Committee to Protect Journalists

Elecciones presidenciales del 2024 en Estados Unidos: Kit de seguridad del periodista

Partidarios de los manifestantes que fueron arrestados en el ataque del 6 de enero de 2021 contra el Capitolio federal, se reúnen frente a la sede de la Corte Suprema de Justicia de Estados Unidos en Washington, D.C., en el segundo aniversario de la insurrección. (Foto: Getty Images / Tasos Katopodis / Getty Images mediante AFP)

Las elecciones presidenciales del 2024 en Estados Unidos se celebrarán el martes 5 de noviembre en un clima político cada vez más polarizado. Es muy probable que el gremio periodístico, además de sentir un elevado nivel de desconfianza respecto a la prensa, tenga que hacer frente a significativos desafíos de seguridad en la antesala de las elecciones, al igual que en la jornada de votación.

Las disputadas elecciones del 2020 y el ataque del 6 de enero del 2021 contra el Capitolio federal han contribuido al auge del extremismo interno y al aumento de la presencia de milicias con motivaciones políticas, las que pueden aparecer en actos políticos y en centros de votación en ciertos estados del país. Como consecuencia, los periodistas pueden ser objeto de represalias, entre ellas el hostigamiento físico, la obstrucción y el abuso verbal. Los trabajadores de medios que dan cobertura a las elecciones deben ser conscientes de que pueden ser víctimas de mayor acoso en la Internet, inclusive de doxeo, y de campañas de desinformación selectivas concebidas para socavar a la prensa. Lo anterior resalta el ambiente cada vez más hostil que viven los periodistas en Estados Unidos, donde hubo como mínimo 40 agresiones contra periodistas en 2023, según el U.S. Press Freedom Tracker, un sitio web que recopila exhaustivamente las violaciones de la libertad de prensa en Estados Unidos y del cual el CPJ es miembro fundador.

La guía que sigue a continuación ha sido concebida para ayudar a las Redacciones y a los periodistas a tener presente y gestionar el riesgo físico y digital en lo referente a la cobertura de las elecciones en Estados Unidos.

Committee to Protect Journalists

Contenido

Committee to Protect Journalists

Lista de verificación del editor

Tener una breve conversación con el editor puede aumentar la conciencia del riesgo y reforzar su seguridad. La siguiente lista de verificación facilita que los editores preparen a periodistas y trabajadores de medios de la mejor manera posible para cubrir puntos de conflicto electoral o realizar coberturas riesgosas.

Al seleccionar su equipo periodístico, tome en cuenta lo siguiente:

- ¿Qué experiencia tienen los periodistas?
- ¿Han cubierto noticias de gran tensión o de intensa emoción que pueden provocar un estallido de violencia?
- ¿Tienen un historial de tomar buenas decisiones en situaciones de presión?
- Si tienen menos experiencia, ¿qué mecanismos de apoyo usted puede implementar para aumentar su protección? Por ejemplo, ¿un periodista más avezado pudiera encargarse de la Mesa de Asignaciones y ofrecer orientación si fuera necesario?
- ¿Su equipo está preparado mentalmente para hacer frente a personas agresivas?
- En las coberturas de mayor riesgo, ¿usted puede enviar a dos periodistas, para que nadie trabaje solo?
- Tenga en cuenta que revelar la identidad del periodista pudiera aumentar las posibilidades de que sufra alguna agresión, por lo que debe planificar en consecuencia. En algunos casos, la identidad de un periodista también puede contribuir a mantenerlo sano y salvo.
- ¿Tienen conocimiento local sobre la zona en la que trabajarán?

Durante la evaluación de riesgo, valore:

- Crear un procedimiento para reportarse.
- Qué imágenes o grabaciones son necesarias para realizar la cobertura. No tiene sentido quedarse en un acto masivo riesgoso recopilando grabaciones que no se utilizarán.
- Realizar una evaluación del riesgo dinámica y utilizar el modelo de evaluación del riesgo elaborado por el CPJ.
- La posibilidad de ataques en la Internet como resultado de la cobertura electoral. Revise la lista de verificación del editor sobre cómo proteger a los periodistas de la Redacción y a los periodistas *freelance* contra el ciberabuso, elaborada por el CPJ.
- En qué señales fijarse para tomar la decisión de retirar al equipo del lugar de la cobertura.
- Tomar nota de los datos y contactos de emergencia de todos los miembros del equipo periodístico que participan en la cobertura.

