CEPAZ
Centro de Justicia y Paz

CONSTRUCCIÓN DEL PLAN DE SEGURIDAD DEL ACTIVISTA CIUDADANO

La construcción de un plan de seguridad para activistas ciudadanos abarca la **auto-evaluación** y **rastreo de riesgos personales**, **construcción de hábitos-revés**, el **análisis de amenazas** y la **reacción ante incidentes** de seguridad.

Autora: Gloria Salazar

Palabras clave:
Empoderamiento ciudadano - activismo colectivo - seguridad digital, matriz de riesgos.

JUNIO 2018

Imágenes: freepik.com

EVALUACIÓN DE RIESGOS,
VULNERABILIDADES Y CAPACIDADES

DEL ACTIVISTA CIUDADANO

RIESGOS	VULNERABILIDADES	CAPACIDADES EXISTENTES	CAPACIDADES REQUERIDAS
Estigmatización (enemigo, apátrida, agente del poder estadounidense)	Pocos espacios comunicativos para contrarrestar efecto	Aliados en comunidad de defensores de DDHH u otros sectores influyentes	Mayor conocimiento específico sobre calumnias y difamación/ Documentación de los casos
Interferencias al libre tránsito en aeropuerto	Podrían presentarse acusaciones falsas	Conocimiento de la legislación	Memorizar el teléfono del abogado/a en caso de que me quiten el teléfono móvil
Detención / arresto / encarcelamiento	Leyes antagónicas/ Podrían presentarse acusaciones falsas	Alto perfil/ Conocimiento de la legislación/ Un abogado al tanto y listo para actuar/ No hay material comprometedor en mi domicilio ni en la oficina (?)	Memorizar el teléfono del abogado/a en caso de que me quiten el teléfono móvil
Agresión física	Andar solo	Teléfono móvil con crédito, teléfonos de emergencia a la mano	Marcado rápido. Comunicarme con mi colega dos veces al día si estoy fuera para confirmar que estoy seguro/a

MATRIZ PARA EL ANÁLISIS DE RIESGO

EVALÚA LA PROBABILIDAD Y EL IMPACTO DEL RIESGO

IMPACTO	PROBABILIDAD 5 MUY ALTO	4 ALTO	3 MEDIO	2 BAJO	1 MUY BAJO
5 MUY ALTO			Detención / arresto / encarcelamiento		Desaparición/ muerte
4 ALTO			Interferencias al libre tránsito en aeropuerto		
3 MEDIO		Estigmatización (traidor a la patria, imperialista, terrorista, golpista, derecha)	Hackeo de redes sociales / Intervención de correo electrónico		
2 BAJO					
1 MUY BAJO					

PLAN DE SEGURIDAD PERSONAL

MUY ALTO IMPACTO

Riesgo de Detención / arresto / encarcelamiento

PROBABILIDAD DE QUE OCURRA

Moderadamente posible. Las amenazas contra la disidencia cada vez son más asociadas a detenciones arbitrarias. Los activistas de derechos humanos en Venezuela han sido incluidos en el grupo de disidentes a ser investigados por "patriotas cooperantes".

IMPACTO SI OCURRE

Alto impacto. Algunos de los presos políticos llevan más de un año detenidos, las condiciones de dichos centros no son aptas para la reclusión, incidiendo rápidamente en la salud de los privados de libertad.

VULNERABILIDADES

- Leyes antagónicas a la libertad de expresión (Ley Contra el discurso de odio, Ley Antiterrorismo) Podrían presentarse acusaciones falsas.
- Aumento de la criminalización de la crítica.

HÁBITO - REVÉS

- Conocimiento de la legislación.
- Un abogado al tanto y listo para actuar.
- No hay material comprometedor en mi domicilio ni en la oficina. (?)
- Tener una agenda de contactos de organizaciones de derechos humanos.

PLAN DE ACCIÓN

1. Si eres arrestado, de ser posible, solicita a un colega o familiar que te acompañe.
2. Contacta a una organización de DDHH y/o a un abogado/a que esté presto(a) para actuar en caso de emergencias de este tipo.
3. Solicita a quienes te están deteniendo que te indiquen la razón precisa de la acción. Pregunta a dónde te trasladan (si no lo sabes).
4. Haz valer tus derechos (por ejemplo a hacer una llamada, a que se informe a tu familia, etc.) y exige su cumplimiento.
5. Siempre lleva contigo tus medicamentos de rutina.
6. Cuenta con un contacto de seguridad que accionará para ubicarte si no te reportas a determinadas horas del día y que sabe a dónde podrías ser trasladado en el caso de que te arresten.
7. No te resistas al arresto, podrías ser agredido y acusado de nuevos cargos.
8. Si es posible llama a un contacto amigo en los medios para que publique tu detención.

