La Protección de la Información

CURSO SEMI-PRESENCIAL

Herramientas de protección integral para activistas y defensoras/es de derechos humanos

III EDICIÓN

Irene Santiago y Vincent Vallies

pbi
Brigadas Internacionales de Paz

La Protección de la Información

Curso semi-presencial: Herramientas de protección integral para activistas y defensoras/es de derechos humanos

III EDICIÓN

Publicado por:

Brigadas Internacionales de Paz (PBI)

Elaboración de la guía y equipo de formación:

Irene Santiago y Vincent Vallies

Edición:

Miriam García Torres

Diseño y maquetación:

Carolina Saiz

Colaboraciones:

La I y II edición de este curso se impulsaron de manera coordinada junto a la Fundación Mundubat, a quien reconocemos y agradecemos su trabajo.

Año: 2023

Brigadas Internacionales de Paz

Con el apoyo de:

GARAPENERAKO LANKIDETZAREN EUSKAL AGENTZIA
AGENCIA VASCA DE COOPERACIÓN PARA EL DESARROLLO

EUSKO JAURLARITZA
GOBIERNO VASCO

Preámbulo

Con este documento no pretendemos agotar todo lo relacionado con la protección de la información. Efectivamente, es un dominio complejo y en constante evolución. Lo que queremos proponer es una aproximación a la problemática, con unas ideas sobre cómo ir avanzando hacia un mejor manejo de nuestra información en lo que tiene que ver con la protección.

Podemos identificar varios riesgos principales relacionados con la información en relación con nuestra protección:

- que la información que publiquemos nos ponga en peligro (o no nos proteja).
- que tengan acceso a nuestra información (robo con fines de copiarla).
- que perdamos nuestra información (por robo, pérdida o fallo tecnológico).
- que manipulen nuestra información.

Cuando la información que publicamos nos pone en peligro

"La mayoría de los casos exitosos de enjuiciamiento de manifestantes es gracias a las propias imágenes o videos colgados por otros manifestantes" – Declaración de un policía belga.

Estamos hablando de la información que publicamos nosotras mismas en redes sociales, en nuestras webs, etc. Debemos siempre tener en mente cuando publicamos algo, cómo esta publicación podría ser un apoyo en términos de protección o, por lo menos, no hacernos daño a nosotras o a las personas con las cuales trabajamos.

Podemos hacernos varias preguntas:

- ¿Cuáles pueden ser los impactos (tanto positivos como negativos) de la publicación?
- ¿Podemos contrarrestar los impactos negativos? ¿Cómo?
- En caso de no poder contrarrestar estos impactos negativos ¿Es necesaria esta publicación? ¿Podemos tomar medidas para prepararnos ante los impactos negativos?
- ¿Cómo podemos incluir el componente de protección en nuestra publicación?

Como seguramente no tendremos la capacidad ni el tiempo de hacernos estas preguntas para cada una de las comunicaciones que hacemos, es necesario ir construyendo un protocolo de manejo de la información pública. De esta forma elaboramos criterios claros y lineamientos generales para quienes están colgando noticias en páginas webs, redes sociales, etc.

Para poder entender bien de lo que hablamos, pondremos algunos ejemplos:

En general nuestras publicaciones nos son útiles para visibilizar nuestro trabajo o para denunciar las violaciones de Derechos Humanos que están ocurriendo.

Como vemos, estas dos publicaciones denuncian, por un lado, la violación del derecho a la consulta previa, libre e informada y, por otro lado, un asesinato poniendo la responsabilidad en las Fuerzas Públicas. Las dos publicaciones son legítimas y correctas pensando en el tema de derechos humanos. Ahora bien, si nos hacemos las preguntas anteriormente propuestas, podemos pensar en que:

- Como impactos positivos esperamos que sirvan para visibilizar la situación y presionar, de una forma u otra, a las autoridades y/o victimarios.
- Como impactos negativos podemos pensar que van a enojar a las autoridades mencionadas, la empresa, los victimarios directos, etc.

