- **SSH Gako Pribatuak:** SSH konexioak autentifikatzeko
- **Ziurtagiriak eta Gako Pribatuak:** TLS/SSL ziurtagiriak

Baldintzak:

- **Sorkuntza:** Kriptografikoki ausazkoa (gutxienez 32 karaktere API gakoetarako)
- **Biltegiratzea:** Kutxa enkriptatua edo sekretuen kudeaketa sistema (HashiCorp Vault, AWS Secrets Manager, Azure Key Vault)
- **Transmisioa:** Kanal enkriptatuak soilik (TLS, SSH)
- **Sarbide Kontrola:** Pribilegio gutxienekoa (sarbidea behar duten aplikazio/erabiltzaileak soilik)
- **Txandakatzea:** Ohiko txandakatzea (90-365 egun erabileraren arabera)
- **Monitorizazioa:** Sarbide eta erabilera guztiak erregistratu
- **Baliogabetzea:** Berehala baliogabetu arriskuan badaude

Debekatuta:

- Sekretuak iturburu kodean hardcodeatzea
- Sekretuak bertsio kontrolean gordetzea (Git biltegiak)
- Sekretuak posta elektronikoz edo txat bidez bidaltzea
- Sekretuak enkriptatu gabeko fitxategietan gordetzea

---

9. Pasahitz Politika Betearaztea

9.1 Kontrol Teknikoak

Active Directory / LDAP:

- Pasahitz konplexutasuna Talde Politikaren bidez behartuta
- Pasahitz historia (azken 12 pasahitzak)
- Gutxieneko/gehieneko pasahitz adina
- Kontu blokeo politika
- Fine-Grained Pasahitz Politika kontu pribilegiatuetarako

Web Aplikazioak:

- Pasahitz indar neurgailua (ikusizko iritzia sortzean)
- Konplexutasun balidazioa (frontend eta backend)
- Pasahitz urraketa egiaztapena (ezagunak diren urratutako pasahitzen datu-basearen aurka konparatu - Have I Been Pwned API)
- Saio denbora-muga betearaztea
- MFA betearaztea ekintza sentikorretarako

Pasahitz Hashing-a:

- Pasahitzak inoiz ez dira testu lauan gordetzen
- Hashing algoritmoak:
    - **Hobetsia:** bcrypt (kostu faktorea 12+), Argon2id

    - **Onargarria:** PBKDF2 (100.000+ iterazio), scrypt
    - **Debekatuta:** MD5, SHA1, SHA256 arrunta (gatz/iterazio gabe)
  - Gatzatutako hash-ak (gatz bakarra pasahitz bakoitzerako)
  - Piperra (sekretu globala) babes gehigarrirako

Inplementazio Erreferentzia:

```
// User ereduaren adibidea (ikus src/api/models/User.js)
const bcrypt = require('bcryptjs');
const saltRounds = 12;

// Pasahitza hash-eatu gorde aurretik
userSchema.pre('save', async function(next) {
  if (!this.isModified('password')) return next();
  this.password = await bcrypt.hash(this.password, saltRounds);
  next();
});

// Konparatu pasahitza autentifikaziorako
userSchema.methods.comparePassword = async function(candidatePassword) {
  return await bcrypt.compare(candidatePassword, this.password);
};
```

9.2 Monitorizazioa eta Auditoretza

Pasahitzekin Lotutako Gertaerak Erregistratuta:

- Pasahitz aldaketak (arrakastatsuak eta huts egindakoak)
- Pasahitz berrezartzeak (auto-zerbitzua eta helpdesk)
- Huts egindako saio-hasiera saiakerak
- Kontu blokeoak eta desblokeoak
- MFA izen-ematea eta aldaketak
- Pribilegio eskalatzea (sudo, administratzaile gisa exekutatu)
- Pasahitz politika urraketak

SIEM Alertak:

- Huts egindako saio-hasiera anitz (balizko indar gordina)
- Kontu blokeo anitz (balizko pasahitz spray erasoa)
- Ezohiko kokapen edo gailutik saioa hastea
- Administrazio pasahitz berrezarpena (justifikazioa eskatu)
- Pribilegiatutako kontu erabilera ordu arruntetatik kanpo
- Erabiltzaile anitz aldi berean blokeatuta (balizko erasoa)