PLAN DE SEGURIDAD PERSONAL

ALTO IMPACTO

Riesgo de Interferencias al libre tránsito en el aeropuerto

PROBABILIDAD DE QUE OCURRA

Moderadamente posible. Los casos de defensores y opositores detenidos en aeropuertos en Venezuela son conocidos. La obstaculización de su derecho al libre tránsito ha sido una forma de hostigamiento contra los defensores de derechos humanos recientemente.

IMPACTO SI OCURRE

De medio a alto. La finalidad principal es intimidar a los DdH, pero ha pasado que algunos de los defensores intimidados fueron también detenidos en el aeropuerto.

VULNERABILIDADES

- Podrían presentarse acusaciones falsas.

HÁBITO - REVÉS

- Conocimiento de la legislación.
- No hay material comprometedor en mi equipaje, domicilio ni en la oficina. (?)

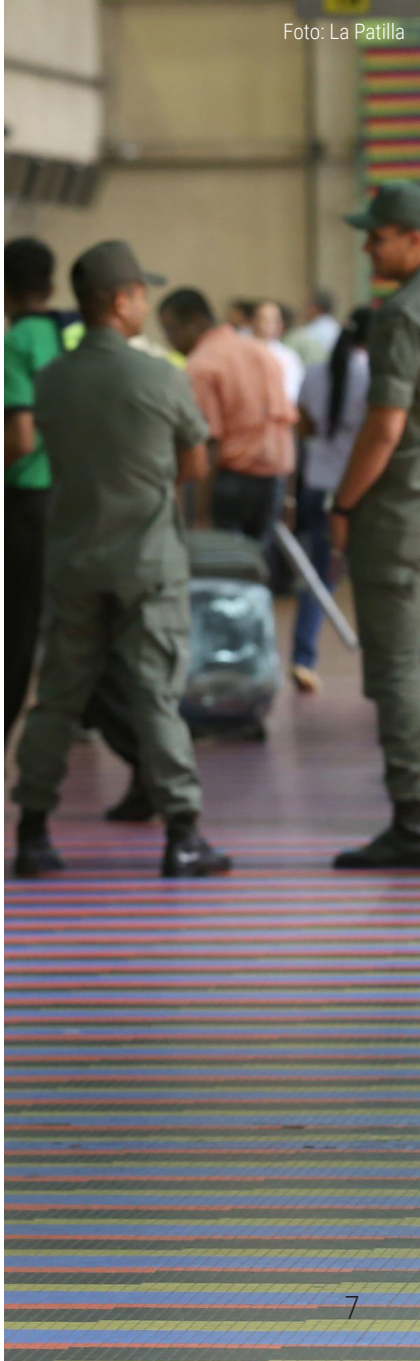
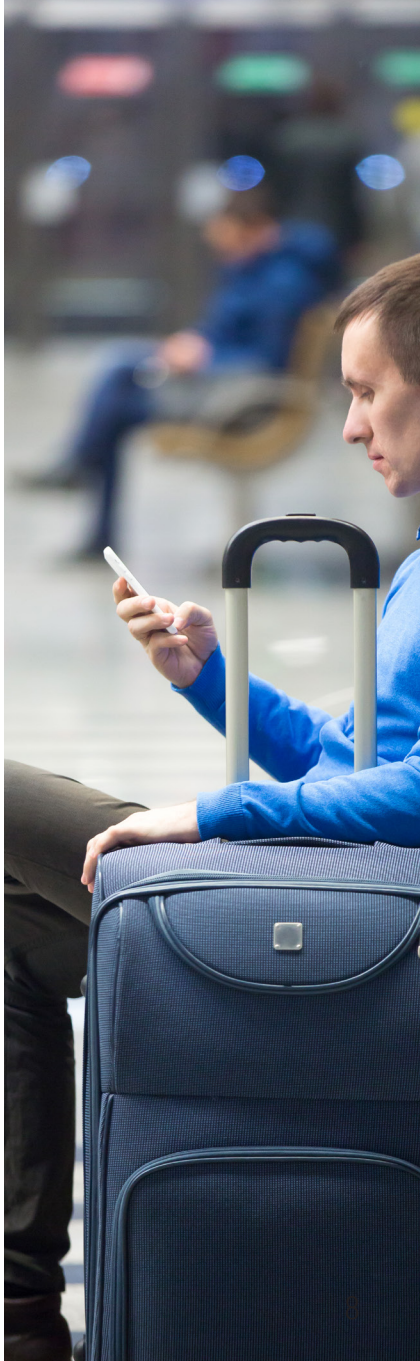


Foto: La Patilla

- Contactos de organizaciones de DDHH y abogados.
- Conoce tus derechos (por ejemplo a hacer una llamada, a que se informe a tu familia, etc.) y exige su cumplimiento.

