#8MCIBERSEGURAS

marzo 2021

10

INSUMOS PRÁCTICOS DE AUTOCUIDADO DIGITAL

POR @DATOSPROTEGIDOS

CONTENIDOS

1.RECOMENDACIONES GENERALES DE SEGURIDAD PARA TUS DISPOSITIVOS

1

Desactiva tu geolocalización y bluetooth si es que no lo estás utilizando.

2

Revisa los permisos que les has otorgado a las aplicaciones. Puedes (1) desactivar los permisos que no son necesarios que la aplicación tenga para funcionar (2) activar la opción para que funcionen solo mientras la App esté en uso.

3

Desinstala las aplicaciones que no utilizas: ocupan espacio en tu teléfono, registran datos aunque no las estés utilizando y pueden intercambiar información entre sí para ofrecer una experiencia de anuncios y servicios más personalizada... y no siempre bajo tu consentimiento.

4

Al momento de instalar una aplicación lo más importante es leer los términos y condiciones y su política de privacidad.

5

Si hay algo que no entiendes, puedes consultar en Internet blogs o análisis sobre las Apps respecto a sus medidas de seguridad y tratamiento de datos. A primeras, te recomendamos el sitio "Terms of service: Didn't read".

6

La regla general para esto es que mientras menos datos innecesarios solicite la aplicación para funcionar y a menos terceros se los envíe, mejor.

2.CONSIDERACIONES PARA REALIZAR REGISTROS A MODO DE #EVIDENCIADIGITAL POR EL #8M

PASO 1

Considera una estrategia. Reúnete con amigas, fija puntos de encuentro, decide si estarán con sus teléfonos encendidos o si es que están dispuestas a compartir sus ubicaciones. Cada una de estas medidas debe ser proporcional a las labores que te encuentres realizando el #8M.

PASO 2

Al momento de registrar, indica FECHA, HORA, LUGAR y una BREVE descripción de los acontecimientos, a modo de introducción.

PASO 3

En caso de ser una agresión, toma registro de las identificaciones de los policías, siempre y cuando esto no afecte tu integridad física y seguridad.

PASO 4

Intenta tomar contacto con las personas afectadas para hacerles llegar el material ya que podría servirles como evidencia.

PASO 5

Si vas a difundir el registro en redes sociales, intenta que sea con la autorización de las personas afectadas. No tener esta consideración podría dañar la integridad de quién se vio expuesta a ello y provocar revictimización.

PASO 6

Al difundir intenta no hacer públicos rostros ni elementos que puedan volver identificable a una persona, por su seguridad.

3.HERRAMIENTAS PARA REALIZAR UNA DESINTOXICACIÓN DE DATOS

DATA DETOX

"Data Detox": Es la guía de desintoxicación de datos por excelencia. Fue creada por Tactical Tech con apoyo de Firefox. En ella podrás encontrar recomendaciones y formas para proteger tu privacidad y dispositivos acorde a lo que necesites, paso a paso. Puedes revisarlo aquí.

CENA DE DESINTOXICACIÓN

"Cena de desintoxicación de datos para seres virtuales": Creada por Fundación Karisma, resulta ser un espacio de encuentro virtual en donde eres acompañad@ para revisar y editar tus dispositivos y configurarlos de manera adecuada. Además, es una invitación para dimensionar tu "huella digital".

4.APLICACIONES SEGURAS PARA TU COTIDIANO

SEGURIDAD ANTE TODO

- **Mail seguro:** https://protonmail.com/ (envío de información sensible)
- **Encriptación de mails:** https://www.openpgp.org/
- **Chat cifrado de extremo a extremo**: https://signal.org/es/ o https://wire.com/en/ . WhatsApp igual cuenta con esta característica, pero de todas formas recomendamos las ya mencionadas.
- **Videoconferencias seguras**: https://jitsi.org/
- **Navegación privada**: https://www.torproject.org/
- **Buscador privado:** https://duckduckgo.com/
- **Almacenamiento y generador de contraseñas**: https://keepass.info/
- **Alternativa a Google Docs**: https://pad.kefir.red/etherpad/home

NOTA: Considerando tus actividades diarias, necesidades y nivel de exposición en línea puedes elaborar tus propios hábitos de seguridad digital, acorde a la información que manejas en tus cuentas y en plataformas.

