ARTICLE 19

GUÍA Y RECOMENDACIONES GENERALES SOBRE LA

DOCUMENTACIÓN Y ATENCIÓN DE AGRESIONES DIGITALES

"Guía y recomendaciones generales sobre la documentación y atención de agresiones digitales"

Artículo 19 México y Centroamérica

Este documento fue elaborado con el apoyo de ARTICLE 19, Oficina para México y Centroamérica y la Embajada de Holanda. La autoría de la guía corresponde a Estrella Soria, a petición de las organizaciones mencionadas.

Diseño y diagramación: Isaac Ávila y Ramón Arceo

Corrección de estilo: David Loria

Contenido

Introducción

Las los periodistas se han volcado al espacio digital por distintas razones. Esto ha generado un nuevo campo para el ejercicio del derecho a la libertad de expresión que también enfrenta amenazas donde los y las periodistas son intimidadas, acosadas y agredidas.

Las tecnologías digitales han abierto un mundo al permitir obtener información a una gran velocidad, lo que ha generado tensiones y disputas por mantener espacios accesibles y democráticos donde sea posible ejercer libertades y derechos.[1]

Durante los últimos tiempos de crisis y pandemia se ha registrado un incremento en la variedad de amenazas y violencias en contra de periodistas y a la libertad de expresión de las personas: amenazas físicas y psicológicas, digitales, legales y políticas,[2] las cuales se convierten en peligros de alto riesgo cuando logran inhibir su labor y, sobre todo, cuando atentan contra sus vidas.

En este contexto, el espacio digital también expone escenarios de exclusión y desigualdad que refuerzan las violencias históricas y estructurales[3] en poblaciones que están en una situación de mayor vulnerabilidad; intimidaciones que repercuten en la relación de estas personas con las tecnologías, en su manejo de emociones y en su integridad individual.

A fin de hacer frente a estos escenarios, ARTICLE 19, Oficina para México y Centroamérica, promueve y defiende el avance progresivo de los derechos de libertad de expresión y acceso a la información mediante el desarrollo de guías, herramientas y materiales de capacitación que contribuyan al fortalecimiento de las tareas de atención a personas agredidas.

Mecanismos de Control

En la era digital, el periodismo y las diversas formas de comunicar han evolucionado de múltiples maneras. Nos relacionamos con las tecnologías según la capacidad de consumo, acceso, formación, afición, habilidad, género, edad, idioma y dominio; pero nos vinculamos también con la transformación permanente de lógicas que conforman la digitalidad, es decir, las arquitecturas y condiciones que suponen el uso de las tecnologías de la información y la comunicación.

Hasta para quienes han nacido en la era digital, algunas condiciones de uso de tecnologías, servicios o plataformas digitales son problemáticas porque no siempre favorecen a las personas usuarias y se desdibujan los alcances sobre los impactos que pueden llegar a tener sobre estas. Por ejemplo, una plataforma sociodigital puede ayudar a dar a conocer un perfil, así como detallar o validar una información, pero en momentos críticos todos esos datos pueden hacer sentir a la persona o medio en demasiada exposición.

También, al enfrentar incidentes o amenazas en entornos digitales, aparece el miedo y es utilizado como un medio de control. Por lo tanto, es necesario que las personas responsables de documentar agresiones sepan identificar y acompañar estos temores. El miedo dificulta la toma de decisiones: paraliza, aísla, genera desconfianza y rompe el tejido social en el entorno.

1 Relatoría Especial para la Libertad de Expresión (RELE), Comisión Interamericana de Derechos Humanos, CIDH, Estándares para una Internet libre, abierta e incluyente, CIDH-RELE, 2017, párr. 184, https://www.oas.org/es/cidh/expresion/docs/publicaciones/INTERNET_2016_ESP.pdf

2 "La crisis ya estaba aquí. Defensoras mesoamericanas ante COVID-19", IM Defensoras, http://im-defensoras.org/wp-content/uploads/2020/06/La-crisis-ya-estaba-aqu%C3%AD-10062020.pdf.

3 ARTICLE19, "Distorsión: el discurso contra la realidad", México 2020, p. 110, https://distorsion.articulo19.org/

Al detonar miedo en una persona, periodista o medio, se busca afectar a una colectividad e imponer un modo de vida, así como determinadas relaciones económicas, valores, modelos y estructuras de poder. El miedo puede llegar a considerarse un medio de control porque, haciendo uso de diversos métodos violentos, revestidos de amenazas, consigue o conserva cierta situación.

