PEACE BRIGADES INTERNATIONAL

CAJA DE HERRA-MIENTAS

ANÁLISIS DE RIESGO PARA PERSONAS DEFENSORAS

2 **CUADERNILLO 2:**
SEGURIDAD
DIGITAL

CONTENIDOS
UNIDAD 1

UNIDAD 1

SEGURIDAD DIGITAL O ESTRATEGIAS DE COMUNICACIÓN SEGURA

Parte 1: ¿Qué es la seguridad digital? ¿Qué redes y medios usamos?
Parte 2: ¿Cómo funciona internet?
Parte 3: ¿Qué información necesita protección? ¿Cómo hacerlo? ¿Qué herramientas tenemos para una comunicación segura?

pbi
abriendo espacios para la paz

SEGURIDAD DIGITAL
O ESTRATEGIAS DE COMUNICACIÓN SEGURA

¿QUÉ ES LA SEGURIDAD DIGITAL? ¿QUÉ REDES Y MEDIOS USAMOS?

90 MINUTOS

DIVIDIR EL GRUPO EN EQUIPOS

MARCADORES DE COLORES Y PAPELÓGRAFOS (PLIEGOS DE PAPEL PERIÓDICO).

CONTENIDOS PARA ESTA ACTIVIDAD

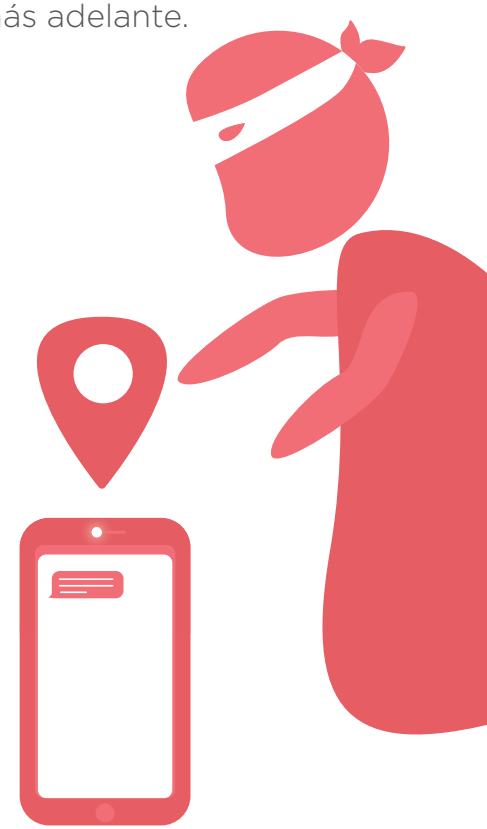
La seguridad digital es un **conjunto de medidas de protección** para minimizar los riesgos que corre nuestra información. Está vinculada a las plataformas, aplicaciones y dispositivos que usamos y a su infraestructura. Estas medidas nos permiten poner capas para **proteger nuestros mensajes**, datos, etc., sin embargo, este término no abarca lo que implica la seguridad integral, la cual se encuentra más cercana al concepto de "estrategias de comunicación segura". Este nos ofrece una visión más allá de las herramientas que usamos para comunicarnos, como la evaluación que hacemos de los lugares en los que estamos, para saber si son los propicios para comunicar información sensible a otras personas, **los dispositivos que empleamos** (propios o prestados), las personas que nos rodean en el momento en que queremos transmitir un mensaje, etc.

En cuanto a nuestras prácticas, lo fundamental es que podamos analizar los datos e información que queremos enviar, cuál es nuestro objetivo con ello y a través de qué tipo de herramientas podemos hacerlo. Esto nos permitirá no condenar el uso de ciertas herramientas que hacen visible, por ejemplo, nuestra ubicación, porque esto, en ciertas ocasiones, puede jugar a favor de nuestra protección.

Por otro lado, volviendo a la seguridad digital, partimos del hecho de que **en Colombia, por ley1, todas nuestras conversaciones** telefónicas, nuestros mensajes de texto y nuestra ubicación, están siendo almacenados por las empresas de telecomunicaciones, por un término de cinco años.

Estos **pueden ser entregados al Estado en caso de que sea requerido,** con el pretexto de la seguridad nacional y sin notificación a quienes somos usuarios de estos servicios. Por ello, **es necesario proteger nuestros datos y conversaciones.**

Para esto hay algunas **herramientas sencillas** de utilizar y, sobre todo, sencillas de compartir con las organizaciones con las que trabajamos, tales como **aplicaciones, sitios web, antivirus, navegadores y extensiones,** que veremos más adelante.



1 Decreto 1704 de 2012:
www.mintic.gov.co/portal/604/articles-3559_documento.pdf

SEGURIDAD DIGITAL
O ESTRATEGIAS DE COMUNICACIÓN SEGURA

PARTE 1

¿QUÉ ES LA SEGURIDAD DIGITAL?
¿QUÉ REDES Y MEDIOS USAMOS?

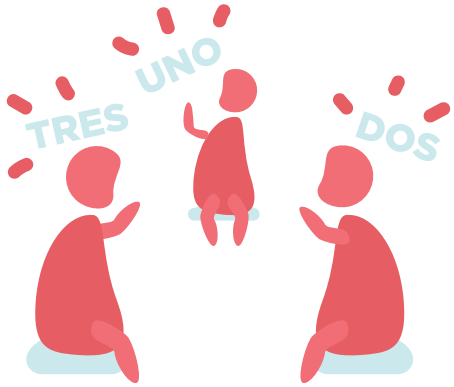
5 MINUTOS

DIVIDIR EL GRUPO EN EQUIPOS

MARCADORES DE COLORES Y PAPELÓGRAFOS (PLIEGOS DE PAPEL PERIÓDICO).

