Consejos de seguridad digital para

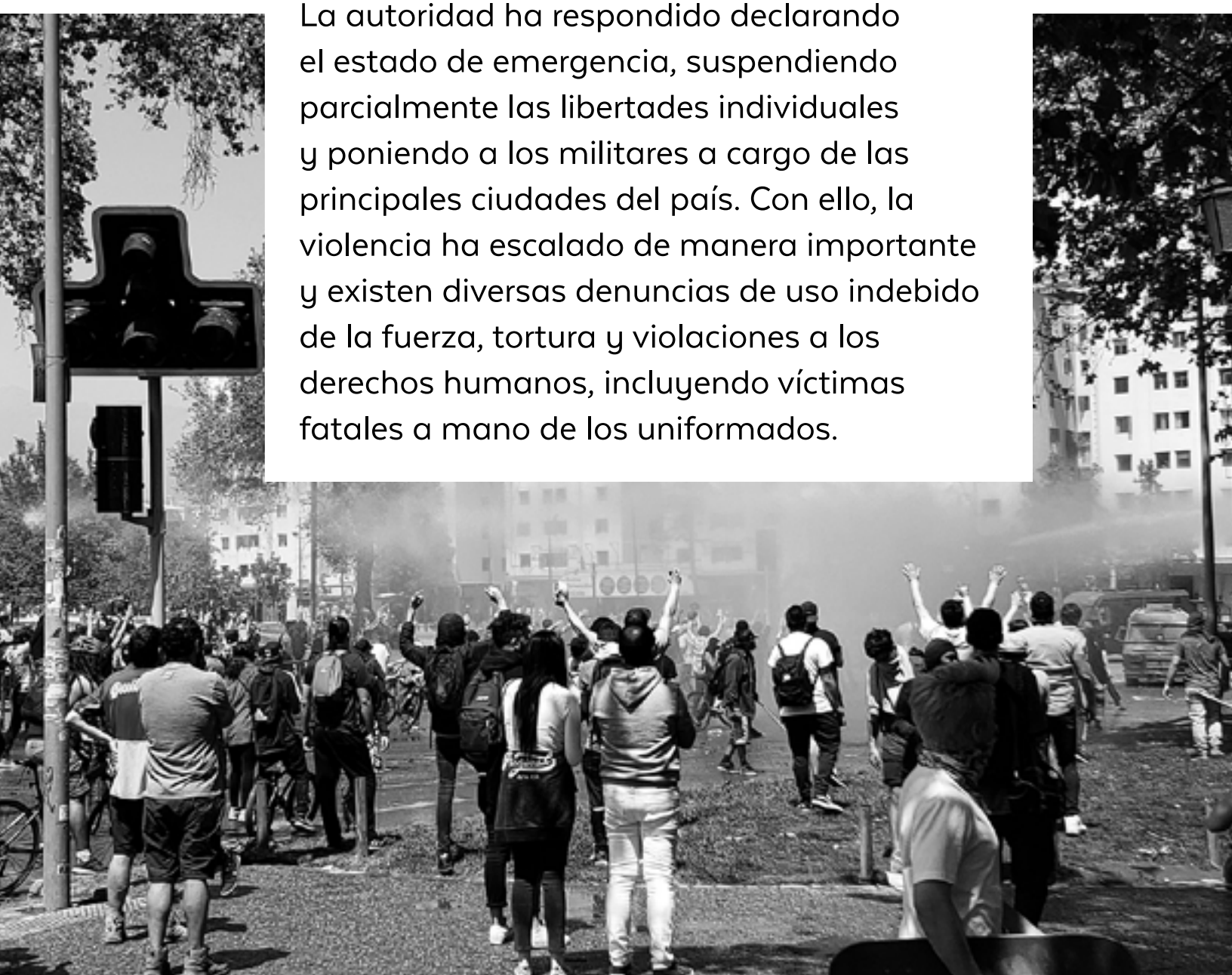
Medios de comunicación independientes

Primera versión, octubre 2019. Santiago de Chile.

DERECHOS DIGITALES
América Latina

Desde la semana pasada, Chile ha vivido intensas jornadas de protesta social que tienen su origen en una deficiente distribución de la riqueza generada en el país y que ha llevado a millones de personas a manifestarse de distintas maneras.

La autoridad ha respondido declarando el estado de emergencia, suspendiendo parcialmente las libertades individuales y poniendo a los militares a cargo de las principales ciudades del país. Con ello, la violencia ha escalado de manera importante y existen diversas denuncias de uso indebido de la fuerza, tortura y violaciones a los derechos humanos, incluyendo víctimas fatales a mano de los uniformados.



En una situación violencia estatal, desconcierto, incertidumbre y protesta, organizaciones sociales, medios de comunicación alternativa y personas naturales se han volcado a internet para denunciar los abusos y organizar la protesta. El uso de plataformas web como Twitter, Instagram y Facebook se han vuelto algunas de las principales maneras de comunicar y documentar lo que está ocurriendo en el país.

