Mochila DeVida

Cómo se autoprotege el liderazgo social en Colombia

¡Conozca las herramientas!

MANUAL

DE HÁBITOS DIGITALES SEGUROS

SISTEMA INTEGRAL PARA LA PAZ
Verdad | Justicia | Reparación | No Repetición

COMISIÓN DE LA VERDAD

JEP
JURISDICCIÓN ESPECIAL PARA LA PAZ

UBPD
UNIDAD DE BÚSQUEDA DE PERSONAS DADAS POR DESAPARECIDAS

Redprodepaz
Red Nacional de Programas Regionales de Desarrollo y Paz

MANUAL
de hábitos digitales
SEGUROS

Mochila DeVida

Estrategias de autoprotección para lideres/as sociales de Colombia, alentadas por el Sistema Integral para la Paz

Manual de hábitos digitales seguros

Publicado por

Red Nacional de Programas Regionales de Desarrollo y Paz, Redprodepaz
Cra. 13A #34-72 Of. 216
Bogotá D.C., Colombia

Fernando Sarmiento Santander
Coordinador Nacional

Para el Sistema Integral para la Paz
Comisión para el Esclarecimiento de la Verdad, la Convivencia y la No Repetición. Presidente: Francisco De Roux

Jurisdicción Especial para la Paz, JEP. Presidente: Eduardo Cifuentes

Unidad de Búsqueda de Personas dadas por Desaparecidas, UBPD
Directora: Luz Marina Monzón

Con la cooperación de

Programa de las Naciones Unidas para el Desarrollo PNUD, Colombia
Fondo Multidonante de las Naciones Unidas para el Sostenimiento de la Paz

Coordinación técnica

Italo Velásquez
María Isabel Sapuy
Valentina Zuluaga Zuliani
Vanessa Castro

Comisión de la Verdad: Presidencia, Equipo de Prevención y Protección, Dirección de Territorios, Estrategia Comunicaciones.

JEP: Unidad de Investigación y Acusación, Equipo de Identificación y Advertencia Oportuna de Riesgos y Amenazas, Equipo de Protección a Víctimas Testigos e Intervinientes.

UBPD: Equipo Asesor de Prevención y Protección, Equipo Asesor de Comunicaciones y Pedagogía

Equipo técnico en Derechos Humanos
Camila Gómez
Francisco Barreto
Malena Rinaudo
Rocío Durán

Equipo técnico en Comunicaciones
César Vanegas
Diana Herrera
Mauricio Vega
Norma Gálvez
Sandra Botero