- Podemos pensar que estas publicaciones son necesarias porque responden a un momento álgido (tanto del proceso con la empresa o el asesinato frente al cual, si no logramos nada, puede repetirse).
- ¿Hemos incluido algo que permita contrarrestar las consecuencias del enojo de los victimarios? ¿Hemos incluido algo que nos pudiera estar protegiendo? Diríamos que no.

¿Qué significa incluir algo para nuestra protección?

En general, a través de nuestras propias publicaciones, una de las formas para incluir el componente de protección es visibilizar el apoyo que tenemos (de otras organizaciones nacionales y/o internacionales, de instituciones, etc.), o también mostrar la fuerza del colectivo (lo que hemos ido hablando desde el inicio de este curso sobre la fuerza del colectivo frente a lo individual).

Como podemos ver en estas dos publicaciones, hay por lo menos mención explícita a otras organizaciones nacionales, internacionales e instituciones. La de la izquierda utiliza claramente los nombres de las cuentas de varias organizaciones internacionales, de la Comisión Interamericana de DDHH, de Naciones Unidas, etc. Es una forma tanto de llamar directamente la atención de quien queremos, como de mostrar públicamente que todas estas instituciones están al tanto de la denuncia y estarán pendientes. La publicación de la derecha menciona el 'acompañamiento internacional'; una mejora hubiera sido mencionar el nombre de este acompañamiento específicamente.

Evidentemente, si podemos obtener publicaciones que no fueran nuestras sino directamente de instituciones u otras organizaciones que muestran un respaldo a nuestra labor y que muestran que están pendientes de nosotras, es lo mejor. Como vemos en el tweet siguiente, el Comité de Solidaridad reutiliza una publicación de PBI que les menciona, que utiliza a su vez un tweet de la embajada de Noruega en Colombia.

En este sentido es importante que, cuando queremos visibilizar los logros que tenemos en labores de cabildeo internacional, es bueno pedirles a las personas con las cuales nos encontramos y que están dispuestas a hacer declaraciones públicas, comunicados, intervenciones en la radio o lo que fuera que sea público, que de forma explícita expresen el apoyo y la vigilancia que ejercerán en cuanto a nuestra situación de riesgo. Evidentemente, estamos hablando además de lo que digan sobre nuestras luchas.

A continuación se exponen algunos posibles impactos negativos de nuestras comunicaciones (sobre todo en redes sociales, donde hay más inmediatez y, por ende, menos control o reflexión sobre lo que se publica) que en muchas ocasiones pasan desapercibidos.

- Poner a personas en riesgo de persecución judicial. En este sentido, en ocasiones se toman fotos o videos de actos de resistencia civil legítimos pero que –desafortunadamente– pueden estar prohibidos por las leyes nacionales. Es importante en esos momentos cuidar a las personas que aparecen en estos videos o imágenes; no debemos facilitar la labor de identificación de estas personas por las autoridades. La pregunta sobre la pertinencia de la publicación en esos momentos es, por ende, importante (¿vale la pena hacer la publicación? en caso de que así sea, debemos mirar –junto con las personas que allí aparecen– cuál es la mejor forma de hacerlo).
- Un impacto que poco se piensa es que, en ocasiones, podemos estar haciendo el trabajo de los victimarios difundiendo sus amenazas. Numerosas publicaciones denuncian una amenaza e incluso cuelgan la amenaza inicial. Debemos recordar que uno de los objetivos principales de las amenazas es crear miedo, desmovilizar a la gente. ¿Difundiéndola estamos logrando mayor apoyo o estamos participando de la creación del miedo? ¿Cómo podemos comunicar sin participar de la estrategia de los victimarios? Una de las ideas es ver cómo, a pesar de la amenaza, podemos mostrar la fuerza del colectivo, los apoyos recibidos, hacer un llamamiento a que todas juntas podemos, etc. Es decir, no olvidar los mensajes positivos, mensajes que muestren que la organización o el colectivo está preparado y que puede haber consecuencias para el autor de la amenaza o las autoridades si no hacen algo.

