KIT DE CIBERCUIDADO PARA ACTIVISTAS

Seguridad digital para cuidar nuestro activismo y reapropiarnos de Internet

HIPER DERE CHO

Tecnología como libertad

Cibercuidado como libertad 4

I. Kit de Cibercuidado para Activistas 5
¿Cómo uso el Kit de Cibercuidado para Activistas? 6
Soy activista, ¿para qué me sirve este Kit? 6

II. Una mirada diferente a la seguridad digital 7
¿Qué es un buen hábito de seguridad digital? 7
Seguridad digital con un enfoque de derechos humanos 7
Seguridad digital con perspectiva holística 8
Seguridad digital con enfoque de género 9
Seguridad digital para reducir la brecha digital de género 9

III. Creando mi plan de seguridad digital 10
Ficha de documentación de incidentes 10
Modelo de riesgos 11
Plan para mitigar amenazas 14
Protocolo de seguridad digital 15

IV. Amenazas comunes hacia activistas 17
Phishing 18
Acoso y amenazas de violencia física o sexual 20
Acceso no autorizado a dispositivos 21
Robo de identidad en redes sociales 23
Monitoreo o vigilancia del gobierno 26
Interceptado de comunicaciones 28
Acoso coordinado en redes sociales 30
Robo de dispositivos físicos 32

V. Privacidad y seguridad en redes sociales 34
Recomendaciones básicas de privacidad y seguridad 34
Reportar a agresores en plataformas 35
Mantén el control de los dispositivos que accedieron a tu cuenta 35

VI. Sanar después de la violencia 36

VII. Metodología para dictar Cibercuidado para Activistas 37
Sumilla de contenidos 37
Criterios para planear tu curso sobre seguridad digital 37
Creando capacitaciones online seguras 39
Cuidando el bienestar de tus participantes 39

VIII. Recursos complementarios 41

Anexos 42
Recurso 1: Abc digital para ciberseguridad

Autores
Daniela Salas
Denisse Albornoz
Edgar Huaranga

Diseño e ilustraciones
HUMANNICO

Agradecimientos especiales a
Colectiva por la Libre Información para las Mujeres (CLIM), Más Igualdad Perú, Colectivo Todas las Sangres y Plataforma Comadres

Financiado por
accessnow

Lima, julio del 2020

Esta y otras investigaciones de Hiperderecho sobre tecnología e interés público pueden descargarse desde hiperderecho.org/publicaciones

Asociación Civil Hiperderecho
Av. Benavides 1944, oficina 901 Lima 15074, Perú
hola@hiperderecho.org

CIBER-CUIDADO COMO LIBERTAD.

Internet se ha convertido en un espacio fundamental para ejercer nuestros derechos. Cuando te conectas, puedes participar políticamente, producir conocimiento y realizar activismo junto a personas que comparten tus ideales. Por eso, hoy vemos en la Internet peruana respuestas directas, dignas y valientes al machismo, racismo, homofobia, transfobia y otras formas de discriminación que vemos en nuestra sociedad. Nos llena de ilusión pensar en la tecnología como una aliada para denunciar injusticias y lograr cambios necesarios en nuestra sociedad.

Sin embargo, las y los activistas están viviendo actos de discriminación y violencia de género en Internet, que limitan su habilidad para participar en este espacio. En la investigación que realizó Hiperderecho en el 2018, encontramos que **mujeres y personas LGBTIQ+ están siendo atacadas por expresar sus opiniones políticas y sociales, por asociarse o expresar apoyo a la agenda feminista y por defender derechos LGBTIQ+.** Esto nos dice que Internet no es un espacio libre para todas las personas. La violencia de género ha encontrado nuevas formas de reinventarse y atentar contra aquellas y aquellos que están en la primera línea de la defensa de los derechos humanos.

Pero no todo está perdido.

Este **Kit de Cibercuidado para Activistas** fue creado para que sepas que existen muchas maneras para cuidarte y defenderte en Internet. Una de ellas es: **el entrenamiento en seguridad o cuidado digital.** Quizás aprender sobre seguridad digital o tecnología te suene difícil, lejano o abstracto. Sin embargo, estamos aquí para decirte que no tiene por qué ser así. **Saber sobre seguridad digital está a tu alcance, es menos complicado de lo que crees y es tu derecho.** Además, te prometemos que si te animas a aprender o a enseñar sobre seguridad digital, estarás contribuyendo a que todas las personas tengamos las mismas oportunidades de disfrutar de este espacio con tranquilidad, seguridad y libertad.

Así que si quieres acabar con el ciberpatriarcado, ¡Empecemos!

I. KIT DE CUIDADO PARA ACTIVISTAS

Este kit fue creado por el grupo de capacitadores en seguridad digital de Hiperderecho, de la mano de activistas de quienes aprendimos y con quienes construimos un curso de 4 meses para hablar sobre seguridad digital con enfoque de género.

Le agradecemos a cada una y uno de elles por su disposición para aprender sobre seguridad digital y sus ganas por construir una Internet feminista en la que todas y todos podamos ser quien queremos ser.

¿Qué puedo encontrar en el Kit de Cibercuidado para Activistas?

Aquí encontrarás:

- Una explicación accesible sobre qué es la seguridad digital:
  Te explicamos por qué es importante pensar en el cuidado o seguridad digital como una cuestión de derechos, con enfoque de género y desde una perspectiva holística que toma en cuenta también tu seguridad física y tu salud mental.

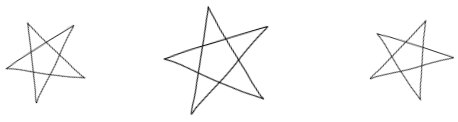
- Plan y protocolos de seguridad digital: Te explicamos cómo puedes empezar a planificar y documentar tus necesidades de seguridad digital junto a tu colectiva, organización o comunidad.

- Amenazas hacia activistas: Te contamos cuáles son las amenazas más comunes para activistas en el país y te damos recomendaciones puntuales para que sepas cómo defenderte desde la seguridad digital

- Consejos de privacidad y seguridad en redes sociales: Muchos de los ataques que reciben activistas aparecen en las redes sociales más populares en el Perú. Te damos algunas recomendaciones para mejores tu configuración de privacidad en Facebook, Twitter, Whatsapp o Instagram.

- Sanando después de la violencia: Te invitamos a que este sea el primer paso para que construyamos una Internet más sorora, libre y segura para todas, todos y todes.

- Metodología para capacitar a tus comunidad sobre este tema: Este kit fue inspirado por las clases que realizó Hiperderecho en el 2020 a cinco colectivas activistas en el Perú que defienden los derechos de las mujeres, los derechos sexuales y reproductivos y derechos LGBTIQ+. Compartimos nuestras lecciones aprendidas.



¿Cómo uso el Kit de Cibercuidado para Activistas?

Este kit está dirigido para personas que son activistas, aplican en su trabajo un enfoque de género y utilizan Internet para defender los derechos humanos. Recomendamos utilizar este Kit como un punto de partida para:

- Conocer conceptos claves y entender la importancia de la seguridad digital para el activismo.
- Familiarizarse con herramientas de planeamiento organizacional en seguridad digital.
- Aprender a diseñar planes de seguridad digital de acuerdo a amenazas específicas.
- Capacitar a tu comunidad sobre seguridad digital.

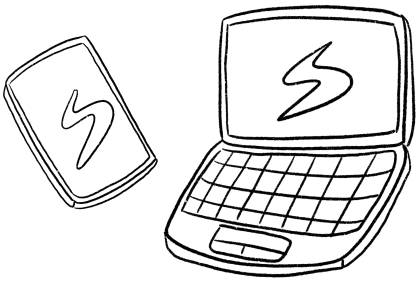
Soy activista, ¿para qué me sirve este Kit?

Como activista, tienes derecho a existir en Internet y utilizarla libremente y de manera segura. Lamentablemente, puede que te encuentres con formas de violencia como estas que buscan entorpecer tu trabajo:

- La captura de tu contraseña por medio de phishing
- Acoso y acoso coordinado
- Amenazas de violencia física o sexual
- Acceso no autorizado a dispositivos
- Robo de identidad en redes sociales
- Monitoreo o vigilancia del gobierno
- Comunicaciones que pueden ser interceptadas

Y otras formas de violencia que ponen en riesgo la integridad de las y los miembros de la colectiva con la que activas.

Por eso, saber sobre seguridad digital es tan valioso. Te permite cuidarte de estas formas de violencia, proteger tu identidad, cuidar a tu comunidad y sobre todo **- asegurarte que el importante trabajo que realizas sea sostenible a lo largo del tiempo.**



II. UNA MIRADA DIFERENTE A LA SEGURIDAD DIGITAL

Definimos a la seguridad digital como el conjunto de hábitos y decisiones que tomamos para mitigar riesgos asociados al uso de la tecnología.

Por si no lo notaste, esta definición no se enfoca en la tecnología, sino en el uso que le damos y las decisiones que tomamos alrededor de ella según nuestro contexto y necesidades. Por eso, aprender sobre seguridad digital implica crear nuevos hábitos, construir nuevos conocimientos y así, tomar decisiones enfocadas en la privacidad y la seguridad. ***Es una invitación a repensar nuestra relación con Internet.***

¿Qué es un buen hábito de seguridad digital?

Un buen hábito de seguridad digital es todo hábito que busca proteger la privacidad de mi información y la seguridad de las personas que están asociadas a ella. Al ser un hábito, se construye a lo largo del tiempo. Por eso, mejorar tu seguridad digital será un proceso de aprendizaje continuo, de constancia y determinación.

Un buen hábito pueden ser hábitos tecnológicos como tener un buen gestor de contraseñas o utilizar aplicaciones con cifrado de extremo a extremo. Sin embargo, existen también varias acciones que realizamos fuera de Internet que nos permiten construir un entorno online seguro. Hábitos tan simples como cerrar sesión en una computadora, cerrar la laptop al terminar de usarla en un espacio compartido, o desconfiar de los enlaces que envían, son parte del conjunto de hábitos positivos que podamos adoptar en nuestra relación con Internet y tecnologías.

Si adoptamos buenos hábitos de seguridad digital, las interacciones que construimos en espacios virtuales no solo serán mejor aprovechadas, sino potencialmente más saludables y más seguras. Esto nos hará sentir capaces de generar espacios seguros para nosotras y para las personas que buscamos proteger.

Seguridad digital con un enfoque de derechos humanos

→ **Defensa de tu derecho a la libertad de expresión:**
La libertad de expresión protege nuestro derecho a buscar, recibir y difundir información en igualdad de condiciones. Con seguridad digital, puedes sentar las bases para que grupos históricamente discriminados puedan seguir expresándose y que la difusión de luchas sociales no sean censuradas.

→ **Derecho a la privacidad:**
Tienes derecho a buscar información en Internet sin que nadie se entere quién eres o por qué la estás buscando. Tu derecho indica que nadie puede acceder, intervenir ni divulgar información relativa a tu vida privada, familiar, correos electrónicos (o de cualquier tipo) o tu domicilio, a menos de que tú le des permiso. Con la seguridad digital, puedes aprender a proteger tu privacidad para que tu información sea vista solo por quien tú quieres que la vea.

→ **Derecho a una vida libre de violencia de género:**
Ya sea en la calle o en Internet, tenemos derecho a una vida libre de violencia de género. Este derecho debe ser protegido a fin de que podamos navegar sin que nadie perturbe nuestra tranquilidad, integridad y seguridad. En la seguridad digital encontramos una primera línea de defensa para evitar que las personas que te quieren hacer daño o causar sufrimiento sobre la base de tu género, no se puedan acercar a ti.

