

# Segurtasun aholkuak

## GISA Elkartea

Arrosa Sareko 1. Jardunaldiak

2012.eko otsailaren 22

- 1 Pasahitzak
  - Pasahitz onak sortzeko teknikak
  - Pasahitzak kudeatzeko teknikak
- 2 Zifraketa
  - Urrutiko sarrerak
  - Epostaren zifraketa
  - Mezuen zifraketa
  - Fitxategien zifraketa
  - Disko gogorren zifraketa
- 3 Datuen ezabaketa
- 4 Sistema Eragile seguruak
- 5 Kontrol soziala sahiesten
  - Google Inc. akatu
  - Sare “sozialak”
  - Gehiago!
- 6 Bukatzeko

Pasahitzek gure datuak eta ekintzen gain ditugun baimenak babesten dituzte, beraz oso garrantzitsuak dira segurtasunari dagokionez. Hala ere, punturik ahulenak izaten dira kasu gehienetan. Ohikoak izaten diren akatsetako batzuk:

- Pasahitz ximpleak (akatsik ohikoena).
- Pasahitzak textu planoan apuntatzea.
- Pasahitz berdina erabiltzea leku ezberdinetan.
- Pasahitzak inoiz ez aldatzea.
- Pasahitza beste jendeari elaraztea bitarteko ez seguruen bidez.

Pasahitzek gure datuak eta ekintzen gain ditugun baimenak babesten dituzte, beraz oso garrantzitsuak dira segurtasunari dagokionez. Hala ere, punturik ahulenak izaten dira kasu gehienetan. Ohikoak izaten diren akatsetako batzuk:

- Pasahitz ximpleak (akatsik ohikoena).
- Pasahitzak testu planoan apuntatzea.
- Pasahitz berdina erabiltzea leku ezberdinetan.
- Pasahitzak inoiz ez aldatzea.
- Pasahitza beste jendeari elaraztea bitarteko ez seguruen bidez.

Pasahitzek gure datuak eta ekintzen gain ditugun baimenak babesten dituzte, beraz oso garrantzitsuak dira segurtasunari dagokionez. Hala ere, punturik ahulenak izaten dira kasu gehienetan. Ohikoak izaten diren akatsetako batzuk:

- Pasahitz ximpleak (akatsik ohikoena).
- Pasahitzak textu planoan apuntatzea.
- Pasahitz berdina erabiltzea leku ezberdinetan.
- Pasahitzak inoiz ez aldatzea.
- Pasahitza beste jendeari elaraztea bitarteko ez seguruen bidez.

Pasahitzek gure datuak eta ekintzen gain ditugun baimenak babesten dituzte, beraz oso garrantzitsuak dira segurtasunari dagokionez. Hala ere, punturik ahulenak izaten dira kasu gehienetan. Ohikoak izaten diren akatsetako batzuk:

- Pasahitz ximpleak (akatsik ohikoena).
- Pasahitzak textu planoan apuntatzea.
- Pasahitz berdina erabiltzea leku ezberdinetan.
- Pasahitzak inoiz ez aldatzea.
- Pasahitza beste jendeari elaraztea bitarteko ez seguruen bidez.

Pasahitzek gure datuak eta ekintzen gain ditugun baimenak babesten dituzte, beraz oso garrantzitsuak dira segurtasunari dagokionez. Hala ere, punturik ahulenak izaten dira kasu gehienetan. Ohikoak izaten diren akatsetako batzuk:

- Pasahitz ximpleak (akatsik ohikoena).
- Pasahitzak textu planoan apuntatzea.
- Pasahitz berdina erabiltzea leku ezberdinetan.
- Pasahitzak inoiz ez aldatzea.
- Pasahitza beste jendeari elaraztea bitarteko ez seguruen bidez.