5.TIPS PARA CREAR CONTRASEÑAS FIRMES Y NO OLVIDARLAS EN EL INTENTO

ATENCIÓN:

- El principal resguardo es no utilizar la misma contraseña en todas las cuentas que tengas.
- Cambia tus contraseñas cada tres meses.
- Para crear contraseñas seguras debes incluir al menos 8 caracteres, mezclados entre números, mayúsculas, minúsculas y en lo posible símbolos.
- Tus contraseñas no deben ser predecibles, ni otra persona aparte de ti debe conocerlas
- En lo ideal no incluyas información personal de ningún tipo en ellas.
- Si crees que puedes llegar a olvidar tantas contraseñas distintas, puedes utilizar KeePass en tu computadora o asociarlas a algún objeto, artista o canción.
- Si necesitas activar la “Clave Única” vinculada a servicios del Gobierno de Chile, procura que esa contraseña sea única y muy segura. Esa plataforma almacenará info sobre tus movimientos y solicitudes , además de información como dirección, rut, motivos de la salida (vinculada a motivos de salud), etc. que puede ser vinculada a tus datos de salud.
- En caso de que la cuenta sea adminsitrada por varias personas, es recomendable que solo UNA persona maneje esa contraseña y sea ella quien digite la contraseña en el dispositivo de la otra persona que necesita tener acceso a ese perfil o información.
- Proteger tu información personal y de las personas que interactúan contigo en línea es clave para construir una Internet más segura de manera transversal.

6.SUGERENCIAS PARA ELABORAR FORMULARIOS Y ENCUESTAS

A CONSIDERAR:

- Intenta recopilar la menor cantidad de datos personales. Toda recolección de datos debe ser proporcional a su uso.
- Si necesitas recopilar la información solo una vez, puedes elegir que la gente responda ingresando su mail como requisito.
- En lo posible, no solicites rut. En caso de ser requerido puede ser solicitado poniéndote en contacto directo con la persona y explicitando para qué será utilizada la información.
- Crea un documento (o escribe algunos párrafos) en donde expliques para qué serán utilizados los datos solicitados y déjalo disponible para consulta en línea.
- Puedes crear un mail solo para trabajar esta información. Debe ser un mail con una contraseña segura y al cual solo algunas personas de la organización/colectiva/comunidad tengan acceso.
- Entre las plataformas que recomendamos para realizar encuestas se encuentra SurveyMonkey, ya que posee opciones para exportar la información a otros formatos, realiza gráficas con las respuestas y su política de privacidad es muy completa. Puedes revisarla haciendo clic aquí.
- Solo recomendamos Google Forms en caso de realizar una consulta general, no para recolectar datos sensibles o específicos. Esta medida se sustenta en que a fin de cuentas desconocemos la exposición a la que pueden estar expuestos aquellos datos entre servicios de Google.

7.MEDIDAS DE SEGURIDAD PARA TUS CUENTAS EN REDES SOCIALES

PASO 1

Lo primero es lo primero, cambia tu contraseña por una segura.

PASO 2

Activa la autentificación en dos pasos. Para activar este mecanismo de seguridad debes revisar el apartado de “configuración” de una plataforma

PASO 3

Para aquel paso, puedes evaluar si utilizas tu mail, un mail basura, un número de teléfono o un generador de contraseñas.

PASO 4

Revisa las configuraciones de privacidad, nunca está de más preguntarse ¿quién ve tu contenido? ¿puedes tener control sobre la cantidad de gente que ve tu contenido?.

PASO 5

Crea un “mail basura” para la recepción y suscripciones a plataformas digitales.

PASO 6

En lo posible, no juntes información de trabajo y personal en un mismo mail, esto para resguardar tu privacidad y para manejar información en cuentas distintas pensadas con un propósito específico.