PASO 1

Dividimos el grupo en **cinco equipos.** Esto, pidiendo a las y los participantes que se numeren **de uno a cinco,** una y otra vez hasta que se complete el grupo. Hecho esto, **los unos** se encuentran **con los unos, los dos con los dos, los tres con los tres,** etc. Repartimos marcadores y un pliego de papel periódico a cada uno de los equipos y les pedimos que **se organicen en mesas de trabajo.**



¿QUÉ ES LA SEGURIDAD DIGITAL?
¿QUÉ REDES Y MEDIOS USAMOS?

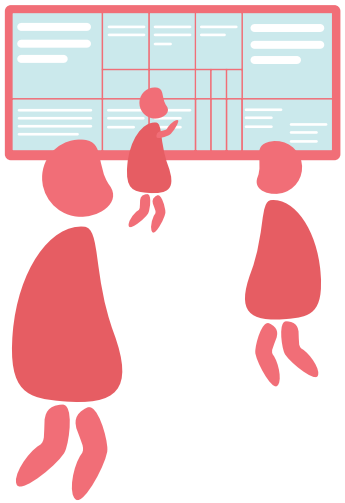
40 MINUTOS

DIVIDIR EL GRUPO EN EQUIPOS

MARCADORES DE COLORES Y PAPELÓGRAFOS (PLIEGOS DE PAPEL PERIÓDICO).

PASO 2

Ya organizados en mesas de trabajo, les pedimos a los equipos que resuelvan las siguientes preguntas: ¿qué es la seguridad digital? ¿Cuál es el uso que hacemos de Internet? ¿Qué redes usamos? Les informamos que estos interrogantes alientan la reflexión respecto al uso que hacemos de nuestras redes, en el marco de lo organizativo.



Así mismo, para facilitar el análisis, debemos llenar la tabla ubicada al respaldo de esta página en los papelógrafos que tenemos. Es importante mantenerla en nuestro equipo, puesto que servirá tanto para esta actividad, como para la relacionada con la Parte 3 de esta Unidad. Por ahora, en lo que respecta a este ejercicio, vamos a llenar las tres primeras columnas.

SEGURIDAD DIGITAL
O ESTRATEGIAS DE COMUNICACIÓN SEGURA

PARTE 1

DATOS E INFORMACIÓN QUE COMPARTIMOS COMO ORGANIZACIÓN -	PERSONA O ÁREA DE TRABAJO DE ORGANIZACIÓN QUE EMITE LA INFORMACIÓN -	MEDIOS QUE USAMOS COMO ORGANIZACIÓN -	SEMÁFORO DE RIESGO -			HERRAMIENTAS DE SEGURIDAD DIGITAL -
¿QUÉ SE COMUNICA?	¿QUIÉN COMUNICA?	¿QUÉ CANAL ESTAMOS USANDO ACTUALMENTE?	¿QUÉ NIVEL DE SENSIBILIDAD TIENE ESTA INFORMACIÓN?			¿QUÉ HERRAMIENTAS SEGURAS PODEMOS USAR?
			ALTO	MEDIO	BAJO	

SEGURIDAD DIGITAL
O ESTRATEGIAS DE COMUNICACIÓN SEGURA
PARTE 1

1

¿QUÉ ES LA SEGURIDAD DIGITAL?
¿QUÉ REDES Y MEDIOS USAMOS?

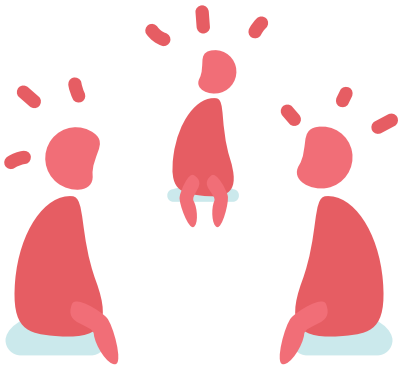
15 MINUTOS

DIVIDIR EL GRUPO EN EQUIPOS

MARCADORES DE COLORES Y PAPELÓGRAFOS (PLIEGOS DE PAPEL PERIÓDICO).

PASO 3

Después de la **conversación grupal** y de la **consignación de los datos en la tabla,** la idea es que podamos **socializar las conclusiones** a las que llegamos como equipo.
Para ello, pasaremos, grupo por grupo, a **exponer nuestras tablas y reflexiones.**



1

¿QUÉ ES LA SEGURIDAD DIGITAL?
¿QUÉ REDES Y MEDIOS USAMOS?