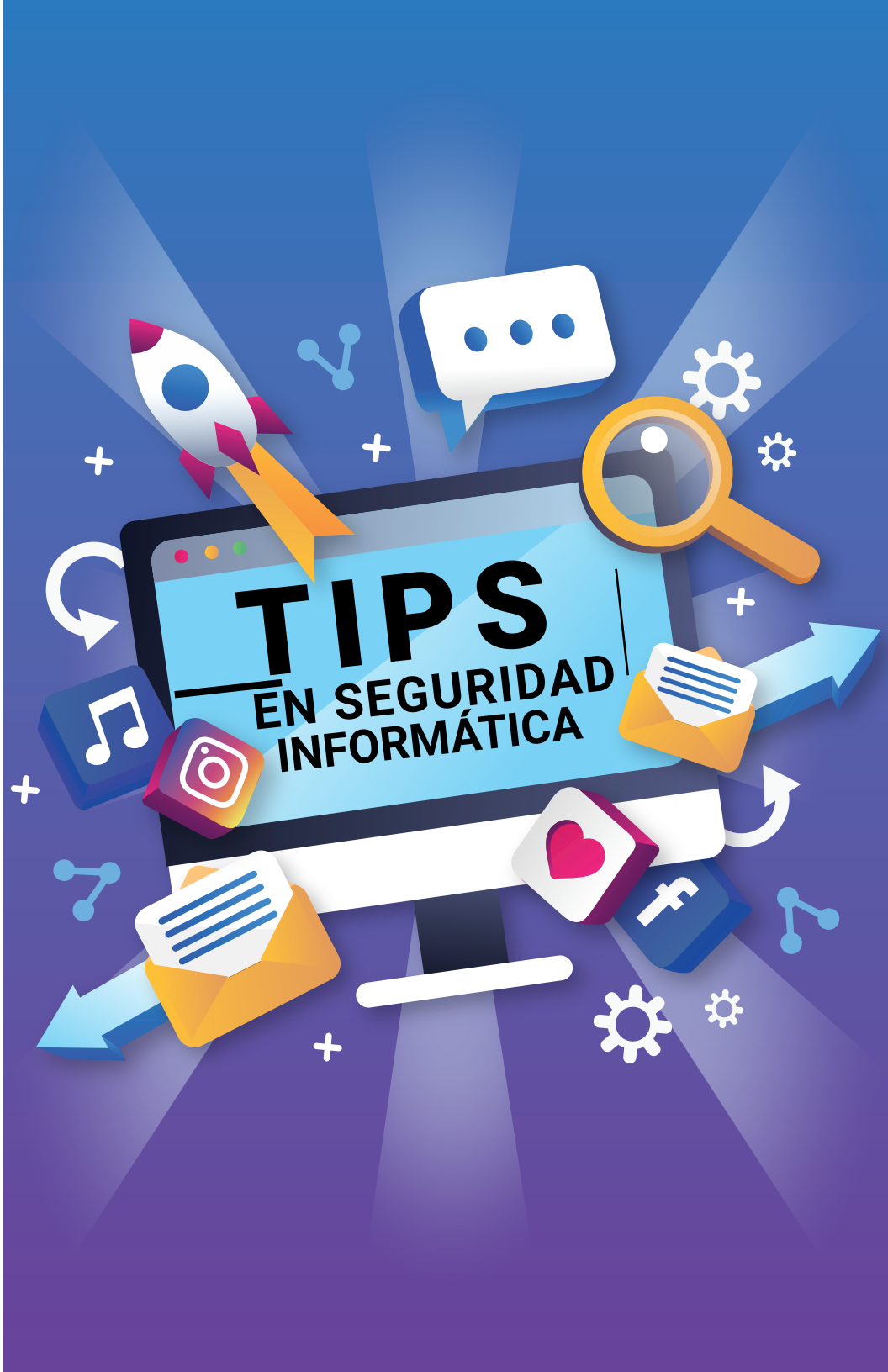
Coordinación general
Valentina Zuluaga Zuliani

Autoría
César Vanegas
Diana Paola Herrera

Esta publicación se produce en el marco del proyecto 'Estrategia de fortalecimiento institucional para el despliegue y funcionamiento territorial articulado del Sistema Integral de Verdad, Justicia, Reparación y No Repetición (SIVJRNR)", hoy Sistema Integral para la Paz (nombre emanado del proyecto), con apoyo del Fondo Multidonante de las Naciones Unidas para el Sostenimiento de la Paz; su producción está relacionada con el desarrollo participativo de protocolos de autoprotección con sujetos colectivos priorizados, para su participación en los mecanismos de Justicia Transicional del Acuerdo Final de Paz firmado en 2016 entre el Gobierno Nacional y la exguerrilla FARC. Las ideas presentes en el texto son responsabilidad de la consultoría para el diseño de los protocolos de autoprotección y no comprometen la línea institucional de las entidades participantes.

Edición y coordinación editorial: Sandra Helena Botero O.
Diseño y diagramación: Sor Diana Paola Herrera C.
Impresión: Panorama Agencia Digital

Bogotá D.C., Colombia, 2022


TIPS
EN SEGURIDAD
INFORMÁTICA

Con las dinámicas actuales de uso de la tecnología y cuando prácticamente todo está digitalizado, es poco probable que una persona se encuentre totalmente desconectada. A pesar de las distancias, las disímiles condiciones geográficas, las redes de comunicación, los recursos económicos con los que se cuente y múltiples factores más, hoy una persona cuenta, por lo menos, con un teléfono celular.

Bien sea que esté hiperconectada (entendiendo el término en su acepción más simple, como la necesidad de estar conectado a internet y a las redes sociales constantemente) o que solo utilice un aparato telefónico para llamadas básicas, por ejemplo, el solo hecho de utilizar esta tecnología trae consigo riesgos en la privacidad y en la seguridad, al involucrar la transmisión de datos de un dispositivo a otro.