La información que se está compilando y compartiendo por medio de estas redes, así como las comunidades que se construyen en torno a ellas son muy valiosas. Y, por lo mismo, es necesario resguardarles debidamente.

Por ello, nunca está de más tomar algunos resguardos extras para proteger tus cuentas y el contenido que albergan:

1. Protege las credenciales de acceso a tus cuentas

a) Correo electrónico:
Muchas veces usamos la misma dirección de correo electrónico y la misma contraseña para todas nuestras cuentas. En el caso del correo electrónico, al perder el control del e-mail, podemos perder acceso a las plataformas que están a él ligadas. Este riesgo se incrementa cuando son múltiples personas las que acceden a la cuenta, como puede ser en un colectivo, una colectiva, un medio alternativo o una organización social.

Ejemplo estrategia de cuentas de altísimo riesgo, pero que muchas veces usamos.

Descripción: *Todos los integrantes del equipo tienen acceso a la cuenta de correo a la que están vinculadas las cuentas de redes sociales y además se realiza la comunicación con personas externas. Además, para todas las cuentas usan la misma contraseña hace años y todos conocen esa contraseña.*

Una forma de proteger mejor nuestras cuentas es utilizando una dirección de correo electrónico especialmente dedicado para cada red social. Así, en caso de cualquier tipo de intrusión, es posible acotar el daño.

b) Contraseñas:
La primera llave de acceso a nuestras cuentas, son nuestras contraseñas.

- Contraseñas largas y diversas
Te recomendamos hacer tus contraseñas muy largas, para que sean más difíciles de vulnerar por mecanismos automatizados. Una manera sencilla de construir contraseñas largas es utilizando una frase que puedas recordar

fácilmente, por ejemplo: “EsaMañanaLaMarraquetaEstaMasCrujiente”

Una variación de esta técnica, es juntar aleatoriamente palabras y generar una frase sin sentido, por ejemplo: “AutoVacaAmarilloPastoEstomagoCandente”. Esta frase es mucho más difícil de vulnerar, pero también más complicada de recordar. Puedes anotarla en un lugar secreto y ojalá irlas cambiando cada cierto tiempo.

Ejemplo básico de compartimentación para cuentas de comunicación externa.

Descripción: *Sólo una parte del equipo tiene acceso al correo y la contraseña del correo que usan para comunicarse desde la colectiva. Para las cuentas de redes sociales, se genera un correo electrónico distinto, solo quienes manejan las redes tienen acceso a esta info. Los correos se aseguran con verificación de dos pasos. Todas las cuentas usan contraseñas distintas.*

- Pro tip: Usa un gestor de contraseñas confiable

Una manera de generar y almacenar distintas contraseñas y tan largas como sea posible, es utilizar un gestor de contraseñas, un software que permite almacenar y gestionar todas nuestras contraseñas, protegiéndolas con una sola contraseña maestra. Así, es posible proteger cada cuenta con una contraseña extremadamente larga, impronunciable e irrecordable, como por ejemplo 3ja8ciG2BbTp&VoaM.zi&We94r,AsygsuLmm;TCTmdzC%36HR64p&.

Algunos gestores de contraseñas que recomendamos son:

- KeePassXC https://keepassxc.org/
- Lastpass https://www.lastpass.com/es/
- 1Password https://1password.com/es/

Los últimos dos gestores permiten crear bóvedas compartidas, lo que quiere decir que si 3 personas manejan una cuenta en una red social, pueden compartir la contraseña sin siquiera conocerla.

En general, adoptar este tipo de herramientas tiene cierta complejidad y requiere un tiempo para acostumbrarse, así que les recomendamos que las adopten paulatinamente.

c) Verificación de dos pasos:
La verificación de dos pasos es una medida de seguridad que dota a tu cuenta de una capa extra de protección, protegiendo tu cuenta con una segunda clave que es requerida cuando, por ejemplo, se está intentando acceder a la cuenta desde una locación nueva o poco frecuente o desde un dispositivo distinto del habitual. Usualmente funciona ligando la cuenta a un teléfono celular, aunque existen otras opciones.

En general, es sumamente útil para corroborar la identidad de la persona que está intentando acceder a la cuenta en circunstancias poco usuales. Si la activas, solicitando el envío de la nueva clave a través de un mensaje de voz o un mensaje de texto, puede haber un riesgo en caso de que pierdes tu celular o si sales del país y no tienes acceso a la red de telefonía.

