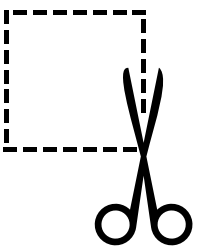
Lleva las cartas MicroSD donde quieras

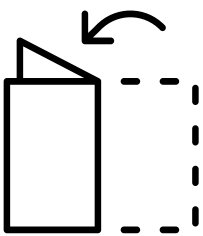
visita: https://www.derechosdigitales.org/microsd

Imprime

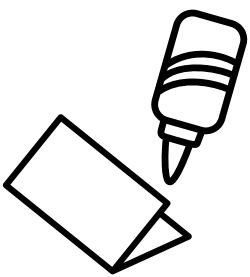
corta



dobla



pega



@ DERECHOS DIGITALES
América Latina

RIESGOS

1

Pérdida de acceso a una cuenta

Es como salir y dejar las llaves dentro de la casa: no sabes cómo, pero un día no pudiste volver a entrar a tu cuenta de correo electrónico o a alguna de tus redes sociales. Puede que hayas olvidado la contraseña o peor, que alguien la haya cambiado sin tu consentimiento (lo que equivaldría a quedarte afuera de tu casa y con un ladrón adentro). Muchas plataformas ofrecen maneras de recuperar tu cuenta asociándola, por ejemplo, a un número de teléfono. La creación de contraseñas fuertes con ayuda de un administrador de contraseñas y la habilitación de la verificación de dos pasos pueden ser buenas medidas preventivas para mitigar el riesgo. De igual forma, una contraseña de inicio ayudará en caso de pérdida del equipo.

busca las cartas con los números
2 • 3 • 4 • 7 • 12 • 14 • 15 • 16 • 29
y construye nuevas relaciones

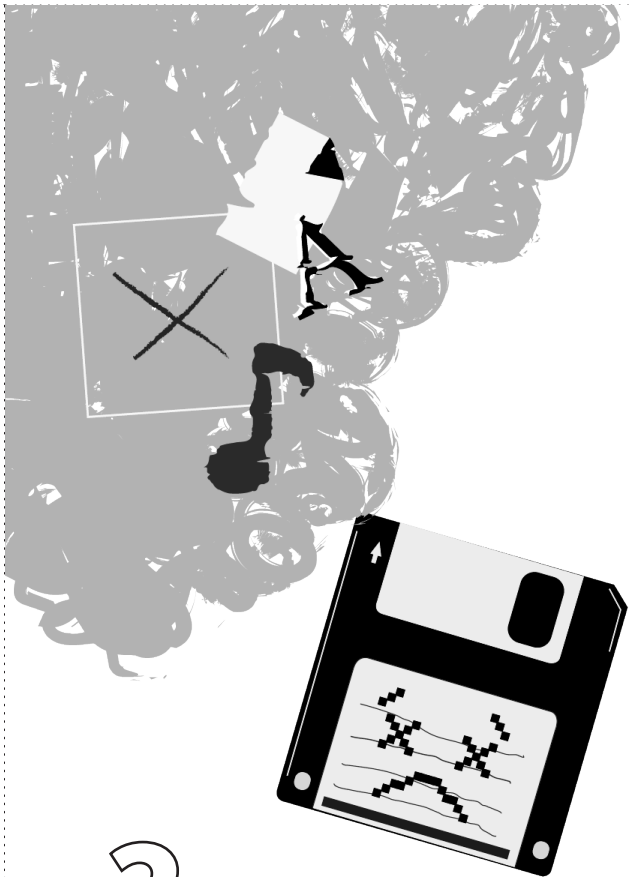
1

RIESGOS

Pérdida de información

Piensa en toda la información importante almacenada en tus dispositivos electrónicos: textos que estás trabajando, archivos de audio, transcripciones de entrevistas, fotografías, documentos escaneados, pantallazos de información eliminada de la web. Toda esta información podría desaparecer porque alguien así lo quiere o, simplemente, porque tu dispositivo se ha estropeado: una mañana tu computador no arranca; tu teléfono celular cae al sanitario o tu disco duro externo ha perdido el formato y es imposible acceder a la información que contiene. Estas cosas pasan. Ningún **hardware** o **software** está exento de sufrir una falla.

busca las cartas con los números
3 · 4 · 6 · 11 · 14 · 15 · 16 · 19 · 20 · 24 · 32
y construye nuevas relaciones



RIESGOS

3

Pérdida del equipo

A veces pasa. Te descuidaste y tu teléfono cayó de tu bolsillo. O te robaron la mochila, con el computador adentro. O quizás no perdiste físicamente tu dispositivo, pero sin darte cuenta terminó en el agua y ya no enciende. Lo grave: perderás también acceso a las fotos, documentos, audios y demás datos allí alojados. Y si es por robo o alguien más lo encuentra, esa persona podría tener acceso a toda tu información ahí almacenada.

busca las cartas con los números
4 • 6 • 11 • 15 • 19 • 24 • 32
y construye nuevas relaciones

3

RIESGOS

RIESGOS

4

Acceso no autorizado a información

¿Qué pasaría si tus equipos caen en manos de quien no quisieras? Alentados por la curiosidad, miembros de tu familia, tus amigos o tu pareja podrían intentar revisar tus dispositivos. Probablemente esta violación de tu privacidad conlleve un mal rato. Pero, ¿qué pasa si una investigación que estás haciendo le interesa a alguien con la capacidad de acceder, por la fuerza o empleando herramientas técnicas sofisticadas, a tu información? Existen algunas precauciones que puedes tomar, como no descuidar tu equipo, proteger el dispositivo con una contraseña y respaldar tu información importante para evitar la pérdida de contenidos.

busca las cartas con los números
1 • 3 • 6 • 9 • 10 • 11 • 14 • 15 • 16 • 18 • 19 • 20
y construye nuevas relaciones

4

RIESGOS

RIESGOS

5

Sobreexposición de información personal

A través de las redes sociales puedes compartir tu trabajo, comunicarte, contactar gente, opinar y debatir sobre cualquier tema. Por eso es la forma más sencilla de que te encuentren. Esto puede ser bueno o malo, dependiendo de quién te busque. ¿Tienes control sobre la información disponible que existe sobre ti? Cada foto, comentario o contacto revela algo sobre quién eres, qué lugares frecuentas, qué haces, cuáles son tus fortalezas y debilidades. Tu "yo digital" es una versión de ti que entre más se parezca a tu "yo físico", más vulnerable te hace.

busca las cartas con los números
3 · 6 · 10 · 18 · 21 · 23 · 34
y construye nuevas relaciones

5

RIESGOS

RIESGOS

6

Exponer a tus fuentes

Como periodista eres una cara visible y puedes ser la vía de acceso a tus fuentes, potencialmente poniéndolas en riesgo. Cualquier comunicación entre ustedes, por internet o por teléfono, dejará un rastro. Si no has tomado las precauciones necesarias para proteger su identidad, podría ser sencillo llegar a ti y a ella: a través de sus cuentas de redes sociales, correo electrónico o número de teléfono. Incluso llevar sus teléfonos cuando se reúnan podría convertirse en evidencia del encuentro. Recuerda: es tu responsabilidad proteger a quienes contribuyen con tu trabajo.

