Preguntas frecuentes

En esta sección podrás consultar las dudas más frecuentes asociadas con el envío de información a través de nuestro portal, así como consideraciones de seguridad que debes tomar en cuenta.

1.–¿Cómo mantenerme completamente anónimo?

Al navegar por internet, dejas huellas digitales que pueden llevar a un tercero a identificar quién eres y dónde estás.

Algunos ejemplos de acciones que dejan rastros digitales son: conectarse a internet, utilizar buscadores, descargar programas, enviar correos electrónicos, visitar páginas, interactuar en redes sociales, entre otras.

Por tal motivo, te sugerimos evitar visitar nuestro sitio **filtracionesdigitales.org** desde tu computadora de trabajo y, mucho menos, enviarnos documentos desde las instalaciones de donde la obtendrás. Es mejor hacer el envío desde un café Internet.

Dado que los navegadores comunes como Firefox, Chrome, Safari, Opera, MS Internet Explorer, etc. no garantizan resguardar tu identidad al utilizarlos, para poder informarnos de alguna vulneración de datos personales te sugerimos instalar el navegador Tor.

También es importante que seas discreto/a respecto a tus intenciones de realizar una denuncia por medio de nuestro portal. Procura no comentar el asunto con nadie y, mucho menos lo menciones en redes sociales o por medios electrónicos como email.

»Acerca de los metadatos

Todo archivo en un dispositivo electrónico tiene metadatos que describen varias de las características del archivo. Los metadatos son diferentes del contenido. Ejemplos de metadatos en el caso de un correo electrónico son el remitente, los destinatarios, el asunto y la hora de envío. Para proteger tu anonimato de manera efectiva, eliminaremos los metadatos incluidos en los documentos que nos envíes, particularmente aquellos que podrían, en un momento dado, revelar tu identidad.

2.–¿Qué tan seguro es el portal Filtraciones Digitales?

Nuestro portal para envío de información funciona con el software GlobaLeaks. GlobaLeaks es un software de código abierto para filtraciones seguras y anónimas. Es desarrollado por el Hermes Center for Transparency and Digital Human Rights.

Así, el portal está diseñado para garantizar tu seguridad y el anonimato tanto tuyo como de tu envío.

Si al enviarnos documentos utilizas la red de anonimato Tor, será casi imposible obtener rastros de tu identidad, procedencia y ubicación del envío.

Es imposible lograr que un sistema sea 100% seguro. Sin embargo, GlobaLeaks fue diseñado para garantizar la seguridad de las y los informantes.

3.–¿Cómo seleccionar que información enviar a través del portal?

En caso de que sospeches que alguna empresa u organización no está protegiendo adecuadamente tus datos personales o los de cualquier otra persona, las pruebas más útiles que puedes enviarnos, para que logremos comprobar violaciones a la legislación aplicable son las siguientes:

a. Correos electrónicos enviados por la propia organización o empresa en los cuales revelen datos personales de uno o más usuarios, clientes o empleados/as a otras personas que no deben conocerla;

b. Correos electrónicos, mensajes de texto o grabaciones de llamadas de empresas u organizaciones con las que no habías tenido contacto anteriormente y que ahora te envían publicidad no deseada.

Recuerda que no importa si tú eres la única persona afectada o si sólo sabes de un caso, tu información será analizada con el fin de detectar otros casos en los que se también se haya violado el derecho a la protección de datos personales de más personas.

En caso de que te haya enterado de alguna vulneración de datos personales que cierta organización o empresa falló en notificar, las pruebas más útiles que puedes enviarnos, para que logremos comprobar violaciones a la legislación aplicable son las siguientes:

a. Archivos extraídos de la organización vulnerada los cuales contengan datos personales que no estén debidamente protegidos. Por ejemplo:

» Bases de datos (totales o parciales) de clientes, proveedores o empleados

» Hojas de cálculo

» Contratos

b. Archivos o documentos en los que conste que ocurrió la vulneración de datos. Por ejemplo, un análisis del incidente de seguridad que contenga:

» Registros de la vulneración

» Reportes generados por herramientas de seguridad

» Bitácoras

» Comunicaciones internas (correos electrónicos, memorandos, entre otros)

c. Archivos o documentos en los que conste que al interior de la empresa u organización se optó por omitir la notificación a las y los afectados.

Opcionalmente, podrás proporcionar vínculos o fotografías de que la base de datos vulnerada está disponible o a la venta en medios públicos como Internet.

Evita enviarnos la base de datos vulnerada, ya que contiene datos personales de las y los afectados. Además, considera que sólo proporcionar esta base de datos no es prueba suficiente de que ocurrió la vulneración y que se omitió la notificación.

También evita enviarnos archivos que contengan información ajena a la vulneración de datos personales como secretos industriales, know how o modelos de negocios, entre otros.

De cualquier forma, al momento de realizar el envío, dependiendo de si tienes una relación laboral con la organización o empresa en cuestión, o si eres cliente o un tercero, el sistema te indicará cuál es la información más útil que nos podrías enviar.

4.–¿Qué debo tomar en cuenta al momento de extraer la información que voy a enviar y cómo debo hacerlo?

Primero que nada, asegúrate de lo siguiente:

» Asegúrate de que el dispositivo en donde guardarás la información no sea rastreable.

» No te envíes la información por medio de correo electrónico, redes sociales, almacenamiento en la nube o similares.– Evita fotografiar la información o realizar capturas de pantalla si existen cámaras de vigilancia o si estás en un ambiente que te exponga.

Procura entonces:

» Utilizar una carpeta comprimida dentro de la cual guardes copias de los archivos. Protege dicha carpeta con una contraseña.

» Guarda cada archivo, cambia sus nombres originales y asígnales una contraseña de apertura.

5.–¿Puedo elegir cualquier equipo para elegir el envío?

Te recomendamos lo siguiente:

» No utilices un dispositivo (laptop, computadora de escritorio, etc.) proporcionado por la organización o empresa en donde ocurrió la vulneración de datos.

» Utiliza un dispositivo que no sea de tu propiedad, y que no contenga rastros de tu identidad ni de otra persona.

» Lo mejor sería que utilices un equipo de un café Internet.

» Finalmente, procura dejar en casa cualquier dispositivo electrónico personal con GPS (smartphone, tableta o similar) para evitar dejar rastros de tus movimientos.

6.–Ya instalé Tor ¿ahora qué sigue?

Dirígete a nuestro portal filtracionesdigitales.org, accede al sistema de envío de documentos y sigue las instrucciones en pantalla.

Si acudiste a un café internet, recuerda extraer y llevarte la memoria USB desde donde nos enviaste la información.

Procura pagar en efectivo (nunca con tarjeta de crédito), y no olvides llevarte todos los documentos que hayas utilizado y o impreso en el establecimiento.

Evita guardar copias de la información revelada.

Deberás suprimir por completo (no basta con borrar) la información de la memoria USB. Existen herramientas de software especializadas para tal propósito.

Es preferible destruir la memoria USB. No la deseches en la basura.

Evita compartir que has utilizado nuestro portal, ni siquiera después de que la información haya sido publicada.

Procura no realizar búsquedas de la información que has proporcionado para evitar que un tercero pueda identificar tu interés por la información.