Pasahitzek gure datuak eta ekintzen gain ditugun baimenak babesten dituzte, beraz oso garrantzitsuak dira segurtasunari dagokionez. Hala ere, punturik ahulenak izaten dira kasu gehienetan. Ohikoak izaten diren akatsetako batzuk:

- Pasahitz ximpleak (akatsik ohikoena).
- Pasahitzak textu planoan apuntatzea.
- Pasahitz berdina erabiltzea leku ezberdinetan.
- Pasahitzak inoiz ez aldatzea.
- Pasahitza beste jendeari elaraztea bitarteko ez seguruen bidez.



## Sinbologia:

- P@s@h1tza
- -->h1tza-->

## Mnemoteknia:

- Ez zarete denak etorriko: Ez100%<--
- 3 poterekin kontten nago: 3U:)nago

## Hizkuntza:

- 16:00tan kafea hartzeko.
- Ze, 10ak goaz?

## Automatikoak

## Sinbologia:

- P@s@h1tza
- -->h1tza-->

## Mnemoteknia:

- Ez zarete denak etorriko: Ez100%<--
- 3 poterekin kontten nago: 3U:)nago

## Hizkuntza:

- 16:00tan kafea hartzeko.
- Ze, 10ak goaz?

## Automatikoak

## Sinbologia:

- P@s@h1tza
- -->h1tza-->

## Mnemoteknia:

- Ez zarete denak etorriko: Ez100%<--
- 3 poterekin kontten nago: 3U:)nago

## Hizkuntza:

- 16:00tan kafea hartzeko.
- Ze, 10ak goaz?

## Automatikoak

## Sinbologia:

- P@s@h1tza
- -->h1tza-->

## Mnemoteknia:

- Ez zarete denak etorriko: Ez100%<--
- 3 poterekin kontten nago: 3U:)nago

## Hizkuntza:

- 16:00tan kafea hartzeko.
- Ze, 10ak goaz?

## Automatikoak

**Pasahitz kudeatzaileak** Pasahitz maisu bat erabiliz pasahitzak zifratzen dituen programa<sup>1</sup>.

**Gakoen deribazio funtzioa** Pasahitz maisu bat edukiz, hitz baten bitartez, beste pasahitz eratorria sortzeko algoritmoa<sup>2</sup>.

**SSSS** Pasahitz bat “zati” ezberdinetan banatzeko algoritmoa. Zati kantitate minimo bat elkartu behar da pasahitza lortzeko<sup>3</sup>.

---

<sup>1</sup>KeePassX, Password-Gorilla, Lastpass Password Manager, Password Protect

<sup>2</sup>pbkdf2, Password Maker, Password Hasher

<sup>3</sup>SSSS

**Pasahitz kudeatzaileak** Pasahitz maisu bat erabiliz pasahitzak zifratzen dituen programa<sup>1</sup>.

**Gakoen deribazio funtzioa** Pasahitz maisu bat edukiz, hitz baten bitartez, beste pasahitz eratorria sortzeko algoritmoa<sup>2</sup>.

**SSSS** Pasahitz bat “zati” ezberdinetan banatzeko algoritmoa. Zati kantitate minimo bat elkartu behar da pasahitza lortzeko<sup>3</sup>.

---

<sup>1</sup>KeePassX, Password-Gorilla, Lastpass Password Manager, Password Protect

<sup>2</sup>pbkdf2, Password Maker, Password Hasher

<sup>3</sup>SSSS

**Pasahitz kudeatzaileak** Pasahitz maisu bat erabiliz pasahitzak zifratzen dituen programa<sup>1</sup>.

**Gakoen deribazio funtzioa** Pasahitz maisu bat edukiz, hitz baten bitartez, beste pasahitz eratorria sortzeko algoritmoa<sup>2</sup>.

**SSSS** Pasahitz bat “zati” ezberdinetan banatzeko algoritmoa. Zati kantitate minimo bat elkartu behar da pasahitza lortzeko<sup>3</sup>.