busca las cartas con los números
2 • 3 • 4 • 5 • 9 • 10 • 19 • 26 • 27 • 31 • 32 • 33
y construye nuevas relaciones

6

RIESGOS

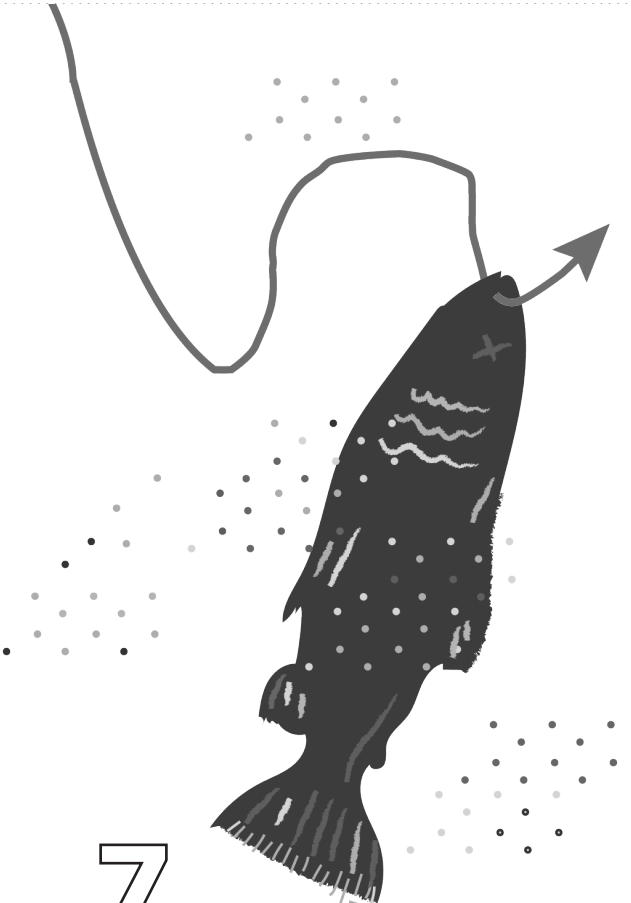
ATAQUES

7

Phishing

Significa literalmente “pescar” y el pez gordo es tu información secreta, como tu contraseña o el número de tu tarjeta de crédito. El pescador intentará engañarte haciéndose pasar por una persona, una empresa o una institución en la cual confías. El anzuelo puede ser tan sencillo como un correo electrónico o el enlace a un sitio web que luce idéntico al de un servicio legítimo, como el de tu banco o la página de acceso a tu cuenta de correo. Para no morder el anzuelo, procura chequear siempre las URLs de los enlaces.

busca las cartas con los números
1 • 2 • 4 • 6 • 8 • 9 • 14 • 17 • 21 • 23 • 38
y construye nuevas relaciones



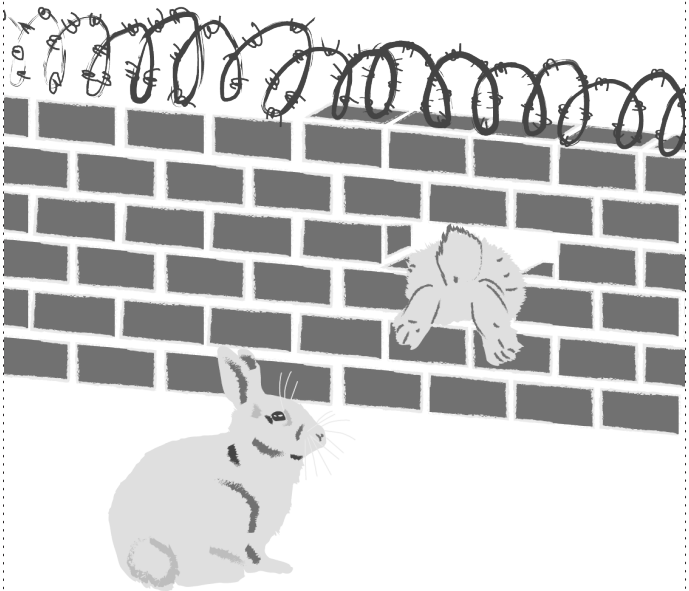
7

ATAQUES

Explotación de vulnerabilidades del software

No hay software perfecto, por eso es importante mantenerlo actualizado. Todos los programas tienen fallas, errores, “agujeros” por donde se puede filtrar información. Cuando alguien en la comunidad técnica identifica estas fallas, informa a quienes han desarrollado el programa para que las corrijan. Pero alguien puede utilizarlas para tener acceso a información protegida, modificar el comportamiento de distintos programas o de los sistemas operativos en su conjunto. Las fallas de seguridad que no son públicamente conocidas son llamadas vulnerabilidades 0-day o “día cero”.

busca las cartas con los números
2 • 4 • 9 • 17 • 22 • 25 • 32 • 36 • 38
y construye nuevas relaciones



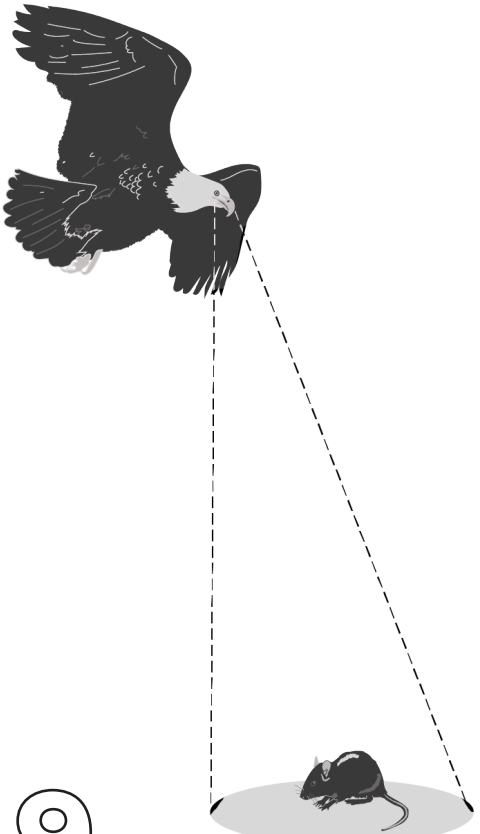
ATAQUES

9

Spyware

Es un programa diseñado para espiar tus actividades, conversaciones y archivos, sin que tú lo notes. Los hay de varios tipos y capacidades, dependiendo del costo: algunos pueden hacer seguimiento a tu historial de navegación o a la frecuencia con que utilizas las diferentes aplicaciones. Otros pueden activar tu micrófono, tu cámara o geolocalizar tu dispositivo. Si manejas información sensible y tienes enemigos poderosos, debes tener mucho cuidado. Algunas precauciones que puedes tomar son chequear las URLs de los enlaces que te envíen, mantener las actualizaciones al día y tener precaución con los adjuntos en los correos electrónicos.

busca las cartas con los números
2 • 4 • 6 • 7 • 8 • 9 • 17 • 19 • 22 • 25 • 26 • 31 • 38
y construye nuevas relaciones