Para estar más alerta cuando el equipo esté en el terreno, recomiende a los periodistas:

- Consultar la guía de seguridad elaborada por el CPJ sobre cómo utilizar la conciencia situacional.
- Actuar con discreción y evaluar el estado de ánimo de las multitudes respecto a la prensa. Comportarse siempre de manera discreta al reportar o grabar, especialmente cerca de personas que estén armadas o sean agresivas.
- Reportarse periódicamente con el editor o la persona de contacto en la Redacción. Si usted trabaja como periodista *freelance*, valore crear un procedimiento para reportarse con otro periodista, un familiar o un amigo.
- Comprobar que su teléfono móvil esté cargado completamente y considerar llevar consigo una batería portátil.
- Dedicar tiempo para planificar una estrategia de salida, por si la situación se vuelve violenta. Buscar lugares para refugiarse si logra escapar o hasta que llegue ayuda.
- Si trabaja solo o cuando ya oscureció, debe estar más alerta, porque aumenta el riesgo.
- Evitar a las personas que estén drogadas o ebrias.
- Si es posible, tratar de establecer una relación con una persona antes de entrevistarla.
- Al realizar una entrevista, evalúe la situación. ¿Está rodeado de otras personas que puedan interesarse en la cobertura? En muchas ocasiones las personas que están alrededor de uno son las que crean problemas, no los entrevistados.
- Cuando esté en el teléfono o transmitiendo una nota o una grabación, asegurarse de estar en un espacio protegido, desde donde pueda ver cualquier amenaza que surja.
- En general, debe prepararse para lo acosen verbalmente, lo intimiden y hasta lo escupan. Mantenga la calma y no caiga en ninguna provocación.
- Valorar qué tipo de ropa debe llevar. Evite llevar ropa de tejidos inflamables como el nailon, o cualquier vestimenta holgada y que se pueda agarrar. Evite usar el logo del medio de prensa y consignas políticas, así como ropa de camuflaje o vestimenta de color negro, que con frecuencia es usada por grupos antifascistas de extrema izquierda.
- Si ocurre algún incidente, tomar nota de lo que sucedió e informar a las autoridades pertinentes.
- Observar constantemente el estado de ánimo y la actitud de las autoridades. Señales visuales como policías con equipo antidisturbios, barreras de escudos o el lanzamiento de objetos son posibles indicadores de que se puede esperar una agresión. Retírese a un lugar seguro cuando semejantes señales de advertencia sean evidentes.
- En general, prepárese para escapar de la situación si siente que aumenta el riesgo o que recurrir a las autoridades sería por gusto.
- Si abandona el lugar, retírese a un lugar seguro antes de reportarse con la Redacción o con la persona de contacto.

Concentración en la Plaza Black Lives Matter, frente a la Casa Blanca, en Washington, D.C. el 8 de noviembre de 2020. (Foto: Daniel Slim / AFP)

Seguridad física: cómo cubrir actos y concentraciones electorales

La muerte de George Floyd y de Breonna Taylor en 2020 puso de manifiesto el menosprecio público y violento de la Policía por el periodismo. La Policía no defendió garantías constitucionales básicas de los periodistas, lo cual provocó arrestos injustos y tácticas de supresión en protestas pequeñas y grandes, según un informe publicado en el 2023 por la Fundación Knight.

Para reducir al mínimo los riesgos al cubrir actos y concentraciones electorales:

- Planifique la cobertura y estudie la zona a la cual se dirige. Decida de antemano lo que haría en caso de emergencia. Lleve un kit de primeros auxilios si sabe cómo utilizarlo.
- Asegúrese de que la batería de su teléfono esté completamente cargada y valore si debe llevar una batería portátil.
- Lleve ropa sin el logo de su medio de comunicación y, si es necesario, retire el logo de su medio de los equipos de trabajo y vehículos. Lleve vestimenta y calzado adecuados.
- Siempre trate de que un compañero lo acompañe, y cree un procedimiento para reportarse periódicamente con sus contactos, particularmente si cubre actos masivos o concentraciones.
- Lleve ropa y calzado que le permita moverse con rapidez. Evite la ropa holgada y cordones para credenciales, ya que los pueden agarrar. Evite también la ropa de material inflamable (por ejemplo, nailon).