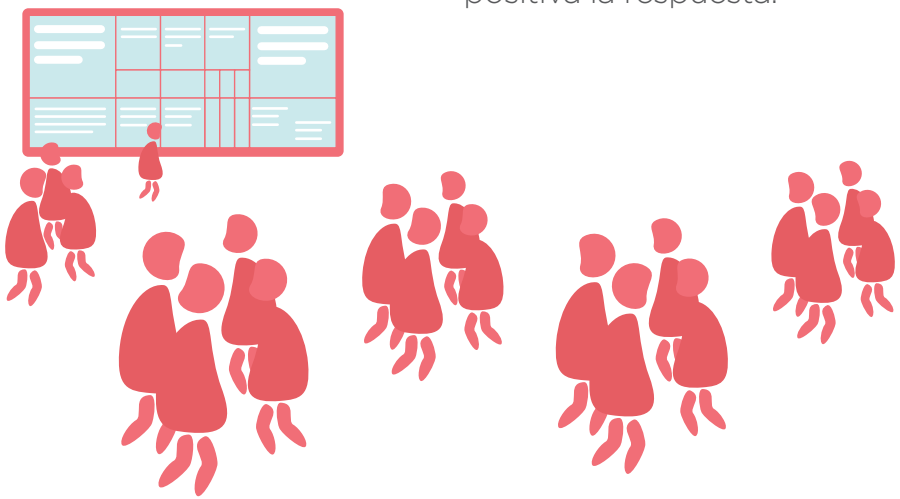
25 MINUTOS

DIVIDIR EL GRUPO EN EQUIPOS

MARCADORES DE COLORES Y PAPELÓGRAFOS (PLIEGOS DE PAPEL PERIÓDICO).

PASO 4

Recogemos las reflexiones por equipos, analizando los casos que propusieron, **qué tienen en común**, sus similitudes y diferencias. Así mismo, este espacio puede ser la oportunidad para **abrir la conversación hacia la no satanización de las redes,** teniendo en cuenta que lo fundamental es el **análisis de la información** que estamos mandando, su nivel de sensibilidad y si queremos que esta sea difundida y por qué medios queremos y creemos que es viable hacerlo, es decir, **aprender a usar las herramientas que tenemos** a nuestra disposición.
Aprovechemos para preguntar si en algún momento han sentido que sus redes están intervenidas y qué tipo de indicadores les han dado pistas sobre eso, en caso de que sea positiva la respuesta.



SEGURIDAD DIGITAL
O ESTRATEGIAS DE COMUNICACIÓN SEGURA

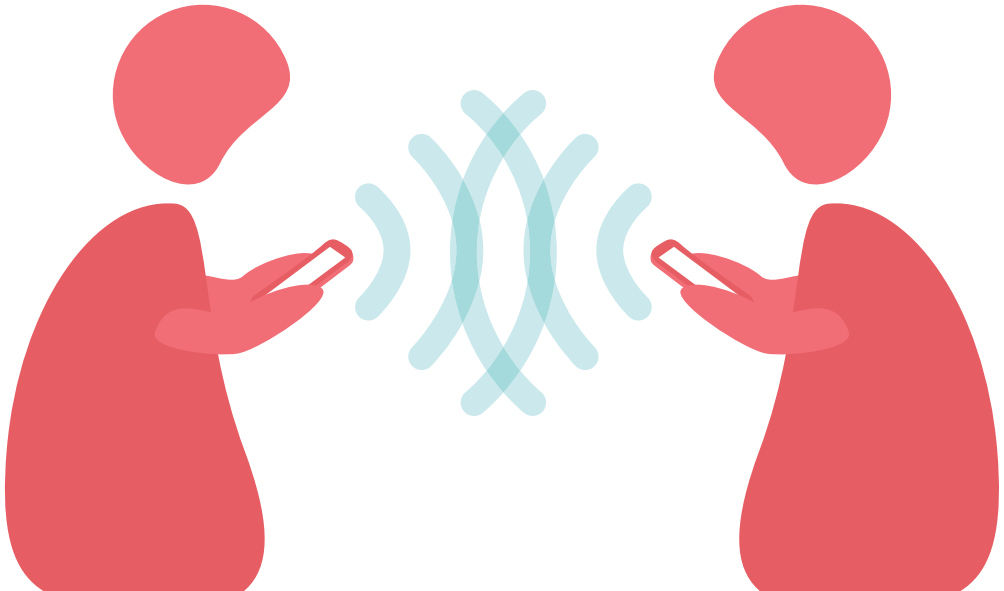
¿QUÉ ES LA SEGURIDAD DIGITAL? ¿QUÉ REDES Y MEDIOS USAMOS?

OBSERVACIONES GENERALES

Este ejercicio puede funcionar muy bien para ayudarnos a identificar factores de riesgo en el ámbito de las comunicaciones, que puedan afectar tanto nuestro trabajo organizativo, así como a las personas que lo realizamos. Asimismo, nos llama a analizar la manera en la que estamos compartiendo nuestra información y si esta responde a los objetivos que tenemos.

Funciona muy bien en espacios en los que se nos dificulte la conexión a internet o hayan dificultades de electricidad.

Otra de sus características a favor es que partimos de la reflexión colectiva sobre nuestras prácticas, lo que permite una mejor incorporación de la información nueva que se nos comparta en este espacio.



1

SEGURIDAD DIGITAL
O ESTRATEGIAS DE COMUNICACIÓN SEGURA
PARTE 2

¿CÓMO FUNCIONA INTERNET?

60 MINUTOS

TODO EL GRUPO

FICHAS BIBLIOGRÁFICAS Y MARCADORES
(TARJETAS CON LOS COMPONENTES DE LA CADENA DE FLUJO DE LA INFORMACIÓN)

CONTENIDOS PARA ESTA ACTIVIDAD

Es importante que conozcamos **la manera en la que viaja nuestra información** en internet, porque esto nos permite **reconocer los puntos de vulnerabilidad** que esta atraviesa, así como saber cuáles son las alternativas que, frente a esto, nos dan diferentes herramientas digitales. En el envío de un mensaje hay involucrados múltiples lugares en los que quedan **huellas o rastros de nuestra información, la cual puede ser copiada,** al tiempo que está siendo almacenada por las compañías que nos proveen los servicios de conexión y distribución de datos.