En Colombia, con una población de 51.7 millones de personas, existen 60.8 millones de dispositivos móviles conectados, entre teléfonos celulares, tabletas y computadores portátiles, y el 68% de los habitantes tiene conexión a internet; de estos, el 76.4% es activo en las redes sociales, lo cual nos da una idea del enorme tráfico de información que se puede presentar.[1]

En este contexto, y sin olvidar que en las zonas rurales del país la conectividad y el acceso a aparatos tecnológicos son mucho más precarios, es indispensable que los líderes y lideresas sociales, y las comunidades a las que representan, tengan siempre en cuenta las recomendaciones de seguridad en las comunicaciones y la tecnología, que acá se presentan como una herramienta más para su protección.

1 Estadísticas de la situación digital de Colombia en el 2020-2021. Información de la agencia de marketing digital Branch. Tomados de www.branch.com.co

CORREO ELECTRÓNICO SEGURO

Uno de los medios más comunes para las comunicaciones, bien sea personales o de trabajo, es el correo electrónico a través de servicios generalmente gratuitos como Gmail, Hotmail, Yahoo y Outlook, entre otros.

Su uso representa cada vez más riesgos para la privacidad de la información y la seguridad. Estos son algunos consejos útiles para prevenirlos:

CORREOS MALICIOSOS

Cientos de mensajes fraudulentos llegan a las cuentas de correo electrónico; por ello, es crucial saber identificarlos:

- Desconfiar es siempre el primer paso.
- La primera señal para estar alerta es el nombre del remitente (¿lo conozco?).
- Desconfíe de los nombres en los correos (llamados "dominios"), que tengan números o letras adicionales. Ejemplo: dane.1@dane.gov.co
- La redacción es importante. Estos correos están mal redactados, con mala ortografía e incluso traducciones mal hechas.
- El asunto es clave. En el apartado del asunto lo "asustan" poniendo cosas como "urgente"; "último plazo"; "presentarse en…", etc.
- No descarte los logos. Mírelos bien: ¿son de una entidad conocida, corresponde con el dominio?).
- Mire quién firma el correo. Casi siempre un correo trae el nombre de la persona, nombre de la empresa, dirección, teléfono, extensión (¿trae esta información, es clara?).
- Ojo con los adjuntos. Muchos de los correos peligrosos traen archivos adjuntos que son aún más peligrosos. NO LOS ABRA. Los puede distinguir porque generalmente poseen extensiones como: .com; .bat; o .exe.
- Así como los adjuntos, los enlaces que trae el correo son fundamentales. No intente abrirlos si no está completamente seguro de su procedencia. Dar clic es abrir una ventana por donde le pueden robar la información o instalar virus de todo tipo.

Puede poner el cursor sobre el enlace y observar la barra inferior del navegador, ahí debe aparecer la dirección web de donde procede el correo.

- Ponga atención a lo que le pide el correo. ¿Es claro?; ¿confía en lo que pide?; ¿tiene que ver con algún aspecto de su vida o su trabajo?
- Nunca responda un correo que no comprenda solicitando información adicional. Lo mejor es indagar por otros medios.
- Si le solicitan información personal y claves, siempre será un correo malicioso. Nunca envíe ninguna contraseña por este medio.
- Nunca se gana un concurso en el que no se participa. Si le anuncian que lo ganó, es un fraude.
- No utilice la misma clave para todo, es un riesgo muy alto.
- Nunca responda un correo electrónico sin estar seguro/a de su veracidad.
- Recuerde que ninguna empresa de tecnología, banco o entidad del Estado pide datos personales ni claves por correo electrónico.

Además de lo anterior, tenga en cuenta que por medio del correo electrónico se presenta un delito cada vez más extendido que se llama phishing (suplantación de identidad). Con este se engaña a la persona para que entregue información confidencial como contraseñas y números de tarjetas de crédito.

La modalidad más conocida de phishing consiste en que la persona recibe un correo electrónico que parece fiable, quizá bien redactado y con los logos de una entidad del Estado o de un banco, por ejemplo; inclusive, de alguien conocido. Al abrirlo hay un mensaje que asusta, que infunde miedo, porque se exige una

acción inmediata bajo alguna amenaza o poniendo un plazo. La persona, desorientada, accede a dar clic en algún enlace o a entrar en un sitio web donde pueden robarle información.