- Evalúe su posición en el terreno. Si puede, busque un punto de observación elevado donde pueda estar más protegido.
- En todo lugar, siempre tenga una ruta de evacuación y un punto para encuentro de emergencia si trabaja en equipo. Conozca la ubicación del punto más cercano donde pueda recibir atención médica.
- Mantenga la conciencia situacional en todo momento y limite la cantidad de pertenencias que lleva. No deje ningún equipo de trabajo en los vehículos, ya que alguien puede forzarlos. Cuando oscurece, aumenta el riesgo de actividad criminal.
- Si está trabajando en una multitud, tenga una estrategia. Es prudente mantenerse afuera de la multitud y evitar que lo arrastren hacia el medio, de donde es difícil escapar. Busque una ruta de escape y tenga un punto para encuentro de emergencia si trabaja en equipo.
- En general los reporteros gráficos tienen que estar en el centro de la acción, por lo que corren más riesgo. Los reporteros gráficos deben ir acompañados de alguien que los vigile, y deben recordar levantar la mirada del visor cada varios segundos. No lleve la correa de la cámara alrededor del cuello, para evitar que lo estrangulen. Con frecuencia los reporteros gráficos no pueden darse el lujo de trabajar desde lejos, por lo que es importante reducir al mínimo el tiempo que se pasa entre la multitud. Grabe las imágenes que necesita y salga.
- Todos los periodistas deben ser conscientes de no permanecer demasiado tiempo en una multitud, que se puede volver hostil rápidamente.
- Valore si es necesario contratar vigilancia si el riesgo es alto. Un vigilante local contratado para protegerlo a usted y a su equipo de trabajo puede estar alerta a una amenaza que surja, mientras usted se concentra en el trabajo.
- La Policía en Estados Unidos ha utilizado gases lacrimógenos, bastones, proyectiles de gas pimienta y balas de goma para dispersar multitudes. Valore utilizar elementos de protección personal y, si esto no es apropiado, preste atención a la Policía. Si ve armas de fuego, protéjase detrás de una superficie dura y no se quede en un lugar que pueda servir de salida, por si ocurre una estampida.

Para reducir al mínimo el riesgo ante la presencia de gases lacrimógenos:

- Debe utilizar elementos de protección personal como máscara antigás, gafas protectoras y un respirador.
- Las personas asmáticas o con problemas respiratorios deben evitar las zonas donde las autoridades lancen gases lacrimógenos. Tampoco se aconseja usar lentes de contacto. Si las autoridades lanzan grandes cantidades de gas lacrimógeno, puede que haya altas concentraciones de gas en áreas sin movimiento de aire.
- Tome nota de posibles puntos de referencia (por ejemplo, postes, bordillos) que se puedan utilizar para orientarse y salir del lugar si no puede ver con facilidad.

- Si se expone a los gases lacrimógenos, busque un terreno alto y coja aire fresco para que la brisa se lleve el gas. No se restriegue ni los ojos ni la cara, pues eso puede empeorar la situación. Si es posible, dese una ducha de agua fría para quitarse el gas de la piel, pero no se sumerja en la bañadera. Es posible que tenga que lavar la ropa varias veces para eliminar los residuos completamente, o hasta desecharla.

Seguridad física: cómo hacer frente a una agresión

- Lea el lenguaje corporal de las personas, y utilice su propio lenguaje corporal para calmar una situación.
- Mantenga el contacto visual con el agresor, haga gestos con las manos abiertas y hable en tono calmado.
- Deje un espacio del largo de un brazo extendido entre usted y la amenaza. Si lo agarran, sepárese firmemente sin agredir a la persona. Si está arrinconado y en peligro, grite.
- Si la situación se agrava, deje una mano libre para protegerse la cabeza y muévase con pasos cortos y firmes para no caer. Si está trabajando en equipo, únase a sus compañeros y formen una cadena con los brazos.
- Esté consciente de la situación y de su propia seguridad. Si bien hay momentos en que documentar una agresión puede tener valor noticioso, tomar fotos de personas agresivas puede empeorar una situación.