Recordemos además, lo anterior, **el Estado puede pedir a las compañías de telecomunicaciones,** como ha quedado establecido en el Decreto 1704 de 2012, que faciliten nuestros datos e información almacenada.

CONTENIDOS PARA ESTA ACTIVIDAD

Para poder entender esta cadena de comunicación, veremos **un ejemplo.**
Clara **envía un correo electrónico** a Luisa, diciéndole que al día siguiente habrá una marcha y **dándole el punto de encuentro** de la misma. Esto lo hace desde el computador de su casa. En este caso, el mensaje es recibido primero por el punto de conexión, que es el router o módem que le ha sido entregado a Clara por parte de la compañía con laque ella ha contratado su servicio de internet (Movistar); la función de este aparato es distribuir datos, tanto recibir como enviar información por la red.
Del módem, el mensaje pasa a una antena cercana, que lo dirigirá probablemente a otra antena, desde la cual viajará hacia el proveedor de internet (Movistar), en donde quedará almacenado en un banco de datos. Este pasa después por el servidor de la empresa de mensajería que usa Clara (Gmail), la cual se encue ntra probablemente en otro país.

2

En el caso de ser un sitio web o una red social (Facebook, WhatsApp), ocurre lo mismo. Este servidor busca automáticamente la dirección de correo electrónico de Luisa, entregando el mensaje a su proveedor de internet (Claro). El proveedor envía el mensaje a su red de antenas, para pasarlo al módem de Luisa, quien recibe finalmente lo que quiere decirle Clara. En caso, por ejemplo, de que Clara vea el mensaje en su celular, este será recibido por la red de antenas de celular y de ahí pasará directamente al dispositivo móvil, todo esto en cuestión de segundos.
En todo este viaje, nuestro mensaje tiene muchísimos **puntos de vulnerabilidad,** los cuales pueden ofrecer desde nuestra ubicación, como ocurre por ejemplo con las antenas, hasta la información que hemos compartido, puesto que, como hemos visto, esta queda almacenada en las compañías que nos ofrecen servicios de internet.

En la página de CIBERMUJERES, las compañeras han identificado estos puntos, los cuales son de mucha ayuda:

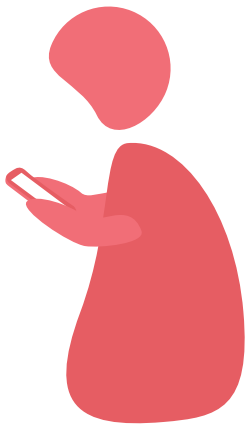
DISPOSITIVO 1 (COMPUTADORA/ CELULAR)	Inseguridad física; pérdida de información.
MÓDEM 1	Sniffing (robo de datos) de WiFi; información sin cifrar..
PROVEEDOR DE SERVICIOS DE INTERNET	Solicitudes de datos y metadatos de instancias gubernamentales locales/nacionales.
SERVIDORES DE GOOGLE	Vigilancia internacional; contraseñas inseguras y phishing (suplantación de identidad), solicitudes de instancias gubernamentales nacionales.
MÓDEM 2	Problemas de seguridad al utilizar las conexiones de terceros (ej. cibercafé).
DISPOSITIVO 2	Software malicioso; borrado inseguro de datos.

Tomado de: tinyurl.com/cibermujeres

Por todo eso, es fundamental que **nos apoyemos en diferentes herramientas,** por ejemplo:

Cambiar la contraseña de nuestro módem
Así podremos usar sitios y aplicaciones que nos permitan cifrar nuestros mensajes.

Transformarlos para que solo puedan ser leídos por las y los destinatarios que hemos elegido.



Si quieres ampliar la información sobre conectividad, puedes dirigirte a estas **fuentes relevantes:**

YOUTUBE.COM

¿Cómo nos vigilan en internet?

WWW.SINMIEDO.COM.CO/ SEGURIDAD.HTML

TINYURL.COM/ CFINTERNET

TINYURL.COM/ CVIAJAINTERNET

SEGURIDAD DIGITAL
O ESTRATEGIAS DE COMUNICACIÓN SEGURA
PARTE 2

2

¿CÓMO FUNCIONA INTERNET?

60 MINUTOS

TODO EL GRUPO

FICHAS BIBLIOGRÁFICAS Y MARCADORES
(TARJETAS CON LOS COMPONENTES DE LA CADENA DE FLUJO DE LA INFORMACIÓN)

PASO 2

Previamente a la actividad, debemos tener listas nuestras tarjetas con los componentes de la **cadena de flujo de la información:**

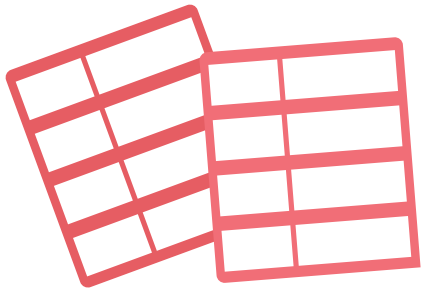
- Usuaria/o 1
- Módem
- Antena A
- Antena B
- Proveedor de servicios (ETB)
- Servidor de la empresa de mensajería (Gmail)
- Proveedor de servicios (Claro)
- Antena C
- Antena D
- Módem
- Usuaria/o 2

En este momento **repartimos las tarjetas al azar,** entre las once personas que nos acompañan en el centro. La idea es que les invites a que **se organicen** como crean que es **la manera correcta en la que viaja la información** al enviar un correo electrónico. Pueden tener ayuda de las personas que están alrededor.