TELÉFONO CELULAR SEGURO

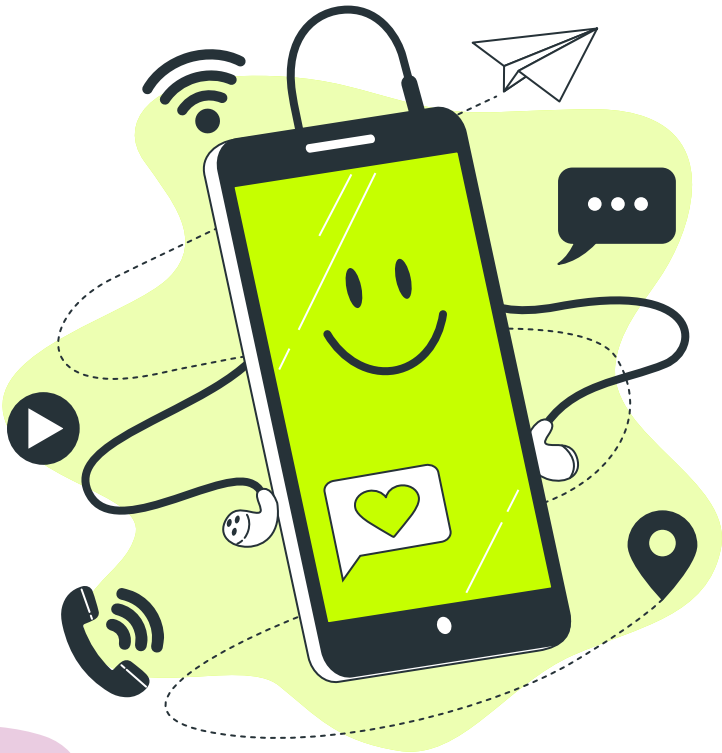
La mayor parte de las personas en Colombia tiene un aparato telefónico celular, aún en las zonas más alejadas donde no existe conectividad o es de mala calidad. Por ello, es fundamental tener en cuenta estas recomendaciones para su uso con seguridad:

¿Qué guarda, generalmente, un teléfono celular?

- **Gustos y preferencias.** A medida que se navega por internet desde el celular, se almacenan en él datos sobre los sitios visitados y los "me gusta" que se dan en las diferentes redes sociales o páginas web.
- **Localizaciones.** El celular guarda los sitios que ha visitado si el GPS está activado.
- **Archivos.** Fotos, documentos, conversaciones, etc. Estos pueden revelar mucha información privada y confidencial.
- **Datos de tarjetas de crédito.** Pueden obtenerse, por ejemplo, de sus tiendas de internet favoritas, o los lugares donde generalmente se pague con este medio, o por la opción de autocompletar de algunos formularios en internet.
- **Credenciales.** La opción de autoguardado que tiene el celular permite que pueda acceder a sus servicios y cuentas de usuario sin ser necesario conocer la clave de acceso.

- **Contactos.** Nombres, teléfonos, correos o direcciones quedan guardadas en el celular para su consulta y uso.
- **Conversaciones y mensajes.** A pesar de haber borrado las conversaciones de una aplicación o red social, éstas pueden quedar en el teléfono, dado que existen copias de seguridad automática.

Tenga en cuenta que, sobre todo en tiendas no autorizadas, se venden celulares nuevos o de segunda mano que vienen con virus espías preinstalados cuya función es robar sus datos y hacerle seguimiento a su ubicación.



Lo que debe tener en cuenta para la seguridad de su información en un teléfono celular:

- Actualice permanentemente el sistema operativo de su celular, además de cada una de las aplicaciones que tenga instaladas en él.
- Active la verificación de dos factores. Esto significa que las entradas a sus cuentas o aplicaciones deberán contar con dos formas de autorizar la entrada a ellas. Generalmente todos los servicios de internet lo tienen.
- Cuide su correo electrónico. Generalmente es el medio más usado para que le lleguen los enlaces que permiten cambiar de clave o cualquier información de su teléfono. Si alguien más tiene acceso puede entrar más fácilmente a los datos de su celular. Además, es por allí por donde entran los virus a su dispositivo.
- Cuidado con las aplicaciones que instala. Asegúrese de que sean las oficiales, que sean conocidas. Estas se prestan para la introducción de virus a su teléfono. Desconfiar es la clave. Sólo descargue aplicaciones de sitios de confianza.
- Procure no utilizar servicios de wi-fi gratuito y desconocido. Al hacerlo pone en riesgo la privacidad y seguridad de sus datos.
- Asegure la entrada a su celular con una clave para evitar que alguien más lo utilice. Sin embargo, evalúe la situación de la zona en la que vive; en algunas, por cuestiones de retenes de grupos al margen de la ley, e inclusive de las mismas fuerzas del Estado, es más conveniente no tener clave para no generar sospechas de información oculta.

