¿CÓMO NOS DEFENDEMOS LAS PERIODISTAS FEMINISTAS FRENTE A LA TECNOVIOLENCIA MACHISTA?

Protocolo de acción con recomendaciones para cuidados digitales personales y gestión segura de medios de comunicación digitales, sitios web y organizaciones.

Con esta guía, desde LatFem pretendemos democratizar estrategias, herramientas, aprendizajes y experiencias. Así como ninguna sale sola de la violencia de género más tradicional, ninguna periodista puede enfrentar sola la tecnoviolencia machista. Este material pudo realizarse gracias al Fondo de Respuesta Rápida (FRR) de Derechos Digitales.

LATFEM

¿CÓMO NOS DEFENDEMOS LAS PERIODISTAS FEMINISTAS FRENTE A LA TECNOVIOLENCIA MACHISTA?

Protocolo de acción con recomendaciones para cuidados digitales personales y gestiónsegura de medios de comunicación digitales, sitios web y organizaciones.

Ciudad Autónoma de Buenos Aires, abril de 2022.

CRÉDITOS

Autora: Azul Cordo
Entrevistas e investigación: Azul Cordo y Carolina Rosales Zeiger
Edición: María Florencia Alcaraz
Diseño: Jimena Zeitune
Coordinación institucional: Mariana Paterlini

¿CUÁLES SON LOS ATAQUES QUE RECIBIMOS LXS PERIODISTAS FEMINISTAS EN EL ÁMBITO DIGITAL?

El primer paso para abordar la tecnoviolencia machista es reconocerla:

AGRESIONES CON DISCURSOS DE ODIO / EXPRESIONES DISCRIMINATORIAS: Cuando publican comentarios agresivos, ofensivos, discriminatorios contra nosotrxs por nuestra condición de género, nacionalidad, raza-etnia, opiniones políticas, creencias, apariencia física, entre otras.

CIBERACOSO Y ACOSO CON MENSAJES PRIVADOS NO DESEADOS: Cuando recibimos en simultáneo muchos mensajes o comentarios en redes sociales, así como fotos o imágenes que no solicitamos; o cuando nos etiquetan en redes sociales con referencias a nuestra persona, a nuestro trabajo, u opiniones sobre cuestiones personales o profesionales.

AMENAZAS: Cuando recibimos mensajes violentos, lascivos, agresivos que tienen la intención de amenazarnos o hacernos daño (amenazas de violencia física o de violencia sexual), contra personas allegadas, contra bienes, o contra nuestro prestigio profesional.

VIGILANCIA, MONITOREO O ACECHO DETECTADO: Cuando realizan una vigilancia constante a nuestra vida en línea (vigilancia al perfil y redes sociales). Ataques a la reputación y abusos basados en la imagen: Cuando publican mensajes que descalifican trayectoria, credibilidad o imagen pública con información falsa, manipulada o fuera de contexto.

JAQUEO (ACCESO O CONTROL NO AUTORIZADO): Cuando alguien entra a nuestros dispositivos, cuentas de redes sociales o correo electrónico sin autorización y desde allí agrede, provoca otros ataques digitales o restringe el acceso a las cuentas y dispositivos.

DIFUSIÓN DE INFORMACIÓN PERSONAL O ÍNTIMA (“DOXING”): Cuando comparten o publican información privada (datos personales, fotografías, vídeos, o capturas de pantalla) de forma intencional.

SUPLANTACIÓN Y ROBO DE IDENTIDAD (“SPOOFING”): Cuando alguien se apropia de nuestra información personal, crea un perfil idéntico y se hacen pasar por nosotrxs para cometer un fraude, dar información falsa, realizar acciones que perjudiquen la imagen de la víctima, o distribuir phishing, malware u otro tipo de piezas de software que permitan efectuar nuevos ataques contra otras personas.

EXTORSIÓN: Cuando nos obligan a hacer algo, bajo la amenaza de difundir información personal en plataformas, sitios web u otros espacios digitales. Abuso sexual relacionado a la tecnología: Cuando nos obligan a mantener alguna relación (virtual o física) o a realizar alguna práctica sexual contra nuestra voluntad, y se contactan a través de redes sociales, llamadas telefónicas o a través de cualquier dispositivo electrónico para obtener un beneficio lucrativo o de otro tipo.