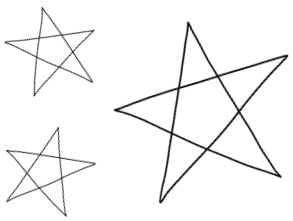
Seguridad digital con perspectiva holística

Desde una perspectiva holística, la seguridad digital comprende tres dimensiones: la seguridad física, la mental y de autocuidados y, por último, la digital.[1] Apostamos por este enfoque porque implica que aquello que vivimos en Internet también es real y, por tanto, reconoce que los riesgos que vivimos en espacios virtuales fácilmente pueden trasladarse al espacio físico.

→ **Cuidando tu seguridad física:**
Por ejemplo, si una persona te está acosando en Internet y accede a tus datos personales como tu número de teléfono o tu dirección, se vuelve más probable que esta persona también te acose físicamente. Al proteger tus datos y tu información en el espacio virtual, estás también protegiendo tu seguridad física. También velas por tu tranquilidad y tu derecho a una vida libre de violencia.

→ **Cuidando tu salud emocional:**
Por ejemplo, pensemos en las labores de las y los community manager.
Frente a comentarios violentos, es evidente que esta persona cargará, con el peso y desgaste emocional que supone leer constantemente este tipo de contenido. Darle herramientas de seguridad digital que alivien su trabajo de moderación y que bloqueen comentarios que le pueden afectar, es una manera de cuidar su salud mental.

En este sentido, la seguridad digital holística nos permite construir una Internet centrada en el bienestar, sobre todo en el de aquellas personas que están en la primera línea de defensa y, por lo tanto, se ven constantemente vulnerados en espacios virtuales.



[1] Definición dada por Digital Defenders Partnership
https://www.digitaldefenders.org/training-and-accompaniment/digital-integrity-fellowship/

Seguridad digital con enfoque de género

Lamentablemente, Internet es un espacio donde las mujeres, las disidencias sexuales y las activistas se sienten inseguras.[2] **Por eso, no podemos hablar de Internet segura sin mencionar el enfoque de género. Esta perspectiva nos lleva a fijar la mirada sobre cómo las mujeres, los cuerpos e identidades femeninas y quienes no se rigen por la cisheteronormatividad, experimentan mayores y determinados riesgos en línea**. También nos permite reflexionar sobre cómo esta violencia está normalizada en espacios digitales a partir de la vigencia de estereotipos, roles y valoraciones de género que norman sobre la identidad, orientación y expresión sexual de las personas.

En esa línea, la seguridad digital con enfoque de género nos invita a adoptar una serie de medidas, hábitos y herramientas para mitigar amenazas de las que son blanco poblaciones históricamente discriminadas sobre la base del género: como mujeres en su diversidad, los activismos feministas y poblaciones LGTBIQ+. Manteniendo a salvo nuestras cuentas y comunicaciones, así como las de personas que nos acompañan en activismos en línea, hacemos todo lo posible por que lo que compartimos no les exponga a riesgos en Internet.

Seguridad digital para reducir la brecha digital de género

Finalmente, otro obstáculo que queremos superar con la educación en seguridad digital es el de la brecha digital de género. **Sabemos que las mujeres peruanas tienen menos acceso a Internet que los hombres y están menos representadas en el contenido que se genera y difunde en línea.**[3] Tener menos acceso también implica que no estamos generando las habilidades digitales que necesitamos para acceder a recursos de educación, salud y trabajar de manera segura y equitativa en este espacio. Al promover buenos hábitos de seguridad digital, estamos promoviendo medidas para que las mujeres puedan conseguir y garantizar su acceso en igualdad de oportunidades.

[2] En: Conocer para resistir
https://hiperderecho.org/tecnoresistencias/wp- content/uploads/2019/01/violencia_genero_linea_peru_2018.pdf
[3] En ¿Estamos conectados? Brecha de género digital en el Perú

III. CREANDO MI PLAN DE SEGURIDAD DIGITAL

Crear un plan de seguridad digital es una acción con la cual afirmamos nuestro derecho a pertenecer a Internet. En esta sección te contamos sobre cuatro herramientas o procesos clave para planear tu estrategia de seguridad digital:

1. Ficha de documentación de incidentes
2. Modelo de riesgos con enfoque de género
3. Plan de seguridad digital
4. Protocolo organizacional de seguridad digital

La seguridad digital no es una receta que debemos seguir sin cuestionar, tenemos que integrar lo que funciona para cada una de nosotres. Cuando diseñes tus planes y protocolos de seguridad digital, recuerda adaptarlos a tu contexto y tus necesidades.

1. Ficha de documentación de incidentes

La ficha de documentación de incidentes es una herramienta para registrar incidentes que hayan ocurrido en el ámbito digital. **Por "incidente" nos referimos a cualquier evento que ocurra que pueda constituir un abuso, acoso o alguna forma de violencia en línea en Internet y haya supuesto algún riesgo o peligro para ti o alguien de tu colectiva.**

¿Cuándo debería utilizarla?

Es importante utilizar esta herramienta una vez que los sucesos ya han ocurrido. Idealmente, inmediatamente después de un incidente o unos días después como máximo, de modo que puedes documentar cómo esto les afectó a les integrantes de tu colectiva y a ti. En ese sentido es una medida de tipo reactiva porque se enfoca en registrar sucesos ya acontecidos.

1. Documentar los incidentes convierte a las amenazas digitales en **algo real, que podemos ver y podemos medir.** Esto nos ayuda a luchar contra la normalización de la violencia.

Debemos cuestionar la normalización de situaciones de violencia de género en línea: No, no es normal que en Internet solo algunas personas puedan expresar libremente su identidad e ideas, afectos y luchas, ¡conociendo y poniendo nombre a los riesgos a los que nos enfrentamos comenzamos a actuar contra ellos!

2. Nos invita a generar el hábito de **conservar evidencia** de los incidentes que más adelante nos pueden servir para reportar los incidentes ante las plataformas intermediarias, o denunciarlas ante las autoridades.

3. Nos permite encontrar **patrones de abuso o ataques** que de otra manera no te hubieras dado cuenta o que, en general, pasan desapercibidos. Con la información recabada podemos luego diseñar planes de acción y prevención aterrizados en situaciones puntuales.

2. Modelo de riesgos

Un modelo de riesgos es una herramienta que te permite medir y evaluar las amenazas que vives en el ámbito digital. Puntualmente, te sirve para conocer el perfil de riesgo de tu organización, y así determinar el tipo de protección que necesitas para cuidar tu información.

¿Qué tan seguido debería modelar mis riesgos?

Es recomendable hacer un modelado de riesgos cada cierto tiempo - puede ser cada 3 o 6 meses, o cada año. Depende de qué tanto cambie el panorama de seguridad digital de tu colectiva.

Recuerda tomarte un descanso cuando estés mapeando esta información. Este es un proceso en el que las personas involucradas estarán expuestas a situaciones de recordar amenazas y esto podría perturbar el bienestar individual y grupal. **Recomendamos prestar mucha atención a nuestro sentir propio y el de los demás y cuidarse mucho en este proceso.**

¿Cómo creo un modelo de riesgos?

Para crear tu modelo de riesgo y conocer el perfil de riesgo de tu organización debes identificar lo siguiente:

1. Identifica **qué es lo que quieres proteger** o tus **activos.** Estos son los datos o información que quieres proteger porque pone en riesgo a tu organización o a tu comunidad. Recuerda que la información que guardas en tus dispositivos o que compartes en tus redes sociales puede revelar mucho sobre ti y personas que quieres cuidar.

2. Identifica **de quién quieres protegerlos** o tus **adversarios**, las personas, organizaciones o comunidades que quieren hacerte daño y buscan censurar, bloquear o detener tu activismo por diferentes motivos. Un adversario puede ser una ex pareja, una colectiva organizada, o el gobierno.

3. Identifica la **capacidad de tus adversarios** o los recursos económicos, sociales y tecnológicos que tiene tu adversario.

Existen diferentes niveles de adversario de acuerdo a sus capacidades:

- **Adversarios poco sofisticados:** Usuarios comunes sin conocimiento profundo de tecnología, pero que buscan hacer daño social o emocional. Por ejemplo, usan redes sociales de manera convencional, pero los utilizan para hacer comentarios agresivos, enviar mensajes directos a quienes no piensen como ellos. Pueden ser compañeros de trabajo, de estudio, roommates, etc.

- **Medianamente sofisticados:** Estas personas saben cómo utilizar herramientas para realizar ataques menores a páginas web y podrían tener acceso a información sensible a partir de su círculo social o laboral. Por ejemplo, un empleado de una empresa de telecomunicaciones podría acceder al registro de llamadas o consultar a quién le pertenece un número celular gracias a su posición.

- **Muy sofisticados:** Este adversario tiene mucho alcance y muchos recursos. Por ejemplo, el gobierno puede adquirir o desarrollar herramientas para la vigilancia de activistas o un miembro de la Policía podría solicitar acceso a la ubicación de tu celular en los últimos tres meses sin necesidad de una orden judicial (DL 1182). Mayor información en hiperderecho.org/dl1182.

4. Identifica las **amenazas** o los ataques, incidentes o cualquier eventos que tus adversarios podrían llevar a cabo para amenazar la seguridad de nuestros activos y la posible consecuencia de esta amenaza.

¡Tomen un enfoque de género cuando identifiquen amenazas!
Asegúrense de identificar los ataques específicos que como activistas feministas que trabajan en defensa de mujeres, disidencias, y la comunidad LGTBIQ+, podrían recibir.

5. Mide el **riesgo** o la posibilidad de que una amenaza se vuelva realidad.

¿Cómo mido el riesgo de mi amenaza?

La organización Level-Up nos sugiere un gran método:

1. **Identifica la probabilidad de que esa amenaza ocurra y se convierta en realidad.** Para evaluar la probabilidad hay que tomar en cuenta factores técnicos y sociales. Toma en cuenta el género y la defensa de los derechos humanos como factores de riesgo. Para medir las probabilidades de estos riesgos, formula una escala simple de 1 a 5, donde 5 equivale a una probabilidad "Muy alta" de que el riesgo podría convertirse en real y 1 es una probabilidad "Muy baja".

Si no estás segura, puedes revisar tu ficha de documentación de incidentes para notar si es algo que pasa frecuentemente.

AMENAZA	RIESGO O PROBABILIDAD 1 = muy bajo 5 = muy alto
Accidentalmente le di click a un link de correo con malware	4
Nuestro disco duro ha sido investigado por autoridades	1

2. **Determina el impacto que estas amenazas tendrían sobre una persona, organización, colectiva si una amenaza se hiciera realidad y cuál sería su reacción:** Crea una escala para medir el impacto; esta puede ser otra escala cuantitativa (numérica) similar a la que se usó para medir la probabilidad, o puede ser una escala cualitativa (descriptiva).

AMENAZA	RIESGO O PROBABILIDAD 1 = muy bajo 5 = muy alto	IMPACTO 1 = severidad baja 5 = severidad alta	REACCIÓN 1 = tranquilo, bajo control. 5 = pánico, alto nivel de estrés.
Accidentalmente le di click a un link de correo con malware	4	3	2
Nuestro disco duro ha sido investigado por autoridades	1	5	5

La naturaleza de un impacto y su gravedad dependen de una serie de factores externos. Por ejemplo, una amenaza puede impactar poco la seguridad de información, **pero mucho la salud mental de tus compañeras. Eso ya la hace urgente de atender.** Debes decidir en qué quieres enfocarte, priorizando el bienestar de tu comunidad.

Este análisis te permitirá saber cuales son las amenazas en las que te tienes que enfocar. Prioriza las que sean más probables, las que crearían un mayor estrés sobre tus compañeras, y las que generen mayor impacto sobre la seguridad de tu información.