9

ATAQUES

ATAQUES

10

Doxxing

Toda la información que pasa por internet queda registrada en alguna parte y es susceptible de ser encontrada. Solo se requieren algunas habilidades técnicas y el suficiente empeño para lograrlo. Doxxing es un término derivado de la palabra “docs” (documentos) y consiste en exponer en línea información personal y sensible que permita identificar a una persona, por ejemplo a ti o a tus fuentes. Esta información puede ser compilada desde bases de datos abiertas al público, cuentas de redes sociales e incluso mediante algunas formas de ingeniería social, induciendo a alguien a revelar información sensible. Algunas medidas de precaución son configurar correctamente la privacidad de tus cuentas y conocer a tu “yo digital”.

busca las cartas con los números

4 • 5 • 10 • 11 • 13 • 14 • 16 • 21 • 23 • 26 • 34 • 35 • 37 • 38

y construye nuevas relaciones

10

ATAQUES

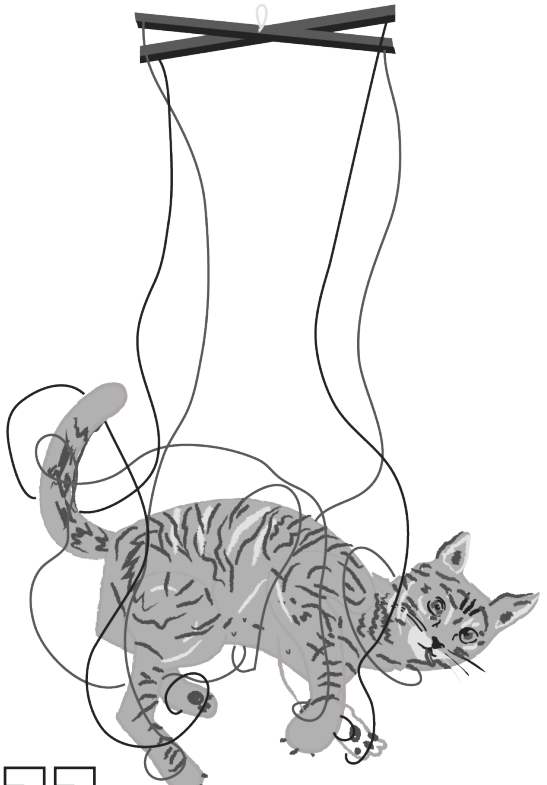
ATAQUES

11

Chantaje

¿Están tus datos personales fácilmente disponibles en internet? ¿Acaso has compartido fotografías eróticas con alguien en el pasado, sin tomar precauciones sobre cómo y dónde quedan registradas? ¿En algún lugar de internet hay información sobre ti que no debería conocerse públicamente? Si alguien con malas intenciones y ciertas capacidades técnicas accede a esa información, puede obligarte a realizar acciones contra tu voluntad, bajo la condición de no revelarla. Eso es un chantaje. Y aunque no es recomendable ceder ante estas amenazas, procura tomar medidas antes que tu información en internet pueda volverse en tu contra. Algunas medidas de precaución son configurar correctamente la privacidad de tus cuentas y conocer a tu "yo digital".

busca las cartas con los números
2 • 3 • 4 • 5 • 7 • 10 • 11 • 13 • 21 • 23 • 26 • 38
y construye nuevas relaciones



11

ATAQUES

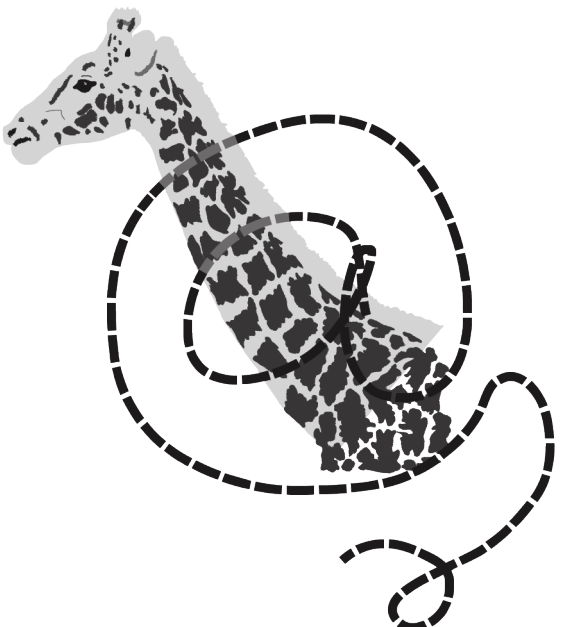
ATAQUES

12

Acoso en línea

No importa que hayas dicho “No, gracias”. Que pidas o exijas respeto de la contraparte o que denuncies. Quien acosa busca provocar daño a través de insultos, amenazas, difamación, rumores, comentarios de índole sexual -especialmente a las mujeres y personas LGBTQI-, divulgación de información personal, robo de identidad o la compilación de información con intenciones de amenazar o avergonzar. El acoso no debe ser normalizado. Y aunque es necesario exigir a las plataformas digitales que se hagan cargo y a las autoridades que te protejan, siempre tienes la posibilidad de restringir el acceso a tu información personal y sensible.

busca las cartas con los números
1 • 5 • 10 • 11 • 13 • 18 • 21 • 23 • 38
y construye nuevas relaciones



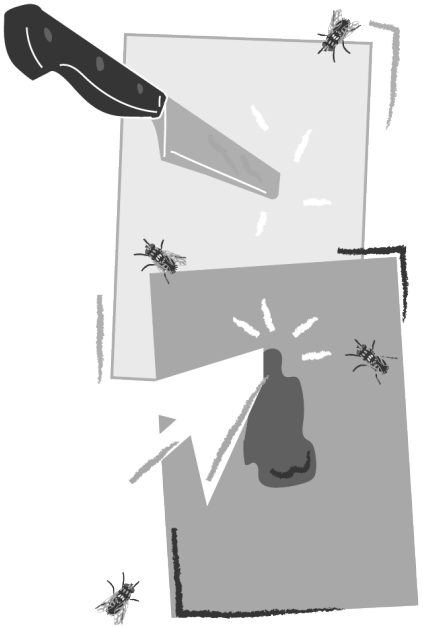
12

ATAQUES

Amenazas

Hay quienes piensan que las amenazas, si ocurren en entornos digitales, son menos graves. Nada más lejos de la realidad, pues el problema central no es cuánto tiempo tardarán en llevarse a cabo, sino los efectos emocionales y físicos que la amenaza misma tiene sobre tu integridad. La amenaza es un delito y puedes exigir a la justicia una respuesta efectiva de protección si alguien te está amenazando. Y aunque no depende de ti el hecho de sufrir este tipo de ataque, puedes realizar algunas acciones preventivas en el manejo de tu información e identidad en plataformas y entornos digitales.

busca las cartas con los números
10 • 11 • 12 • 18 • 21 • 23 • 38
y construye nuevas relaciones