Seguridad física: cómo hacer frente a extremistas armados

Las milicias han hecho sentir su presencia en el espacio político estadounidense en los últimos años. La mayoría de estos grupos se oponen a los poderes del Gobierno y de los organismos del orden público, aunque algunos se consideran posibles aliados de ciertos organismos de seguridad. Un informe de ISD Global afirma que las ideologías extremistas han evolucionado constantemente en las últimas dos décadas y que ha surgido una generación más joven de extremistas. Lo anterior se puede atribuir al uso de plataformas digitales para llegar a mayores audiencias y promocionar ideologías extremas al conjunto de la sociedad.

Las investigaciones de ACLED muestran que grupos como Three Percenters, Proud Boys, Patriot Prayer y Boogaloo Bois tienen un historial, en ocasiones amplio, de emplear la violencia en época electoral. Desde las elecciones del 2020, las milicias de extrema derecha han estado implicadas en el 91 % de las manifestaciones violentas, según ACLED.

De acuerdo con ACLED, los grupos extremistas adoptan tácticas híbridas. Es común que estos grupos entrenen para el combate urbano y rural y al mismo tiempo difundan mensajes propagandísticos y de relaciones públicas para interactuar con una audiencia mayor. A menudo, estos grupos adoptan papeles de supuesta “protección pública” que aumentan la amenaza que enfrentan los periodistas. Entre los lugares donde pudiera haber estallidos de violencia se encuentran los estados péndulo, capitales estatales, poblados periféricos y zonas suburbanas y rurales.

Se ha documentado ejemplos de extremistas y miembros de milicias armados que se colocan como supuestos "vigilantes de urnas" en los centros de votación, con el aparente propósito de intimidar y acosar a los votantes y a los trabajadores electorales.

Debe tomarse en cuenta lo siguiente a la hora de reportar desde lugares con posible presencia de extremistas armados:

- Cree un plan de acción con su editor que incluya indicadores para retirarse.
- Planifique reportarse periódicamente con su editor o con su contacto en la Redacción. Si trabaja como periodista *freelance*, valore crear un procedimiento para reportarse con otro periodista, un familiar o un amigo.
- Siempre que sea posible, evite trabajar solo. Un compañero puede vigilarlo mientras usted se concentra en la cobertura.
- Estudie el lugar de la cobertura. Si es posible, revise en persona el lugar o utilice la función Google Street View para detectar cualquier punto de difícil acceso y así evitar quedar atrapado en la posición de la cobertura.
- Observe continuamente la atmósfera y el comportamiento de las personas. Retírese a un lugar seguro cuando vea señales de advertencia que indiquen una agresión, o cuando vea que están lanzando proyectiles.
- Tenga un plan de escape. Asegúrese de estacionar los vehículos en lugares con claras rutas de salida.
- Evalúe si mostrar el logo de su medio de comunicación o su credencial de prensa puede causarle problemas y aumentar el riesgo personal.
- Estudie las leyes federales y estatales relacionadas con la posesión de armas de fuego y la actividad paramilitar, para entender los tipos de conducta que podrían ser ilegales.
- Consulte las recomendaciones anteriores sobre cómo hacer frente a una agresión.

La candidata presidencial republicana y exembajadora de Estados Unidos ante las Naciones Unidas Nikki Haley, vista desde el teléfono de una reportera, cuando responde una pregunta de los medios luego de una visita de campaña a Newberry, Carolina del Sur, el 10 de febrero de 2024. (Foto: Elijah Nouvelage / Reuters)

Seguridad digital: el ciberacoso, las campañas de desinformación y el doxeo

Es probable que el ciberacoso y las campañas de desinformación contra periodistas aumenten durante el período electoral. Los periodistas y trabajadores de medios enfrentan un entorno digital cada vez más hostil, lo cual es exacerbado por la difusión de desinformación y de información falsa, y con frecuencia son acosados en la Internet por personas que quieren desprestigiarlos. A menudo, estos ataques consisten en campañas coordinadas que pueden hacer que el periodista deje de usar las redes sociales y, en la práctica, expulsarlo de la Internet. Protegerse contra el ciberacoso no es fácil; sin embargo, mientras más usted pueda protegerse antes de un ataque, más seguro estará.