¿Por qué debería utilizarla?

1. El modelo de riesgos nos permite identificar de manera **proactiva** las amenazas a las que queremos darle prioridad en nuestros planes o protocolos de seguridad digital.

2. Es una oportunidad para planear, y tomar decisiones conjuntas sobre cómo abordaremos estas amenazas y crear estrategias de respuesta y prevención. **¡El diálogo y la construcción colectiva de la seguridad digital es muy importante!**

3. Es una herramienta que te permitirá cuidar a tu equipo y **manejar el nivel de estrés que generan las amenazas de seguridad digital.** Cuando hagan un modelo de riesgos, asegúrense de tomar intervalos frecuentes y recordar que este proceso les ayudará a enfrentar riesgos en el futuro.

3. Plan para mitigar amenazas

Un plan de seguridad digital es el conjunto de medidas que tomará una persona o colectiva para mejorar su seguridad digital. La respuesta a esta pregunta debe estar basada en nuestro perfil de riesgos y enfocada en crear respuestas y soluciones para atenderlos.

¿Se acuerdan cuando indicamos que no existe una fórmula mágica que nos solucione o ayude a enfrentar los distintos riesgos y amenazas en Internet? No hay una opción perfecta para la seguridad. No todos tienen las mismas prioridades, preocupaciones o acceso a los recursos. En esa línea, **tu plan de acción te permitirá planificar la estrategia adecuada, equilibrando la conveniencia, el costo y la privacidad, elementos centrales a la hora de elaborar tu plan.**

Para armar tu plan debes tomar nota de todo lo que te gustaría hacer para mitigar las amenazas que tu colectiva y tú experimentan. Para cada amenaza, pregúntate: ¿Qué puedo hacer para abordar un riesgo y / o evitar que ocurra?

RIESGO DIGITAL	**PROBABILIDAD** 1 = muy bajo 5 = muy alto	**IMPACTO** 1 = severidad baja 5 = severidad alta	**REACCIÓN** 1 = tranquilo, bajo control. 5 = pánico, alto nivel de estrés.	**¿QUÉ PUEDO HACER?**
Accidentalmente le di click a un link decorreo con malware (Phishing)	4	3	3	Cambiar de contraseñas, descargar e instalar un antivirus; advertir a otras personas en mi círculo y/u organización para que estén atentos de no darle click a ese link.

Ten en cuenta tus capacidades y si tienes restricciones financieras, técnicas o sociales.

Recuerda que las medidas que tomes para abordar tu amenaza pueden ser divididas en reactivas y proactivas. Por ejemplo, si lo que quiero es una medida que atienda a una situación que ya ocurrió y mitigue los riesgos más inmediatos, buscaría una solución reactiva. Pero si quiero anticiparme a una posible situación de riesgo a futuro, buscaré una medida proactiva.

AMENAZA	¿QUÉ PUEDO HACER?	¿CÓMO LO VOY A HACER?	RESTRICCIONES O DESAFÍOS
Accidentalmente le di click a un link decorreo con malware (Phishing)	1. Cambiar las contraseñas de mis perfiles.	Crear contraseñas nuevas e informar a quienes tienen acceso. **(medida reactiva)**	Recordar o memorizar las nuevas contraseñas.
	2. Descargar e instalar un antivirus.	Investigar un antivirus apropiado para mis necesidades **(medida proactiva)**	Costo y brecha de conocimiento sobre cuál es el mejor antivirus.
	3. Advertir a otras personas en mi círculo y/u organización para que estén atentos de no darle click a ese link.	Dictar capacitaciones internas sobre phishing y enlaces maliciosos. **(medida proactiva)**	Tiempo de compañeras.

¿Por qué debería armar mi plan de seguridad digital?

1. Te permite tomar pasos concretos para reducir los riesgos a los que está expuesta tu colectiva, y así proteger su información y a tu comunidad.

2. Tener un plan de acción le puede dar tranquilidad y serenidad a quienes manejan las redes sociales y tecnologías de tu organización.

3. Te da ideas y crea una base sólida para diseñar un protocolo de seguridad digital para tu organización que puedes implementar de manera sistemática.

4. Protocolo de seguridad digital

A diferencia de un plan, un protocolo es un conjunto de medidas o acciones relacionadas con la seguridad digital que están conectadas a una actividad o proceso específico dentro de una organización o colectivo. Los protocolos son prácticas continuas que siguen vigentes incluso cuando un plan de seguridad digital se ha implementado por completo, y evolucionará con el tiempo en respuesta a los cambios que implementes en tu organización.

¿Cuándo debo crear mi protocolo de seguridad digital?

Es recomendable que implementes tu protocolo al mediano plazo, para que identifiques lo que funciona y lo que no y que lo revises cada cierto tiempo (a tu discreción). Recomendamos también que armes el protocolo organizacional de manera colectiva para que refleje las necesidades, intereses, fortalezas y vulnerabilidades de todo tu equipo.

¿Cómo construyo mi protocolo de seguridad digital?

El siguiente formato puede ser útil como un punto de partida:

AMENAZAS Y RIESGOS	¿Qué amenazas y riesgos nos enfrentamos actualmente? ¿Cuál podríamos enfrentarnos potencialmente en el futuro?
VULNERABILIDADES IDENTIFICADAS	¿Cuáles de nuestras prácticas como individuos, o circunstancias como organización, podría exponernos a ser atacados?
FORTALEZAS Y CAPACIDADES	Como organización, ¿Con qué capacidades contamos que nos den una ventaja en la respuesta a amenazas y riesgos identificados?
ACCIONES PARA MITIGAR	¿Qué acciones necesitamos emprender para mitigar riesgos identificados?
RECURSOS REQUERIDOS	¿Qué recursos (económicos, humanos, etc.) y herramientas necesitamos para implementar estas acciones?
¿QUIEN DEBE ESTAR INVOLUCRADX?	¿Qué áreas o personas dentro de nuestra organización tienen que estar involucradas en la implementación? ¿Se requerirá alguna autorización u otros permisos?
PLAN DE MONITOREO	¿Cómo sabremos que las acciones están funcionando? ¿Cómo identificar los obstáculos? ¿Qué tan seguido revisaremos este protocolo?

Con toda esta información, podrás diseñar protocolos concretos para cada tipo de amenaza.

¡Ahora estamos listxs para mitigar riesgos en nuestro activismo online!

IV. AMENAZAS COMUNES HACIA ACTIVISTAS

Las organizaciones activistas, están expuestas a amenazas desde diferentes frentes. Aquí resaltamos tres:

1. Amenazas que buscan cerrar los canales de expresión o espacios donde organizaciones comparten su mensaje.

2. Amenazas dirigidas a perseguir a las personas que dirigen las organizaciones y/o que manejan estas plataformas.

3. Amenazas dirigidas a divulgar las identidades y datos de las personas que participan en eventos o actividades comunitarias de la organización.

Una de las actividades de una colectiva es brindar información, capacitar y compartir su mensaje con muchas otras personas, ya sea para dar apoyo técnico, psicológico, legal, etc. **Por ello es importante identificar el tipo de información que la colectiva tiene en su poder sobre estas personas y cuidarla. Buenas prácticas de seguridad digital mantendrá segura también a tu comunidad.**

	ACTIVOS		
AMENAZAS	**Canales de expresión de la organización**	**Datos de personas que manejan los canales de expresión**	**Datos de la comunidad que me sigue o participa de mis eventos**
Phishing	No	Sí	Sí
Acoso y acoso coordinado	Sí	Sí	Sí
Acoso no autorizado o dispositivos	No	Sí	No
Robo de identidad en redes sociales	Sí	Sí	No
Monitoreo o vigilancia	Sí	Sí	No
Interceptado de comunicaciones	No	Sí	No
Ataque coordinado en redes sociales	Sí	Sí	No
Robo de dispositivos	Sí	Sí	Sí

En la sección correspondiente encontrarás una breve descripción de cada amenaza, un ejemplo de cómo puede afectar a cada tipo de activo en caso corresponda, las recomendaciones y herramientas que te recomendamos para mitigar estas amenaza y finalmente, de manera puntual, los conceptos necesarios para poder entender la base de estas recomendaciones. Estos conceptos también pueden ser el punto inicial para un estudio más profundo de las herramientas y tecnologías utilizadas.

Phishing

Esta es una técnica maliciosa utilizada para ***obtener información sensible (datos de tarjetas de crédito, nombres de usuario y contraseñas, etc.) de los usuarios.*** Los atacantes se hacen pasar por una entidad de confianza para que las víctimas confíen en ellos y revelen sus datos confidenciales. Los datos recogidos a través de phishing se pueden utilizar para el robo financiero, robo de identidad, para obtener acceso no autorizado a las cuentas de la víctima o a las cuentas que tienen acceso, a la víctima de chantaje y más.

COMO AFECTA A:		
Canales de expresión de la organización	**Datos de personas que manejan los canales de expresión**	**Datos de comunidad que me sigue o participa de mis eventos**
No aplica	Un miembro de una colectiva brindando apoyo podría ser objetivo de este tipo de ataque a través de **enlaces maliciosos** que son enviados a su correo electrónico, teléfono celular, cuentas en redes sociales, etc.	El ***phishing*** puede ser utilizado por un adversario que se robe la identidad de la organización, para pedir información sensible a la comunidad. Es importante que las colectivas instruyan a sus comunidades sobre cómo identificar y evitar esos enlaces.

¿Qué hábitos de seguridad digital debo practicar para evitar que esto pase?

Hiperión recomienda:

Analiza la veracidad de los mensajes que recibas vía SMS, Mail, WhatsApp u otra aplicación de mensajería. Se puede tomar un Test de phishing para conocer qué tanto podemos identificar posibles amenazas de phishing.

Utiliza un **Password Manager** para asegurar las recomendaciones de **contraseñas seguras.**

Activa un método de **autenticación de dos pasos** para el ingreso a tus cuentas. Esto permite que los atacantes, a pesar de tener tu contraseña, no sean capaces de ingresar.

Mantén actualizado tus programas y sistema operativo tanto como sea posible. Las actualizaciones siempre vienen con parches y mejoras de seguridad.

Recordemos:

- Una contraseña se considera segura si no es una palabra o frase relacionada a tu vida personal (cumpleaños, mascota, fecha de nacimiento, nombre, etc).
- Mientras más larga la contraseña, más segura.
- Otra característica de una contraseña segura es que sea una diferente para cada red social o cuenta en Internet (no utilices la misma contraseña para todo).

- En caso quisieras saber si tu contraseña fue filtrada en algún ataque a una aplicación o servicio web lo puedes comprobar en haveibeenpwned.com.
- Un gestor de contraseñas nos facilita la manera de escoger contraseñas seguras. Existen opciones gratuitas como LastPass, Firefox Lockwise pero también otras muy buenas de pago como 1Password.
- La autenticación en dos pasos nos permite adicionar una segunda capa de seguridad para acceder a nuestras cuentas en Internet. Esto significa que incluso cuando alguien conozca tu contraseña, no les será posible acceder a tus cuentas.
- Según la configuración, este factor puede ser un código enviado al teléfono celular o correo electrónico. En otras ocasiones es posible tener una aplicación a manera de Token. Para este último caso tenemos alternativas como Authenticator de Google, Microsoft Authenticator o Authy.

Acoso y amenazas de violencia física o sexual

La violencia de género y las distintas formas de vulneraciones, amenazas, agresiones y abuso a nuestra integridad y bienestar también están presente en Internet y en las redes sociales usadas por les activistas. El acoso es una de las más presentes y puede llegar a escalar a situaciones que suponen aún más peligro para quienes las experimentan. Al respecto, definimos que el acoso en línea consiste en que una o varias personas utilicen la tecnología para vigilar, perseguir, hostigar, asediar o buscar establecer contacto o cercanía con una persona de tal modo que pueda alterar el normal desarrollo de su vida cotidiana.