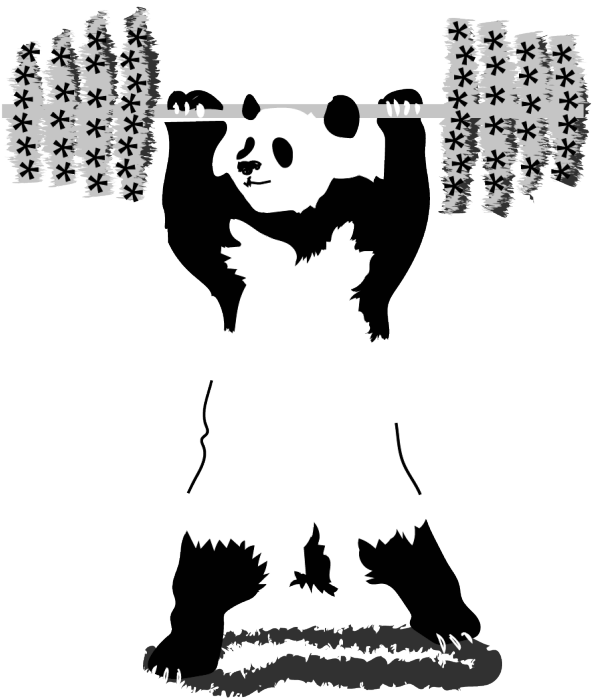


BUENAS PRÁCTICAS 14

Contraseñas fuertes. Siempre

El propósito de una contraseña es evitar que otros entren. Qué tan fácil o difícil será acceder a tu información dependerá de tu contraseña; no importa que se trate de tus cuentas de redes sociales, correo, cuenta bancaria, dispositivos electrónicos o un documento en concreto. Hay tres reglas principales que debe cumplir cualquier contraseña: ser única, fuerte y larga. ¿Cómo? No tiene que ser una palabra o una fecha, menos el nombre de alguien importante; mejor una frase, utilizando algunos símbolos y números entre palabras. Como recordar contraseñas no siempre es fácil, una buena alternativa es utilizar un administrador de contraseñas.

busca las cartas con los números
4 • 6 • 16 • 29 • 32 • 33
y construye nuevas relaciones



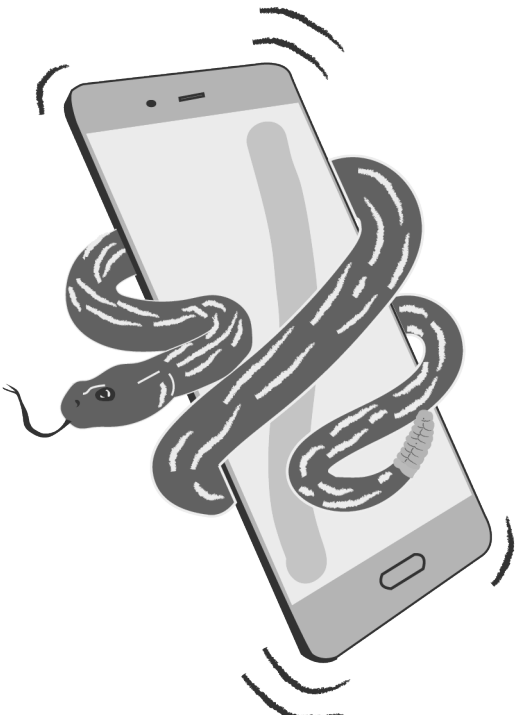
14 BUENAS PRÁCTICAS

BUENAS PRÁCTICAS 15

Protege tus dispositivos con una contraseña de inicio

Establecer una contraseña de inicio de sesión es una forma sencilla de hacer más difícil que otras personas accedan a los datos contenidos en tus dispositivos cuando los dejas solos o en caso de robo. Teléfonos celulares, tablets y computadores admiten esta función, utilízala.

busca las cartas con los números
4 • 6 • 14 • 18 • 19 • 23 • 26
y construye nuevas relaciones



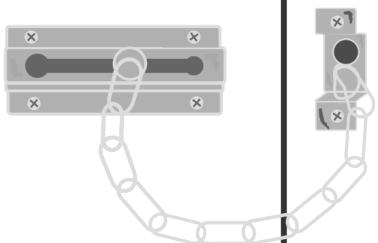
15 BUENAS PRÁCTICAS

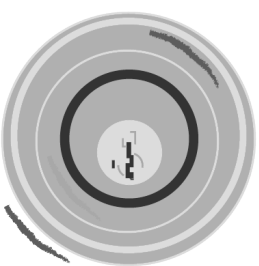
BUENAS PRÁCTICAS 16

Verificación de dos pasos

La verificación de dos pasos agrega una capa de seguridad a tus cuentas de correo electrónico, redes sociales y otros servicios en línea. El principio es simple: en vez de una contraseña, necesitas dos, una que conoces y otra que se genera en alguna herramienta a la que tengas acceso físico (como tu teléfono). Si tu primera contraseña es vulnerada, el acceso sigue protegido por la segunda. Las formas más comunes de conseguir la segunda contraseña es a través de un SMS, un llamado telefónico o una aplicación instalada en tu teléfono. Esto significa que la empresa que provee el servicio liga tu número de teléfono con tu cuenta (y pierdes anonimato). También existen dispositivos USB que cumplen la misma función pero ayudan a tu anonimato.

busca las cartas con los números
4 • 6 • 14 • 18 • 23 • 26
y construye nuevas relaciones





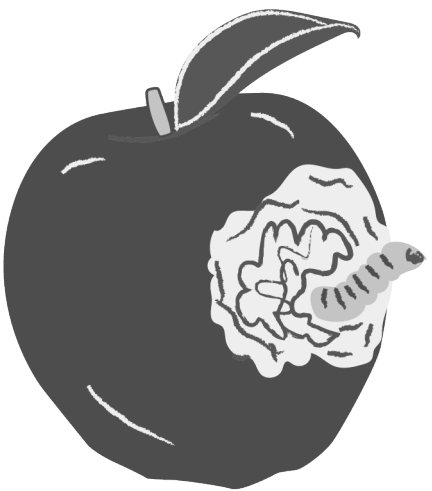
16 BUENAS PRÁCTICAS

BUENAS PRÁCTICAS 17

Desconfía de cualquier adjunto en correos electrónicos

La forma más común de infectar un dispositivo es a través de archivos adjuntos en correos electrónicos. Como regla general, no los abras, especialmente si provienen de remitentes desconocidos o en los que no confías plenamente. De ser estrictamente necesario hacerlo: 1) Confirma antes con el remitente (pues falsear una cuenta de e-mail es sencillo); 2) Puedes subir el archivo a una plataforma como Google Drive y revisarlo desde ahí (esta opción no es recomendable si la información es potencialmente confidencial o altamente sensible); 3) Puedes iniciar una sesión con el navegador Tails para evitar comprometer tu equipo.