2

PASO 3

Ahora, **quienes estamos facilitando la actividad, repasaremos la organización de los componentes,** haciendo uso de otra tarjeta, llamada mensaje, la cual nos ayudará a ir explicando, poco a poco, **cómo viaja la información.** Nos podemos apoyar en el apartado de Contenido vinculado a esta actividad.

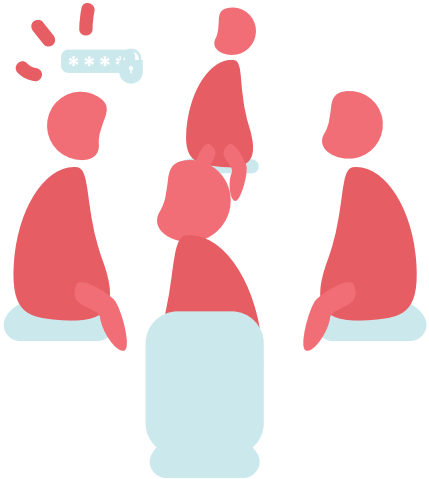


PASO 4

Aprovechemos para **diversificar la actividad,** invitando a las y los participantes a que exploremos **cómo sería el envío de un correo electrónico** si las dos personas son usuarias del mismo proveedor de internet, o **si estamos enviándolo o recibiéndolo desde un celular, etc.** Para estos nuevos casos es importante que tengamos **tarjetas en blanco y marcadores,** por si necesitamos cambiar alguno de los componentes en nuestra representación del flujo de información.

PASO 5

Este ejercicio nos puede permitir **identificar cuáles son los puntos de vulnerabilidad** en este flujo de información y las razones de ello. Preguntemos a las y los participantes **qué puntos son los que podemos identificar,** ayudándoles a complementar y explicar lo que haga falta, **haciendo uso del apartado de Contenido de esta actividad (especialmente la tabla)** y de los recursos virtuales dejados allí, así como de ejemplos de nuestra experiencia.



PASO 6

Para finalizar, podemos **reflexionar** alrededor de preguntas como: **¿por qué es importante cuidar nuestros datos? ¿Cómo podemos hacerlo? ¿Cómo construir estrategias de comunicaciones seguras?** Individuales y colectivas. allí, así como de ejemplos de nuestra experiencia.

2

OBSERVACIONES GENERALES

Esta actividad puede ser la oportunidad para que, como facilitadoras y facilitadores, investiguemos acerca de la manera en la que viaja la información, así como las vulnerabilidades a las que se expone la misma. En esa medida, podemos apoyarnos y compartir, con quienes estén en la actividad, videos, cartillas, sitios web, etc., respecto a este tema. En cuanto a las tarjetas, podemos hacerlas más grandes o incluso graficarlas, para que el ejercicio adquiera otras características visuales que nos ayuden a comprenderlo. De hecho, podemos plastificarlas, para que permanezcan en buenas condiciones, a pesar de usarlas varias veces y con diferentes grupos. Todo esto depende de nuestros recursos y de la cantidad de veces que planeemos hacer el ejercicio.

SEGURIDAD DIGITAL
O ESTRATEGIAS DE COMUNICACIÓN SEGURA

PARTE 3

¿QUÉ INFORMACIÓN NECESITA PROTECCIÓN? ¿CÓMO HACERLO? ¿QUÉ HERRAMIENTAS TENEMOS PARA UNA COMUNICACIÓN SEGURA?