- Como todo, en temas de protección debemos tomar en cuenta a las personas afectadas directamente. Existen casos donde la familia cercana (hija, hijo, compañera/o) de una persona defensora de derechos humanos se entera de una amenaza que incluye a la familia por un comunicado público sacado por una organización internacional (sin consultarlo con la persona implicada). Evidentemente, puede ser un caso extremo pero debemos preguntarnos antes de hacer una comunicación pública si las personas que nombramos, las personas que aparecen, los familiares de la víctima, están de acuerdo con esta estrategia de visibilización.

Acceso a nuestra información con fines criminales

No queremos que los victimarios puedan acceder a nuestra información ya que esto significaría poner en peligro nuestras estrategias –por ejemplo, se podrían preparar frente a una estrategia judicial–, podrían poner en peligro a víctimas que nos están dando sus testimonios, o podrían también, si logran tener acceso a nuestro ordenador, modificar ciertos documentos o incluir documentos para montarnos un proceso judicial posteriormente. Es necesario entender que los victimarios tienen numerosas formas para tener acceso a esta información a través de programas que pueden acceder a nuestras computadoras a través de internet, a través del correo electrónico, cuando transferimos datos, etc.

Es también importante entender que la seguridad digital puede representar un mundo complejo y que nos va a ser importante decidir qué nivel de seguridad digital queremos, frente a qué capacidad u obstáculos nos puede estar creando esta seguridad digital.

Existen varias herramientas para poder proteger y/o esconder nuestra información. Únicamente os proponemos acá herramientas de uso libre –programas abiertos– y sin coste.

Una de ellas, muy fácil de utilizar a pesar de las apariencias, es **VeraCrypt**. Es una herramienta de cifrado de archivos de software gratuito y código abierto que permite almacenar información sensible de manera segura.

Básicamente, lo que hace Veracrypt es esconder toda la información que se desea en un archivo secreto que solo se puede abrir con una contraseña fuerte. Es como una caja fuerte, pero una caja fuerte escondida dentro de una pared. Cuando se requiera trabajar con o sobre la información confidencial, se tendrá que ir a la caja fuerte para abrirla, tomar los documentos y una vez modificados, cerrar la caja fuerte.

Os proponemos en este módulo la lectura de unas fichas realizadas para un caso específico.

Evidentemente, como organización se debe tener una reflexión previa sobre qué información necesitamos proteger y qué información no necesita este nivel de protección.

> ***OJO:*** *Si se pierde la contraseña, es totalmente imposible tener acceso a la caja fuerte. En este caso se correrá el riesgo de perder toda la información (ver el punto sobre contraseñas, o el punto sobre pérdida de la información).*

Siguiendo con el tema de **las contraseñas**, la mayoría de las veces las personas utilizamos una contraseña –la misma– para todas nuestras cuentas (correo, redes sociales, banco, etc.). Evidentemente, es una muy mala idea, partiendo del hecho de que hay sitios que van a proteger menos nuestras contraseñas y si un victimario logra tener acceso a ella, tendrá acceso a todos nuestros correos, por ejemplo. Lo ideal es tener contraseñas distintas para cada cuenta o red social, y que todas sean contraseñas fuertes.

Aquí os dejamos dos sitios para comprobar la fuerza de nuestras contraseñas: ***https://password.kaspersky.com/es/ y https://www.security.org/how-secure-is-my-password/***

Para tener una contraseña fuerte, lo mejor es que sea lo más larga posible, modificar letras de una palabra por números o símbolos, etc.

Evidentemente, tener 20 contraseñas distintas y fuertes y recordarlas sin apuntarlas en una hoja en el cajón de nuestra oficina, o en un archivo llamado 'contraseñas' es muy difícil. Por eso existen programas de almacenamiento de nuestras contraseñas –que además nos ayudan a definir buenas contraseñas–. Es como un armario donde estarían todas nuestras contraseñas, y este armario a su vez está cerrado con una contraseña, que llamamos la contraseña madre, la única que debemos recordar. El programa que os proponemos se llama **Keepass**.