busca las cartas con los números
4 • 7 • 8 • 9
y construye nuevas relaciones



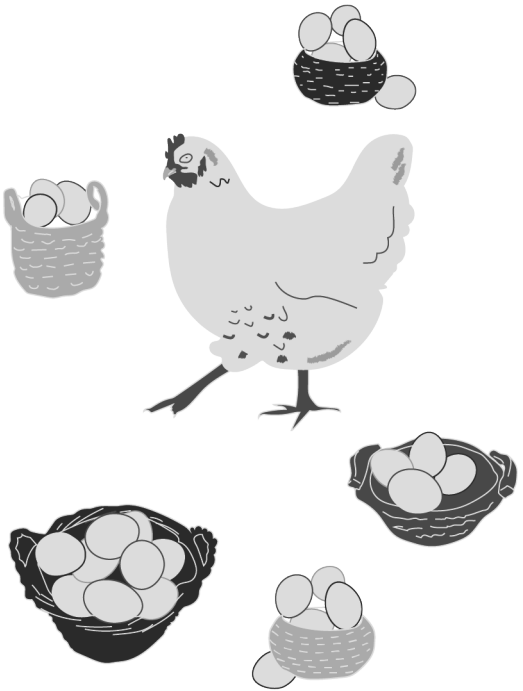
17 BUENAS PRÁCTICAS

BUENAS PRÁCTICAS 18

Compartimenta tu información

¡No pongas todos los huevos en la misma canasta! Distintos tipos de información requieren de precauciones diferentes. Usa distintas cuentas de correo electrónico, navegadores web y aplicaciones de mensajería, dependiendo del nivel de resguardo que requiera la información. Mantén distintas cuentas de correo electrónico para propósitos diferentes (trabajo, personal, spam, etc.) y no las mezcles. Usa distintas aplicaciones de mensajería, dependiendo del nivel de seguridad que requieran las conversaciones y distintos navegadores dependiendo de lo que estés haciendo.

busca las cartas con los números
2 • 5 • 6 • 10 • 20 • 26 • 32
y construye nuevas relaciones



18 BUENAS PRÁCTICAS

BUENAS PRÁCTICAS 19

No descuides tu dispositivo

Si estás trabajando en una historia que podría ser perjudicial para gente capaz de allanar tu casa u oficina, o simplemente robar tus dispositivos, entonces lo más sencillo es trabajar en una máquina portátil que siempre puedas llevar contigo y nunca despegarte de ella. Adicionalmente puede ser necesario que protejas el inicio de sesión con una contraseña, cifres el disco duro y guardes un respaldo de tu trabajo siempre en un lugar seguro.

busca las cartas con los números
2 • 3 • 4 • 6 • 9 • 15 • 20 • 24
y construye nuevas relaciones

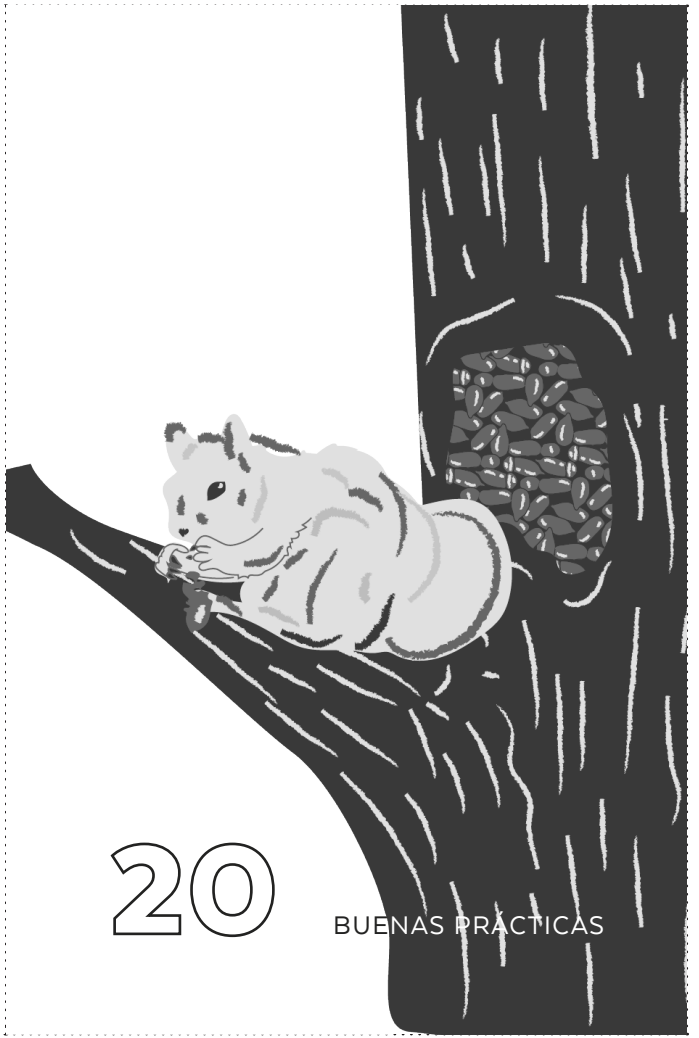
19 BUENAS PRÁCTICAS

BUENAS PRÁCTICAS 20

Respalda tu información periódicamente

Piensa en la historia más importante en la que has trabajado en tu carrera. ¿Qué hubiese ocurrido si la información que habías recopilado desapareciera? Cuando estás trabajando en un computador, esa es una posibilidad real: los computadores a veces fallan. Y cuando esa historia es perjudicial para alguien, cabe preguntarse si esa persona tiene la motivación y los medios para robar, incautar o incluso infectar tu computador con spyware. Por eso es importante realizar respaldos constantes de tu trabajo, puede ser en un disco duro externo, en varias memorias USB, en un servidor compartido, pero de tu entera confianza. En cualquiera de los casos, siempre será preferible que la información esté, además, cifrada.

busca las cartas con los números
2 • 18 • 19 • 24 • 32
y construye nuevas relaciones



20 BUENAS PRÁCTICAS

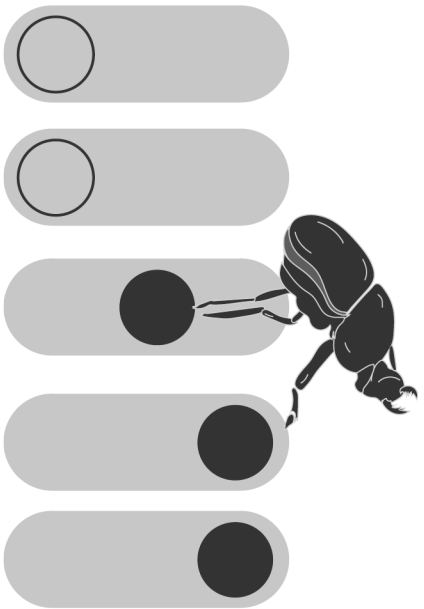
BUENAS PRÁCTICAS

21

¡Configura tu privacidad!