- Cierre todas las sesiones al terminar de usarlas. Si su celular cae en malas manos, aunque sea por pocos minutos, puede estar expuesto al robo de información.
- Tenga en cuenta a quién le presta el celular y dónde lo deja.
- Mantenga desactivadas las conexiones de bluetooth, infrarrojo y wi-fi cuando no las esté usando. Por este medio existe la posibilidad de fuga de datos y de la entrada de virus por esos medios.
- Antes de deshacerse de un teléfono celular haga una copia de seguridad de la información que quiera guardar y borre todo lo demás. La mejor opción para mantener la privacidad y la seguridad es siempre restablecer el dispositivo a valores de fábrica.

FRAUDES ELECTRÓNICOS Y COVID-19

La pandemia ha sido usada por los delincuentes para robar información a través de redes sociales, correos electrónicos y cualquier actividad que se realice en la red de internet, aprovechando un tema tan sensible como este, del que todo el tiempo se habla y está en todos los medios de comunicación.

Según la Oficina de Seguridad del Internauta de España (OSI), las siguientes son algunas de las formas que se utilizan para robar información, que hemos adaptado al contexto colombiano:

- **Consejos sobre Covid -19 por WhatsApp.** Se trata de una estafa que se genera con la llegada de mensajes a través de esta aplicación

de mensajería. En ellos, supuestos expertos pretenden dar consejos de cómo manejar el virus e invitan a abrir enlaces que finalmente se usan para robar información o dinero, en el caso de que la persona acceda a "apoyar la causa".

- **Apoyo para los profesionales de la salud.** Aprovechándose de la buena voluntad de las personas, que ven en los profesionales de la salud a los héroes de esta pandemia, los delincuentes piden aportes económicos o información personal para beneficio de médicos, enfermeras y demás trabajadores de la salud. Al final, pueden llegar a robarle su dinero y su información.

- **Suplantación de identidad por correo electrónico.** Como vimos antes, la suplantación de identidad es un delito muy común (phishing), y en el caso de la pandemia, los delincuentes se hacen pasar por entidades conocidas como el Ministerio de Salud o algún organismo sanitario y aprovechando la obvia preocupación de las personas por el virus, envían correos electrónicos con enlaces o archivos adjuntos que dicen contener información de gran interés y lo que hacen es robar datos sensibles de su teléfono celular o de su computador. Por ejemplo, usted puede recibir un correo procedente de un supuesto hospital que le informa sobre una nueva variante del Covid, una nueva vacuna o nuevas normas sobre manejo de la pandemia, y para ello debe hacer clic en un enlace sospechoso.

- **Suplantación de identidad por mensajes de texto.** Así como el anterior fraude por correo electrónico (phishing), éste, que se produce a través de los mensajes de texto que llegan al celular, y que se denomina smishing, tiene el objetivo de robar la información de su dispositivo para fines fraudulentos, siempre haciéndose pasar por entidades del Estado, bancos o personas conocidas. En este caso le pedirán actuar con urgencia en algún tema relacionado con el Covid y le enviarán enlaces maliciosos.

- **Secuestro de datos.** En el contexto de la pandemia pueden llegarle correos electrónicos, mensajería instantánea tipo WhatsApp o mensajes de textos con recomendaciones o noticias de última hora sobre el Covid-19. Puede ser un enlace, un archivo adjunto o un video. Al abrirlos, los delincuentes se apoderan de su dispositivo o de los archivos que contenga. Esto es lo que se denomina ransomware (de la palabra en inglés "ransom", que significa rescate).

Y justamente eso pedirán al afectado, un rescate; es decir, deberá pagar para poder volver a utilizar el dispositivo o los archivos, que quedan bloqueados para el dueño y a plena disposición del delincuente.