Ohiko Berrikuspenak:

- Hiruhileko sarbide berrikuspena (egiaztatu erabiltzaileek oraindik sarbidea behar duten)
- Hileroko kontu pribilegiatuen berrikuspena (egiaztatu admin sarbidea oraindik beharrezkoa den)
- Berehalako berrikuspena segurtasun intzidenteen ondoren
- Urteroko auditoria integrala (pasahitz politika betetzea)

---

10. Erabiltzaile Hezkuntza eta Kontzientziazioa

10.1 Prestakuntza

Langile Berriak:

- Pasahitz politikaren ikuspegi orokorra onboarding-ean (30 minutu)
- Pasahitz sendoak nola sortu
- Pasahitz kudeatzailearen konfigurazioa eta erabilera
- MFA izen-ematea
- Phishing kontzientziazioa (pasahitz lapurreta)

Langile Guztiak (Urteroko Freskatzea):

- Pasahitz jardunbide egokien oroigarria
- Azken mehatxuak (kredentzial stuffing-a, phishing joerak)
- MFA garrantzia
- Intzidente kasu azterketak (anonimizatuak)

Prestakuntza Espezializatua:

- Administratzaileak: Pribilegiatutako sarbide kudeaketa, kristala apurtu prozedurak
- Garatzaileak: Sekretuen kudeaketa, pasahitz biltegiratze segurua
- Kudeatzaileak: Betearazpen erantzukizunak, jarduera susmagarrien ezagutza

10.2 Kontzientziazio Materialak

Eskuragarri dauden Baliabideak:

- Pasahitz politika erreferentzia azkarreko gida (orrialde bateko PDF)
- Pasahitz sendoak sortzeko gida
- Pasahitz kudeatzailearen konfigurazio bideoak
- MFA izen-emate argibideak
- Phishing identifikazio aholkuak
- Segurtasun kontzientziazio kartelak (atseden gelak, lan-estazioetatik gertu)

Komunikazio Kanalak:

- Hileroko segurtasun buletina
- Intranet segurtasun orria
- Email oroigarriak pasahitza iraungitze aurretik
- Saio-hasiera pantailako pasahitz aholkuak
- IT helpdesk ezagutza oinarria

---

11. Salbuespenak eta Uko Egiteak

11.1 Salbuespen Prozesua

Noiz Eman Daitezkeen Salbuespenak:

- Sistema zaharren muga teknikoak
- Saltzaileak eskatutako pasahitz formatuak
- Betetze baldintza zehatzak
- Larrialdiko negozio beharra

Salbuespen Eskaera:

1. Bidali idatzizko eskaera CISOri
2. Sartu:
    - Kaltetutako sistema/kontua

        - Bete ezin den baldintza zehatza
        - Negozio justifikazioa
        - Proposatutako konpentsazio kontrolak
        - Arrisku ebaluazioa
        - Salbuespen iraupena (gehienez 6 hilabete)
3. CISO berrikuspena eta arrisku ebaluazioa
4. Onarpena edo ukazioa dokumentazioarekin
5. Onartzen bada: Konpentsazio kontrolak inplementatu, berrikuspena programatu

Konpentsazio Kontrolak:

- Monitorizazio hobetua
- Sarbide mugatua (IP zerrenda zuria, sare segmentazioa)
- Autentifikazio faktore gehigarria
- Baimen esparru murriztua
- Maizko pasahitz aldaketak
- Aldizkako auditoriak

Adibidezko Salbuespenak:

- Gehienez 8 karaktereko pasahitzak onartzen dituen OT sistema → Konpentsatu sarbide fisiko kontrolatua + sare isolatuarekin
- Pasahitz estatikoa behar duen zerbitzu kontua → Konpentsatu sekretuen kutxarekin + erregistro hobetuarekin
- MFA euskarririk gabeko aplikazio zaharra → Konpentsatu IP zerrenda zuriarekin
- maizko pasahitz aldaketekin