---

<sup>1</sup>KeePassX, Password-Gorilla, Lastpass Password Manager, Password Protect

<sup>2</sup>pbkdf2, Password Maker, Password Hasher

<sup>3</sup>SSSS

**Zifraketa simetrikoa** Pasahitz edo gako berdina erabiltzen da zifratzeko eta deszifratzeko. Arriskua beraz, pasahitz hori bitarte seguruen bidez elaraztean datza.



# Zifraketa simetrikoa



A eta  $B$ k gako edo pasahitz berdina eduki behar dute.





**Zifraketa asimetrikoa** Bi pasahitz edo gako daude. Gako publikoa bakarrik zifratzeko balio du eta gako pribatua bakarrik deszifratzeko. Ez dago beraz inongo pasahitza elarazteko beharrik.

ARANTXA

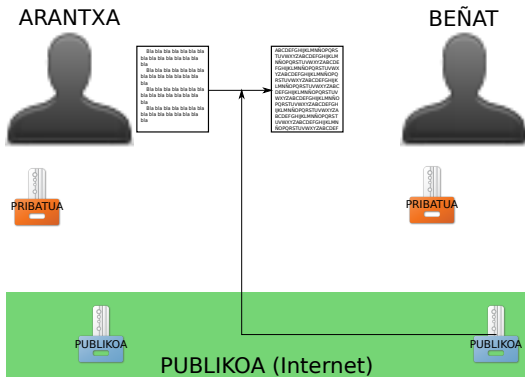


BEÑAT

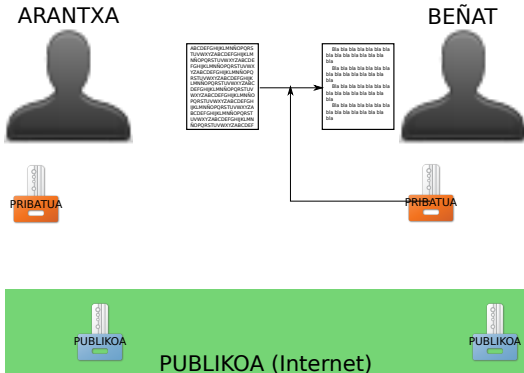


PUBLIKOA (Internet)

A eta Bk gako pribatu eta publikoak dituzte.



Gako publikoak konpartitu daitezke, beraz Internetera igotzen dituzte. Ak Bri mezu bat bidaltzeko, *Bren* gako publikoa hartu eta horrekin textu planoaz zifratzen du.



Bk zifratutako textua bere gako pribatuarekin deszifratzen du textu planoan lortuz.

OpenSSH<sup>4</sup> erabiliz, ordenagailu batetik beste bat erabili dezakegu komunikazioa zifratuz.

- 1 SSH zerbitzaria instalatu eta konfiguratu<sup>5</sup>.
- 2 Makinak ez badu IP helbide finkorik, dyndns<sup>6</sup> kontu bat iriki eta makinan<sup>7</sup> konfiguratu.
- 3 SSH bezeroa jeitsi eta beste makinan sartu gaitezke.
- 4 Segurtasuna (eta erosotasuna) hareagotzeko, gako pare publiko-pribatu bat sortu<sup>8</sup>.

---

<sup>4</sup><http://www.openssh.com/>

<sup>5</sup><http://www.yolinux.com/TUTORIALS/LinuxTutorialInternetSecurity.html#SSH>

<sup>6</sup><http://free.domain.name/>

<sup>7</sup>ddclient

<sup>8</sup><http://www.debian->



OpenSSH<sup>4</sup> erabiliz, ordenagailu batetik beste bat erabili dezakegu komunikazioa zifratuz.

- 1 SSH zerbitzaria instalatu eta konfiguratu<sup>5</sup>.
- 2 Makinak ez badu IP helbide finkorik, dyndns<sup>6</sup> kontu bat iriki eta makinan<sup>7</sup> konfiguratu.
- 3 SSH bezeroa jeitsi eta beste makinan sartu gaitezke.
- 4 Segurtasuna (eta erosotasuna) hareagotzeko, gako pare publiko-pribatu bat sortu<sup>8</sup>.