Es posible saber mucho sobre ti a partir de la información que publicas en tus redes sociales. De caer en las manos equivocadas, esta información podría volverte vulnerable a ti y a tu red cercana de contactos. Una forma de resguardarte es cuidar a quién das acceso a tu "vida en línea", ajustando la configuración de privacidad de tus cuentas.
La mayoría de las redes sociales te permiten elegir si quieres compartir tus publicaciones con todo el mundo o solamente con tus seguidores.
Una buena configuración de privacidad y un desarrollado sentido de la responsabilidad para publicar en internet es fundamental para mantenerte segura o seguro.

busca las cartas con los números
5 • 6 • 10 • 11 • 12 • 23
y construye nuevas relaciones



21

BUENAS PRÁCTICAS

BUENAS PRÁCTICAS 22

Mantén tus actualizaciones al día

Todos los programas y las aplicaciones que utilizamos tienen fallas que las hacen vulnerables y, en consecuencia, te vuelven vulnerable a ti también. Estas fallas pueden ser aprovechadas para acceder y ganar control sobre tus dispositivos. Es por ello que cada vez que una de estas fallas es detectada, los programadores lanzan una actualización que soluciona el problema. Mantener las actualizaciones al día es una forma sencilla de minimizar riesgos.

busca las cartas con los números
8 • 9 • 38
y construye nuevas relaciones

22 BUENAS PRÁCTICAS

BUENAS PRÁCTICAS 23

Conoce a tu “yo” digital

¿Cuánta información sobre ti existe en internet? Todo lo que haces en línea deja un rastro, toda la información que publicas puede revelar algún detalle sobre ti y tu red de contactos. Es como un rompecabezas: solo se necesita juntar piezas para tener la imagen completa. Si quieres establecer una estrategia de seguridad, el primer paso es contar las piezas. Abre una sesión en el modo incógnito del navegador y búscate. ¿Cuánta información hay sobre ti? ¿Te sientes cómoda con esa información? ¿Cuánta de esa información podrías remover si te lo propusieras? Cualquier momento es bueno para comenzar.

busca las cartas con los números
5 • 6 • 10 • 11 • 12
y construye nuevas relaciones

23 BUENAS PRÁCTICAS

BUENAS PRÁCTICAS 24

Cifra todo lo que puedas cifrar

Imagina que guardas tu información importante en una caja que se cierra con candado. Una vez cerrada, la caja cambia de forma, parece un animal. Al tocar el candado e ingresar la clave -que por supuesto, solo tú conoces- el candado se abrirá, tu caja recuperará su forma y la información que guardaste seguirá allí. Para que ocurra esta ilusión de la caja al animal, se requiere un protocolo de cifrado. Con este protocolo puedes cifrar un dispositivo, un mensaje de chat o correo, un archivo que enviarás adjunto o el acceso a una aplicación. Y, sin duda, tendrás una capa de seguridad extra en toda tu información digital.

busca las cartas con los números
4 • 6 • 14 • 18 • 19 • 29 • 31 • 32 • 33 • 36 • 37
y construye nuevas relaciones

24 BUENAS PRÁCTICAS

BUENAS PRÁCTICAS 25

Procura utilizar solo conexiones Wi-Fi de confianza

Mientras puedas, evita conectarte a redes públicas o desconocidas, pues podrías estar corriendo varios riesgos. En una red abierta, cualquiera con los conocimientos necesarios podría revisar todos los datos que transfieras en sitios web no protegidos por **HTTPS**, incluyendo tus contraseñas o el número de tu tarjeta de crédito. Además, podrían insertar malware en tus dispositivos. Si es absolutamente necesario utilizar una red Wi-Fi desconocida, mejor si lo haces utilizando una *VPN*.

busca las cartas con los números
9 · 22 · 24 · 30 · 38
y construye nuevas relaciones

25 BUENAS PRÁCTICAS

BUENAS PRÁCTICAS 26

Desconecta la información más sensible

Cuando estás trabajando en una historia importante, manejando datos de alta confidencialidad, y crees que alguien podría intentar interferir con tus dispositivos, es recomendable trabajar en un equipo que nunca esté conectado a internet. Con esto aseguras que no sea infectado a través de phishing, archivos adjuntos o vulnerabilidades de software; y si llegara a infectarse a través de un dispositivo USB, tampoco hay manera de extraer o eliminar información a distancia.

busca las cartas con los números
4 • 7 • 8 • 9 • 18 • 24 • 32 • 36
y construye nuevas relaciones

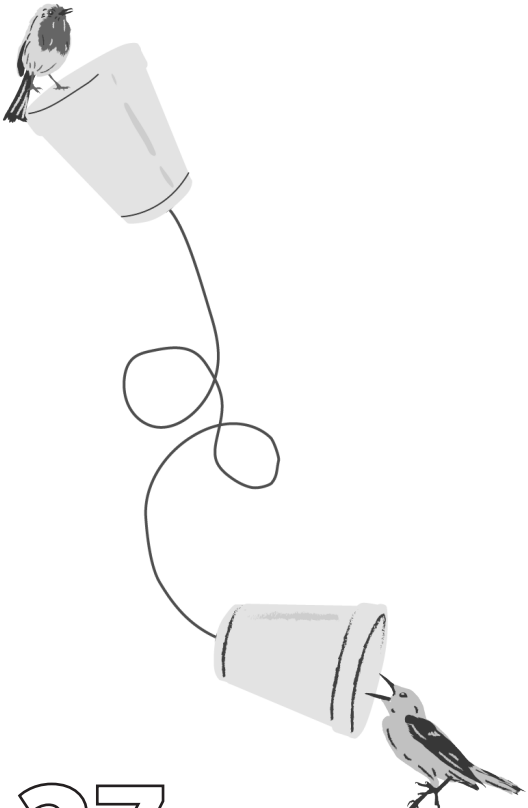
26 BUENAS PRÁCTICAS

BUENAS PRÁCTICAS 27

Comunícate de manera segura con tu fuente

Para tomar decisiones al respecto, pregúntate: ¿corre algún riesgo tu fuente?, ¿necesita protección? Si su identidad fuera revelada, ¿podría pasarle algo?, ¿alguien podría sentirse amenazado por lo que tu fuente sabe? Y ese alguien, ¿cuánto poder tiene? Aunque no hay soluciones completas y ninguna decisión de seguridad digital puede asegurarte que se elimine el riesgo, a veces es mejor no dejar registros de la comunicación entre ustedes. Quizás la mejor forma de hacerlo es acordar un encuentro en persona, aunque en ocasiones eso puede ser todavía más riesgoso. No tomes estas decisiones apresuradamente.

busca las cartas con los números
6 • 23 • 26 • 27 • 31 • 33 • 36
y construye nuevas relaciones



27 BUENAS PRÁCTICAS

MUY BUENA PRÁCTICA 28

Busca apoyo

En caso de que algo malo ocurra siempre es bueno buscar apoyo, tanto emocional, como profesional y legal. Situaciones como las descritas pueden ser sumamente estresantes y no hay necesidad de sufrir en soledad y por tu cuenta. ¿Sabes dónde puedes acudir si sufres, o crees que sufres, un ataque digital? De acuerdo al tipo de ataque busca apoyo:

emocional

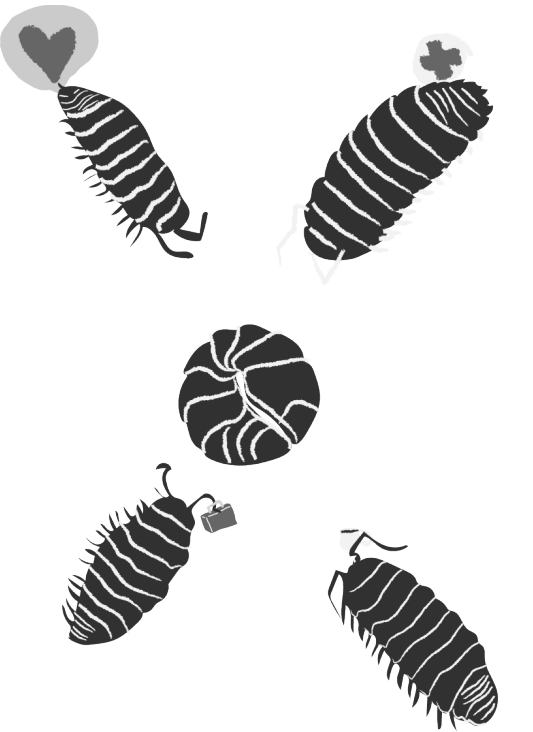
11 9 10 12 13

técnico

7 8

legal

11 13



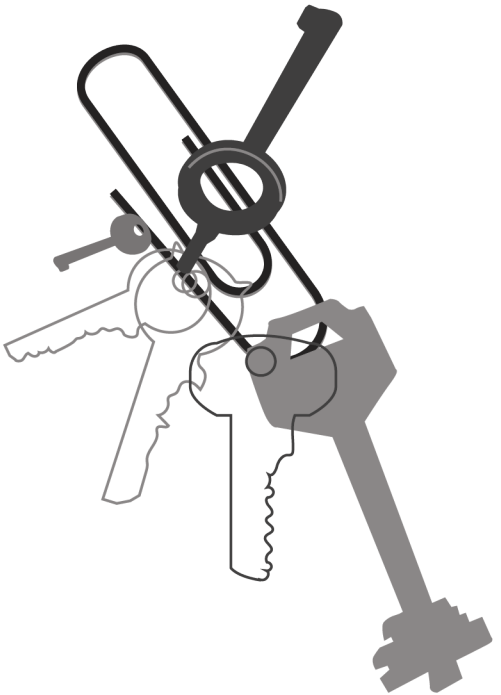
28 MUY BUENA PRÁCTICA

HERRAMIENTAS 29

Administrador de contraseñas

Si te cuesta trabajo recordar todas las contraseñas que usas, no eres la única persona a la que le pasa. Es algo tan común que existen programas donde es posible almacenar grandes cantidades de contraseñas de forma cifrada. Así, solo debes recordar una contraseña maestra con la cual tienes acceso a todas las demás. Estos gestores son muy útiles porque te permiten crear contraseñas fuertes, largas y diferentes para cada uno de los servicios que utilizas, sin necesidad de tener que recordarlas.

busca las cartas con los números
4 • 14 • 16 • 24 • 33
y construye nuevas relaciones



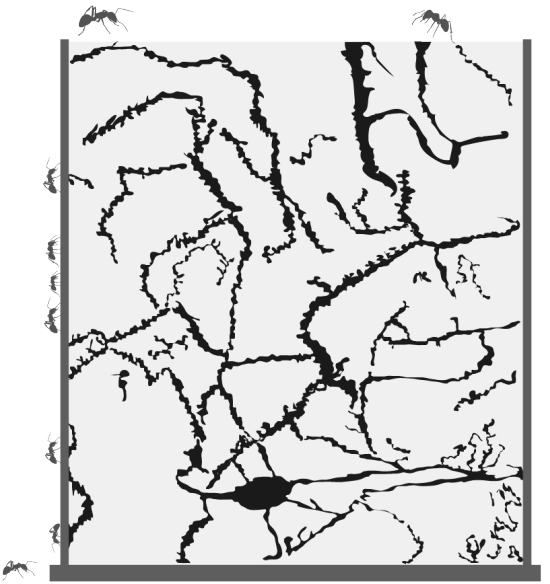
29 HERRAMIENTAS

HERRAMIENTAS 30

Red de navegación privada: VPN

Cada vez que visitas un sitio web, tu número IP (que identifica tu dispositivo de forma unívoca) queda registrado, en los servidores de la empresa que te provee el servicio de internet y en los del sitio que estás visitando. En medio de tu conexión puede haber interferencias maliciosas que buscan rastrear tu actividad o bloquear el tráfico de ciertos contenidos. Las **VPN** (Red Privada Virtual) funcionan como tubos de transporte privado de tus datos. La información va cifrada hasta una IP específica, desde donde se hacen las solicitudes a la red. Utilizando VPN proteges tus datos en redes públicas o compartidas, y puedes evitar bloqueos geográficos de contenido, por ejemplo en países donde hay censura de sitios web.

busca las cartas con los números
24 · 25 · 25 · 36
y construye nuevas relaciones

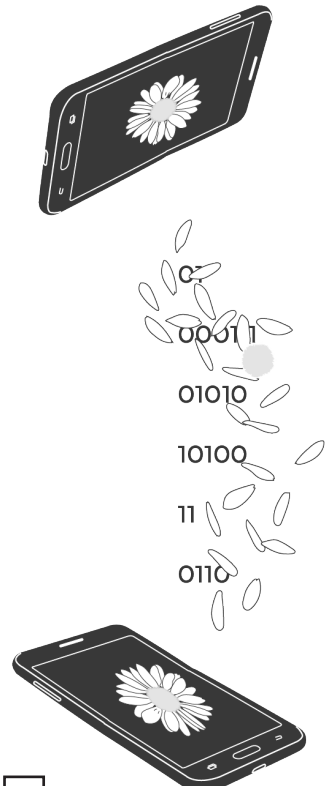


30 HERRAMIENTAS

Cifrado de extremo a extremo

Funciona para correos electrónicos o mensajes de chat y consiste en que el contenido de un mensaje está protegido por una llave que identifica a cada una de las personas involucradas en una comunicación. Así, para cualquier ente externo (por ejemplo la empresa que te presta el servicio de internet, la plataforma de correo o chat que utilizas, o algún intruso), la comunicación aparecerá como un código sin sentido. Debes tener en cuenta que el **cifrado** es para el contenido, no necesariamente para los datos de la comunicación (remitente y destinatario, hora de envío, **IP**, entre otros), información que también podría hacerte vulnerable. Para más información revisa *correo electrónico cifrado*.

busca las cartas con los números
4 · 6 · 24 · 33 · 36 · 38
y construye nuevas relaciones



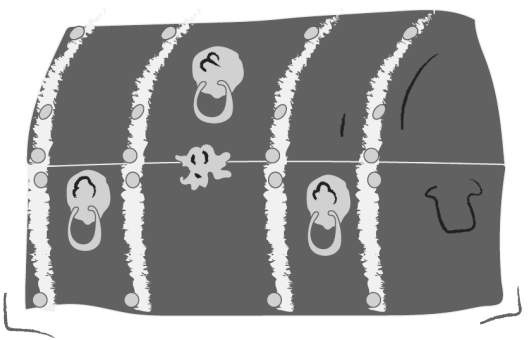
31 HERRAMIENTAS

HERRAMIENTAS 32

Almacenamiento cifrado de archivos

El almacenamiento cifrado de archivos permite proteger con una contraseña documentos y carpetas, con información delicada, alojados en tu computador o dispositivos USB, haciéndolos inaccesibles para terceros en caso de pérdida, robo o cualquier otra forma de acceso sin tu consentimiento. Para más información revisa *cifrado de archivos y carpetas*.

busca las cartas con los números
4 • 18 • 20 • 24 • 27 • 37
y construye nuevas relaciones