PLAN DE ACCIÓN

1. Al viajar repórtate siempre con el chat de control o con tu contacto de seguridad, al entrar a la sección de revisión de equipajes y al salir de inmigración
2. Cuenta con un contacto de seguridad (familiar) que accionará para ubicarte si no te reportas a determinadas horas del día (defínelo previamente) y que sabe dónde podrías ser trasladado en el caso de que te arresten.
3. Haz valer tus derechos (por ejemplo a hacer una llamada, a que se informe a tu familia, etc.) y exige su cumplimiento.
4. No te resistas a las autoridades, podrías ser agredido y acusado de nuevos cargos.
5. Solicita a quienes te están reteniendo que te indiquen el motivo de la acción.
6. Si eres arrestado, de ser posible, solicita a un colega que te acompañe.
7. Asegura con antelación los servicios de un abogado/a que esté presto para actuar en caso de emergencias de este tipo.
8. Memoriza el número de teléfono de ese abogado/a, podrían quitarte tu teléfono móvil, pero tal vez tengas oportunidad de hacer una llamada.
9. Siempre lleva contigo tus medicamentos de rutina.
10. Si es posible llama a un contacto amigo en los medios de comunicación para que publique tu detención.



PLAN DE SEGURIDAD PERSONAL

IMPACTO MEDIO

Riesgo de hackeo de redes sociales y/o intervención de correo electrónico

PROBABILIDAD DE QUE OCURRA

Moderadamente posible. Los casos de defensores, activistas y figuras públicas a los que se les ha invadido la privacidad de sus correos y usurpado sus redes sociales son muchos. Con un buen manejo de las herramientas de seguridad digital las probabilidades pueden disminuir considerablemente.

IMPACTO SI OCURRE

De medio a alto. La finalidad principal es intimidar, pero también perjudicar información que puede ser reservada o sensible. En principio hay que preguntarse: ¿qué información manejo? ¿Dónde está resguardada? ¿Estoy en riesgo si alguien encuentra esa información en mis equipos? ¿Cómo publico información de manera privada?

VULNERABILIDADES

- Claves débiles.
- Abrir correos de remitentes desconocidos.
- Antivirus desactualizado.

HÁBITO - REVÉS

GUÍA BÁSICA DE SEGURIDAD DIGITAL

Manejador de contraseñas

Usar un manejador de contraseñas como **LastPass**.

LastPass es un servicio de gestión de contraseñas. En todas tus cuentas y dispositivos: utiliza contraseñas con más de 25 caracteres alfanuméricos y especiales, que incluyan mayúsculas y minúsculas.

Lastpass y su generador de contraseñas asegura que sea muy difícil invadir la seguridad de tus cuentas. Además, autocompleta los formularios con tus claves, con esto te protege de malwares o el pishing, que espían lo que tipeas en tu teclado.

El phishing es un intento malicioso de acceder a tu cuenta o recoger información personal sobre ti haciéndote ingresar los datos de inicio de sesión u otra información confidencial en un sitio web falso.

Es habitual que los estafadores ofrezcan bienes digitales gratuitos, inusuales, secretos o exclusivos (como monedas, fichas, regalos) para engañar a sus víctimas.

Para acceder a LastPass: https://www.lastpass.com/es.

En tus correos, Twitter y Facebook:

Las cuentas de correo electrónico más seguras son las de Gmail, si no tienes una, es recomendable comenzar a usarla. Puedes activar el mecanismo de seguridad de doble paso. La verificación de dos pasos se ajusta en tu configuración de seguridad de cada una de tus cuentas. Es importante configurar los teléfonos de emergencia y descargar una lista de códigos de uso único que te permitirá acceder a través de los celulares.

Antivirus actualizado

Para evitar la invasión de software maligno en tus dispositivos, puedes instalar **Avast** en tu computadora y **AGV** como aplicación para dispositivos móviles gratuitamente. Accede en el URL: www.avast.com/

Privacidad de los datos a través de VPN (Virtual Private Network)

El **VPN** es una red privada virtual que oculta cuáles son los datos que se transmiten: identifica tu dirección IP pero resguarda la información que se recibe y envía creando un túnel seguro en Internet. "María y Paula hablan pero no se ve que se dice".

Crea un túnel privado de información entre tu dispositivo y el servidor VPN, por lo que el ISP no puede ver los datos encriptados que se transmiten. En pocas palabras, te protege haciendo invisible para la vigilancia lo que estás haciendo en Internet. URL: https://goo.gl/Mhs5ET

Anonimato

A través de la dirección IP es posible identificar quién o la ubicación desde dónde se publicó una información; por lo tanto, es necesario que al colgar información en nuestra página web, lo hagamos de forma segura, escondiendo nuestra identidad.

Para esto, la mejor herramienta gratuita y fácil de usar es **TOR**, un explorador de internet con tres pasos de IP antes de hacer la solicitud a tu ISP.