---

<sup>4</sup><http://www.openssh.com/>

<sup>5</sup><http://www.yolinux.com/TUTORIALS/LinuxTutorialInternetSecurity.html#SSH>

<sup>6</sup><http://free.domain.name/>

<sup>7</sup>ddclient

<sup>8</sup><http://www.debian->

OpenSSH<sup>4</sup> erabiliz, ordenagailu batetik beste bat erabili dezakegu komunikazioa zifratuz.

- 1 SSH zerbitzaria instalatu eta konfiguratu<sup>5</sup>.
- 2 Makinak ez badu IP helbide finkorik, dyndns<sup>6</sup> kontu bat iriki eta makinan<sup>7</sup> konfiguratu.
- 3 SSH bezeroa jeitsi eta beste makinan sartu gaitezke.
- 4 Segurtasuna (eta erosotasuna) hareagotzeko, gako pare publiko-pribatu bat sortu<sup>8</sup>.

---

<sup>4</sup><http://www.openssh.com/>

<sup>5</sup><http://www.yolinux.com/TUTORIALS/LinuxTutorialInternetSecurity.html#SSH>

<sup>6</sup><http://free.domain.name/>

<sup>7</sup>ddclient

<sup>8</sup><http://www.debian->

OpenSSH<sup>4</sup> erabiliz, ordenagailu batetik beste bat erabili dezakegu komunikazioa zifratuz.

- 1 SSH zerbitzaria instalatu eta konfiguratu<sup>5</sup>.
- 2 Makinak ez badu IP helbide finkorik, dyndns<sup>6</sup> kontu bat iriki eta makinan<sup>7</sup> konfiguratu.
- 3 SSH bezeroa jeitsi eta beste makinan sartu gaitezke.
- 4 Segurtasuna (eta erosotasuna) hareagotzeko, gako pare publiko-pribatu bat sortu<sup>8</sup>.

---

<sup>4</sup><http://www.openssh.com/>

<sup>5</sup><http://www.yolinux.com/TUTORIALS/LinuxTutorialInternetSecurity.html#SSH>

<sup>6</sup><http://free.domain.name/>

<sup>7</sup>ddclient

<sup>8</sup><http://www.debian->

OpenSSH<sup>4</sup> erabiliz, ordenagailu batetik beste bat erabili dezakegu komunikazioa zifratuz.

- 1 SSH zerbitzaria instalatu eta konfiguratu<sup>5</sup>.
- 2 Makinak ez badu IP helbide finkorik, dyndns<sup>6</sup> kontu bat iriki eta makinan<sup>7</sup> konfiguratu.
- 3 SSH bezeroa jeitsi eta beste makinan sartu gaitezke.
- 4 Segurtasuna (eta erosotasuna) hareagotzeko, gako pare publiko-pribatu bat sortu<sup>8</sup>.

---

<sup>4</sup><http://www.openssh.com/>

<sup>5</sup><http://www.yolinux.com/TUTORIALS/LinuxTutorialInternetSecurity.html#SSH>

<sup>6</sup><http://free.domain.name/>

<sup>7</sup>ddclient

<sup>8</sup><http://www.debian->

- 1 GnuPG instalatu <sup>9</sup>.
- 2 Eposta bezero bat instalatu<sup>10</sup>.
- 3 Eposta bezerorako plugina instalatu<sup>11</sup>.
- 4 Gako pare bat sortu.
- 5 Gako publikoa Interneten jarri.
- 6 Hitzegin nahi den jendearen gako publikoak hartu.