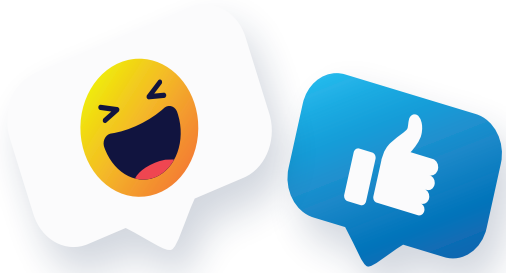
Siga desconfiando, nunca abra enlaces, correos o videos que lleguen por cualquier medio. Si ve el remitente, trate de buscar más información sobre este en otro lado. Generalmente lo aconsejable es buscar las páginas web oficiales o las redes sociales de las

entidades o personas que dicen estar enviando el mensaje.

- **¿Trabajo sí hay?** En el marco de la pandemia los ciberdelincuentes no pierden la oportunidad de hacer de las suyas, inclusive enviando falsas ofertas de empleo para trabajar haciendo material para hospitales o centros de salud, o apoyando procesos sanitarios. Y dado el desempleo y la necesidad de ocuparse, la persona envía datos personales e inclusive paga una 'inscripción' que obviamente no conducirá a un nuevo empleo, sino a perder su privacidad y seguridad.

- Por lo anterior, en un caso como estos revise bien de dónde proviene la información, indague en otros lugares, preferiblemente los oficiales. Si sospecha, no se arriesgue. Generalmente estos ofrecimientos no abundan, ni se dan a través de estos mensajes.[2]

2 Tomado y modificado de: Top 10 fraudes que utilizan COVID-19 para engañar a los usuarios. Oficina de Seguridad del Internauta. Publicado el 27/03/2020. www.osi.es



REDES SOCIALES SEGURAS

Con el aumento del uso del internet en el mundo, donde hay más de 4.700 millones de personas con conexión, y sobre todo con el auge de las redes sociales (4.330 millones de usuarios)[3] , el tema de la seguridad es más que fundamental, toda vez que en estos servicios se publica casi todo, de tal manera que encontrar a una persona y su ubicación física es una tarea de apenas unos pocos clics, con los problemas de privacidad y de seguridad que esto conlleva.

Aunque el primer paso será siempre desconfiar en las redes sociales y quizá el segundo sea utilizar el sentido común, dado que generalmente se estará expuesto en la medida en se usen, estas son algunas recomendaciones, que pueden ser útiles para exponer menos su seguridad como usuario/a de las redes:

1. Si sospecha, es mejor que desinstale las redes sociales del teléfono

Si piensa que quizá alguien entró a sus redes sociales sin su permiso, y que posiblemente está actuando a su nombre, la recomendación es desinstalar completamente Facebook u otra red social de su teléfono.

Tenga en cuenta que redes sociales como Facebook pueden controlar los aparatos que conecte a su teléfono, como la cámara y el micrófono, y se pueden usar para almacenar información sobre usted, generalmente para venderla a anunciantes que luego le ofrecerán sus productos por medio de publicidad.

3 Seis de cada diez personas del mundo son usuarios de internet. Portafolio 04/22/2021. https://www.portafolio.co/internacional/seis-de-cada-diez-personas-del-mundo-son-usuarios-de-internet-551200

2. Ojo con las contraseñas

Ocultarlas es una de las cosas más simples que puede hacer para aumentar la seguridad en sus cuentas de redes sociales. Esta acción le ayuda a protegerse del robo de información de sus redes.

3. Fíjese muy bien qué permisos tiene cada aplicación

Cada aplicación que instala en su teléfono pide una serie de permisos; algunos de ellos no sirven para nada. Revise cuáles permisos están habilitados y desactive los que no requiera verdaderamente. Así su privacidad está más segura. Lo más común es que las aplicaciones que use tengan activada la localización por GPS de su teléfono, así como el micrófono y la cámara.

Si tiene activado el GPS, cualquier aplicación puede recopilar información sobre dónde está usted y los sitios que frecuenta. Alguien que quiera hacerle daño puede interceptar esta información y usarla para sus fines.

4. No sea amigo de cualquiera

Si alguien solicita ser su amigo en las redes sociales y usted no lo conoce, averigüe primero de quién se trata, busque su perfil, antes de permitirle tener acceso a sus datos personales.

5. No se muestre a todo el mundo

Todo lo anterior no sirve de nada si su perfil es público, pues cualquiera podrá ver toda su información. Todo lo que publica en redes sociales es visible para el resto de usuarios. Cualquiera puede encontrarlo. La recomendación es que su cuenta privada, para que solo sus amigos puedan ver sus publicaciones, fotos, historias e información privada.