11.2 Salbuespen Berrikuspena

- Salbuespenak hiruhilero berrikusten dira
- Berritzea 6 hilabetero beharrezkoa (etengabeko beharra justifikatu)
- Salbuespenak baliogabetzen dira honako kasuetan:
    - Konpentsazio kontrolak huts egiten dutenean
    - Sistema berritzeak betetzea ahalbidetzen duenean
    - Negozio beharra jada existitzen ez denean
    - Arrisku maila onartezina bihurtzen denean

---

12. Pasahitz Politika Urraketak

12.1 Ohiko Urraketak

Larritasuna: Baxua (Abisua)

- Pasahitz ahula konplexutasuna betetzen ez duena (sistemak detektatua)
- Pasahitza idaztea (leku seguruan ez)
- Pasahitz bera erabiltzea barne eta kanpo kontuetarako (urraketa monitorizazio bidez detektatua)

Larritasuna: Ertaina (Idatzizko Ohartarazpena, Berriro Prestatzea)

- Pasahitza lankidearekin partekatzea (nahiz eta asmo onekin izan)
- Pasahitz zaharrak berrerabiltzea (historia saihestu nahian)
- Pasahitza ez aldatzea ustezko konpromisoaren ondoren
- Pasahitzak enkriptatu gabeko fitxategian gordetzea

Larritasuna: Handia (Etenaldia, Kaleratze Posiblea)

- Administrazio pasahitza partekatzea
- Nahita pasahitz ahula erabiltzea erosotasunagatik abisu anitzen ondoren
- Ezaguna den konpromisoa ez jakinaraztea
- Pasahitz partekatze maltzurra (baimenik gabeko sarbidea ahalbidetuz)

12.2 Konponketa

Berehalako Ekintzak:

- Pasahitza berrezartzea behartu
- Arriskuan dagoen kontua eten
- Kontu jarduera berrikusi (baimenik gabeko ekintzak identifikatu)
- Kaltetutako erabiltzaile/sistemak jakinarazi
- Diziplina prozesua HR politikaren arabera

Jarraipena:

- Derrigorrezko berriro prestatzea
- Monitorizazio hobetua (90 egun)
- Zuzendaritzari txostena
- Langile fitxategian dokumentatu

---

13. Lotutako Politikak eta Estandarrak

Barne Dokumentuak:

- Informazioaren Segurtasun Politika (ISP-001)
- Erabilera Onargarriaren Politika (AUP-001)
- Sarbide Kontrol Politika
- Intzidente Erantzun Prozedura

Kanpo Estandarrak:

- ISO/IEC 27001:2022 - A Eranskina 5.17 (Autentifikazio Informazioa)
- NIST SP 800-63B - Identitate Digitalaren Gidalerroak (Autentifikazioa eta Bizi-zikloaren Kudeaketa)
- CIS Controls v8 - 6. Kontrola (Sarbide Kontrol Kudeaketa)
- GDPR 32. Artikulua - Tratamenduaren Segurtasuna

---

14. Politika Berrikuspena eta Eguneraketak

Berrikuspen Maiztasuna: Urtero edo honakoek eraginda:

- Pasahitzekin lotutako segurtasun intzidenteak
- Mehatxu paisaian aldaketak
- Teknologia eguneraketak (autentifikazio metodo berriak)
- Arau aldaketak
- Erabiltzaile iritzia eta erabilgarritasun kezkak

Eguneratze Prozesua:

1. CISO berrikuspena hasten du
2. IT, segurtasun talde eta erabiltzaileekin kontsulta
3. Eguneraketa zirriborroa
4. Zuzendaritza onarpena
5. Erabiltzaile komunikazioa
6. Prestakuntza eguneraketak
7. Inplementazio teknikoa
8. Monitorizazioa eta iritzia

---

15. Harremanetarako Informazioa

Galderak edo Arazoak:

- **IT Helpdesk:** helpdesk@zabalagailetak.com | +34 XXX XXX XXX
- **Pasahitz Berrezartzeak:** https://password.zabalagailetak.com
- **CISO:** ciso@zabalagailetak.com | +34 XXX XXX XXX
- **Segurtasun Intzidenteak:** security@zabalagailetak.com | +34 XXX XXX XXX (24/7)

Eranskina A: Pasahitz Politika Erreferentzia Azkarra

Erabiltzaile Estandarrentzat

- ✅ **Gutxienez 12 karaktere** (luzeagoa hobe!)
- ✅ **Maiuskula, minuskula, zenbaki eta karaktere berezien nahasketa**
- ✅ **Pasahitz bakarra sistema bakoitzerako**
- ✅ **Erabili pasahitz kudeatzailea**
- ✅ **Gaitu MFA ahal den guztietan**
- ✅ **Aldatu 90 egunero** (oroigarri automatikoa)
- ❌ **Inoiz ez partekatu pasahitzak inorekin**
- ❌ **Inoiz ez idatzi pasahitzak**
- ❌ **Inoiz ez berrerabili pasahitz zaharrak**
- ❌ **Inoiz ez erabili informazio pertsonala (izena, jaioteguna)**

Administratzaileentzat

- ✅ **Gutxienez 14 karaktere**
- ✅ **Karaktere mota guztiak beharrezkoak**
- ✅ **Administrazio kontu bereizia**
- ✅ **Hardware MFA tokena (YubiKey)**
- ✅ **Aldatu 60 egunero**
- ❌ **Inoiz ez partekatu administrazio pasahitzak**
- ❌ **Inoiz ez erabili administrazio kontua eguneroko lanerako**

Eranskina B: Pasahitz Indar Adibideak

Pasahitza	Indarra	Zergatik?
password	❌ Oso Ahula	Hitz arrunta, hiztegian
Password123	❌ Ahula	Eredu arrunta, aurreikusgarria
Zabala2026!	⚠️ Eskasa	Enpresa izena, urtea, karaktere berezi bakarra
JuanGarcia1975	⚠️ Eskasa	Info pertsonala (izena, jaiotze urtea)
K0ff33&K00k!et4k	✅ Ona	14 karaktere,
nahasketa, baina ordezkapen aurreikusgarriak		
Urdina#Elefantea$Dantzan77	✅ Sendoa	24 karaktere,
ausazko hitzak, zenbakiak, bereziak		
NireTxakurrakZabalaGailetakMaiteDitu!	✅ Sendoa	36 karaktere,
pasaesaldia, gogangarria		
Xk9$mP2#vQ7!nR5@wL3%	✅ Oso Sendoa	20 karaktere,
guztiz ausazkoa (erabili pasahitz kudeatzailea)		

Eranskina C: Pasahitz Kudeatzailea Konfiguratzeko Gida

1Password Konfigurazioa (Gomendatua)

1. IT administratzaileak 1Password Business kontua sortzen du zuretzat
2. Gonbidapen emaila jasotzen duzu
3. Klikatu estekan eta sortu Pasahitz Maisua:
    - Gutxienez 16 karaktere
    - Erabili pasaesaldia edo oso pasahitz sendoa
    - Idatzi Pasahitz Maisua BAKARRIK eta gorde leku seguruan (etxeko kutxa gotorra)
    - Gaitu MFA 1Password kontuan
4. Instalatu 1Password aplikazioa:
    - Mahaigainean: Windows/Mac/Linux
    - Nabigatzaile luzapena: Chrome/Firefox/Edge
    - Mugikorrean: iOS/Android
5. Gorde laneko pasahitzak “Lana” kutxan (ITrekin partekatua beharrezkoa bada)
6. Gorde pasahitz pertsonalak “Pertsonala” kutxan (pribatua)
7. Sortu pasahitz sendo berriak laneko pasahitzak aldatzean

1Password Erabiliz

- **Auto-betetzea:** Nabigatzaile luzapenak saio-hasiera orriak detektatzen ditu, kredentzialak betetzea eskaintzen du
- **Sortu:** Klikatu “Sortu Pasahitza” kontu berriak sortzean
- **Segurtasun Egiaztapena:** Pasahitz ahulak, berrerabiliak edo arriskuan daudenak identifikatzen ditu
- **Larrialdi Sarbidea:** Izendatu konfiantzazko pertsona bat (IT kudeatzailea) larrialdi kontaktu gisa