110 MINUTOS

TODO EL GRUPO

VIDEOBEAM, COMPUTADOR, INTERNET, PAPELÓGRAFOS **PARTE 1:** MARCADORES

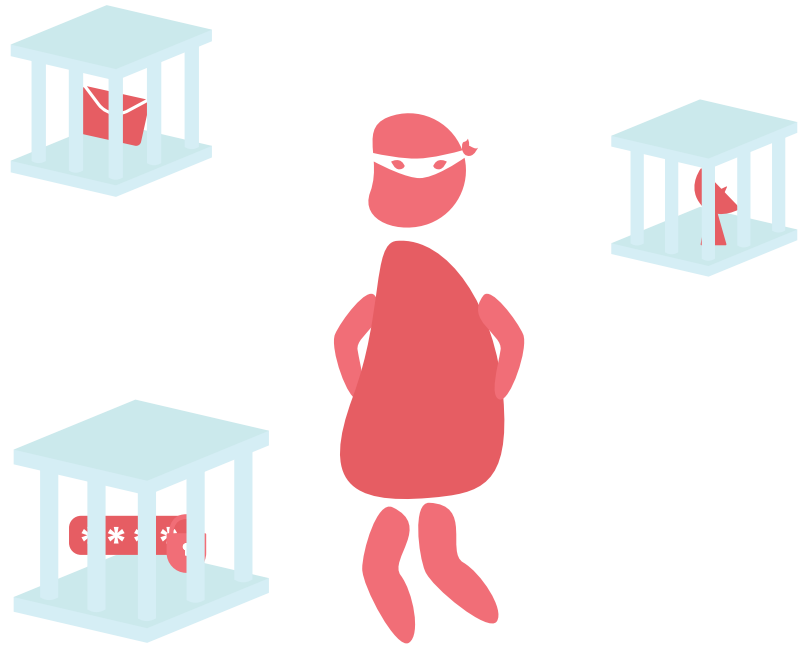
CONTENIDOS PARA ESTA ACTIVIDAD

Como vimos en apartados anteriores, una de las prácticas más importantes en cuanto a seguridad digital tiene que ver con el **análisis de la información,** para saber qué tanta privacidad necesitamos al enviarla y el **riesgo que tenemos al compartirla.** Vale diferenciar el riesgo vinculado a comunicar y el que tiene que ver con las actividades relacionadas al contenido de la información. Por ejemplo, **no es igual el riesgo que hay al enviar un mensaje en el que decimos el punto de encuentro** para una marcha y el de la marcha como tal.

Sumado a esto, debemos **analizar los riesgos contextualmente,** puesto que el envío de los mismos datos, con distintos fines, puede **necesitar en algunas ocasiones de la mayor privacidad** y en otras del hacerse visible y público, incluso **como una medida de protección.** Viéndolo en un caso concreto, no siempre el compartir una ubicación se considera como algo inseguro, sino que, **por el contrario, puede hacer parte de una estrategia de seguridad.**

Este análisis **posibilita crear protocolos de seguridad** dentro de las organizaciones, en la medida en que, quienes las componemos, podemos identificar **nuestras prácticas comunicativas,** revisar qué está funcionando, qué debemos modificar y **qué tipos de estrategias pueden funcionarnos para una mayor protección.**

Precisamente para ello contamos, entre otras herramientas, con algunas **aplicaciones, páginas, antivirus, navegadores, extensiones,** que pueden hacer parte de nuestras prácticas y protocolos de seguridad. Estas son sencillas de utilizar y, sobre todo, de compartir con las organizaciones con las que trabajamos.



Algunas de ellas son:

Contraseñas seguras

El primer **filtro de seguridad en nuestros computadores, celulares y cuentas** (correo, banco, etc.) **es nuestra contraseña.** Por tanto, es necesario corroborar el nivel de seguridad que tienen. Esto se refiere a la dificultad que implica para otros averiguarla, tanto manualmente como a través de programas destinados para ello.

Algunas recomendaciones para crear nuestras contraseñas involucran el **no recurrir a aquellas formas en que nos parece más fácil recordarlas,** es decir, no haciendo uso de información personal, como fechas, números de cédula, nombres de nuestras especies de compañía (mascotas) y/o familiares, etc.

De hecho, **es fundamental que no publiquemos ni compartamos de ninguna manera nuestra contraseña** con otros, ni escribiéndola en agendas, cuadernos, post-it, etc.

Entre los consejos que podemos tener en cuenta para crear contraseñas más seguras está, por ejemplo, **el uso de canciones y o frases que podamos recordar,** configuradas a partir de letras y números, algo como: qui3r0_much0_4_m1_p3rr0. También podemos emplear, para distinguir las contraseñas de diferentes plataformas, letras que, al final hagan alusión al sitio en el que tenemos nuestra cuenta: qui3r0_much0_4_m1_p3rr0_gm.

¿QUÉ TAN SEGURA ES MI CONTRASEÑA?

HOWSECUREISMYPASSWORD.NET

Es un sitio web que determina el tiempo en el cual un software podría descifrar nuestras contraseñas.
Pasos para hacer uso de este sitio:

1) Abrir el link en internet.
2) Insertar en el recuadro la contraseña sobre la que queremos corroborar su seguridad (no nos debemos preocupar por ponerla, ya que la página no identifica de qué cuenta es dicha contraseña, no se hace visible y no guarda información).
3) Mirar el color y los años que nos dice que tardaría un software en descifrar la contraseña. Puede parecer, por el tiempo que muestra, que nuestras contraseñas son muy seguras. Sin embargo, los software que realizan el trabajo de descifrar contraseñas evolucionan mes a mes. Así que, más allá de fijarnos en los años, nos tenemos que fijar en el color que toma la página. De esta manera, rojo indica que la contraseña es muy insegura, amarillo que es medianamente segura y verde que es muy segura.

Infoencrypt

Es una página web en la que podemos **encriptar textos,** es decir, **ocultarlos a través de una clave.** Es muy útil si tenemos que enviar información por un medio no seguro, por ejemplo WhatsApp, correo electrónico, mensaje de texto, Facebook, etc. Si tenemos abierta la página en el navegador (procedimiento que se debe hacer cuando estemos en línea), esta **funciona sin necesidad de conectividad a Internet,** por lo tanto, es una herramienta muy útil para trabajar en terreno. Podemos utilizarla desde el celular o el computador.

Pasos para encriptar (cuando eres quien envía el mensaje):

1) Escribir el texto en la página.
2) Asignar una contraseña (la pide dos veces) que previamente hayamos acordado con la persona con la que nos queremos comunicar.
3) Dar click en el botón "encrypt".
4) Seleccionar TODO el texto encriptado (de inicio a fin) y pegarlo en el medio de comunicación con el que queremos transmitir el mensaje, sea WhatsApp, correo electrónico, mensaje de texto de celular, Facebook, etc.