No es necesario que la conducta sea reiterada, continua o habitual para que sea considerada acoso y reciba una sanción. Una vez es suficiente para alterar el desarrollo de nuestra vida cotidiana, perturbando nuestra tranquilidad. Por ejemplo, escribir mensajes en sus redes sociales a una activista con insultos y amenazas de violación, o que un compañero de trabajo escriba mensajes insultantes son conductas de acoso.

COMO AFECTA A:		
Canales de expresión de la organización	**Datos de personas que manejan los canales de expresión**	**Datos de comunidad que me sigue o participa de mis eventos**
No aplica	Usualmente, en redes sociales, es fácil identificar a las personas que están administrando una organización activista. El acoso masivo dirigido a la organización puede seguir su flujo a las cuentas personales de quienes la administran o quienes están a favor del mensaje.	No aplica

¿Qué hábitos de seguridad digital debo practicar para evitar que esto pase?

Hiperión recomienda:

1. Googleate a ti mismo(a) para ver qué información personal está disponible en Internet, y de ser posible, solicita eliminarla a la persona que administre la cuenta o el sitio en la que esté publicada esta información.

2. Para el caso de redes sociales como Facebook, puedes configurar las opciones de privacidad para que tu perfil no se muestre como resultado de las búsquedas por nombre, número de celular o correo electrónico.

3. De ser necesario, configurar sus redes sociales en privado, deshabilitar la opción de recibir mensajes de personas que no conoces o también filtrar el contenido que pueden escribir en nuestras publicaciones, videos en vivo, etc. Un ejemplo para Instagram es habilitar el filtro de palabras ofensivas. También está disponible una opción para páginas de Facebook.

4. Limitar el alcance de las personas que pueden ver tu contenido (fotos, publicaciones).

5. Considera crear una cuenta aparte para tus actividades como activista. De ser posible, no compartas - o mantén al mínimo - fotos personales o taggees amistades o familiares. Asimismo, podrías deshabilitar la opción de geolocalización cuando tus posts sean públicos. Toda esta clase de información sobre tu vida personal podría ser usada en tu contra por alguien que busque hacerte daño. Nunca olvides: son tus decisiones y no hay una fórmula única para estar segures.

Recordemos:

- La salud psicológica de las personas detrás de las actividades y plataformas de la organización son tan importantes como cualquier otro activo.
- Recordemos nuestro espacio en Internet y quiénes son las personas que están expuestas en los frentes de este espacio y que, por lo tanto, están expuestas a este tipo de ataques.

Acceso no autorizado a dispositivos

Esta modalidad consiste en ingresar a cuentas personales mediante el robo de contraseñas o la intervención de dispositivos de una persona, generalmente con el objetivo de obtener datos privados e información personal. Esta modalidad de violencia es utilizada para capturar datos personales de las víctima o imágenes íntimas, que luego pueden ser utilizadas para ejercer otro tipo de violencia: la difusión de contenido íntimo sin consentimiento.

COMO AFECTA A:		
Canales de expresión de la organización	**Datos de personas que manejan los canales de expresión**	**Datos de comunidad que me sigue o participa de mis eventos**
Este tipo de amenaza ataca directamente a los **activos** de la organización que ayuda a la difusión de su mensaje. Por ejemplo, para adversarios con un alto conocimiento informático, los **servidores** alojan información importante de la organización. Por el lado de redes sociales, es posible un acceso a una de estas cuentas por mala práctica en el uso de contraseñas o si uno de los dispositivos con acceso a esta han sido robados.	En este caso se deben analizar los hábitos que tiene cada persona de la organización con sus dispositivos o hacer un análisis de los equipos que utilizan para realizar su activismo. Porque es a través de estos dispositivos que algunos adversarios tienen acceso a más información del grupo y de las personas que dan soporte.	No aplica

¿Qué hábitos de seguridad digital debo practicar para evitar que esto pase?

Hiperión recomienda:

1. Asegurate de tener una página web que esté protegida ante distintos tipos de ataque. Una buena alternativa es utilizar Cloudflare.
2. Utiliza un **Password Manager** para asegurar las recomendaciones de contraseñas seguras.
3. Habilitar autenticación por dos pasos en las diferentes plataformas de uso.
4. Realiza un **backup** constante y mantenlo en el lugar más seguro que considera la organización (Puede ser un lugar físico o digital). En lo posible, su traslado debe ser mínimo.
5. Para el backup en equipos de Apple se puede utilizar Time Machine y como una capa extra de seguridad encriptar esta información.
6. Existen opciones de backup online (no es gratis) como BackBlaze o IDrive.
7. Los backup en computadoras o laptops con sistema operativo Windows 10 o más reciente se puede habilitar la opción de Respaldo y Restauración. Y si es posible encriptar esta información haciendo uso de BitLocker.

8. Las últimas versiones de los sistemas operativos Android e iOS realizan el encriptado por defecto de su disco pero únicamente si se establece una contraseña de bloqueo. ¡No dejes de activarlas!

9. Configurar las notificaciones de tus aplicaciones de mensajería y desactivar la vista previa de sus notificaciones. De esta forma evitamos que una persona externa vea nuestros mensajes sin necesidad de desbloquear el teléfono.

Recordemos:

- Recordar el concepto de activos utilizado en el modelado de riesgos.
- Un servidor, dentro de la infraestructura de Internet, es una computadora ejecutando ciertas tareas de manera constante. Usualmente se utilizan para alojar páginas web pero pueden ser utilizados para otros trabajos específicos como por ejemplo únicamente de almacenamiento de archivos.
- Un gestor de contraseñas te facilita la manera de escoger contraseñas seguras. Existen opciones gratuitas como LastPass, Firefox Lockwise pero también otras muy buenas de pago como 1Password.
- La autenticación en dos pasos te permite adicionar una segunda capa de seguridad para acceder a nuestras cuentas en Internet. Esto significa que incluso cuando alguien conozca tu contraseña, no les será posible acceder a tus cuentas.
- Según la configuración, este factor puede ser un código enviado al teléfono celular o correo electrónico. En otras ocasiones es posible tener una aplicación a manera de Token. Para este último caso tenemos alternativas como Authenticator de Google, Microsoft Authenticator o Authy.
- Encriptar un documento significa que únicamente tú puedes hacer legible su contenido haciendo uso de una contraseña que se establece antes del proceso de encriptación. ¡No confundir con encriptado de punto a punto P2P! El cual es utilizado para aplicaciones de mensajería.
- Una buena recomendación de backup es seguir la regla del 3-2-1; tres copias de tu información, dos de manera local en diferentes dispositivos y una copia en un sitio remoto. Para la mayoría, esto se puede entender como la información original en tu computadora, un backup en un disco duro externo y otro en un servicio de backup en la nube.

Robo de identidad en redes sociales

Como persona activista que probablemente cuenta con una voz y opinión públicas, ¿te imaginas lo peligroso que sería que se creara una cuenta falsa que contenga tu nombre, datos personales y contactos que difunda información con la que no estás de acuerdo o,

peor aún, rechazas? Este tipo de violencia se refiere al uso y/o falsificación de la identidad de una persona sin su consentimiento, por medio de la creación de perfiles falsos que utilizan la imagen o información de una persona u organización. La persona agresora roba o duplica la identidad virtual de la víctima, con el objetivo de circular información falsa adoptando su identidad o acercarse a su círculo cercano. El objetivo puede variar desde buscar dañar la reputación de una persona, hasta intimidar a la víctima haciéndola sentir que pueden apropiarse de su información.

COMO AFECTA A:		
Canales de expresión de la organización	**Datos de personas que manejan los canales de expresión**	**Datos de comunidad que me sigue o participa de mis eventos**
Se han visto casos donde los adversarios más organizados (y financiados) se dan el trabajo de replicar una página de Facebook o la página web con un dominio similar al de la organización con el objetivo de confundir a las personas que quieran acceder a ella, entregar información errónea o captar a las personas que siguen el mismo pensamiento.	Como ya se explicó líneas más arriba, en muchas ocasiones es fácil identificar a las personas que administran una página web o fanpage en redes sociales. Adversarios dedicados pueden crear un perfil falso con las fotografías e información pública para contactar a personas e intentar recoger más información o brindar información errónea.	No aplica

Hiperión recomienda:

1. Dentro de las posibilidades de la organización, seguir el proceso de verificación en redes sociales (check azul) como en Facebook, Instagram o Twitter.
2. De ser posible adquirir los **dominios** más parecidos al de la organización para evitar suplantaciones o confusión con las personas de tu comunidad.
3. Asegurarse (de tener una web) que esté protegida ante distintos tipos de ataque. Una buena herramienta es utilizar Cloudflare.
4. Analizar la veracidad de los mensajes que recibas vía SMS, Mail, WhatsApp u otra aplicación de mensajería.[Test de phishing].
5. En caso quisieras saber si tu contraseña fue filtrada en algún ataque a una aplicación o servicio web lo puedes comprobar en este enlace.
6. Para el caso de redes sociales como Facebook, puedes configurar las opciones de privacidad para que tu perfil no se muestre como resultado de las búsquedas por nombre, número de celular o correo electrónico.

7. De ser necesario, configurar sus redes sociales en privado, deshabilitar la opción de recibir mensajes de personas que no conocemos o también filtrar el contenido que pueden escribir en nuestras publicaciones, videos en vivo, etc. Un ejemplo para Instagram es habilitar el filtro de palabras ofensivas. También está disponible una opción para páginas de Facebook.

8. Limita el alcance de las personas que pueden ver tu contenido (fotos, publicaciones).

9. Si consideras necesario, crea una cuenta para hacer activismo, o no poner fotos personales ni taggear familiares, desactivar la opción de geolocalización, etc.

10. Utiliza un **Password Manager** para asegurar las recomendaciones de contraseñas seguras.

11. Habilitar autenticación por dos pasos en las diferentes plataformas de uso.

12. Evita utilizar **redes abiertas** que puedan parecer sospechosas.

13. Hacer un **backup** constante y mantenerlo en el lugar más seguro que considera la organización (Puede ser un lugar físico o digital). En lo posible, su traslado debe ser mínimo.

Recordemos:

- Un dominio o nombre de dominio, es la dirección de tu sitio web. Algunas personas también le dicen URL, por ejemplo facebook.com, google.com o hiperderecho.org.
- Un servidor, dentro de la infraestructura de Internet, es una computadora ejecutando ciertas tareas de manera constante. Usualmente se utilizan para alojar sitios web pero pueden ser utilizados para otros trabajos específicos como por ejemplo únicamente de almacenamiento de archivos.
- Un gestor de contraseñas nos facilita la manera de escoger contraseñas seguras. Existen opciones gratuitas como LastPass, Firefox Lockwise pero también otras muy buenas de pago como 1Password.
- La autenticación en dos pasos nos permite adicionar una segunda capa de seguridad para acceder a nuestras cuentas en Internet. Esto significa que incluso cuando alguien conozca tu contraseña, no les será posible acceder a tus cuentas.
- Según la configuración, este factor puede ser un código enviado al teléfono celular o correo electrónico. En otras ocasiones es posible tener una aplicación a manera de Token. Para este último caso tenem os alternativas como Authenticator de Google, Microsoft Authenticator o Authy.

- Una red puede considerarse insegura si no nos garantiza el transporte de información de manera encriptada. Un buen indicador en los navegadores es el candado verde en la sección donde aparece el nombre de la página que estamos visitando.