AFECTACIONES A CANALES DE EXPRESIÓN: Cuando las cuentas en redes sociales u otros canales de comunicación son censurados.

→

OMISIONES POR PARTE DE ACTORES CON PODER REGULATORIO: Cuando autoridades, intermediarios de Internet e instituciones que pueden regular, solucionar o sancionar la violencia en línea, actúan con negligencia, tienen falta de interés o directamente no reconocen, solucionan o castigan los ataques digitales que enfrentaste.

Fuentes: ICFJ y UNESCO (2020); Luchadoras (s/f)

¿QUÉ PODEMOS HACER LXS PERIODISTAS FEMINISTAS ANTE LA TECNOVIOLENCIA MACHISTA?

La forma de abordar este tema tiene que ser holística e integral: desde una mirada que considera a los cuidados digitales en una tríada física, psicoemocional y de gestión de los datos y comunicaciones. Escuchar a las personas que son atacadas es siempre lo primero.

Puede que la persona atacada subestime lo sucedido, lo minimice o hasta le parezca gracioso. Si bien no hay recetas ni fórmulas únicas, contar con información puede dar certezas en un momento en el que no se sabe lo que vendrá o cómo continuará el ataque. Las experiencias de los casos de estudio recientes evidencian que es necesario llevar adelante una serie de pasos para anticiparse a las agresiones e ir instalando prácticas de cuidados digitales. No son pasos consecutivos sino que se trata de una serie de acciones posibles que hemos inventariado para este protocolo.

RECOMENDACIONES GENERALES DE CUIDADOS FRENTE A LOS ATAQUES DIGITALES A PERIODISTAS FEMINISTAS Y MEDIOS DE COMUNICACIÓN:

REGISTRAR LOS ATAQUES DIGITALES RECIBIDOS.
Podemos hacerlo nosotrxs mismxs o también pedir ayuda. Si integramos un medio de comunicación u organización es conveniente que el equipo designe unx responsable del registro de incidentes digitales.
Es útil hacer fichas de registro de incidentes en el ámbito digital. “Incidente” es cualquier evento que pueda constituir un abuso, acoso o alguna forma de violencia en línea en Internet y haya supuesto algún riesgo o peligro para nosotrxs o alguien de nuestra organización, medio o colectivo. Es importante utilizar esta herramienta cuanto antes, apenas hayan ocurrido los ataques.

¿Para qué sirve registrar? Documentar los incidentes convierte a las amenazas digitales en algo real que podemos ver y medir. La evidencia de los ataques sirve para reportar ante las plataformas intermediarias o denunciar ante las autoridades y permite encontrar patrones de tecnoviolencias que pasan desapercibidos. Con la información recabada podemos diseñar planes de acción y prevención aterrizados en situaciones puntuales.

ACTIVAR REDES DE APOYO LOCAL Y REGIONAL.
Dar aviso a redes de periodistas y comunicadoras feministas para que den acompañamiento y ayuden a la estabilidad emocional, así como contactar a organizaciones ciberfeministas para asesoramiento. Pueden ser redes formales (asociaciones) o informales (grupos de Whatsapp).
En esta instancia es conveniente hacer un "análisis de riesgo" colectivo y luego decidir si actuaremos: se puede hacer desde una denuncia ante las plataformas o un bloqueo masivo de las cuentas que están atacando. También podemos redactar un comunicado público para denunciar y advertir sobre esta situación. Son formas de dejar registro. No toda denuncia tiene que ser en sede judicial.

BUSCAR APOYO DEL SINDICATO DE PRENSA LOCAL y analizar qué estrategia de acompañamiento, difusión y/o denuncia pueden dar al caso de ataque digital.

REALIZAR UN ANÁLISIS DE RIESGO con organizaciones ciberfeministas. Es fundamental que la persona u organización tome conciencia de las amenazas que enfrenta, reconozca las propias vulnerabilidades e incremente las capacidades para tener el menor riesgo posible.

IDENTIFICAR LOS INTERESES, RECURSOS Y MOTIVACIONES DE LOS ACTORES QUE ESTÁN DETRÁS DE LAS AMENAZAS EN NUESTRA CONTRA, ASÍ COMO SUS REDES.
Es importante identificar aquellos aliados de los actores oponentes que se mueven en el ámbito digital.