6. Navegue seguro

Siempre que esté navegando por Internet, evite los sitios que no son seguros. Los sitios que sí lo son se identifican con las letras HTTPS antes de la URL (es decir, la dirección que aparece en la barra superior del navegador que usa).

7. No deje las puertas de la casa abiertas

Si está usando cualquier plataforma de medios sociales, antes de cerrar el portátil o dejar el teléfono, desconéctese de esta. Las redes sociales tienen la capacidad de rastrear toda su actividad cuando deja abierta la aplicación, aunque no la esté usando, para recopilar datos sobre usted. Esta información se comparte con anunciantes, así que su privacidad no está muy asegurada.

8. Borre el pasado

Si tiene cuentas en redes sociales que no usa, elimínelas para que nadie pueda acceder a ellas. Todos los datos personales que se puedan rastrear deben eliminarse al cerrar cuentas antiguas.

Recuerde que el mundo sabe de usted lo que usted le cuente. Los datos que aparecen en la red de internet en algún momento los dio usted, los lugares que visitó, las personas con las que departió, sus gustos, los lugares que frecuenta, sus datos de contacto, etc. Entonces, antes de publicar analice si vale la pena hacerlo y quién podría verlo.

CÓMO HACER CONTRASEÑAS SEGURAS

Las contraseñas que nos permiten acceder al correo electrónico, a las redes sociales y a una innumerable cantidad de aplicaciones y servicios en internet, se asemejan a las llaves de la casa; es decir, no se le pueden dar a todo el mundo y solo usted es responsable de a quién se las entrega. Estas son algunas recomendaciones:

- Cree contraseñas complicadas. Más de 8 caracteres, con mayúsculas, minúsculas, algún número y caracteres especiales (*;+;#...). Nunca fechas de cumpleaños de hijos, o sus nombres, ni de aniversarios, eventos o año en curso; estas son fácilmente identificables.

- No use la misma contraseña. Si usa la misma clave para todos los servicios y aplicaciones puede que la recuerde más fácilmente, pero también más fácilmente multiplica la posibilidad de que extraños accedan a su información.
- Cambie la contraseña con regularidad. Esto permite asegurar mucho más su información.
- No vuelva a utilizar una anterior ya usada.
- No memorice contraseñas teniendo en cuenta el teclado: no use el teclado como guía para recordar contraseñas fácilmente (ej.: "345678" o "qwerty").
- No use expresiones fácilmente deducibles como: teamobebe; gorditalinda; hijodemialma; padretodopoderoso; etc.
- No utilice el nombre de su equipo de fútbol favorito o de un grupo musical de su gusto.
- No escriba su clave en ningún lugar; mejor memorícela.[4]

4 Tomado y modificado de: Alejandro Luzán. 10 consejos para garantizar la seguridad en redes sociales. www.marketerosdehoy.com

IMPORTANCIA DE CONTAR CON BASES DE DATOS Y ACCESO A MEDIOS DE COMUNICACIÓN.

Una herramienta primordial, en lo que tiene que ver con la seguridad en las comunicaciones, y que se constituye en una necesidad de primer orden para los líderes y lideresas sociales y las comunidades que representan, es contar con una base de datos de organismos nacionales e internacionales, así como de líderes y personas con influencia en diferentes sectores; que incluya su número celular, correo electrónico, usuarios en redes sociales. Al menos uno de esos datos, para intentar tener suerte al contactarlos.

Esto incluye datos de medios de comunicación y sus voces, tanto locales como nacionales e internacionales, preferiblemente independientes. Lo anterior es fundamental para lanzar llamados de alerta ante eventualidades que pongan en riesgo a líderes/as y comunidades, y se convierte muchas veces en un seguro que refuerza la capacidad de autoprotegerse.

Una base de datos actualizada, en donde se establezca claramente el ente competente para cada fin, los nombres de los funcionarios/colaboradores encargados, sus números de teléfono y toda la información que se pueda recabar, así como los datos de los medios de comunicación, será un poderoso recurso, de gran utilidad.

Mochila DeVida

Cómo se autoprotege el liderazgo social en Colombia

¡Conozca las herramientas!

Con el apoyo de:

FONDO MULTIDONANTE DE LAS NACIONES UNIDAS PARA EL SOSTENIMIENTO DE LA PAZ

PNUD