- Una buena recomendación de backup es seguir la regla del 3-2-1; tres copias de tu información, dos de manera local en diferentes dispositivos y una copia en un sitio remoto. Para la mayoría, esto se puede entender como la información original en tu computadora, un backup en un disco duro externo y otro en un servicio de backup en la nube.

Monitoreo o vigilancia del gobierno

De acuerdo con Amnistía Internacional,[4] algunos gobiernos espían lo que hacemos en Internet. Esta organización señala también que los documentos que Edward Snowden hizo públicos en 2013, por lo cual tuvo que huir de Estados Unidos, han revelado cómo las agencias de seguridad estatales utilizan la vigilancia masiva para recoger, almacenar y analizar en secreto millones de comunicaciones privadas de personas en todo el mundo. Si un gobierno espía a sus habitantes de esta manera, está violando sus derechos humanos. A partir de esta información, valdría la pena preguntarnos qué significa esto para aquellas personas activistas por la defensa de derechos de las mujeres y poblaciones LGTBIQ+ que además sostienen posturas críticas contra el gobierno, así como de distintas instituciones e instancias del poder gubernamental.

COMO AFECTA A:		
Canales de expresión de la organización	**Datos de personas que manejan los canales de expresión**	**Datos de comunidad que me sigue o participa de mis eventos**
En estos casos, las amenazas más frecuentes son aquellas en redes sociales donde personal policial o de un partido político específico con buenos recursos (económicos, técnicos, organización) hace seguimiento de la actividad de la organización. Principalmente a sus eventos, convocatorias, líderes, reuniones etc.	La vigilancia en el espacio digital les permite a estos adversarios conocer más sobre la organización, sus participantes y su público objetivo. Esta vigilancia también puede continuar su flujo en los perfiles personales de quienes manejan estos recursos al punto de buscar información más sensible como datos de familiares, dirección de su trabajo o vivienda, información de antecedentes, etc. Otro tipo de vigilancia se puede dar desde el lado de telecomunicaciones, donde las operadoras de telefonía pueden acceder ainformación de las páginas que visitamos o también la ubicación aproximada a partir de la señal GSM.	No aplica

[4] Ver: https://www.es.amnesty.org/en-que-estamos/temas/vigilancia-masiva/

¿Qué hábitos de seguridad digital debo practicar para evitar que esto pase?

Hiperión recomienda:

1. Googleate a ti mismo(a) para ver qué información personal está disponible en Internet, y de ser posible, solicita eliminarla a la persona que administre la cuenta o el sitio en la que esté publicada esta información.

2. Para el caso de redes sociales como Facebook, puedes configurar las opciones de privacidad para que tu perfil no se muestre como resultado de las búsquedas por nombre, número de celular o correo electrónico.

3. Revisa el contenido en las plataformas digitales sobre la información brindada de los/las participantes de la organización y analizar si algunos datos son relevantes o no.

4. Utiliza aplicaciones de mensajería **encriptadas** de punto a punto.

5. Desactiva la visibilidad de las notificaciones en tus smartphone.

6. Navega de manera segura, con plugins **anti-trackers** como Privacy Badger o utilizando navegadores con esta capacidad activada por defecto como Brave

7. Utiliza un **Password Manager** para asegurar las recomendaciones de contraseñas seguras.

8. Habilitar **autenticación por dos pasos** en las diferentes plataformas de uso.

Recordemos:

- Un gestor de contraseñas nos facilita la manera de escoger contraseñas seguras. Existen opciones gratuitas como LastPass, Firefox Lockwise pero también otras muy buenas de pago como 1Password.
- La autenticación en dos pasos nos permite adicionar una segunda capa de seguridad para acceder a nuestras cuentas en Internet. Esto significa que incluso cuando alguien conozca tu contraseña, no les será posible acceder a tus cuentas.
- Según la configuración, este factor puede ser un código enviado al teléfono celular o correo electrónico. En otras ocasiones es posible tener una aplicación a manera de Token. Para este último caso tenemos alternativas como Authenticator de Google, Microsoft Authenticator o Authy.
- Una red puede considerarse insegura si no nos garantiza el transporte de información de manera encriptada. Un buen indicador en los navegadores es el candado verde en la sección donde aparece el nombre de la página que estamos visitando.

- Una buena recomendación de backup es seguir la regla del 3-2-1; tres copias de tu información, dos de manera local en diferentes dispositivos y una copia en un sitio remoto. Para la mayoría, esto se puede entender como la información original en tu computadora, un backup en un disco duro externo y otro en un servicio de backup en la nube.
- La encriptación de punto a punto se encarga de cifrar nuestros mensajes de tal manera que únicamente el emisor y receptor del mensaje puedan entenderlo (descifrarlo). Esto significa que incluso cuando el mensaje sea interceptado, será imposible de leer o entender.
- Es importante analizar sobre nuestra presencia en Internet y cómo nuestros dispositivos pueden llegar a tener una huella única. Esta información puede ser utilizada para el perfilado a partir de la información recolectada sobre nuestras actividades de navegación.

Interceptado de comunicaciones

Por interceptado de comunicaciones nos referimos a la escucha o grabación del contenido de una comunicación, o la captación de sus datos, durante su transmisión. Es decir, en el transcurso del día de tus datos de un punto al otro.

COMO AFECTA A:		
Canales de expresión de la organización	**Datos de personas que manejan los canales de expresión**	**Datos de comunidad que me sigue o participa de mis eventos**
No aplica	Esto aplica para adversarios con recursos económicos y de organización, aquellos que pueden financiar o haciendo uso de su poder político/administrativo para conseguir el equipo necesario e interceptar las comunicaciones a través de Internet o de telefonía. Otros tipos de adversarios, aunque menos frecuentes, pueden ser aficionados y capturar información de quienes utilizan zonas Wi-Fi abiertas.	No aplica

¿Qué hábitos de seguridad digital debo practicar para evitar que esto pase?

Hiperión recomienda:

1. Navegación segura, asegurando que los sitios que ingresemos tengan el indicador desitio seguro o utilizar la herramienta **HTTPS Everywhere.**
2. Utilizar aplicaciones de mensajería con **encriptación de punto a punto.**
3. De ser posible, tener líneas telefónicas dedicadas para las actividades de la organización.
4. Googleate a ti mismo(a) para ver qué información personal está disponible en Internet, y de ser posible, solicita eliminarla a la persona que administre la cuenta o el sitio en la que esté publicada esta información.
5. Para el caso de redes sociales como Facebook, puedes configurar las opciones de privacidad para que tu perfil no se muestre como resultado de las búsquedas por nombre, número de celular o correo electrónico.
6. Procura ser precavide al ingresar a las zonas de WiFi gratuito. Analiza su seguridad o evita ingresar a cuentas de información sensible o de gran importancia como la del banco, formularios con datos personales, etc.
7. Utiliza navegadores que mantengan anonimidad o herramientas que permitan conservar la anonimidad de la actividad en Internet como VPNs, Tor o utilizar buscadores que sean respetuosos con la privacidad como DuckDuckGo.

Recordemos:

- Una conexión HTTP no puede considerarse segura porque, si alguien intercepta ese flujo de datos, podrá ver todos los parámetros que estamos enviando. Por ejemplo un formulario, un usuario y contraseña, etc.
- HTTPS por el contrario, permite una comunicación cifrada. Existen plugins para instalar en nuestros navegadores para asegurar este tipo de configuración.
- Una red puede considerarse insegura si no nos garantiza el transporte de información de manera encriptada. Un buen indicador en los navegadores es el candado verde en la sección donde aparece el nombre de la página que estamos visitando.
- La encriptación de punto a punto se encarga de cifrar nuestros mensajes de tal manera que únicamente el emisor y receptor del mensaje puedan entenderlo (descifrarlo). Esto significa que incluso cuando el mensaje sea interceptado, será imposible de leer o entender.

- Es importante analizar sobre nuestra presencia en Internet y cómo nuestros dispositivos pueden llegar a tener una huella única. Esta información puede ser utilizada para el perfilado a partir de la información recolectada sobre nuestras actividades de navegación.
- Recordar también que Internet no es un espacio invisible. Existe toda una infraestructura física que soporta esta tecnología.

Acoso coordinado en redes sociales

Los ataques de acoso coordinado son acciones conjuntas realizadas en Internet con el objetivo de dañar a una persona o una organización. Inclusive cuando las acciones parezcan inocuas por sí solas, logran un efecto abrumador e inhabilitante porque son llevadas a cabo en simultáneo por decenas de personas que se esconden detrás de perfiles falsos o pseudónimos
En Hiperderecho, hemos identificado hasta tres tipos de acoso coordinados:

- El uso de datos personales para crear campañas coordinadas de desprestigio y dañar tu reputación.
- El uso de datos personales para vigilarte: te dicen que ya saben dónde vives o cómo se llaman tus familiares para darte a entender que pueden acercarse a ti en cualquier momento.
- Y el «reporte masivo» o el abuso de los mecanismos de reporte en redes sociales para eliminar un perfil o una publicación y, de esa manera, eliminarte de ese espacio.

COMO AFECTA A:		
Canales de expresión de la organización	**Datos de personas que manejan los canales de expresión**	**Datos de comunidad que me sigue o participa de mis eventos**
Para el caso específico de **canales digitales** tendríamos como un buen ejemplo las denuncias masivas a las redes sociales de la organización. O en un caso un poco más especializado, ataques a los servidores que alojan la página web de la organización.	Usualmente, en redes sociales, es fácil identificar a las personas que están administrando una organización activista. El acoso masivo dirigido a la organización puede seguir su flujo a las cuentas personales de quienes la administran o quienes están a favor del mensaje. Como resultado de este tipo de ataque se pueden tener cuentas dadas de baja, consecuencias emocionales en las personas, etc.	Malas prácticas de almacenado de información podría poner en riesgo a las personas a las que la organización da soporte. Por ejemplo, un formulario mal realizado podría exponer información sensible de estas personas de tal manera que permita identificarlas en redes sociales

¿Qué hábitos de seguridad digital debo practicar para evitar que esto pase?

Hiperión recomienda:

1. Dentro de las posibilidades de la organización, seguir el proceso de verificación en redes sociales (check azul) como en Facebook, Instagram o Twitter.
2. Control adecuado de los permisos en carpetas compartidas o formularios.
3. Googleate a ti mismo(a) para ver qué información privada está disponible en Internet,y de ser posible solicita eliminarla a la persona que administre la cuenta o el sitio en laque esté publicada esta información.
4. Asegurarse (de tener una web) que esté protegida ante distintos tipos de ataque. Unabuena herramienta es utilizar Cloudflare.
5. De ser necesario, configurar sus redes sociales en privado, deshabilitar la opción de recibir mensajes de personas que no conocemos o también filtrar el contenido que pueden escribir en nuestras publicaciones, videos en vivo, etc. Un ejemplo para Instagram es habilitar el filtro de palabras ofensivas. También está disponible una opción para páginas de Facebook.
6. Para el caso de redes sociales como Facebook, puedes configurar las opciones de privacidad para que tu perfil no se muestre como resultado de las búsquedas por nombre, número de celular o correo electrónico.
7. Como organización, definir roles de respuesta ante este tipo de ataques.
8. Si tienes una cuenta personal, recomendamos limitar el alcance de las personas que pueden ver tu contenido (fotos, publicaciones) de tu cuenta privada. Al paralelo, puedes crear una cuenta únicamente para hacer activismo, en la que no publiques fotos personales ni etiquetas familiares, etc.