En contextos como el de México, donde la violencia es crónica y se ha normalizado, los impactos de agresiones en línea ño fuera de ellañ no son menores. Lo que sucede en entornos digitales es tan real en sus repercusiones como lo que ocurre en otros espacios físicos, tangibles. Cuando una persona es atacada, y especialmente cuando se trata de mujeres periodistas o de personas que pertenecen a la comunidad LGBTIQ+, la agresión no se queda únicamente en sus dispositivos digitales, sino que los trasciende y afecta de forma integral su vida cotidiana.[4] En este terreno, la producción de miedo es un modo de operar muy económico y de amplia propagación para quien desee implementarlo.

Analizar una amenaza a través de Internet u otros entornos digitales no es una tarea fácil. Requiere de mucha atención no solo porque es un aviso sino porque opera como un estímulo que puede dañar desde el momento en que se recibe, porque causa malestar, inestabilidad o recelo, y así inhibe el ejercicio de derechos y libertades. Es por ello que demanda documentarse cuidadosamente con las personas que las experimentan, además de registrar cada una de las evidencias de las agresiones.[5]

Cuando se enfrentan ataques como denegación de servicio[6] (DoS), intervención de cuentas, amenazas, suplantación o remoción de contenidos, los riesgos que se pueden documentar están asociados con la percepción de los impactos psicosociales de quien los reporta. Cada persona reacciona de manera diferente al estrés que provocan las agresiones, la vulnerabilidad o la impotencia que conlleva una "brecha digital" (económica, educativa, psicológica o de género), y es importante validar su percepción o vivencia sin juzgarle.

El cuidado en describir la percepción y las evidencias permitirá orientar y canalizar de forma correcta a la persona, además de agregar información contextual y factual para realizar un análisis de riesgos.[7] Además, este registro puede ser útil para desarrollar un estudio psicoemocional sobre los impactos, derivar una valoración prospectiva sobre posibles daños futuros o poner en marcha múltiples estrategias preventivas.

De acuerdo con el modelo de análisis y acompañamiento de "Aluna Psicosocial",[8] el miedo también puede entenderse como una forma con diversas estrategias de coerción individual o comunitaria porque tiene una impronta simbólica sobre la colectividad: a mayor violencia, mayor control del tejido social.

En las siguientes páginas encontrarás un resumen diagnóstico del proceso de documentación y acompañamiento de personas que enfrentan agresiones a su libertad de expresión en entornos digitales, así como una guía breve para su atención que se apega a los flujos de trabajo en ARTICLE 19. Esta guía es una aproximación que explora procesos de archivo, preocupaciones y afrontamientos psicosociales provocados por el uso de tecnologías digitales para el ejercicio y la defensa de los derechos humanos; en particular, para la libertad de expresión.

4 Luchadoras et. al, "La violencia en línea contra las mujeres en México", México 2017, Internet es Nuestra, https://shortly.cc/7zgGY

5 ARTICLE 19, "Disonancia: voces en disputa", México, 2019, https://articulo19.org/disonancia/

6 Un ataque de DoS (Denial of Service) o DDoS (Distributed Denial of Service), o en español "Denegación de Servicio Distribuido" se caracteriza por deshabilitar un sitio web por un tiempo determinado. Consiste en que la saturación de los servidores de la página impide que las personas tengan acceso a la información que aparece en el medio. ARTICLE 19 ha documentado estos casos en un contexto donde los ataques DDoS son dirigidos para bloquear el flujo informativo.

7 Aluna Psicosocial, "Redefiniendo el Enfoque de Riesgo. Nuevas recomendaciones para la aplicación del enfoque de riesgo", s/f, https://www.alunapsicosocial.org/single-post/nuevas-recomendaciones para-la-aplicaci%C3%B3n-del-enfoque-de-riesgo

8 ídem.

Diagnóstico

Responsable de la documentación.

El Programa de Protección y Defensa en Artículo 19 realiza un proceso de documentación[9] sobre agresiones a periodistas o medios de comunicación con respecto al ejercicio de sus labores periodísticas. En el caso de las agresiones digitales, mantiene una relación constante con el programa de Derechos Digitales y con otras organizaciones especializadas en la atención de ataques virtuales como Social Tic.

En el proceso de documentación, las personas responsables deben recolectar información confiable y clara que permita reconstruir la agresión y el contexto en el cual ocurrió. Los siguientes apartados profundizan sobre este proceso y brindan información que pueda orientar a otras organizaciones y/o colectivos que realizan procesos similares.