Medidas esenciales para protegerse del doxeo

- De manera periódica, búsquese en la Internet y elimine información de carácter personal.
- Para eliminar datos personales, inscríbase en servicios como DeleteMe.
- Proteja las cuentas con la autenticación de dos factores.
- Hable con familiares y amigos sobre lo que usted desea compartir o no en la Internet.
- Elabore un plan de lo que debe hacer si es víctima de doxeo.

Para reducir al mínimo el riesgo:

Proteja los datos personales

- Algunos datos son más importantes que otros. Siempre que sea posible, es mejor no hacer pública ninguna información que se pueda utilizar para localizarlo, para comunicarse con usted por medios que no desee, o para confirmar su identidad. Esta información abarca la dirección particular, el número telefónico móvil personal y otros datos como el número del Seguro Social y la fecha de nacimiento. Con frecuencia esta información se utiliza para amenazar a periodistas en la Internet y para robarles la identidad.

- Compruebe si su dirección particular y otros datos personales como su fecha de nacimiento y su número telefónico están disponibles en la Internet. Debe encargarse de eliminar esa información o solicitar que la eliminen, siempre que sea posible. Para más información, consulte la guía elaborada por el CPJ sobre cómo eliminar los datos personales de la Internet.

- Inscríbase para que le eliminen la información personal de los sitios web de intermediarios, utilizando servicios como DeleteMe, que es propiedad de la empresa Abine. Tenga en cuenta que estos servicios eliminan los datos de los sitios web de intermediarios más comunes, por lo que su información personal probablemente seguirá existiendo en la Internet de alguna u otra manera. Valore inscribir a sus familiares, si considera que corre un gran riesgo de ser acosado. Tenga presente que eliminar los datos puede demorar hasta un mes.

- Revise su perfil digital en busca de imágenes e información que pudieran manipularse o utilizarse para desacreditarlo. Los periodistas deben tomar medidas para eliminar toda información que crean que pueda ser utilizada contra ellos.

- Durante el período electoral, vigile sus cuentas de redes sociales para ver si el acoso y los comentarios abusivos han aumentado.

- Tenga en cuenta que, con frecuencia, el abuso en la Internet se incrementa durante los períodos electorales, y pudiera incluir campañas de desprestigio selectivas contra un periodista o su medio de comunicación.

Proteja sus cuentas

- Proteja sus cuentas creando contraseñas largas y distintas para cada cuenta. Active la autenticación de dos factores en todas sus cuentas. Lo ideal es utilizar una aplicación y no el teléfono para recibir el código. Una alternativa es proteger las cuentas utilizando una clave de paso, también conocida como clave de acceso. Consulte el kit de seguridad digital elaborado por el CPJ para conocer más sobre la seguridad de las cuentas.

- Revise los ajustes de privacidad en sus cuentas de redes sociales. Puede conocer más sobre qué datos es mejor no publicar en la guía elaborada por el CPJ sobre cómo eliminar los datos personales de la Internet. Las cuentas de redes sociales también pueden revelar su ubicación, por lo que debe desactivar el rastreo de ubicación si piensa que lo puede poner en riesgo.

- Desactive la geolocalización de las publicaciones en todas las cuentas. Si va a publicar fotos que muestran su ubicación exacta, valore esperar hasta que haya salido de la zona.
- Siempre que sea posible, cree cuentas profesionales para las redes sociales.

Prepárese contra el ciberacoso

- Si puede, hable con su editor o con la Redacción sobre cualquier preocupación que tenga respecto a la posibilidad del ciberacoso. Compruebe si su medio de comunicación tiene alguna política sobre el ciberacoso o algún sistema de apoyo para los periodistas que sean atacados en la Internet. Los editores pueden consultar la lista de verificación previa a la cobertura, elaborada por el CPJ, sobre cómo proteger a los periodistas contra el ciberacoso.
- Distintas coberturas implican distintos riesgos en la Internet. Hable con su editor sobre la posibilidad de amenazas y cómo mitigarlas, incluyendo las medidas preventivas que usted pueda tomar. Pregunte si otros periodistas que hayan trabajado en coberturas similares han sido objeto de abuso en la Internet. Tenga en cuenta que corre mayor riesgo de un ataque en la Internet luego de publicar una noticia.
- Conozca qué tipo de apoyo puede ofrecer la Redacción. Por ejemplo, ¿puede proporcionarle apoyo de informática o apoyo de salud mental?
- Realice una evaluación del riesgo en materia de seguridad digital. Para comenzar, utilice el modelo elaborado por el CPJ.
- Hable con familiares y amigos sobre la amenaza del ciberacoso y qué tipo de información usted quiere que se publique o no en la Internet. En muchos casos, los periodistas pueden ser objeto de doxeo o de ataques con contenido publicado por amigos y familiares.