Recordemos:

- Recordar nuestro espacio en Internet y quiénes son las personas que están expuestas en los frentes de este espacio y que, por lo tanto, están expuestas a este tipo de ataques.
- Los canales digitales más frecuentes son las cuentas de redes sociales, páginas web, correos electrónicos y cuentas en las aplicaciones de mensajería para dar apoyo a su comunidad (WhatsApp, Telegram, Signal, etc).
- Es importante documentar estos eventos como evidencia y como parte de la ficha de

- La salud psicológica de las personas detrás de las actividades y plataformas de la organización son tan importantes como cualquier otro activo.

Robo de dispositivos físicos

Sabemos que probablemente alguna vez en la vida te hayas enfrentado a un robo de, por ejemplo, tu celular en el espacio público o en un medio de transporte. Aparte de preocuparte por la pérdida económica que supone comprarte otro celular, ¿Te has puesto a pensar en la cantidad de información personal y de otros que llevamos en estos dispositivos? Desde archivos, accesos a cuentas, fotos personales y de tu familia y amistades. Ahora imagínate que el dispositivo robado es tu PC o laptop: la cantidad de información a la que el ladrón o atacante podría llegar a tener acceso es mayor.
Como activista, que un potencial adversario acceda a la información que cargas en tus dispositivos no solo podría vulnerar tu integridad, sino la de toda tu organización y de aquellas personas con las que trabajas y a las que apoyas.

COMO AFECTA A:		
Canales de expresión de la organización	**Datos de personas que manejan los canales de expresión**	**Datos de comunidad que me sigue o participa de mis eventos**
Los dispositivos físicos (laptops, PCs, smartphones) donde se tiene guardada no solo documentos importantes sino también, probablemente, accesos a las principales cuentas y servidores de los canales digitales de la organización (páginas web o redes sociales). Estos dispositivos, de no ser cuidadosamente protegidos, ponen en riesgo información de las personas a las que dan soporte, los sponsors, los miembros de la organización y mucha más información relevante y crucial.	En este caso se puede considerar el robo de uno de los dispositivos a uno de los miembros de la organización, que en caso no lo tenga protegido, puede poner en riesgo la identidad del resto del equipo así como información relevante según su rol dentro de la organización, accesos a las cuentas de redes sociales, etc.	La información almacenada de las personas puede estar almacenada en discos duros, USBs, discos, etc. En caso estos dispositivos sean robados o extraviados pueden poner en riesgo la identidad de las personas a quienes la organización da soporte.

¿Qué hábitos de seguridad digital debo practicar para evitar que esto pase?

Hiperión recomienda:

1. Establecer un protocolo de transporte de dispositivos físicos (disco duro, USB, CDs).
2. Hacer un **backup** constante y mantenerlo en el lugar más seguro que considera la organización (Puede ser un lugar físico o digital). En lo posible, su traslado debe ser mínimo.
3. Para el backup en equipos de Apple se puede utilizar Time Machine y como una capa extra de seguridad encriptar esta información.
4. Existen opciones de backup online (no es gratis) como BackBlaze o IDrive.
5. Los backup en computadoras o laptops con sistema operativo Windows 10 o más reciente se puede habilitar la opción de Respaldo y Restauración. Y si es posible encriptar esta información haciendo uso de BitLocker.
6. Las últimas versiones de los sistemas operativos Android e iOS realizan el encriptado por defecto de su disco pero únicamente si se establece una contraseña de bloqueo.

Recordemos:

- La información que tienes guardada en tu dispositivo o celular está asociada a las comunidades con las que te comunicas. Cuidar su información es cuidar a tu comunidad.
- La salud psicológica de las personas que manejan los dispositivos de tu organización son tan importantes como cualquier otro activo. Tener un plan de acción ante un posible robo de dispositivos ayudará a que esta persona pueda manejar este incidente, en caso de que ocurra, con serenidad.
- Una buena recomendación de backup es seguir la regla del 3-2-1; tres copias de tu información, dos de manera local en diferentes dispositivos y una copia en un sitio remoto. Para la mayoría, esto se puede entender como la información original en tu computadora, un backup en un disco duro externo y otro en un servicio de backup en la nube.

V. PRIVACIDAD & SEGURIDAD EN REDES SOCIALES

En el contexto de los activismos, las redes sociales son utilizadas como espacio principal de conexión con el público, de incidencia y difusión de información sobre sus causas. No obstante, es en ellas en donde podemos observar la mayor cantidad de vulneraciones hacia estos grupos activistas por parte de trolls o, más específicamente, *machitrolls*.

Recomendaciones básicas de privacidad y seguridad

Una buena configuración de privacidad en las redes sociales podría ayudarte a sentir

1. **Crea listas de contactos y amistades con quienes te sientas segura o seguro:** Es habitual que con el tiempo tengamos en nuestras redes sociales a personas que no conocemos muy bien o en quienes no confiamos mucho. Si no confías en ellos, lo ideal sería que los elimines. Además, puedes crear listas de contactos seguros en Facebook para que compartas tu información más sensible y privada solo con las personas que están en la lista. Mientras que en Instagram puedes limitar las personas que pueden interactuar contigo.

2. **Restringir contactos:** El objetivo de esta función es **acabar con las interacciones no deseadas.** Cuando el usuario seleccione una cuenta para restringir, dicha cuenta podrá seguir comentando las publicaciones pero con la diferencia de que el comentario solo será visible para quien lo envía. **Ni el usuario ni sus seguidores recibirán este mensaje,** salvo que la cuenta que restringe permita que sus seguidores lean este mensaje.

3. **Filtros de comentarios:** El objetivo es quitar de tu vista comentarios con los que no quieres lidiar y que pueden afectar a tu comunidad. En Facebook, puedes bloquear palabras para que no aparezcan en tu página o aplicar un 'Filtro de groserías', que bloquea las palabras más denunciadas en la plataforma. En Instagram también puedes bloquear comentarios abusivos o violentos. Utilizando 'Filtro automático' o activando el 'filtro manual' para bloquear palabras, frases o incluso emojis que tú no quieras ver. Además, puedes evitar que personas a las que no sigues, te dejen comentarios.

Reportar a agresores en plataformas

Otra estrategia válida para hacerle frente a las distintas formas de violencia de género online es mediante el registro y reporte de estos casos a manera de denuncias. Si bien somos conscientes que la configuración de estas opciones creadas por las redes sociales pueden mejorar, **es importante que las y los usuarios estemos informados sobre los canales y procedimientos disponibles para llevar a cabo estas acciones.** De este modo, también podemos organizarnos como usuarixs y pedirle a estas plataformas cambios, reajustes o nuevas consideraciones a la hora de recepcionar denuncias o, en general, cómo lograr que el contenido o cuentas reportadas atienda efectivamente a situaciones que atenten contra la integridad y bienestar de las demás personas.

Mantén el control de los dispositivos que accedieron a tu cuenta

Un buen hábito es realizar de manera periódica un análisis de los dispositivos que tienen acceso a tus cuentas y verificar que son equipos que te pertenezcan y consideres que están en un lugar seguro para ti y para tu colectiva. Otro control que debes considerar es revisar el listado de aplicaciones de que comparten información con Facebook, interacciones que pueden van desde visitar su sitio web o iniciar sesión con Facebook en su app.

VI.SANAR DESPUÉS DE VIOLENCIA

La recurrente mención de palabras como "riesgos" o "amenazas", así como la experiencia de enfrentarlas, puede potencialmente generar ansiedad, desgano y preocupación en ti o tu comunidad. Incluso,en algunos casos, puede ocasionar que veamos a Internet como un espacio "tóxico" - una noción que no hace más que incrementar la percepción de lejanía que tenemos sobre la tecnología. Por eso, les proponemos que incluyan en su plan de seguridad digital medidas para que una persona puede emprender el camino de la sanación después de la violencia:

1. **Construye redes de apoyo para asegurar el cuidado de estos grupos y la respuesta organizada.** Recuerda que hay muchas personas luchando contigo. Por ejemplo, ante un ataque coordinado en Twitter, imagínate lo poderoso que puede ser que otras mujeres que están en esta red decidan realizar un "tuitazo" con el cual pelear, simbólicamente, con la cantidad de odio a la que se enfrenta esta persona. Esto se relaciona con la seguridad digital porque, así, las personas vulneradas, reconocen el poder de la unión de mujeres que se apoyan[5] entre mujeres, y sentirán menos riesgos y angustia en su interacción y navegaciones posteriores en Internet.

2. **Busca acompañamiento psicológico si te sientes agobiada, cansada o angustiada:** Recuerda que la violencia que vives en Internet es real, y debemos tratarla como tal. El trabajo que haces en la primera línea de defensa virtual, te expone a comentarios, actitudes y acciones que pueden afectar tu salud mental. Busca acompañamiento psicológico y emocional, si lo necesitas. Conversa con tu organización sobre cómo te pueden ayudar a obtener estos recursos.

3. **Autocuidado y descansos estratégicos ;) :** A veces sentimos que es imposible alejarnos de las pantallas, pero es importante darle tiempo a aquellas actividades que te dan paz y tranquilidad. Encuentra una serie que te haga sentir bien, pasa tiempo con tu mascota, o retoma ese pasatiempo que tenías abandonado. Cuidarnos a nosotres mismes es una forma de autocuidado que nos hace recargar energías y emprender nuestras luchas recordando que el cambio es posible (¡y necesario!). Cuídate para que puedas cuidar a las demás.

4. **Busca una fuente de motivación:** Si te encuentras desmotivada frente a emprender cambios en tu seguridad digital, pregúntate: ***¿Qué tipo de Internet quieres y qué necesitamos para lograrlo?*** La noción de una **Internet feminista** - que Internet puede ser un espacio de empoderamiento y el pleno disfrute de derechos de mujeres y personas e identidades sexogenéricas diversas - se vuelve cada vez más posible con buenas prácticas de seguridad digital. Así como el feminismo, la seguridad digital es una lucha de largo aliento e implica un proceso largo de aprendizaje y deconstrucción. Lo importante es empezar a caminarlo y recuerda que vas acompañada.

[5] De hecho, esta es la función de Trollbusters: campañas contra-respuesta y mensajes de apoyo.

VII. METODOLOGÍA PARA DICTAR CIBERCUIDADO PARA ACTIVISTAS

Hiperderecho dictó el programa **Cibercuidado para activistas** entre mayo y septiembre del 2020. Consistió en una serie de talleres sobre seguridad digital para activistas, colectivas organizadas y defensores de derechos humanos. Los objetivos del programa eran:

- Que grupos activistas adquieran una comprensión integral sobre las amenazas relacionadas al acceso, privacidad, seguridad en línea.
- Desarrollen habilidades para permanecer en el anonimato en espacios digitales hostiles.
- Desarrollen la confianza de gestionar la seguridad digital de sus organizaciones de manera independiente y autónoma.

En esta sección elaboramos más sobre los componentes del curso para que puedan ser utilizados, aprovechados o adaptados por otras capacitadoras y capacitadores en sus propias comunidades.

Sumilla de contenidos

La capacitación contó con tres módulos orientados a generar distintas capacidades en el participante:

1. **Módulo 1:** Abrimos el curso, con una introducción a conceptos básicos de seguridad digital, y herramientas de documentación de incidentes y modelado de riesgos de seguridad digital.
2. **Módulo 2:** Enseñamos a utilizar herramientas para asegurar conexiones, navegadores, datos y dispositivos. Dedicamos la mayoría de sesiones a explicar la tecnología detrás de estas herramientas para perderle el miedo y saber cómo utilizar estas medidas y de qué manera nos hacían sentir más seguras.
3. **Módulo 3:** Finalmente, buscamos que el estudiante integre las herramientas aprendidas a sus planes y protocolos de seguridad digital.