NOTIFICAR O DENUNCIAR ANTE LAS AUTORIDADES CORRESPONDIENTES EN CADA PAÍS.
Es útil contactar a la Defensoría del Público, el Tribunal de Ética, o el Ministerio del Interior, según la estructura institucional de cada país.

IGNORAR PÚBLICAMENTE TAMBIÉN ES UNA OPCIÓN.
Muchas veces los agresores buscan llamar la atención, desviar la conversación o tener una respuesta. Podemos ignorarlos públicamente y desplegar acciones en el ámbito privado. No toda respuesta es pública.

RECOMENDACIONES SI EL ATAQUE ES CONTRA UN SITIO WEB O REDES SOCIALES DE UN MEDIO DE COMUNICACIÓN FEMINISTA U ORGANIZACIÓN:

BUSCAR APOYO DE PERSONAS DE CONFIANZA y abrir un diálogo sobre la situación para conformar un equipo que maneje la misma información.

ANALIZAR LA SEGURIDAD DE LA PÁGINA WEB y tomar las medidas necesarias para proteger la información que esta contiene.

HACER COPIAS DE SEGURIDAD FÍSICAS Y DIGITALEs del archivo de tu trabajo y/o el medio digital en el que trabajas en redes.

REVISAR LA CONFIGURACIÓN de las cuentas de lxs integrantes y de las colectivas.

HACER UN ANÁLISIS INDIVIDUAL DE CUENTAS y de configuración de las mismas.

HACER UN ANÁLISIS INDIVIDUAL DE WIFI siguiendo este documento.

U**SO DE CONTRASEÑAS SEGURAS** actualizadas cada 3 meses.

DESIGNAR UN RESPONSABLE del registro de incidentes digitales

CONTAR CON ACOMPAÑAMIENTO PSICOSOCIAL. Solicitar un diagnóstico psicosocial colectivo y, si el caso lo requiere, acompañamientos individuales.

CUIDADOS DIGITALES PERSONALES: ¿CÓMO PREVENIR NUEVOS INCIDENTES Y SOSTENER EL AUTOCUIDADO DIGITAL?

MANEJAR DOS O MÁS PERFILES: uno personal para estar en contacto con amigas y familia y otro del medio donde trabajamos.

USAR CONTRASEÑAS SEGURAS EN CELULARES. Cambiar frecuentemente las contraseñas de nuestras cuentas y correo electrónico y evaluar ciertas medidas como cambiar durante unos días nuestro perfil público a privado.
·Respaldar la información guardada en celulares, computadoras y memorias externas.

REVISAR QUÉ MEDIDAS DE SEGURIDAD TENEMOS sobre nuestras cuentas en redes sociales, qué configuraciones de seguridad tienen Facebook, Twitter, Instagram, Tik Tok, entre otras.

DESACTIVAR LA GEOLOCALIZACIÓN.

BLOQUEAR Y SILENCIAR EN TWITTER. En esta red social se puede bloquear y silenciar individualmente. Bloquear eliminará de nuestro timeline los tuits de una cuenta que nos acose e impedirá a esa persona ver nuestra cuenta de Twitter. Al silenciar dejarás de ver los tuits de una cuenta en nuestro timeline pero esa cuenta no será notificada.

VIGILAR LA INFORMACIÓN ONLINE. Desde Ciberseguras recomiendan opciones gratuitas como Google Alerts y Talkwalker Alerts, que envían avisos por correo electrónico cuando nuestro nombre aparezca online. Podemos buscar también nuestros apodos habituales, formas incorrectas de nuestro nombre, nuestro número de teléfono y domicilio para revisar si alguien los está compartiendo públicamente.

BUSCAR IMÁGENES Y FOTOS que puedan estar vinculadas a nuestra persona. Podemos hacer una búsqueda reversa de imágenes a través de sitios como Google Images o Tineye, que realizan una búsqueda a través de todos los sitios indexados de la web al subir una imagen.

CREAR ESTRATEGIAS PARA CONTACTO DE LAS FUENTES: evitar una conversación completa en Whatsapp o vía mensaje de texto; usar plataformas seguras para llamadas y mensajes (Jitsi, Signal); usar estrategias mixtas como iniciar contactos vía digital y luego seguir de manera presencial.

LATFEM