El proceso general de documentación y registro consiste en:

1. Identificación del caso;
2. Asignación de la persona responsable de la documentación;
3. Registro inicial;
4. Primer contacto con la persona o medio;
5. Entrevista con la persona o medio;
6. Entrevista con por lo menos tres fuentes distintas;
7. Registro del caso (en la base de datos de Artículo 19);
8. Seguimiento y actualización del caso.

Una persona responsable de documentación y registro es una persona que acompaña en representación de Artículo 19.

> "El acompañamiento se basa en la información que la persona responsable de la documentación haya obtenido mediante el análisis y el contraste de la información proporcionada por diversas fuentes. El objetivo es mejorar las condiciones para el ejercicio de la libertad de expresión, desde un enfoque de seguridad integral y con una vocación de cambio estructural"
>
> ARTICLE 19 México y Centroamérica

El proceso de asignación y niveles de acompañamiento se basa en criterios, esquemas y consideraciones que incorporan:

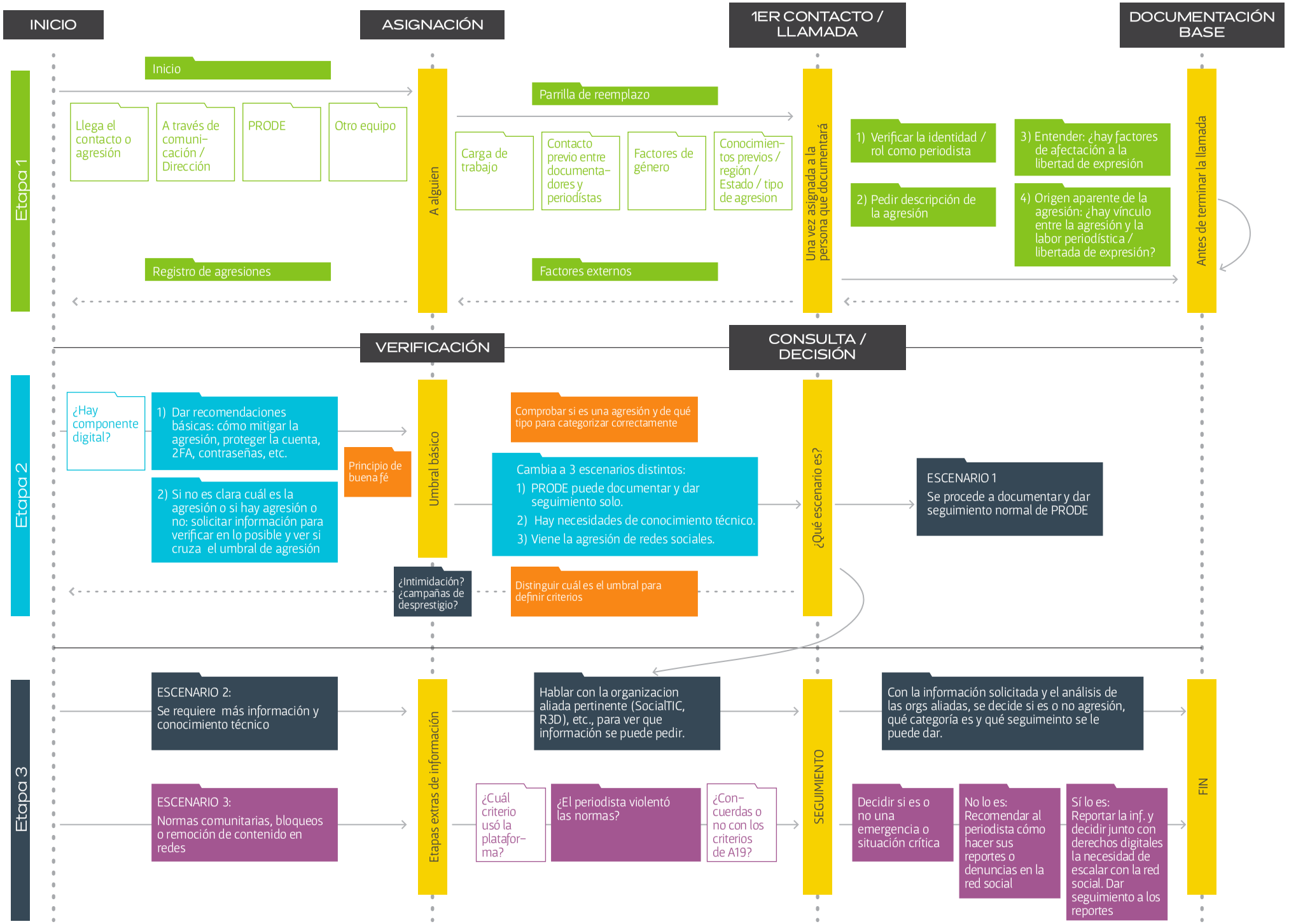
1. Valoración del caso;
2. Propuesta de nivel de acompañamiento;
3. Asignación del nivel de acompañamiento;
4. Determinación de las acciones iniciales;
5. Presentación de las propuestas a la persona o medio agredido;
6. Implementación de las acciones iniciales;
7. Evaluación;
8. Seguimiento;
9. Conclusión.