- Verificación de dos pasos en Instagram https://www.facebook.com/help/instagram/566810106808145?helpref=related
- Verificación de dos pasos en Facebook https://www.facebook.com/help/148233965247823
- Verificación de dos pasos en Twitter https://help.twitter.com/es/managing-your-account/two-factor-authentication
- Verificación de dos pasos en Google/Gmail https://www.google.com/landing/2step/

2.- Protege tu contenido

a. ¿Tu contenido ha sido reportado, marcado como sensible o dado de baja?
Nos han llegado algunas preguntas por casos en los cuales cierto contenido publicado en redes sociales podría detonar algún tipo de alerta de moderación, lo que podría implicar que el contenido es marcado como sensible o retirado, limitando su alcance.

Los motivos no siempre son claros, así como tampoco el mecanismo que detonó la alerta de moderación, que puede ser automatizada - el sistema detecta contenido potencialmente infractor y levanta la alerta sin mediación humana- o producto de un reporte realizado por otro usuario o usuaria de la plataforma.

Junto con ello, es posible que el contenido que hayas publicado entre en conflicto con los términos de servicio de la plataforma. Un ejemplo de ello es el contenido que presenta violencia gráfica. Evidentemente, en un contexto de protesta y violencia social como el que estamos viviendo, no es inusual que la documentación del uso excesivo de la fuerza policial o militar adquiera una forma particularmente explícita y delicada, lo que en ningún caso resta su valor, sino al contrario.

Junto con ello, desde Facebook e Instagram se nos ha explicado que las amenazas, los llamados a quemar edificios o que incitan al saqueo también están prohibidos. Evidentemente, esto implica poder determinar con cierto nivel de certeza que se trata de expresiones literales y no metafóricos, simbólicos o -incluso- humorísticos. Por lo que la posibilidad de cometer errores en la moderación es alta.

b. Apelación por bajada de contenido y moderación de cuentas.
De cualquier modo, en situaciones como esta es posible apelar para que los incidentes puedan ser revisados con mayor detención por funcionarios de las plataformas, que tienen la misión de ponderar la manera en que las normativas son aplicadas.

Usualmente, las plataformas piden realizar una exposición del caso. Hazlo en términos claros y sencillos, con una explicación breve del incidente, el tipo de contenidos que usualmente publicas en tus cuentas, una descripción del contenido que fue marcado y porqué este es relevante (por ejemplo, por tratarse de un registro de violaciones a los derechos humanos). También

puedes agregar el número de seguidores de tu comunidad y las variaciones en el alcance que ha tenido tu contenido.

Además es buena idea mantener un registro de los incidentes. Para ello, guarda pantallazos de las notificaciones que te lleguen y una copia del contenido original. Guarda todo con hora y fecha. Además, si es que tuvieses pruebas de que hay esfuerzos organizados para reportar o atacar tu cuenta, guarda esa información también. Del mismo modo, si es que has sufrido ataques o amenazas en tus cuentas, esa información puede eventualmente ser valiosa a la hora de apelar.

c. Revisa las normativas de las plataformas
Es útil para tener una idea de por qué el contenido pudo haber sido dado de baja y cómo argumentar para su restauración. Puedes encontrar las normativas acá:

- Twitter: https://help.twitter.com/es/rules-and-policies/twitter-rules
- Facebook: https://www.facebook.com/communitystandards/
- Instagram: https://www.facebook.com/help/instagram/477434105621119/?helpref=hc_fnav

Respecto a los procedimientos de apelación, puedes encontrar más información acá:

- Twitter: https://help.twitter.com/forms/general?subtopic=suspended
- Facebook: https://ltam.newsroom.fb.com/news/2018/04/publicando-mas-detalles-sobre-nuestras-normas-comunitarias-y-expandiendo-la-funcion-de-apelacion/
- Instagram: https://www.facebook.com/help/instagram/366993040048856?helpref=related

3.- Protege la identidad de tus fuentes y la de las personas que participan en las manifestaciones.

Cuando se trate de un registro potencialmente delicado, que vas a distribuir de manera pública, toma en cuenta la información delicada que puedes compartir. Si una persona es identificable en una fotografía de alguna manifestación, esto puede ponerla en riesgo. Si alguien accede a los metadatos de las fotos que compartes, pueden identificarte. El anonimato nos protege, por eso te recomendamos usar:

- ObscuraCam (https://play.google.com/store/apps/details?id=org.witness.sscphase1) para difuminar los rostros de las personas que aparezcan en tus fotografías.
- Scrambled Exif (https://play.google.com/store/apps/details?id=com.jarsilio.android.scrambledeggsif) para eliminar los metadatos de tus fotografías.

Para respaldar la información pública y contribuir a la memoria colectiva te recomendamos sumar tus registros a iniciativas que apuestan por la información libre y abierta, como los esfuerzos que realiza WikimediaCL. Puedes contribuir a este esfuerzo creando una cuenta y subiendo tus registros aquí: https://commons.wikimedia.org/w/?title=Special:UploadWizard&categories=2019_Santiago_protests

DERECHOS DIGITALES
América Latina

¿Tienes más preguntas?
Revisa nuestra **guía de preguntas frecuentes**