Criterios para planear tu curso sobre seguridad digital

Los siguientes recursos fueron útiles para demostrar a nuestro público el compromiso por queremos construir una comunidad que se apoye en la seguridad digital para obtener bienestar, justicia e igualdad:

1. **Nivel principiante en seguridad digital:** A partir de los hallazgos de investigaciones realizadas por Hiperderecho sobre violencia de género en línea, ***sabemos que la seguridad digital sigue siendo un concepto lejano y nebuloso para la mayoría de organizaciones de base.*** Por ello es importante partir desde un nivel principiante, que busque aclarar conceptos y herramientas clave de seguridad digital de manera accesible y lúdica.

2. **Jugar y experimentar:** Utilicen un enfoque lúdico que preste atención especial sobre cómo las y los participantes conectan con los temas propuestos. Recomendamos sobre todo contenidos y apoyos visuales (ej. emojis de gatitos, imágenes motivadoras y gifs graciosos) que construyan horizontalidad en las clases, y señalen la disposición a divertirse y aprender en conjunto (en lugar de abordar los riesgos y amenazas en línea como un tema lúgubre que nos lleve a pensar la Internet como un espacio "tóxico").

En nuestras clases llevamos a cabo sesiones de **'Círculos de brujas'** en los que hacíamos rondas para contar historias o compartir experiencias relacionadas al tema propuesto, o sesiones de **'Hackeando el patriarcado'** en las que hacíamos ejercicios.

3. **Afinidad con perspectiva de género y derechos humanos:** Para que el curso sea relevante para grupos activistas, es recomendable abordar a la seguridad digital con perspectiva de género y derechos humanos. Los conceptos, herramientas y estrategias sugeridas deben dialogar con las necesidades y riesgos en línea que ellos enfrentan y el lenguaje, cercano a las luchas feministas y LGTBIQ+. Además, el curso es una oportunidad para empezar a construir una comunidad alrededor del género, los derechos humanos y la tecnología.

4. **Situar la seguridad digital en la cotidianidad:** Recomendamos el uso de ejemplos que resuenen en la experiencia cotidiana de las personas presentes y la formulación de temáticas que llamaran la atención del público. Los talleres empezaban situando a les participantes en un riesgo específico que han enfrentado y buscamos relacionarlo a las herramientas que veríamos en ese taller.

5. **Mantener grupos pequeños:** Con grupos pequeños tendrás la oportunidad de trabajar personalizadamente con cada grupo y proveer apoyo empático y oportuno. Al tratarse de un grupo pequeño, el público también tiene la oportunidad de conectar entre sí, compartir y aprender colectivamente.

6. **Flexibilidad y adaptación:** Ya que la seguridad digital puede ser un nuevo concepto para las personas del curso, es importante seguir el proceso de aprendizaje de las y los estudiantes. Conforme van pasando las clases, el orden de contenido y puntos a resaltar durante los talleres va modificándose.

7. **Recoger activamente la experiencia de lxs participantes.** El espacio del taller no debe ser entendido como unidireccional respecto al capacitador, sino que debe ser abordado como un momento de aproximarnos a los insights de las participantes y necesidades específicas de cada grupo presente. Esta información es importante porque sirve para afinar conocimientos, metodologías y ejercicios a futuro, así como identificar necesidades específicas y puntos en común entre asociaciones y colectivas.

Creando capacitaciones online seguras

Ya que las personas de la comunidad LGTBIQ+ y las feministas forman parte del grupo de personas que enfrentan con mayor frecuencia e intensidad distintas formas de violencia en entornos online, resultaba muy importante fomentar un espacio en el que todas y todos se sintieran seguros. En ese sentido, se acordaron normas de convivencia para proteger la identidad y seguridad de todas las personas de la clase.

Entre las que más recomendamos están:

1. Que cada persona pueda participar **utilizando seudónimos** y sus pronombres de preferencia.

2. Utilizar la **plataforma Jitsi** para que cada participante pueda usar un seudónimo y escoger hasta qué punto quiere revelar su identidad. Si se escoge otra aplicación de videollamada, procurar dar instrucciones sobre cómo mantenerse anónimos durante la llamada.

3. Mantener comunicación fuera de las clases por **Telegram** para continuar el acompañamiento y apoyo fuera de clases. Esa aplicación es útil para crear grupos sin que el número telefónico de los participantes sea visible para los demás. Esto le impide a las demás personas registrar los números y deducir sus identidades. También se bloqueó la posibilidad de registrar la conversación mediante pantallazos.

4. Plantear normas de convivencia basadas en el **respeto por el anonimato y el consentimiento.** Pedir que se evite usar la información compartida para deducir quienes son y qué hacen, respetando la decisión que cada compañera ha tomado sobre su cuerpo, voz, e identidad digital en la clase.

5. Prohibir la grabación y registro de las clases para **proteger la confidencialidad** de las historias compartidas.

Cuidando el bienestar de tus participantes

Llevar un curso de capacitación en línea - sobre todo, en tiempos de pandemia- no es una tarea sencilla: Tanto profesores, capacitadores y talleristas como estudiantes tienen mérito de hacer que funcione. Ahora no solo debemos pensar en cómo interactuamos distinto en las clases, a partir de la virtualidad, sino en qué puede estar pasando alrededor de una persona, aquello que facilita o, por el contrario, establece obstáculos en nuestro proceso de aprendizaje. Ponle todas las ganas para crear un espacio que se acomode a las necesidades de les participantes de tu clase y modifica la sumilla si se presentan los siguientes desafíos:

1. **Desafíos logísticos:** Dificultades en las conexiones a Internet o acceso y disponibilidad a dispositivos electrónicos. Tomar en cuenta también, la división sexual del trabajo vigente en nuestra sociedad que limita la cantidad de tiempo libre que tienen las mujeres que pertenecen a una familia.

2. **Desafíos emocionales:** Dificultades relacionadas a la saturación de estar permanentemente conectadas y los cambios en nuestros estilos de vida por la pandemia.

También tomar en cuenta que los temas tratados pueden generar incomodidad o desasosiego en quienes lo han vivido.

3. **Desafíos físicos:** Dificultades relacionadas a discapacidades de vista, lectura, uso de colores, entre otras que dificultan el acceso equitativo al material de aprendizaje.

¿Alguna vez te has puesto a pensar en lo liberadores que son espacios LGTBIQ+ y feministas en los que podemos ser quienes queremos ser, sin miedo y con mucha amistad y comprensión de por medio? ¡Probablemente, sí! Precisamente, el tipo de aprendizaje que **espacios feministas** y **LGBTIQ+** promueven está construido sobre las bases de la igualdad, la búsqueda de representación digna de poblaciones históricamente discriminadas y un carácter críticos respecto de sistemas de opresión que afectan a los cuerpos que atentan contra la cisheteronorma. Es fundamental que traslademos esta visión del mundo a cómo pensamos "nuestra aula de clase", nuestro taller. Mapeando los desafíos y retos junto a las colectivas que cuestionan la realidad social y sus desigualdades, proponemos co-construir alternativas pedagógicas y abordar su seguridad desde un proceso de **empatía revolucionaria**. Así, vamos sembrando las semillas del cambio no solo con nuestros contenidos, sino en las formas en la que enseñamos, nos aproximamos y construimos saberes.

Hemos llegado al fin de este kit. Los desafíos de crear un Internet como espacio de libertad e igualdad para todes son muchos, pero tú y tu colectiva están liderando el cambio. ***¡Muchas gracias por eso!***

Y recuerda que la información y acompañamiento vencen al miedo.
Con ustedes en pie de lucha, el ciberpatriarcado tiene los días contados.

RECURSOS COMPLEMENTARIOS

Glosario de Seguridad Digital

Autoprotección Digital Contra La Vigilancia: Consejos, Herramientas y Guías Para Tener Comunicaciones Más Seguras [Electronic Frontier Foundation]

Seguridad digital, conceptos y herramientas básicas [Conexo]

Seguros y documentados para el activismo [Derechos Digitales América Latina]
A Security Auditing Framework and Evaluation Template for Advocacy Groups [Internews]

Checklist de seguridad digital [Protege.la]

Security Planner [Citizen Lab]

ANEXOS
ABC DIGITAL PARA LA CIBERSEGURIDAD

Espacio para potenciar al máximo nuestra comprensión de las herramientas y hábitos propuestos como ciberseguridad

A:

Comenzamos el vocabulario con una de las letras que más definiciones nos suscita, la letra A! En ese sentido, podríamos armar un listado con solo palabras que comiencen con esta letra, pero aquí te dejamos 6 que te serán súper útiles de tener a la mano:

- **Administrador de contraseñas:** Una herramienta que puede cifrar y guardar tus contraseñas usando una sola clave maestra, haciendo práctico el uso de diferentes contraseñas en diferentes sitios y servicios sin tener que memorizarlas éstas.

- **Adversario:** Tu adversario es la persona u organización que intenta pasar por alto tus objetivos de seguridad. Los adversarios pueden ser diferentes, dependiendo de la situación. De hecho, quizás te preocupes de un criminal espiando en un café, o tu compañero de clase en la escuela. Muchas veces el adversario es hipotético.

- **Análisis de riesgo:** Este tipo de análisis se refiere a calcular las posibilidades que tiene una amenaza en poder ser ejecutada. De esa manera, puedes saber cómo defenderte contra ella. Hay muchas maneras en que puedes perder el control o el acceso a tu data, pero algunos de ellos son menos probables que otros. El análisis de los riesgos quiere decir que tengas que decidir cuáles de las amenazas te vas a tomar en serio y cuales son las menos probables que sucedan o, en todo caso, aquellas más difíciles de combatir. Ver también: Modelo de amenazas

- **Antivirus:** El software antivirus, a veces llamado también programa anti-malware, apareció hace unos años para proteger ordenadores de virus y otras amenazas que afectan a los ordenadores. Hoy en día, los usuarios de los programas antivirus están protegidos de los peligros en línea más avanzados, como ransomware, rootkits, troyanos, spyware, ataques de phishing o redes de bots. Sin embargo, el nombre "antivirus" se conservó para estas soluciones de software en general.

- **Autenticación:** El proceso de autenticación (o identificación) de un individuo se basa generalmente en un nombre de usuario y una contraseña. Este proceso se utiliza para permitir el acceso a un sitio en línea o recurso a la persona adecuada mediante la validación de la identificación. Ver también: Verificación (o autenticación) de 2 pasos

- **Autocuidado:** Serie de medidas, comportamientos y actitudes con los cuales una persona puede gestionar la conservación de su salud mental y física. En el marco del programa de capacitación, nos referimos a las reflexiones y enseñanzas provenientes de los feminismos a partir de la noción de “autocuidado feminista”:

B:

- **Backup:** Una copia de seguridad es, como su nombre lo indica, una copia exacta de tus archivos, los archivos del sistema o cualquier otros recursos de este que necesites proteger. Esta precaución es necesaria para todo tipo de eventos impredecibles, como una caída del sistema, la pérdida o daño de archivos. Esta se supone que es independiente de su sistema y debe ser usada sólo cuando sea necesario. Hay casos en los que el sistema o los archivos se infectan, ¿Qué podríamos hacer? Podríamos recuperar fácilmente estos archivos con un backup. Del mismo modo, esto también nos serviría en caso el sistema esté bloqueado por un ransomware.

- **Bot:** Con Bot o Web Bots nos referimos a programas de software que realizan tareas automatizadas y operaciones específicas. Aunque algunos bots tienen propósitos inofensivos en videojuegos o ubicaciones en línea, hay una serie de robots que se pueden emplear en grandes redes, que pueden ofrecer anuncios maliciosos en sitios populares o lanzar ataques distribuidos en línea contra una serie de objetivos designados.