9 La documentación se refiere al proceso por el que ARTICLE 19 contacta tanto a periodistas que hayan sido objeto de agresiones como a fuentes cercanas a la víctima y/o al contexto en el que ocurrió la agresión, con la finalidad de recopilar información que le permita generar un análisis y un registro del caso. El registro se refiere al caso que fue consignado de la agresión de acuerdo a una "Categoría de Agresiones". Cuando la persona haya tenido más de una agresión, se registrará aquella que se considere de mayor gravedad. Véase también "ARTICLE 19 trabaja para denunciar la violencia contra la prensa de la que no se hace cargo el Estado", 2021, https://articulo19.org/wp-content/uploads/2021/04/A19_EDITORIAL2021_V3-2.pdf

Flujograma sobre el registro y la documentación

Objetivos: visualizar el flujo de trabajo de documentación de ARTICLE19 México y Centroamérica, la configuración del equipo de apoyo, las etapas y la identificación de problemas o desafíos para la documentación de violaciones a los derechos de libertad de expresión y el acompañamiento a las personas cuyos derechos han sido violados.

Documentación y registro



Este es un resumen y recordatorio de los desafíos existentes en el proceso de documentación de agresiones en entornos digitales que conducirá a conversaciones internas entre personas y equipos sobre la prioridad de los esfuerzos, la conveniencia de la categorización y el esquema de acompañamiento.

Niveles de acompañamiento

La atención de personas que enfrentan alguna violación de sus derechos a la libertad de expresión e información contempla cinco niveles de acompañmiento. Esta guía se enfoca en los niveles primario y preventivo.

Recomendaciones para quien documenta

Al hacer tareas de registro y documentación se requieren muchas habilidades para tratar con las personas desde un lugar de dignidad humana, evitando los sesgos personales y preguntas o situaciones que puedan revictimizarlas o invisibilizar factores de riesgo.

A lo largo de la vida, desarrollamos sesgos en relación con nuestro contexto y condiciones socioeconómicas, formación, posición política o género que, entre otros juicios o percepciones, intervienen para que otorguemos atención desproporcionada a favor o en contra de algo, ya sea una circunstancia, persona o grupo.

Considera que muchas veces podemos encontrar errores en las tecnologías digitales por falta de recursos, estudios o pruebas. Otras tantas hallamos que las tecnologías priorizan sus intereses lucrativos y contienen sesgos por diseño que dificultan mantener una relación ética con las personas que las emplean. Hay que recordar que las tecnologías están diseñadas por personas y pueden contener sesgos por defecto.

Respira. Para documentar agresiones con componentes digitales no es necesario que sepas de todo, pero es importante entender la situación y las necesidades para registrarlas con el mayor detalle posible. Te puedes basar en dichos datos para orientar sobre procedimientos o guías de prevención, o para realizar análisis más profundos.

Por ejemplo, si la persona te dice que le *hackearon* el correo, pregunta a qué se refiere. ¿Alguien ingresó a tu cuenta de correo electrónico? ¿Compartes la computadora con más personas? ¿Recuerdas si compartiste tu contraseña con alguien? ¿Dejaste alguna sesión abierta, por ejemplo, en alguna sala de redacción, café Internet o similar?¿Tenías activa la verificación en dos pasos?

- En caso de que alguien no tenga la verificación de dos pasos, doble verificación o autenticación multifactor, puedes compartirle el siguiente recurso: https://seguridadintegral.articulo19.org/infografias/autenticacion-dos-factores-y-dos-pasos/

- En caso de tener indicios de que la persona fue *hackeada,* recomienda cambiar todas las contraseñas.