---

Eranskina D: MFA Izen-emate Argibideak

Microsoft Authenticator Konfigurazioa

1. Instalatu Microsoft Authenticator aplikazioa smartphonean:
    - iOS: App Store
    - Android: Google Play Store
2. Ireki aplikazioa, klikatu “+” kontua gehitzeko
3. Hautatu “Laneko edo eskolako kontua”
4. Eskaneatu izen-ematean bistaratutako QR kodea:
    - Bisitatu https://aka.ms/mfasetup
    - Edo nabigatu Kontu Ezarpenak → Segurtasun Info → Gehitu Metodoa
5. Aplikazioak 6 digituko kodea erakusten du (30 segundoro aldatzen da)
6. Sartu kodea konfigurazioa egiaztatzeko
7. Gaitu push jakinarazpenak saio-hasiera onarpen errazerako
8. **GARRANTZITSUA:** Gorde babeskopia kodeak pasahitz kudeatzailean (gailua galtzen bada)

Babeskopia Metodoak

- Eman izena bigarren gailu batean (tableta, bigarren telefonoa)
- Gehitu babeskopia telefono zenbakia SMS bidez (azken aukera gisa bakarrik)
- Inprimatu babeskopia kodeak eta gorde segurtasunez etxean

Eranskina E: Intzidente Erantzuna - Arriskuan Dagoen Pasahitza

Zure pasahitza arriskuan dagoela susmatzen baduzu:

1. **GELDITU** kontua erabiltzea berehala
2. **ALDATU** pasahitza berehala:
    - Auto-zerbitzua: https://password.zabalagailetak.com
    - Edo deitu IT helpdesk-ari: +34 XXX XXX XXX
3. **JAKINARAZI** segurtasun taldeari:
    - Emaila: security@zabalagailetak.com
    - Telefonoa: +34 XXX XXX XXX (24/7)
4. **EMAN** xehetasunak:
    - Noiz susmatu zenuen arriskua?
    - Nola aurkitu zenuen? (ezohiko kontu jarduera, phishing emaila, malware alerta)
    - Zein sistema/kontu daude kaltetuta?
    - Zer ekintza har zitzakeen erasotzaileak?
5. **LAGUNDU** ikerketan:
    - Segurtasun taldeak eska dezake:
        - Azken saio-hasiera historia berrikustea
        - Gailuaren forentse eskaneatzea

        - Lotutako kontuetarako sarbidea
    - Ez ezabatu ezer (ebidentzia gordetzea)
6. **JARRAIPENA:**
    - Aldatu pasahitzak kontu GUZTIETAN pasahitz bera erabiltzen bazenuen (lana eta pertsonala)
    - Berrikusi kontu jarduera baimenik gabeko ekintzetarako
    - Gaitu MFA oraindik gaituta ez badago
    - Eman izena pasahitz kudeatzailean

Zure pasahitza arriskuan egon daitekeen seinaleak:

- Azalpenik gabeko kontu blokeoak
- Saio-hasiera jakinarazpenak ezohiko kokapen edo orduetatik
- Ezagutzen ez duzun kontu jarduera (bidalitako emailak, sartutako fitxategiak)
- Ezohiko sistema portaera
- “Zure pasahitza aldatu da” dioen emaila jasotzea (baina zuk ez duzu aldatu)
- Erabiltzaile-izen/pasahitza datu-urraketa jakinarazpen batean aurkitzea

---

PASAHITZ POLITIKAREN AMAIERA

AITORTZA

Aitortzen dut Zabala Gailetak-en Pasahitz Politika (PWD-001) irakurri eta ulertu dudala. Pasahitz baldintza guztiak betetzea onartzen dut eta ulertzen dut urraketek diziplina ekintzak ekar ditzaketela.

Langilearen Izena: _____
Langilearen IDa: _____
Sinadura: _____
Data: _____