Os inlcuimos también un manual para su instalación y uso.

> ***OJO:*** *Si se olvida la contraseña madre o si se daña el ordenador donde están almacenadas las contraseñas, se puede perder el acceso a todas las demás contraseñas. Por ello, es importante tener una copia de la base de datos de las contraseñas y estar seguras de cómo recordar la contraseña madre.*

Ahora bien, en muchas ocasiones, lo que hemos podido ver en cuanto a ataques contra la información de las organizaciones de derechos humanos, es la interceptación de los correos

electrónicos. Por lo tanto, una buena estrategia es la encriptación de los correos electrónicos. Para ello se puede utilizar el **programa libre GPG4win**. GPG es un sistema de encriptación que utiliza lo que se llama dos llaves, una llave pública y una llave privada. De forma simplificada, la llave pública es como un candado que se abre solamente con la llave privada. Lo que se debe hacer es compartir con todos los contactos que deseemos nuestro candado –la llave pública–, y cuando nos escriban activamos dicho candado. Y así solo con nuestra llave privada podemos abrir este correo.

Os incluimos en el módulo una pequeña ficha, así como el link al manual completo de GPG4win (en inglés): ***https://files.gpg4win.org/doc/gpg4win-compendium-en.pdf***

Por otro lado, muchas de las amenazas ocurren cuando estamos conectadas/os a internet. Para protegernos podemos tomar en cuenta varias pautas:

- En caso de trabajar sobre casos muy confidenciales o de alto perfil que serán de alta vigilancia por parte de posibles victimarios, podemos decidir trabajar estos casos en una computadora que no tenga acceso a internet.
- Debemos asegurar tener las herramientas que nos protejan como:
  - Un programa contra los *malware* (programas que permiten a los victimarios espiarnos). Existen varios programas contra ello, como ClamAv (*https://www.clamav.net*) o Malwarebytes (*https://es.malwarebytes.com*)
  - Un cortafuego que funciona como un vigilante a la puerta de nuestra casa y que decide quién puede entrar y salir. En general, viene de fábrica con Windows o Mac. Si no, se puede también instalar uno propio; por ejemplo, el "Comodo Firewall".
  - Asegurar tener instalado el *plugin* HTTPS en nuestros exploradores de internet. La S final significa que es una conexión segura.

Existe una alternativa bastante potente para la protección de nuestras comunicaciones: la instalación de una VPN (Virtual Private Network, en español red privada virtual). Es una tecnología de red de ordenadores que permite una extensión segura de la red de área local sobre una red pública o no controlada como Internet. Permite que el ordenador en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada, con toda la funcionalidad, seguridad y políticas de gestión de una red privada.

Por otra parte, es importante cuidar los programas que vamos utilizando para el chat, para nuestras reuniones virtuales, para explorar internet. Es difícil dar una lista acá ya que la evolución en el mundo digital es muy rápida, pero en este momento se recomienda lo siguiente:

- Exploradores: el uso de Firefox (con distintos plugins que nos protejan)
- Mensajería instantánea: el uso de Signal (en vez de Whatsapp)
- Servidores: el uso de servidores de correo seguros:
  - Riseup (*https://riseup.net*)
  - Proton (*https://protonmail.com/es/*)

- Plataformas para reuniones: el uso de Jitsi desde servidores seguros:
  - *https://meet.greenhost.net/*
  - *https://meet.mayfirst.org/*
  - *https://framatalk.org/es*
  - *https://calls.disroot.org/*
  - *https://talk.greenhost.net*
- Intercambio de archivos: el uso de programas seguros para intercambio de archivos o para trabajo colaborativo online como *https://cryptpad.fr/index.html*
  - se puede seleccionar el idioma en español.
  - para registrarse no se pide una dirección de correo electrónico.
  - todos los archivos están encriptados y solo quienes tengan la clave y el link creado puede acceder a los documentos.