---

<sup>9</sup> GnuPG, Seahorse, KGPG

<sup>10</sup> Thunderbir, Claws Mail

<sup>11</sup> Enigmail, Claws Mail GPG plugin

- 1 GnuPG instalatu <sup>9</sup>.
- 2 Eposta bezero bat instalatu<sup>10</sup>.
- 3 Eposta bezerorako plugina instalatu<sup>11</sup>.
- 4 Gako pare bat sortu.
- 5 Gako publikoa Interneten jarri.
- 6 Hitzegin nahi den jendearen gako publikoak hartu.

---

<sup>9</sup> GnuPG, Seahorse, KGPG

<sup>10</sup> Thunderbir, Claws Mail

<sup>11</sup> Enigmail, Claws Mail GPG plugin

- 1 GnuPG instalatu <sup>9</sup>.
- 2 Eposta bezero bat instalatu<sup>10</sup>.
- 3 Eposta bezerorako plugina instalatu<sup>11</sup>.
- 4 Gako pare bat sortu .
- 5 Gako publikoa Interneten jarri.
- 6 Hitzegin nahi den jendearen gako publikoak hartu.

---

<sup>9</sup> GnuPG, Seahorse, KGPG

<sup>10</sup> Thunderbir, Claws Mail

<sup>11</sup> Enigmail, Claws Mail GPG plugin

- 1 GnuPG instalatu <sup>9</sup>.
- 2 Eposta bezero bat instalatu<sup>10</sup>.
- 3 Eposta bezerorako plugina instalatu<sup>11</sup>.
- 4 Gako pare bat sortu.
- 5 Gako publikoa Interneten jarri.
- 6 Hitzegin nahi den jendearen gako publikoak hartu.

---

<sup>9</sup> GnuPG, Seahorse, KGPG

<sup>10</sup> Thunderbir, Claws Mail

<sup>11</sup> Enigmail, Claws Mail GPG plugin



- 1 GnuPG instalatu <sup>9</sup>.
- 2 Eposta bezero bat instalatu<sup>10</sup>.
- 3 Eposta bezerorako plugina instalatu<sup>11</sup>.
- 4 Gako pare bat sortu.
- 5 Gako publikoa Interneten jarri.
- 6 Hitzegin nahi den jendearen gako publikoak hartu.

---

<sup>9</sup> GnuPG, Seahorse, KGPG

<sup>10</sup> Thunderbir, Claws Mail

<sup>11</sup> Enigmail, Claws Mail GPG plugin

- 1 GnuPG instalatu <sup>9</sup>.
- 2 Eposta bezero bat instalatu<sup>10</sup>.
- 3 Eposta bezerorako plugina instalatu<sup>11</sup>.
- 4 Gako pare bat sortu.
- 5 Gako publikoa Interneten jarri.
- 6 Hitzegin nahi den jendearen gako publikoak hartu.

---

<sup>9</sup> GnuPG, Seahorse, KGPG

<sup>10</sup> Thunderbir, Claws Mail

<sup>11</sup> Enigmail, Claws Mail GPG plugin

- 1 **Pidgin** instalatu.
- 2 **Pidginerako OTR plugina** instalatu.
- 3 Beste pertsonak berdina egin dezala.
- 4 Batak bestea autentifikatu.

- 1 Pidgin instalatu.
- 2 Pidginerako OTR plugina instalatu.
- 3 Beste pertsonak berdina egin dezala.
- 4 Batak bestea autentifikatu.

- 1 Pidgin instalatu.
- 2 Pidginerako OTR plugina instalatu.
- 3 Beste pertsonak berdina egin dezala.
- 4 Batak bestea autentifikatu.

- 1 Pidgin instalatu.
- 2 Pidginerako OTR plugina instalatu.
- 3 Beste pertsonak berdina egin dezala.
- 4 Batak bestea autentifikatu.

**GnuPG** Fitxategiak banaka banaka zifratzeko<sup>12</sup>.

EncFS<sup>13</sup> Direktorio osoak zifratzeko<sup>14</sup>.