Intervención de cuentas, suplantación de identidad	
Pregunta	Observaciones
¿Qué tipo de cuenta es: correo electrónico, perfil o página de red social?	Aunque por lo general presentan similitudes, los mecanismos de reporte pueden variar entre una y otra.
¿La persona defensora o periodista tenía activada la verificación en dos pasos?	Este es un indicador para saber si hubo alguna posibilidad de que se haya pasado este filtro de acceso, o si se trata de algún otro incidente.
¿La persona defensora o periodista tenía activada la notificación de inicio de sesión?	Esto permite observar si la persona recibió alguna notificación previa a su cuenta de correo o teléfono de que hubo un inicio de sesión no autorizada o fuera de lo común.
¿La persona defensora o periodista generó algún reporte con el intermediario (Facebook, Twitter) a través de una cuenta de terceros, o bien, a través de algún otro mecanismo de reporte?	Con esta acción se puede saber si la persona ya inició algún tipo de procedimiento de recuperación de la cuenta. También ayuda para después escalar el caso frente a la asistencia técnica de las plataformas.
¿Tenía actividad la recuperación de la cuenta a través de la función de Facebook "amigos de confianza"?	
De haber hecho el reporte ¿recibió alguna respuesta?	
¿Cuándo fue la última vez que tuvo acceso a la cuenta de correo electrónico, página o perfil de red social?	Esto permite identificar la temporalidad y las posibles acciones que se puedan emprender, y si el/la periodista recibió alguna notificación del cambio de contraseña.
¿Recibió alguna notificación del cambio de contraseña y/o el cambio de correo electrónico asociado al perfil?	

Cuando alguien diga que le "tumbaron la página", pregunta ¿por qué consideran que su página está fuera de línea? ¿En qué plataforma está hospedada? ¿Cuándo vence su contrato o vigencia de hospedaje? ¿Tiene activada la verificación en dos pasos para ingresar? ¿Tiene registro de logs o de las peticiones del sitio?

Otras preguntas:

Ataque DoS, página inactiva	
Pregunta	Observación
¿Cuál es la URL de la página atacada?	
¿En qué plataforma está montada la página? Por ejemplo, Wordpress, Drupal, etc.	Esto permite distinguir si el problema puede estar relacionado con la administración del sitio, es especial si se trata de Wordpress.
¿Cuentan con un informe de Google Analytics o algún otro análisis de tráfico de la página?	El informe de Google Analytics permite observar el tráfico del sitio, si hubo un comportamiento inusual que identifique si hubo peticiones de una sola dirección IP o de un conjunto de IP.
¿Tiene un respaldo de la página?	Saber si están en posibilidades de realojar el sitio en otro host.
¿Cuentan con algún sistema de protección frente a algún ataque DoS como Deflect, Cloudflare?	Si tienen algún sistema de protección podrá descartarse que es un ataque DoS. Si no cuentan con algún sistema, se puede sugerir la activación Deflect como una medida preventiva.
¿Cuál es el host de la página?	Esto permite saber en qué tipo de servicio de host está hospedada la página. También para saber si no se trata de algún problema directamente con el host. Para conocer más información sobre el sitio y verificar bien su estatus se puede acceder a: – https://downforeveryoneorjustme.com/ –https://whois.icann.org/es
¿Han realizado actualizaciones de los plugins en la plataforma de wordpress?	En ocasiones la página caída o con alguna frase de lo que pudo haber sido hackeada se trata de un plug in que contenía algún programa malicioso. Esto hace que aparezcan mensajes intrusivos en la página, que se traduzca a otro idioma sin permiso, etc.
¿Hubo algún problema con el host relacionado con la renovación de los servicios provistos para la página?	Es posible que la inactividad de la página se deba a un conflicto con el host provider, falta de pago, no se hizo la renovación de los servicios o algún otro debido a la relación entre el sitio y el proveedor de los servicios para hospedar el sitio.

Remoción de Contenido: si en la conversación te dicen "ÁCensuraron mi publicación!", pregunta "¿te llegó alguna notificación por parte de la plataforma?, ¿te permitieron apelar?, ¿qué te respondieron?"

Otras preguntas:

Remoción de contenidos, suspensión/cancelación de cuentas	
Pregunta	Observación
¿Recibieron alguna notificación previa a la remoción/baja de la publicación, el video, imagen o información compartida?	Las plataformas deben avisar al usuario/a si infringió alguna de sus normas y por tal motivo la publicación fue removida.
¿Revisaron el registro de actividad para identificar si hubo alguna notificación de eliminación de la publicación?	Permite observar el comportamiento de la cuenta e identificar si hubo alguna acción para eliminar contenido.
¿Alguien más administra la cuenta de correo, perfil o página de red social?	Existe la posibilidad de un tercero.
¿Hubo algún pago para promocionar la publicación?	Las normas comunitarias son distintas de las políticas de publicidad. Esto puede hacer que las plataformas impidan que se realice una publicación si esta infringe algunas de sus políticas. Por ejemplo, por tratarse de un asunto de propiedad intelectual al mencionarse el nombre de una marca.
¿Presentaron algún tipo de reporte al intermediario por la suspensión, remoción o cancelación de la cuenta?	Los reportes son una forma de tener registro acerca de las acciones que el usuario/a realizó y, sobre todo, como un precedente para escalar el caso ante un intermediario. Con respecto a Twitter, el número de reporte es fundamental.
¿Utilizaban algún tipo de mecanismo de automatización como tweetdeck, hootsuite o algún otro para publicar tuits?	Un problema al que se puede enfrentar la personas periodista o medio es la cancelación/suspensión de su cuenta por el comportamiento tipo "spam" de la cuenta. Por ejemplo, si tenía tres o cuatro cuentas que interactuaran entre sí con *retweets* o *likes,* podría considerarse como una forma de comportamiento no está aceptada en dicha red social. Es decir, la suspensión de la cuenta no necesariamente se da por los contenidos publicados. https://help.twitter.com/es/rules-and-policies/twitter-automation
¿Conoces las reglas de las plataformas de las redes sociales?	
¿Han recibido alguna notificación sobre cuáles fueron las razones de la suspensión/cancelación o remoción de contenidos?	

Recolecta suficiente información sobre cuándo y dónde ocurrió la agresión, quiénes sufrieron la agresión, qué dispositivos, aplicaciones o servicios digitales fueron afectados y, de ser posible, compila evidencias sobre la agresión (URLs, capturas de pantalla, etc.).[10]

Otras preguntas:

10 En el siguiente enlace aparece el tratamiento que damos a la información recopilada: ARTICLE19, "Aviso de Privacidad", https://articulo19.org/wp-content/uploads/2019/09/AVISO-DE-PRIVACIDAD-Documentacion.pdf

Amenazas, hostigamiento, intimidación	
Pregunta	Observaciones
¿Cuál es la URL del agresor o tienes alguna captura de pantalla de su perfil?	Es preferible contar con la URL y no solamente con la captura de pantalla.
¿Cuál es la URL del perfil del periodista?	
¿Hubo algún reporte de la cuenta agresora?	En este caso es importante considerar si debe o no hacerse el reporte. En ciertos casos es preferible documentar lo más posible sobre la cuenta antes de que la suspendan. De acuerdo con Facebook, el perfil solo queda almacenado por un periodo de tres meses.
¿Se aplicó una medida de contención como bloquear o silenciar la cuenta agresora?	Esto puede ser una recomendación para que la o el periodista, persona defensora deje de recibir mensajes. La herramienta de silenciar en Twitter y permite que la cuenta no se suspenda y continúe.

Phishing	
Pregunta	Observación
¿Qué tipo de cuenta es: correo electrónico, perfil o página de red social?	Aunque por lo general presentan similitudes, los mecanismos de reporte pueden variar entre una y otra.
¿Qué tipo de información fue la que recibió y a través de qué vía?	Identificar cuál es la vía para ver si se trató de un correo electrónico, un mensaje vía SMS "personalizado", entre otros.
¿La persona defensora o periodista generó algún reporte con el intermediario (Facebook, Twitter) a través de una cuenta de terceros, o bien, a través de algún otro mecanismo de reporte?	Con esta acción se puede saber si la persona ya inició algún tipo de procedimiento de denuncia de *phishing*. Esto funciona sobre todo en Gmail, que tiene activada esta función.
¿Tenía actividad la recuperación de la cuenta a través de la función de Facebook "amigos de confianza"?	
De haber hecho el reporte ¿recibió alguna respuesta?	
Si fue un correo electrónico, ¿ingresó a la URL e introdujo los datos solicitados?	En el caso de los SMS, es importante señalar al periodista o persona defensora que no dé clic a la URL si se trata de un SMS. En caso de que sea un correo electrónico, que no ingrese a la URL ni introduzca los datos solicitados. Aunque varía según cada modelo de teléfono, es probable que, para documentar el caso de mensaje enviado vía SMS, deba seguirse este proceso: 1) poner en modo avión el teléfono; 2) ir al mensaje y dejar presionado para que aparezca la URL completa; 3) hacer captura de pantalla.

Entorno de trabajo para tareas de documentación:

- Organiza el escritorio de tu computadora por área de trabajo.[11] Mantén un orden sobre tus herramientas y una ecología de la atención[12].