Cómo gestionar las agresiones en la Internet

Existen distintos tipos de ataques en la Internet y es probable que su respuesta varíe de acuerdo con la amenaza. Consulte los pasos a continuación para orientarse.

- Si en la Internet están circulando datos personales suyos como la dirección particular o el número de su teléfono móvil personal, esto significa que usted corre mayor riesgo.
- Trate de no interactuar con las personas que lo acosan en la Internet, pues eso puede empeorar la situación. Si es blanco de una campaña de desprestigio organizada, puede ser útil escribir una declaración factual que describa la situación y fijarla en la parte superior de sus cuentas de redes sociales. Los medios de prensa también pueden redactar declaraciones de apoyo como forma de contrarrestar una campaña selectiva.
- Valore convertir todas sus cuentas de redes sociales en cuentas privadas, y pídales a sus familiares que hagan lo mismo.

- Informe a sus familiares, empleados y amigos que lo están hostigando en la Internet. Con frecuencia los adversarios se comunican con los familiares de un periodista y con su lugar de trabajo, y les envían información o imágenes para perjudicar su reputación.
- Hable con la Redacción para ver qué tipo de apoyo le pueden ofrecer. Si usted es un periodista freelance, o su Redacción no sigue ninguna política al respecto, puede consultar el centro de recursos sobre el ciberacoso, creado por la Coalición contra la Violencia en la Internet.
- Esté alerta a un posible intento de jaqueo contra sus cuentas, y asegúrese de revisar sus ajustes de privacidad, activar la autenticación de dos factores y crear contraseñas largas y distintas para cada cuenta.
- Revise sus cuentas de redes sociales en busca de comentarios que puedan indicar que una amenaza en la Internet puede agravarse y convertirse en un ataque físico. Ejemplos de lo anterior son cuando alguien publica la dirección suya en la Internet y exhorta a otras personas a atacarlo, o cuando un individuo en particular aumenta el acoso contra usted. Pídale a una persona de confianza que lo ayude a revisar las menciones de su nombre y vigilar su cuenta, para proteger su salud mental si usted no es capaz de vigilar su cuenta.
- Documente todo intento de acoso que sienta que es amenazante. Haga capturas de pantalla de los comentarios, e incluya la cuenta de redes sociales de la persona que lo amenaza. Esta información puede ser útil si luego hay una investigación policial.
- Quizás deba bloquear o silenciar a las personas que lo acosan en la Internet. También debe reportar todo contenido abusivo a las empresas de redes sociales y a los proveedores de correo electrónico. Guarde copias de su contacto con estas empresas.
- Quizás deba salir de la Internet por un tiempo, hasta que se haya calmado el acoso.

Para más información y sugerencias sobre cómo protegerse en la Internet, consulte la lista de recursos para protegerse contra el ciberacoso, creada por el CPJ.

El Comité para la Protección de los Periodistas (CPJ, por sus siglas en inglés) es un miembro de la Coalición contra la Violencia en la Internet, un grupo de organizaciones internacionales que buscan mejores soluciones para las periodistas que enfrentan acoso, hostigamiento y otras formas de ataque digital en el ciberespacio.

Periodistas toman fotos de una persona que protestaba frente a la sede de los Juzgados Penales (Criminal Courts Building) mientras un gran jurado conocía las pruebas contra el expresidente Donald Trump el 22 de marzo de 2023 en la ciudad de Nueva York. (Foto: Scott Olson / Getty Images North America / Getty Images mediante AFP)

Seguridad digital: cómo proteger los dispositivos y su contenido

Es importante seguir las mejores prácticas a la hora de proteger los dispositivos y su contenido. Si lo detienen cuando esté cubriendo las elecciones, es posible que le quiten los dispositivos y los inspeccionen, lo que pudiera tener serias consecuencias para usted y sus fuentes. El allanamiento policial realizado el año pasado contra el periódico de Kansas *The Marion County Record*, como lo documentó el CPJ, resalta la importancia de que las Redacciones almacenen sus datos de manera segura. Las siguientes medidas pueden ser útiles:

Seguridad digital: mejores prácticas generales para cubrir actos y concentraciones electorales

- Bloquee las computadoras portátiles y los teléfonos con un PIN o una contraseña. Así protegerá mejor el contenido de sus dispositivos si se los quitan.
- Tenga en cuenta que las autoridades pudieran tener acceso a su teléfono incluso si está protegido con un código. Utilizar la identificación biométrica puede ser útil si necesita acceder rápidamente a su teléfono, pero los periodistas deben tener presente que también puede permitir a otras personas, como las autoridades, obtener acceso más fácilmente a su dispositivo. Conozca sus derechos con respecto a lo que las autoridades pueden y no pueden hacer con sus dispositivos y el contenido almacenado en ellos.
- Actualice el sistema operativo cuando el dispositivo se lo indique, para protegerlo contra los últimos programas maliciosos, incluyendo el software de espionaje.

- Active la encriptación en sus dispositivos si no está habilitada por defecto.
- No descuide los dispositivos en público, inclusive cuando los esté cargando, para evitar que los roben o los alteren.
- Evite utilizar memorias USB que sean repartidas en actos electorales, pues podrían contener programas maliciosos que pudieran infectar sus dispositivos.
- Sea consciente de que cualquier conversación telefónica o mensaje SMS que se envíe por medio de un operador móvil puede interceptarse y el contenido revelarse. Para evitar esto, utilice aplicaciones de mensajería con encriptación de extremo a extremo como WhatsApp y Signal. Conozca más sobre cómo utilizar estas aplicaciones de manera segura en la guía del CPJ sobre comunicaciones encriptadas.
- Tenga en cuenta que los contactos de su teléfono pueden almacenarse en más de un lugar, como en las aplicaciones del teléfono o en una cuenta en la nube vinculada con el teléfono como Google Drive o iCloud. Dedique tiempo a revisar sus contactos y borre a toda persona que pudiera estar en riesgo si a usted le quitan los dispositivos y los inspeccionan.
- Cuando esté cubriendo el acto, siga un procedimiento para proteger las grabaciones y demás contenidos que haya recogido. Así, si lo detienen, las autoridades solamente tendrán acceso al contenido más reciente y no a todos los materiales. Para más información, revise las recomendaciones del CPJ sobre el riesgo de arresto y detención.
- Anote en un papel o en su brazo los datos de contacto de personas clave, como su editor o un compañero de confianza, por si lo detienen y le quitan los dispositivos. Valore anotar el número de un asesor legal. El Reporters Committee for Freedom of the Press tiene una línea telefónica de asistencia legal para periodistas que trabajan en Estados Unidos.
- Piense si debe configurar los dispositivos para que borren su contenido a distancia. Esto borrará todo el contenido de su teléfono o computadora portátil cuando esté activado, pero solamente si el dispositivo está conectado a una señal WiFi o de datos móviles. Tendrá que configurar el borrado a distancia por adelantado, y debe darle a una persona de confianza la contraseña para que pueda borrar el contenido si a usted lo detienen.
- Tenga en cuenta que hacer una directa desde un acto puede revelar su ubicación.
- Lo ideal es que los periodistas no lleven sus teléfonos personales a cubrir una concentración o protesta. Si usted trabaja para un medio que tenga presupuesto para pagar por un teléfono de trabajo, debe solicitar uno.

Los periodistas que lleven el teléfono personal deben tomar las siguientes precauciones para proteger sus datos:

- Revisar la información que esté almacenada en los dispositivos, incluidos teléfonos y computadoras. Cualquier cosa que lo ponga en riesgo o contenga información delicada debe protegerse con una copia de respaldo y luego borrarse. Puede hacer una copia de respaldo conectando el teléfono a la computadora mediante un cable USB, o en la nube. Los periodistas deben ser conscientes de que existen formas de recuperar la información borrada si le quitan los dispositivos y los inspeccionan.
- Al revisar el contenido del teléfono, los periodistas deben chequear la información almacenada en las aplicaciones y en la nube.
- Piense en qué aplicaciones necesitará en el dispositivo para cubrir una concentración o una protesta. Las aplicaciones de correo electrónico y redes sociales contienen gran cantidad de información personal que las autoridades u otras personas pueden obtener si le quitan el teléfono. Piense en desinstalar temporalmente las aplicaciones que no va a necesitar. Puede instalarlas de nuevo cuando haya terminado de cubrir el acto.