Pasos para desencriptar (cuando eres quien recibe el mensaje):

1) Copiar el mensaje que nos ha llegado encriptado, completo (de inicio a fin).
2) Entrar al sitio web y **pegar el texto en el recuadro** que aparece allí.
3) Introducir la contraseña que acordamos previamente (dos veces).
4) Dar click en el apartado **"Decrypt".**
5) Ahora podemos **leer el texto.**

Esta opción es muy útil también cuando **escribimos informes en terreno,** en el computador, **y queremos asegurarlos.** Una vez terminemos el documento, **lo encriptamos y guardamos.** Al llegar a la oficina o a una zona segura, lo podemos desencriptar. **En caso de robo de** computador, **las y los agresores** e interesados en esta información **no tendrán acceso a ella.**

WWW.INFOENCRYPT.COM

Signal

Es una aplicación de chat para comunicarnos vía celular, de manera segura y cifrada. Tiene las mismas funciones que WhatsApp, con la diferencia de que la comunicación es privada. A través de ella podemos hacer llamadas y audios, al igual que compartir documentos. En esta app, una vez que borremos un mensaje, este queda eliminado definitivamente de todos los lugares. Es un software libre, lo que significa que no es una iniciativa de una empresa. De igual manera, está sujeto a monitoreo constante para determinar su nivel de seguridad. Lo anterior, a diferencia de los software privados, en los que la empresa es la que determina el nivel de seguridad y, además, puede compartir con otros nuestra información. Al igual que WhatsApp, únicamente la podemos usar si la persona con la que queremos hablar tiene descargada la aplicación. En caso de que no la podamos descargar, debemos eliminar fotos y archivos pesados de nuestro teléfono.

WWW. SIGNAL.ORG

Firefox Send

Es una herramienta para compartir archivos de forma sencilla y privada. Permite cifrar documentos de extremo a extremo, es decir, dificulta el trabajo de alguien que quiere interceptar los correos. Lo hace a través de la generación de un link, al que solo tenemos acceso quienes enviamos y recibimos los archivos, pues podemos añadirle una contraseña y/o un tiempo para que el enlace caduque automáticamente. Este tiempo de caducidad puede ser por número de descargas o días. De esa manera, aseguramos que nadie pueda leer nuestro documento (ni siquiera Firefox lo puede hacer, pues se almacena cifrado) y también evitamos que permanezca en línea para siempre.

Para enviar los archivos:

1) Abrir en una página de internet, escribiendo el **link del sitio web.**

2) Dar click en el recuadro izquierdo de la pantalla, en **“Seleccionar archivos para subir”.**

3) Elegir un archivo de nuestro computador.

4) Elegir el número de descargas o días en que el documento va a estar disponible.

5) Seleccionar **“proteger con contraseña”.** Asignar una.
6) Dar click en **“subir el archivo”**.

7) Dar click en **“copiar el enlace”**.

8) Por un medio seguro -como Signal-, a la persona a la que queremos hacer llegar nuestros archivos.

Pasos para recibir los archivos:

1) Escribir en la barra de direcciones del navegador **el enlace que hemos recibido.**

2) Poner la clave que nos han compartido para poder descargar el archivo.

3) Descargar.

SEND.FIREFOX.COM

Complementos de Firefox

Mozilla Firefox (conocido simplemente como Firefox) es un **navegador web gratuito** y de código abierto que mejora con la disponibilidad de **numerosos complementos,** incluidos algunos que **están diseñados para proteger nuestra privacidad y seguridad** al navegar por la web.
En este enlace:

tinyurl.com/mseguridadonline

podemos encontrar **algunas de estas extensiones,** que funcionan para impedir la ejecución de scripts (archivos de procesamiento) por parte de páginas que no sean de confianza, eliminar cookies que puedan acceder a nuestros datos, tomar decisiones informadas sobre la información que compartimos en las webs, etc.

Jitsi

Es una **aplicación** para **realizar videoconferencias de manera cifrada.** Es un software libre y, a diferencia de Skype (que es una empresa privada), **no nos pide ningún tipo de información** para acceder a su sitio. No tenemos que insertar nombre, correo, ni ningún otro dato personal. **Una vez se termina la llamada y se cierra la página,** no queda ningún registro de la conversación ni de las personas que estaban en ella. Para celular, existe aplicación.
Para computador no es necesario, ya que es una página en línea. Esta página **funciona con baja conexión a internet,** por lo que es fácil realizar la videoconferencia. También permite trabajar documentos en línea.

Los pasos para hacer uso de Jitsi son muy sencillos:

1) Abrir en una página de internet, **escribiendo el link del sitio web.**

2) Insertar una palabra o frase (sin espacios), por ejemplo compañeras, en un recuadro que aparece en la ventana (parecido al que muestra Google) **y dar "enter". La plataforma creará un link con la palabra o frase** que escribimos, en el caso del ejemplo puesto previamente, sería algo así: **https://meet.jit.si/compañeras.**

3) Copiar el link generado por la plataforma y mandarlo a las personas con las cuales queremos mantener una conversación.

4) Corroborar que el número de personas en la llamada corresponde al número de personas que invitamos a la misma.

MEET.JIT.SI

Protocolo seguro de transferencia de hipertexto

Https **es la versión segura de http.** Tiene como función **proteger información sensible en la web,** como usuarios y claves, para que estos queden cifrados y los atacantes no puedan acceder a ellos.