- Despliega ventanas con guías útiles que apoyen paso a paso el auto-diagnóstico de la persona agredida o el diagnóstico asistido por ti.

- Por ejemplo:

  - En la base de datos se crea un caso y, si después no tiene vínculo con la labor periodística, se puede eliminar.
  - Ficha de caso.
  - Evita buscar en el momento o sugerir guías que no has revisado previamente. Recomendamos el *hub* de Seguridad Integral que tiene muchos recursos elaborados por ARTICLE 19.

- Ante la duda, consulta siempre con colegas del equipo sobre los procedimientos, los umbrales de las categorías de agresiones que tienes en tu colectivo u organizaciones, sugerencias y recomendaciones. Puedes guiarte de la categoría de agresiones de ARTICLE 19, la cual está disponible aquí.

Atender a la persona agredida

Ejemplos:

¿Qué hacer cuando no se tiene confianza en algún dispositivo?

Si está en tus posibilidades, propón cambiar a otro dispositivo, uno del que no sospeches que se encuentra comprometido, aunque sea uno prestado al que no se pueda comprometer. Después de haberse movido a un nuevo dispositivo, propón crear una cuenta nueva con una contraseña más fuerte, procura que no se vincule a sus antiguas cuentas, al menos hasta que pueda tener control de los accesos.

¿Qué hacer cuando no puede confiar en sus canales de comunicación?

Si considera que sus comunicaciones están siendo vigiladas, debería dejar de usar las cuentas y servicios que cree que se podrían comprometer. Propón y apoya a crear cuentas nuevas y recomienda no utilizar los pseudónimos o nombres de usuario, contraseñas y correos electrónicos vínculados, hasta que se pueda aclarar la situación.

Es bueno en tender por qué te está ocurriendo esto...

¿Quién crees que pueda estár interesado en ti o en tu medio? ¿Esta agresión está relacionada con tu trabajo? ¿Qué información te interesa resguardar? ¿de quién?

11 Ventanas y áreas de trabajo, Gnome Help, https://help.gnome.org/users/gnome-help/stable/shell-windows.html.es

12 La ecología de la atención significa decidir conscientemente en dónde redirigir la atención frente a la cantidad de estímulos y relaciones que se tienen en los entornos digitales. Se habla de la ecología de la atención en el desarrollo de herramientas digitales o estrategias donde las incluyes, se intenta que filtre exceso o información redundante y que te notifique únicamente lo necesario, lo que te interesa. Citton, Yves, "De la economía de la atención a la ecología de la atención, Tabakalera, 23 de mayo de 2019, https://www.tabakalera.eus/es/de-la-economia-de-la-atencion-la-ecologia-de-la-atencion

Índice de guías útiles

La recomendación de guías es fundamental para ayudar a las personas a reducir los riesgos ante agresiones y amenazas de manera autónoma y establecer o implementar cambios necesarios, por ejemplo, en sus dispositivos móviles. Muchas veces será útil que realices una introducción a las guías y acompañes los primeros pasos de su consulta, a manera de presentación. Cuando se identifican casos similares, ARTICLE 19 organiza talleres y seminarios en línea que quedan accesibles como material de consulta.

Las guías recomendadas para consultar procedimientos preventivos (análisis de riesgo, protocolos de seguridad, entre otros) y reactivos sobre seguridad y derechos digitales se encuentran en Seguridad Integral de ARTICLE 19, disponibles para casos de:

- *Phishing*
- Derecho de autor (DMCA)
- Remoción de contenido: sobre las reglas y políticas...
- Remoción de contenido: sobre las normas comunitarias de...
- Mensajerías instantáneas
- Aplicaciones seguras para mujeres
- La protesta en línea
- Contraseñas seguras
- Navegador Tor
- Autenticación de dos pasos
- Cifrado de sistemas operativos

Guía: Seguridad Integral
Vínculo: https://seguridadintegral.articulo19.org/guias/

Si la persona está dispuesta y solicita alguna orientación sobre lo que debe hacer para entender mejor el riesgo de las agresiones o amenazas en línea, puedes apoyarte de la guía "Modelado de riesgos" que ofrece la organización Asuntos del Sur. De una forma interactiva, esta identifica tu perfil y hace una aproximación sobre los niveles de riesgo. También te permite avistar las posibles amenazas, las acciones que puedes emprender y qué tipo de información es más importante proteger.