Seguridad digital: mejores prácticas generales para proteger los datos en la Redacción

Estas recomendaciones son para medios noticiosos pequeños y medianos que quizás no tengan un departamento de informática especializado.

- Realice un análisis de los datos que tiene la Redacción y dónde están almacenados física y digitalmente. Esto puede abarcar los datos almacenados en dispositivos en la oficina, en los dispositivos de trabajo en los hogares de los periodistas, en los teléfonos personales y de trabajo, y en las cuentas en la nube y en discos duros externos.
- Conozca qué datos es esencial proteger y comprenda cuál pudiera ser la amenaza. Por ejemplo, pudiera ser una orden judicial, un intento de jaqueo o un acceso no autorizado a documentos. Comprender el tipo de amenaza lo ayudará a decidir qué medidas debe tomar para proteger la información.
- Comprenda los términos y servicios de las empresas de Internet que usted utiliza. Averigüe cómo las empresas almacenan los datos, por cuánto tiempo los almacenan, si han tenido alguna vulneración de datos, y si han acatado solicitudes judiciales de datos. Esto lo ayudará a decidir si la Redacción debe utilizar determinado servicio o si utilizarlo pone en riesgo los datos y las fuentes periodísticas.

- Proteja las cuentas activando la autenticación de dos factores (2FA). Utilice una aplicación como Authy para recibir el código y asegúrese de tener una copia de los códigos de respaldo de cada cuenta en la cual esté activada la autenticación de dos factores. Utilice un gestor de contraseñas para generar contraseñas largas con un mínimo de 15 caracteres. Cada cuenta debe tener una contraseña distinta. Si corre un gran riesgo de sufrir un intento de phishing, valore utilizar la opción de clave de paso para proteger la cuenta. Inste a los periodistas de la Redacción y a los periodistas freelance a hacer lo mismo con sus cuentas personales, incluyendo las de redes sociales. Esto lo ayudará a proteger mejor las cuentas de intentos de jaqueo. Conozca más sobre la seguridad de las cuentas en el kit de seguridad digital elaborado por el CPJ.

- Tome medidas para encriptar los datos:

    - Active la encriptación de las computadoras portátiles y de escritorio. Utilice Bitlocker para Windows Pro y FireVault para Mac. También puede utilizar estos programas para encriptar discos duros externos.

    - Encripte el sistema de respaldo en la nube utilizando Cryptomator. También puede utilizar Cryptomator para encriptar documentos o carpetas individuales.

    - Asegúrese de que los teléfonos están encriptados. Los usuarios de Android deben activar la encriptación en la sección de ajustes del dispositivo. En el iPhone la encriptación viene instalada de serie, pero los periodistas deben asegurarse de que el sistema de respaldo en la nube esté encriptado, activando para ello la opción de protección avanzada de datos en sus dispositivos.

- Proteja con una contraseña o un PIN todas las computadoras portátiles y de escritorio y los teléfonos. Sea consciente de que los agentes del orden público pudieran solicitarle que los desbloquee. Conozca sus derechos respecto al desbloqueo de los dispositivos.

- Para reducir el acceso no deseado a los documentos almacenados en la nube, permita el acceso solamente a las personas que deban conocerlos, y proteja los documentos y carpetas con una contraseña o un PIN.

- Cree una política de retención de datos para la Redacción, en la cual especifique dónde deben almacenarse los datos, con qué frecuencia se deben respaldar los datos y por cuánto tiempo se deben almacenar.

- Siga un procedimiento de integración de nuevos empleados y un documento que estipule cómo y cuándo se dará acceso a las cuentas, y asegúrese de revocar el acceso a las personas que ya no trabajen en el medio de prensa.

- Conozca sus derechos para el caso de que las autoridades confisquen los datos.

Para recibir asistencia adicional, para hablar directamente con el equipo de Emergencias del CPJ o para solicitar capacitación en seguridad para usted o su organización de noticias, escríbanos a emergencies@cpj.org. Podrá encontrar otros recursos sobre seguridad física, seguridad digital y salud mental en la página de Emergencias del CPJ.