SEGURIDAD DIGITAL
O ESTRATEGIAS DE COMUNICACIÓN SEGURA

PARTE 3

¿QUÉ INFORMACIÓN NECESITA PROTECCIÓN? ¿CÓMO HACERLO? ¿QUÉ HERRAMIENTAS TENEMOS PARA UNA COMUNICACIÓN SEGURA?

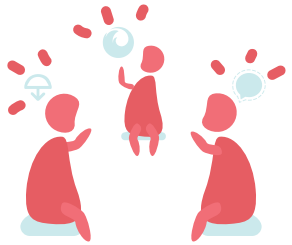
40 MINUTOS

TODO EL GRUPO

VIDEOBEAM, COMPUTADOR, INTERNET, PAPELÓGRAFOS **PARTE 1:** MARCADORES

PASO 1

Compartimos algunas herramientas sencillas que están especialmente diseñadas para seguridad digital. La idea es que **podamos irlas mostrando una a una** y que las y los participantes **puedan probarlas en sus celulares y/o computadores.**
Puede funcionar muy bien que **vayamos preguntando, conforme vamos viendo cada herramienta,** si algunas y algunos las han usado, cuáles ven que son sus puntos a favor y cuáles sus puntos en contra.



OBSERVACIONES GENERALES

Si no contamos con internet, es importante que llevemos la información sobre estas herramientas en un Power Point o en algún programa que nos permita visualizarlas sin conexión. Asegurémonos de que las personas que apenas conocen estos sitios, aplicaciones, etc., puedan recibir después esta información para poder en práctica lo aprendido en el taller, en el momento en que puedan tener conexión a internet.

¿QUÉ INFORMACIÓN NECESITA PROTECCIÓN? ¿CÓMO HACERLO? ¿QUÉ HERRAMIENTAS TENEMOS PARA UNA COMUNICACIÓN SEGURA?

40 MINUTOS

TODO EL GRUPO

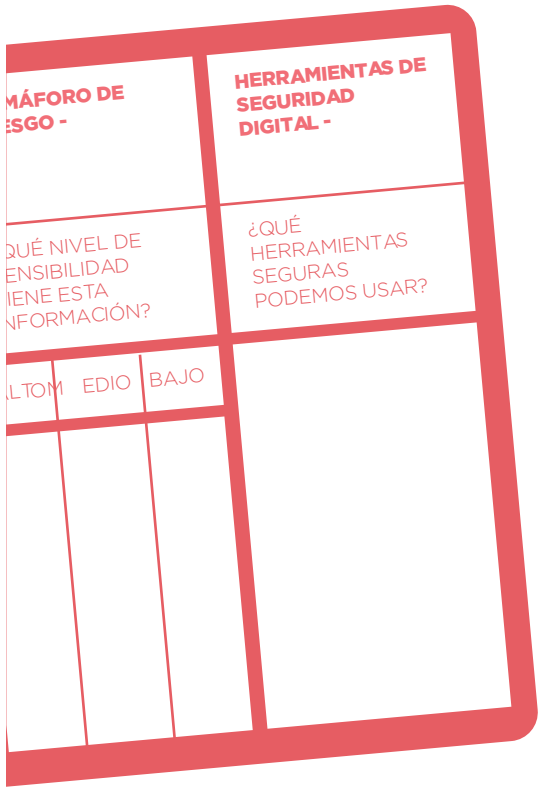
VIDEOBEAM, COMPUTADOR, INTERNET, PAPELÓGRAFOS **PARTE 1:** MARCADORES

PASO 2

Volvemos a organizarnos en los equipos con los que hemos trabajado previamente.

Repartimos las tablas desarrolladas en la actividad de la Parte 1.

La idea es que, para este momento, completemos **dos nuevas columnas,** primero, para que podamos **identificar el nivel de sensibilidad** de la información que estamos compartiendo como organización, teniendo en cuenta si esta implica un riesgo alto, medio o bajo. De acuerdo a ello, también vamos a identificar **qué herramientas de seguridad pueden ayudarnos** en los casos de la información categorizada como riesgosa.



SEGURIDAD DIGITAL
O ESTRATEGIAS DE COMUNICACIÓN SEGURA

PARTE 3

¿QUÉ INFORMACIÓN NECESITA PROTECCIÓN? ¿CÓMO HACERLO? ¿QUÉ HERRAMIENTAS TENEMOS PARA UNA COMUNICACIÓN SEGURA?

30 MINUTOS

TODO EL GRUPO

VIDEOBEAM, COMPUTADOR, INTERNET, PAPELÓGRAFOS **PARTE 1:** MARCADORES

PASO 3

Socializamos las tablas.

Después de ello, como facilitadoras y facilitadores **recogemos lo dicho, encontrando puntos en común y posibles estrategias que podríamos plantearnos** para mejorar la seguridad de nuestras comunicaciones, **invitando a generar protocolos en nuestra organización.**

abriendo espacios para la paz

Ministerie van Buitenlandse Zaken

Esta publicación ha sido financiada por el Ministerio de Asuntos Exteriores de Holanda. Los contenidos de esta publicación son responsabilidad exclusiva de PBI y no pueden ser entendidos como un reflejo de las opiniones de los donantes.

Metodología y contenidos desarrollados desde el área de reconstrucción del tejido social (ARTS) de PBI Colombia con colaboración de la Corporación Centro de Atención Psicosocial (CAPS) y el Movimiento Nacional de Víctimas de Crímines del Estado (MOVICE).

www.pbicolombia.org