32 HERRAMIENTAS

Pretty Good Privacy: PGP y GnuPG

PGP, y su versión libre GnuPG, es un protocolo que permite cifrar los correos electrónicos de extremo a extremo. Cuando envías un correo, este se almacena sin cifrar en tu servidor de correos y el del destinatario. Si alguien más accede a cualquiera de las dos cuentas - mediante un ataque o con una orden judicial - podrá acceder al contenido de todos los correos recibidos o enviados. Pero si el correo ha sido cifrado con *PGP* o *GnuPG*, solo quien conozca la contraseña para descifrar un mensaje y tenga la del archivo que la acompaña, a modo de llave, puede acceder a su contenido. Además, este protocolo te permite verificar mediante firmas digitales la identidad del remitente, evitando así la suplantación. Revisa *correo electrónico cifrado*.

busca las cartas con los números
6 • 31 • 36 • 37
y construye nuevas relaciones

igN4sMQB+kQyOGbpz1RHJbFzDPtb+noi/-
DKN/+k1t5jWs7KjLXwv/CQCeasX-
VlRHM5gZgp2NDK3hrV5/Wrf8zKOd7jG+sFlPY21
BHMvQ6S7sNjDyQSpUDlRqPeWK6hlaHwgEioEn
UPVM8es8GaG1FZqSil7NVgp5i/B6BcrbpAG7EN3
17xHAcN9dtnBOteh5xeQ6 tDhfCFQ
D4Wq5ONb0pUE8x2g8S OPGW
7aZFKAfQC/GZz454dCG iPjGY
HM58GmpZj0ZM5XvsIZ UcNTZ
lGu1OM48LTivgXXhFdx qyERu
nPsaZVPU7Czl/j/208 NiDhNW
GXisPl0QOxggqKM ZNy+iei15AlYoE+9
4YbPohkFW4EC MwrE aMTdWyUmEGZnO
vnbRs7D00K xpe5HTbD/gQzucfhguNj808
8KFQbs9h n3fBwmTA+JkZZIjS/oFw92hCV
Qm1w qKqsiS1bFCFBO3RMQnkkGdpr8Eu
8TGY +PhUk0waXPw3ywgHpmfhQyG+m4
5BD8qKNmeHe70vgG0LWki4YQRw0lzgFQHTKGy
I5NjHZL3rwTQUNMs89IYWxmvUAURPG37k01VT
Nx4oQXjVLH34kGJEFSaQ9dle4SnZE4lWVlocDiuG
F9PKVt1dJY5geQvMigN4sMQB+kQZynuK1MxOz
dFHqZ2Id2aQVIEUtt0vmRYiWCLRNBDLCdReDpk
xkGqmkOPKcVfswoG8E7tHIRf4mVVrSakHPYKH0
8l4UWBF2YUEBWh1mfraTdVobadeRBxCAyOGbp
z1RHJbFzDPtb+noi/DKN/+k1t5jWs7KjLXwv/CQC
easXVlRHM5gZgp2NDK3hrV5/Wrf8zKOd7jG+sFl
PY21BHMvQ6S7sNjDyQSpUDlRqPeWK6hlaHwgE

HERRAMIENTAS 34

Extensiones de privacidad para el navegador

Los navegadores web más utilizados permiten instalar complementos (extensiones, plugins o add-ons) que agregan nuevas funcionalidades. Algunos de ellos pueden ayudarte a manejar mejor tu privacidad, impidiendo que los sitios web te rastreen a través de las cookies, bloqueando la publicidad o forzando el HTTPS. Consulta *complementos para el navegador* para obtener algunas recomendaciones, y si no entiendes qué son las **cookies** o el **HTTPS** revisa nuestro glosario.

busca las cartas con los números
5 • 23 • 35
y construye nuevas relaciones

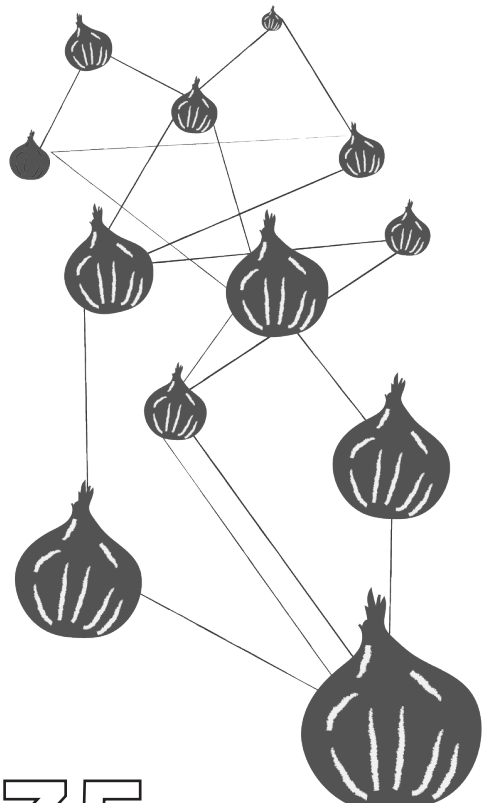
34 HERRAMIENTAS

HERRAMIENTAS 35

Navegación anónima

Tu **número IP** identifica tu computador de forma unívoca. ¿Quieres ocultarlo? Puedes utilizar herramientas como *VPN* o routers que funcionan con el **sistema Onion**. Una de las formas más confiables es *Tor*, **software** que genera una red de comunicación anónima, a través de la búsqueda aleatoria de servidores desde donde salen tus solicitudes de conexión. Una de sus aplicaciones más utilizadas es el *Tor Browser*, una versión modificada de Firefox que permite navegar anónimamente y con algunas precauciones adicionales de seguridad.

busca las cartas con los números
5 • 23 • 30 • 36
y construye nuevas relaciones



35 HERRAMIENTAS

HERRAMIENTAS 36

Sistema operativo amnésico: Tails

Tails es un sistema operativo que no guarda ningún dato en nuestro computador y que cifra todas nuestras conexiones a internet. Es útil para quienes quieran navegar de forma anónima, revisar archivos de procedencia dudosa en forma segura y quienes necesiten no dejar rastros del uso en el computador. Se ejecuta desde una USB y arrancará en cualquier computador.

busca las cartas con los números
24 • 27
y construye nuevas relaciones

36 HERRAMIENTAS

HERRAMIENTAS 37

Compartir archivos de forma segura

Tanto en el trato con fuentes como en la colaboración con colegas, a veces tendremos que compartir archivos y documentos de forma segura. Existen algunas herramientas que nos pueden ayudar, por ejemplo, para compartir archivos de forma efímera o quizás anónima, dependiendo de tus necesidad. Revisa *compartir archivos de forma segura* para más información.

busca las cartas con los números
7 • 9 • 32 • 33 • 35 • 36
y construye nuevas relaciones

37 HERRAMIENTAS

??

38

In-comodín: el cracker mala onda

También conocido como atacante o adversario, este personaje puede presentar muy diversas características. Se trata de alguien con destacables habilidades para burlar la seguridad de tu información, no importa que lo haga a través de agresiones o ingeniería social, no importa que lo logre gracias a un accidente, un descuido o como producto de su delicado trabajo informático.
El problema es que accede a tu información con la intención de perjudicarte a ti o a tus fuentes. En el trabajo periodístico, debes protegerte de dos perfiles especialmente peligrosos: quienes trabajan para alguien que quiere lastimarte y quienes quieren agredirte en razón de tu identidad de género.