Para ir más allá en nuestra protección y en el anonimato, se recomienda el uso del sistema operativo Linux o Ubuntu, y el explorador TOR para internet –que permite un anonimato total y sirve especialmente en países con fuerte censura–.

Además, como organización y dependiendo de la información que manejemos, debemos decidir qué personas de la organización tiene acceso a qué tipo de información. Si somos una organización grande que acoge a pasantes de fin de carrera, por ejemplo, puede ser que decidamos que cierta información no debe ser de conocimiento de todas las personas que pasan por la organización. Dependerá de decisiones estratégicas y políticas, de quiénes somos, del nivel de confianza creado en la organización, etc.

Para ir más allá, unos links interesantes:
https://securityinabox.org/es/
https://tacticaltech.org/projects
https://www.digitalfirstaid.org/es/
https://www.torproject.org

La pérdida de nuestra información

Por múltiples razones podemos perder la información que tenemos. Puede ser de forma intencional –robo, por ejemplo– o accidental – un problema técnico, la pérdida del portátil, etc–. Perder nuestra información nos puede hacer perder años de trabajo en favor de los derechos humanos, nos puede hacer perder la capacidad de justificar proyectos y perder financiación, etc.

Acá hablamos solamente del impacto de la pérdida de la información y de cómo protegernos, no hablamos del riesgo de que otras personas tengan acceso a esta información (ver el apartado anterior).

Frente a ello, la única solución es la de realizar *back-up* –copias de seguridad– de nuestra información. Para ello podemos utilizar ciertos programas (*https://www.cdlibre.org/consultar/catalogo/Utilidades_Copias-de-seguridad.html*) o copiar manualmente las carpetas que sean importantes –para lo cual debemos tener una organización de archivos clara–.

A tomar en cuenta:

- El *back-up* o la copia de seguridad no debe ser almacenada en la misma computadora (si perdemos o nos roban la computadora perderíamos la copia de seguridad también).
- El *back-up* o la copia de seguridad no debe ser almacenada en nuestras oficinas o nuestras casas (efectivamente, si se da un allanamiento legal o ilegal pueden llevarse todos los discos duros y podemos perder nuestra copia de seguridad).

Tomando en cuenta lo anterior y dependiendo del nivel de riesgo que tengamos y en qué fase de peligro nos encontremos, podemos pensar en varios niveles; por ejemplo:

- un *back-up* diario o semanal (dependiendo de la cantidad de información que movamos al día) que puede mantenerse en la oficina o en nuestro servidor.
- un *back-up* mensual que podemos dejar en la sede de otra organización en el país –aliada, pero con menor nivel de riesgo– o con alguien de confianza que no sea un familiar o una persona que tenga un nivel de riesgo como el nuestro.
- un back-up semestral que saquemos del país con una organización aliada internacional.

Palabras finales

La seguridad digital es algo que evoluciona mucho y debemos mantenernos al tanto de vez en cuando a través de las páginas web mencionadas en este documento o compartiendo también con nuestras organizaciones aliadas –puede ser que algunas tengan personal específico para ello–.

Por otra parte, ciertas medidas pueden ser engorrosas y debemos adaptar nuestro nivel de protección a nuestro nivel de riesgo y la fase del peligro en la cual nos encontremos.

Como se menciona a lo largo de este documento, debemos asegurarnos de que nuestra protección no se transforme en un riesgo –por ejemplo, olvidar las contraseñas y perder toda nuestra información–.

Brigadas Internacionales de Paz (PBI) es una organización no gubernamental de carácter internacional con más de 40 años de experiencia en la protección de los derechos humanos y la apertura de espacios para la paz. Desde 1981 brinda acompañamiento a personas, organizaciones y comunidades defensoras que trabajan de forma no violenta en favor de los derechos humanos y que se encuentran en una situación de riesgo debido a su labor.

www.pbi-ee.org