Se puede descargar en https://www.torproject.org/ y utilizarlo como Chrome o Firefox, pero resguardando nuestra identidad. Además, TOR permite evadir los bloqueos de páginas web que son exclusivos a usuarios venezolanos, aplicados por ABA y otros proveedores de Internet.

Información completa para Windows en https://securityinabox.org/es/guide/torbrowser/windows/

Para garantizar estos dos niveles de protección, debes conectarte primero a un servidor VPN y, una vez establecida esa conexión, utilizar TOR browser.

Otra práctica recomendada es eliminar el historial de navegación y archivos temporales con herramientas como **CCleaner** (www.piriform.com/ccleaner) que permite borrar el rastro que se produce mientras se visitan diferentes sitios web.

PLAN DE ACCIÓN

1. Si te han vulnerado tu cuenta de correo electrónico Gmail: Intenta determinar cuál fue la vía por dónde accedieron a tu cuenta (un correo desconocido abierto, robo de un dispositivo vinculado a tus cuentas, phishing por Google Docs, aplicaciones, o si usaste una clave muy evidente como tu cédula: cámbiala de inmediato si aún tienes acceso a tu cuenta).

   Una vez determinado, corta el vínculo que une tu cuenta a estos dispositivos o aplicaciones. Para hacerlo debes ir a "*Mi Cuenta*" pulsando sobre el icono que aparece en la esquina superior derecha. Allí pulsa sobre "*Aplicaciones y sitios conectados a mi cuenta*" y desconéctalo.

2. Facebook: Hay disponible una guía en la sección "*Ayuda Rápida*" de tu perfil de **Facebook** con todos los pasos a seguir en caso de que hayan vulnerado tu clave de esta red social:
   - Ve a la página "*Recupera tu cuenta*".
   - Escribe el correo electrónico, número de teléfono celular, nombre completo o nombre de usuario asociado a tu cuenta, y haz clic en *Buscar*.
   - Sigue las instrucciones que aparecen en pantalla.

3. Instagram: Activa a tu comunidad de amigo y familiares para que denuncien el perfil si te ha sido suplantada tu identidad. Entra al servicio de ayuda de Instagram y sigue los pasos. Es importante que en tu cuenta tengas una foto

de tu rostro, porque para recuperar tu cuenta te pedirán que envíes un selfie y otra serie de datos que contrastarán para corroborar tu identidad.

4. Twitter: Si no puede abrir una sesión, debido a que el hacker ha cambiado su contraseña, puede hacer clic en "*Olvidé mi contraseña*". Al hacer clic en el enlace, se le enviará un correo electrónico con el ID de correo electrónico registrado con Twitter. Este correo electrónico contendrá instrucciones sobre cómo restablecer su contraseña.

   Si Twitter no reconoce el ID de correo electrónico que indique, debe notificar a Twitter sobre la cuenta hackeada en https://help.twitter.com/forms/hacked. En la página, se le pedirá su nombre de usuario de Twitter, el ID de correo electrónico que fue asociada con su cuenta de Twitter, si ha asociado un teléfono a la cuenta de Twitter y la fecha / hora de la última vez que ha iniciado sesión.

   Basándose en esta información, Twitter tratará de recuperar su cuenta de la información de acceso para que pueda iniciar sesión y recuperar su cuenta.

ORGANIZACIONES DE DDHH CON

ACOMPAÑAMIENTO LEGAL

Aragua

-AMNISTÍA INTERNACIONAL ARAGUA:
Teléfono: (412)033.16.12

Bolívar

-CODEHCIU
Teléfonos: (424)902.47.00)

Carabobo

-FORO PENAL CARABOBO:
Teléfono: (412)533.30.78

Caracas

-CEPAZ
Teléfonos: (0212) 310.59.14

-PROVEA: Sede Principal de Provea
Teléfonos: (0212) 860.6669 (0212) 862.1011 (0212) 862.5333

Lara

-MOVIMIENTO VINOTINTO
Teléfono: (0424) 558.11.26

Zulia

-CODHEZ
Teléfonos: (0261) 792.18.15 (0261) 325.92.34

REFERENCIAS

- Security in box. Tactical Technology Collective and Front Line. Consultado en: https://security.ngoinabox.org/es

- Seguridad Digital y privacidad digital para los defensores de Derechos Humanos. Front Line. Consultado en http://www.frontlinedefenders.org/es/digital-security

- Buenas prácticas para la distribución y publicación de información sensible en Internet. Rafael Nuñez. Consultado en http:// www.slideshare.net/espaciopublico/buenas-prcticas-para-la-distribucin-y-publicacin-de-informacin-sensible?from=ss_embed

- Guía de seguridad digital para activistas y defensores de derechos humanos.
  Consultado en: www.espaciopublico.ong