Guía: Modelado de riesgos
Disponible en: https://modeladoriesgos.asuntosdelsur.org/

El Kit de Primeros Auxilios Digitales te ayudará a diagnosticar y mitigar los problemas que la persona agredida esté experimentado:

- Perdí/Me robaron mi dispositivo
- Perdí/Suplantaron elacceso a mis cuentas
- Mi dispositivo está actuando de forma inusual (se abren aplicaciones de forma espontánea, alto consumo de datos, se descarga la batería con rapidez, etc.).
- He recibido mensajes sospechosos
- Mi sitio web no está funcionando
- Alguien me está suplantando en Internet
- Estoy siendo acosada/o en línea
- Mi información fue removida
- Alguien que conozco ha sido arrestada/o

Guía: Kit de Primeros Auxilios Digitales
Vínculo: https://digitalfirstaid.org/es/

Protege.la es un sitio desarrollado por la organización Social Tic que contiene guías, consejos y herramientas para mejorar tu seguridad y privacidad digital. Aquí puedes revisar los niveles de seguridad de tus dispositivos electrónicos y tu navegación en Internet.

Guías: ¿Qué hacer ante agresiones y ataques en línea?
Vínculo: https://protege.la/checklists/

Índices de guías útiles para la autoformación

Para continuar con la revisión de herramientas y tácticas de privacidad y protección digital con metodologías interactivas para el aprendizaje individual, recomendamos los siguientes proyectos:

- Contraseñas seguras
- Aplicaciones de mensajería seguras
- Phishing
- Exploremos Internet ¿cómo funciona?
- Cómo eludir la censura en Internet
- Cuida tu privacidad

Guía: Entrenamiento de Seguridad Digital para Activistas y Periodistas
Vínculo: https://totem.project.org/

A través de la Plataforma Inteligencia en Riesgos Digitales se puede acceder a micro cursos que se proponen desarrollar capacidades para responder a distintos riesgos digitales, así como generar estrategias de resiliencia y atención a incidentes.

- Atención de incidentes
- Phishing e ingeniería social
- Censura e interrupción de redes
- Seguridad para periodistas
- Seguridad de la información
- Modelado de riesgos

Guía: Plataforma INTELIGENCIA en riesgos digitales
Vínculo: https://riesgosdigitales.academiainnovacionpolitica.org/

Para su consulta, existe una colección de ideas y consejos para personas defensoras de los derechos humanos que puede ser muy útil para personas comunicadoras y periodistas que realizan tareas laborales desde su casa, así como proteger su información al:

- Proteger la Wi-Fi;
- Proteger de forma básica los dispositivos digitales;
- Almacenamiento de información sensible;
- Copias de seguridad;
- Correos electrónicos;
- Transferencia de archivos.

Guía: Protección física, emocional y digital para el trabajo desde casa.
Vínculo: https://www.frontlinedefenders.org/es/resource-publication/physical-emotional-and-digital-protection-while-using-home-office-times-covid

Fuentes adicionales consultadas:

Aluna Acompañamiento Psicosocial, A.C., Modelo de acompañamiento psicosocial de Aluna, Ciudad de México, Pan para el Mundo de Alemania, s/f.

---. Redefiniendo el Enfoque de Riesgo. Nuevas recomendaciones para la aplicación del enfoque de riesgo, s/f, https://www.alunapsicosocial.org/single-post/nuevas-recomendaciones-para-la-aplicaci%C3%B3n-del-enfoque-de-riesgo

---. ¿Cómo enfrentamos el miedo en el contexto actual las defensoras? , 2018, https://www.alunapsicosocial.org/single-post/2018/12/10/-c%C3%B3mo-enfrentamos-el-miedo-en-el-contexto-actual-las-defensoras

Article 19, Disonancia: voces en disputa, el informe anual 2019, 2019, https://articulo19.org/disonancia/

Cyberstalking Victims Emotional Support, s/f, https://www.fightcyberstalking.org/emotional-support/

Digital Security Helpline Community Documentation, s/f, https://communitydocs.accessnow.org/index.html

La clicka, s/f, http://www.libresenlinea.mx/

La Violencia en Línea Contra las Mujeres en México, *Internet Es Nuestra,* 2017, https://luchadoras.mx/wpcontent/uploads/2017/12/Informe_ViolenciaEnLineaMexico_InternetEsNuestra.pdf

OIT, Gestión de los riesgos psicosociales relacionados con el trabajo durante la pandemia de COVID-19, 2020, https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/instructionalmaterial/wcms_763314.pdf

ARTICLE 19

GUÍA Y RECOMENDACIONES GENERALES SOBRE LA

DOCUMENTACIÓN Y ATENCIÓN DE AGRESIONES DIGITALES