---

<sup>12</sup><http://www.techrepublic.com/blog/opensource/encrypting-and-decrypting-files-with-gnupg/168>

<sup>13</sup>EncFS, K-EncFS

<sup>14</sup><http://www.arg0.net/encfsintro>

- GnuPG Fitxategiak banaka banaka zifratzeko<sup>12</sup>.
- EncFS<sup>13</sup> Direktorio osoak zifratzeko<sup>14</sup>.

---

<sup>12</sup><http://www.techrepublic.com/blog/opensource/encrypting-and-decrypting-files-with-gnupg/168>

<sup>13</sup>EncFS, K-EncFS

<sup>14</sup><http://www.arg0.net/encfsintro>



TrueCrypt<sup>15</sup> Iturburu kodea itxia du eta bere zifraketa algoritmoa (aes-xts-plain) ez da segurua.

LUKS<sup>16</sup> Sistema eragile osoak, disko gogorrak, partizioak eta fitxategiak zifratzen ditu<sup>17</sup>.

---

<sup>15</sup><http://www.truecrypt.org/>

<sup>16</sup><https://code.google.com/p/cryptsetup/>

<sup>17</sup><http://www.hermann-uwe.de/blog/howto-disk-encryption-with-dm-crypt-luks-and-debian,>  
[http://www.finnie.org/2009/07/26/howto-encrypt-an-existing-debian-installation/,](http://www.finnie.org/2009/07/26/howto-encrypt-an-existing-debian-installation/)  
<http://www.finnie.org/2009/07/26/keyfile-based-luks-encryption-in-debian/>

TrueCrypt<sup>15</sup> Iturburu kodea itxia du eta bere zifraketa algoritmoa (aes-xts-plain) ez da segurua.

LUKS<sup>16</sup> Sistema eragile osoak, disko gogorrak, partizioak eta fitxategiak zifratzen ditu<sup>17</sup>.

---

<sup>15</sup><http://www.truecrypt.org/>

<sup>16</sup><https://code.google.com/p/cryptsetup/>

<sup>17</sup><http://www.hermann-uwe.de/blog/howto-disk-encryption-with-dm-crypt-luks-and-debian,>  
[http://www.finnie.org/2009/07/26/howto-encrypt-an-existing-debian-installation/,](http://www.finnie.org/2009/07/26/howto-encrypt-an-existing-debian-installation/)  
<http://www.finnie.org/2009/07/26/keyfile-based-luks-encryption-in-debian/>

Datuak “ezabatzen” ditugunean, ez ditugu ezabatzen. Soilik datuek okupatzen zuten lekua libre bezala markatzen dugu.

`shred`<sup>18</sup> Fitxategiak, partizioak eta disko gogorrak bizpahiru alditan gainidatzi, izena aldatu eta ezabatzen ditu.

`secure-delete`<sup>19</sup> Fitxategiak, RAMa, partizioak, disko gogorrak, SWAPa eta diskoko leku librea ezabatzen ditu era oso seguru batean.

---

<sup>18</sup>[https://www.gnu.org/software/coreutils/manual/html\\_node/shred-invocation.html#shred-invocation](https://www.gnu.org/software/coreutils/manual/html_node/shred-invocation.html#shred-invocation)

<sup>19</sup><http://sourceforge.net/projects/securedelete/>

Datuak “ezabatzen” ditugunean, ez ditugu ezabatzen. Soilik datuek okupatzen zuten lekua libre bezala markatzen dugu.

`shred`<sup>18</sup> Fitxategiak, partizioak eta disko gogorrak bizpahiru alditan gainidatzi, izena aldatu eta ezabatzen ditu.

`secure-delete`<sup>19</sup> Fitxategiak, RAMa, partizioak, disko gogorrak, SWAPa eta diskoko leku librea ezabatzen ditu era oso seguru batean.