8.CONSIDERACIONES PARA CHEQUEAR VERACIDAD DE LA INFORMACIÓN EN LÍNEA

NO OLVIDES

- Revisa el link recibido. ¿Es el sitio oficial de la organización o medio de comunicación que entrega la información?.
- La información incluye fuentes ¿expert@s, autoridades o instituciones?.
- Si el contenido es relativo a cifras, verificalo en su fuente principal (institución u organismo que maneje y difunda aquella información de manera oficial)
- Verifica su fecha ¿Es una información reciente?.

9.¿QUÉ HACER EN CASO DE VIVIR ALGÚN EPISODIO DE HOSTIGAMIENTO EN LÍNEA?

NO OLVIDES

- Toma registro de todo tipo de violencia, hostigamiento, agresión o irregularidad que identifiques en alguna red social o plataforma.
- Es importante que no borres los mensajes ya que esta información es tu evidencia digital.
- En medida de lo posible, levanta una “minuta” en donde registres la URL de la cuenta que agrede, registros disponibles, plataforma en la que ocurrieron los hechos, fecha y hora.
- Luego de registrar esta información, reporta las cuentas y bloquearlas
- EN TWITTER puedes bloquear la cuenta o denunciarlas por discursos de odio o cuenta abusiva.
- EN FACEBOOK puedes denunciar un perfil por discursos de odio o por ser abusivo.
- EN INSTAGRAM puedes reportar otra cuenta por spam o por ser inapropiada.
- EN WHATSAPP bloquea el número desde la App y luego desde tu móvil.

Si una amiga tuya vive hostigamiento en línea puedes revisar Take Back The Tech, Acoso.online y Hablemos de ciberacoso. .

10.INFORMES SOBRE VIOLENCIA DE GÉNERO EN INTERNET EN LATINOAMÉRICA

2017

REPORTE DE LA SITUACIÓN DE AMÉRICA LATINA SOBRE LA VIOLENCIA DE GÉNERO EJERCIDA POR MEDIOS ELECTRÓNICOS.

Coding Rights, Karisma, Derechos Digitales, Internet Lab Brasil, Ipandetec, R3D y TEDICpy

2017

LA VIOLENCIA EN LÍNEA CONTRA LAS MUJERES EN MÉXICO

Luchadoras MX

2017

VIOLENCIA EN LÍNEA CONTRA LAS MUJERES EN PARAGUAY

TEDICpy

2017

VIOLENCIA EN LÍNEA CONTRA LAS MUJERES EN COLOMBIA

Fundación Karisma

2018

VIOLENCIA DE GÉNERO EN INTERNET EN CHILE

Fundación Datos Protegidos

10.INFORMES SOBRE VIOLENCIA DE GÉNERO EN INTERNET EN LATINOAMÉRICA

2019

VIOLENCIA CONTRA LA MUJER EN LA REALIDAD DEL MUNDO DIGITAL: DERECHOS, CONCEPTOS Y RECOMENDACIONES

Defensoria CABA

2019

VIOLENCIA DE GÉNERO EN LÍNEA EN PERÚ

Hiperderecho

2020

COVID-19 AND THE INCREASE OF DOMESTIC VIOLENCE AGAINST WOMEN IN LATIN AMERICA: A DIGITAL RIGHTS PERSPECTIVE

Derechos Digitales

2020

JUSTICIA EN TRÁMITE: EL LIMBO DE LAS INVESTIGACIONES SOBRE VIOLENCIA DIGITAL EN MÉXICO

Luchadoras MX

2020

CHILE Y LA VIOLENCIA DE GÉNERO EN INTERNET: EXPERIENCIAS DE MUJERES CIS, TRANS Y NO BINARIES

Proyecto Aurora y ONG Amaranta

10.INFORMES SOBRE VIOLENCIA DE GÉNERO EN INTERNET EN LATINOAMÉRICA

2020

VIOLENCIAS Y DISCURSOS DE ODIO EN LÍNEA

Agrupación Lésbica Rompiendo el Silencio

2020

SER PERIODISTA EN TWITTER: VIOLENCIA DE GÉNERO DIGITAL EN AMÉRICA LATINA

Sentiido y Comunicar Igualdad

ESTA RECOPILACIÓN FUE ELABORADA POR EL EQUIPO DE FUNDACIÓN DATOS PROTEGIDOS ENTRE NOVIEMBRE DE 2020 Y MARZO DE 2021