---

<sup>18</sup> [https://www.gnu.org/software/coreutils/manual/html\\_node/shred-invocation.html#shred-invocation](https://www.gnu.org/software/coreutils/manual/html_node/shred-invocation.html#shred-invocation)

<sup>19</sup> <http://sourceforge.net/projects/securedelate/>

Sistema Eragile asko <sup>20</sup>daude pribatasuna eta anonimotasuna ahalbideratzen dutenak. Defektuz, beharrezko tresna guztiak dakartzate instalatutak eta ez dago beharrik sistema ordenagailuan instalatzeko.

Gure egunerokoan guri eta besteei buruzko informazio pilo ematen diegu ezagutzen ez ditugun enpresa eta gobernuei, askotan jakin gabe.

- Ez utzi zure bizitzaren informazio guztia Google Inc. enpresaren esku, alternatibak badaude:

- Bilatzailea → [DuckDuckGo](#)
- Gmail → [Riseup](#)
- Google Calendar → [N-1](#)
- Google Docs → [Riseup PAD](#)
- Google Groups → [Riseup Lists](#)
- Google Talk → [Pidgin](#)
- Google Maps → [OpenStreetMap](#)
- Blogger → [N-1](#)
- Google+ → [N-1](#)
- Picasa → [GThumb](#)
- Google Reader → [Liferea](#)
- Android → [OpenMoko](#)
- Chrome → [Firefox](#)
- Chrome OS → [Debian GNU/Linux](#)
- Youtube → [Internet Archive](#)
- Google Public DNS → [OpenNic](#)
- etab. asko → [alternatiba asko](#)

Sare “sozialak” erabiltzeko orduan:

- Ez eman beste pertsoneri buruzko informaziorik pertsona horiei galdetu gabe.
- Zuri buruzko informazioa ematean, jakin zazu ez dakizula zer egingo duten informazio horrekin.
- Sare sozial alternatiboak erabili<sup>21</sup>.

edo...

- Ez erabili sare sozialik.



Sare “sozialak” erabiltzeko orduan:

- Ez eman beste pertsoneri buruzko informaziorik pertsona horiei galdetu gabe.
- Zuri buruzko informazioa ematean, jakin zazu ez dakizula zer egingo duten informazio horrekin.
- Sare sozial alternatiboak erabili<sup>21</sup>.

edo...

- Ez erabili sare sozialik.

Sare “sozialak” erabiltzeko orduan:

- Ez eman beste pertsoneri buruzko informaziorik pertsona horiei galdetu gabe.
- Zuri buruzko informazioa ematean, jakin zazu ez dakizula zer egingo duten informazio horrekin.
- Sare sozial alternatiboak erabili<sup>21</sup>.

edo...

- Ez erabili sare sozialik.

Sare “sozialak” erabiltzeko orduan:

- Ez eman beste pertsoneri buruzko informaziorik pertsona horiei galdetu gabe.
- Zuri buruzko informazioa ematean, jakin zazu ez dakizula zer egingo duten informazio horrekin.
- Sare sozial alternatiboak erabili<sup>21</sup>.

edo...

- Ez erabili sare sozialik.

- Adblock Plus
- BetterPrivacy
- HTTPS Everywhere
- BrowserMasquerade
- TrackMeNot
- BeeFree
- VPNbat erabiliRiseup VPN
- Proxyak erabili<sup>22</sup>

Kontaktua [kontaktua@gisa-elkartea.org](mailto:kontaktua@gisa-elkartea.org) edo  
[unai@gisa-elkartea.org](mailto:unai@gisa-elkartea.org).

Aurkezpena <http://www.gisa-elkartea.org/komunitatea/dokumentazioa/aurkezpenak/seguraholkuak/view>

Informazio gehio <https://ssd.eff.org/> eta  
<https://help.riseup.net/es/security>

## Galderarik?

(etorkizunean galderak edukiz gero kontaktu epostara bidali beldurrik gabe)