- **Bug:** Un bug es un fallo de software que produce un resultado inesperado que puede afectar al rendimiento del sistema. Por lo general, un error puede causar cuelgues del sistema o la congelación. El principal problema de seguridad que podría aparecer es que los errores permiten a los hackers privilegios de acceso de bypass o recuperar datos sensibles desde una red.

C:

- **Cache:** Una memoria caché es una tecnología para almacenar datos y permitir futuras
solicitudes para ser servido a una velocidad mayor. Este método de almacenamiento de alta velocidad se utiliza generalmente para las páginas web y documentos en línea, como páginas HTML y las imágenes, para aumentar la velocidad de carga y evitar el retraso no deseado.

- **Certificado de seguridad:** Es un tipo de llave privada usada para prevenir ataques de intermediarios. Un sitio que cuenta con un certificado puede probar a cualquier sistema remoto que es poseedor de uno y, al mismo tiempo, demostrar que ningún sistema sin el certificado está interfiriendo con la comunicación.

- **Cifrado de punto a punto:** Este proceso implica el uso de cifrado de comunicaciones para que la información no esté disponible para terceros. Cuando se pasa a través de una red, la información sólo estará disponible para el emisor y el receptor, evitando que los ISP o proveedores de servicios de aplicaciones para descubrir o manipular el contenido de la comunicación.

- **Cookies:** Esta es una tecnología que permite a los sitios web reconocer tu navegador. Las cookies fueron originalmente diseñadas para permitir a los sitios ofrecer canastas de compras, guardar las preferencias o mantenerte logueado en un sitio. Ellos también permiten rastrear y perfilar, para que de esta manera los sitios puedan reconocerte y conocer más sobre tu navegación.

- **Contraseña:** Piensa en una contraseña o clave como un secreto destinado a ser memorizado con el cual podrás limitar el acceso a algo, de modo que sólo quien conozca la contraseña puede tener acceso. Esto podría limitar el acceso a una cuenta en línea, un dispositivo o cualquier otra cosa. Recuerda que una contraseña segura siempre debe ser sobre algo que solo tú conoces (por favor, no uses el nombre de tu mascota con la que posteas fotos en redes sociales),

- **Contraseña maestra:** Una clave usada para desbloquear el almacenaje de otras contraseñas u otras maneras de abrir programas o mensajes. Debes de hacer que tus contraseñas maestras sean lo más fuertes posibles.

D:

- **Data:** Cualquier tipo de información, normalmente almacenada en formato digital. Los datos pueden incluir documentos, imágenes, claves, programas, mensajes y otra información o archivos digitales.

- **Deep Web:** La web profunda tiene una naturaleza menos sombría de lo que usualmente podríamos pensar. Se refiere al contenido web en todo el mundo que no está indexado por los motores de búsqueda tradicionales. Por este motivo, es el preferido por ciertos grupos de usuarios debido al aumento de sus niveles de privacidad. Sin embargo, a diferencia de la web oscura, la web profunda no requiere que sus usuarios sean particularmente conocedores de la tecnología, y no está oculta por métodos sofisticados: todo lo que se necesita para usarla es conocer la dirección del sitio web al que se desea acceder.

- **Dirección IP:** Un dispositivo en la red de Internet necesita su propia dirección para recibir data, de la misma manera que una casa o un negocio necesita su propia dirección para recibir su correspondencia físicas. Esta dirección es su dirección IP (Internet Protocol/ Protocolo Internet). Cuando usted se conecta a un sitio web u otro servidor en línea, usualmente revela su dirección IP. Esto no revela, necesariamente, su identidad (es muy difícil hacer un mapa de las direcciones IP para conocer las direcciones reales o una computadora en particular). Una dirección IP puede dar cierta información sobre ti, y esta sería de forma general como la localidad o nombre de tu Proveedor de Servicios de Internet. Servicios como TOR permiten que escondas tu dirección IP, lo cual te ayuda a tener anonimato en la línea. Ver también: TOR

E:

- **Encriptación:** El cifrado es un proceso que utiliza medios criptográficos para convertir los datos o información accesible en un código ininteligible que no puede ser leído o entendido por medios normales.

- **Exploit:** Un "exploit" es una pieza de software, un fragmento de datos o una secuencia de comandos que se aprovechan de un error, un fallo o una vulnerabilidad en el software con el fin de penetrar en el sistema de un usuario con intenciones maliciosas. Estas pueden incluir la obtención de control de un sistema informático, lo que permitiría, por ejemplo, lanzar un ataque de denegación de servicio.

- **Extensión que bloquea el tráfico de un navegador:** Cuando visitas un sitio web, tu buscador le envía alguna información a los operadores de ese sitio, o dirección IP, otra información sobre tu computadora y cookies (nombre del sitio y su dirección específica/IP), las cuales son enlazadas a visitas previas utilizando este buscador. De hecho, si el sitio web contiene imágenes y contenido tomados de otros servidores de web, esa misma información es enviada a otros sitios web como parte de la descarga o la visita a esa página. Las redes de publicidad, proveedores de analíticas, y otros recopiladores de data podrían colectar información de ti de esta manera. Puedes instalar un software que se ejecute junto a tu navegador y limitará la cantidad de información que se filtre a terceros de esta manera. Los ejemplos más conocidos son los programas que bloquean anuncios. Por ejemplo, podrías considerar usar la extensión "Privacy Badger".

F:

- **Firewall:** Esta es una herramienta que protege a una computadora de conexiones no deseadas de un sistema local y la red de la Internet. Esto funciona como una barrera (como nos indica su nombre, una barrera de fuego) y puede ser utilizada como primera línea de defensa para proteger un dispositivo de interferencias inesperadas.

- **Flooding:** Del inglés "inundación". Son un ataque a la seguridad utilizado por piratas informáticos contra un número de servidores o sitios web determinados. La inundación es el proceso de enviar una gran cantidad de información a una ubicación tal con el fin de bloquear su capacidad de procesamiento y detener su funcionamiento correcto.

G:

- **Gestor de contraseñas:** Un gestor o administrador de contraseñas es un programa de cómputo que se utiliza para almacenar una gran cantidad de parejas usuario/contraseña. La base de datos donde se guarda esta información está cifrada mediante una única clave o "contraseña maestra", de forma que el usuario solo tenga que memorizar una sola clave para acceder a todas las demás. Esto facilita la administración de contraseñas y fomenta que los usuarios escojan claves complejas sin que tengan miedo de olvidarse de ellas posteriormente.

H:

- **Hacker:** Un hacker es generalmente considerado como una persona que se las arregla para obtener acceso no autorizado a un sistema informático con el fin de causar daño. No obstante, hay que tener en cuenta que hay dos tipos de hackers: whitehat piratas informáticos, que hacen pruebas de penetración y revelan sus resultados para ayudar a crear sistemas más seguros y software, y los hackers blackhat, que utilizan sus habilidades para fines maliciosos.

- **Hacktivismo:** Así se conoce a la actividad que lleva a la utilización de técnicas de hacking para protestar en contra o luchar por objetivos políticos y sociales. Uno de los grupos hacktivistas más conocidos en el mundo es Anonymous.

- **Hardware:** Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

- **Honeypot:** Este programa se utiliza para fines de seguridad, que es capaz de simular uno o más servicios de red que se parecen a los puertos de un ordenador. Cuando un atacante intenta infiltrarse en el sistema, el Honeypot hará que el sistema de destino parezca vulnerable. En el fondo, se registran los intentos de acceso a los puertos, que incluso pueden incluir datos como las pulsaciones de teclado del atacante. De este modo, los datos recogidos por un honeypot se pueden utilizar para anticipar los ataques entrantes y mejorar la seguridad en las empresas.

- **HTTPS:** Si alguna vez has visto una dirección web como "http://www.ejemplo.com/", podrás reconocer la parte "http" de este término. HTTP (hypertext transfer protocol o, en español, protocolo de transferencia de hipertexto) es la manera en la que un navegador en tu computadora conversa con un servidor web remoto. Desafortunadamente, el HTTP estándar puede enviar textos inseguros a través de la Internet. HTTPS - sí, con la S de "seguridad" extra - usa el cifrado para proteger mejor la data que envías a los sitios web, así como la información que te devuelven, de terceros malintencionados.

I:

- **Identidad (robo de):** El robo de identidad se refiere al proceso de robar los datos de identificación personales de alguien y usarlo en línea con el fin de hacerse pasar por esa persona. Los hackers pueden hacer uso del nombre, fotos, documentos, número de la seguridad social de una persona y así sucesivamente, para obtener una ventaja financiera a costa de esta persona (mediante la obtención de crédito o chantajeando), o como un medio de dañar la reputación de la persona, etc.

- **Intrusión:** En la seguridad cibernética, la intrusión se refiere al acto de moverse por los mecanismos de seguridad de un sistema para obtener acceso no autorizado.

J:

- **J de... ¡NADA QUE VER AQUÍ!** No se preocupen, probablemente los ciberdelincuentes nos presenten un término con J sobre el cual pensar y actuar muy pronto. Como siempre, les recordamos que la mejor medida de precaución es comenzar por estar atentxs e informadxs :)

K:

- **Keylogger:** Se refiere a un programa maligno o dispositivo que graba todo lo que escribas en el dispositivo, incluyendo contraseñas y otros detalles personales, permitiendo a otros colectar secretamente esa información. La "key/llave/tecla" en keylogger se refiere a las llaves/teclas que tienes en tu tablero alfabético. Es común que estos sean malwares con los que los usuarios han sido engañados para ser descargados y operen en tu dispositivo. Ocasionalmente, se trata de un hardware físico secretamente instalado dentro de tu tablero alfabético o dispositivo.

L:

- **Llave:** En criptografía, alude a una parte de la data que te da la capacidad de cifrar o descifrar un mensaje.

- **Llave de cifrado:** Esta es una porción de información utilizada para convertir un mensaje a un formato ilegible. En algunos casos, necesitarás la misma llave de cifrado para descifrar el mensaje en cuestión. En otros, tanto la llave de cifrado como la de descifrado son diferentes.

M:

- **Malware:** "Malware" es una forma abreviada de "software maligno", es decir, un programa que ha sido diseñado para realizar acciones no requeridas en tu dispositivo. Los virus de computadoras son malwares, como también lo son los programas que roban tus claves, aquellos que secretamente te graban o los que borran tu data.

- **Metadata:** Con "metadata" nos referimos a una o las piezas de información, aparte de la información que intencionalmente se registró, envió y/o transfirió. Es decir, es la data de la data. No debemos confundirnos: ¡El contenido de un mensaje no es metadata!, sino quien lo envía, cuando, donde, y a quien: todos estos son ejemplos de metadata. Muchas veces, los sistemas legales protegen el contenido más que a la metadata; de hecho, en los Estados Unidos, los cuerpos del orden público necesitan una orden judicial para poder escuchar las llamadas telefónicas de una persona. Ante esto, es más sencillo reclamar el derecho a obtener la lista de a quién llamas frecuentemente. Por lo tanto, la metadata puede revelar muchas cosas que las y los usuarios no hemos previsto intencional describe.

- **Modelo de amenaza:** Es una herramienta con la cual puedes enfocarte en qué tipo de protección requieres para tus datos a partir de la documentación de riesgos y amenazas a las que te has enfrentado y sobre aquellas a las que potencialmente podrías enfrentarte. Es imposible protegerse contra todo tipo ataques, por eso debes concentrarte en el tipo de persona que querría acceder a tu data, qué quisieran ellos de ésta, y cómo podrían conseguirla. Imaginándote un grupo de posibles ataques, puedes levantar un plan de defensa llamado un modelo de amenaza. A partir de esto, puedes conducir acciones sobre los potenciales riesgos.

N:

- **Navegador web:** Es el programa que usas para ver sitios web. Firefox, Safari, Internet Explorer y Chrome son todos navegadores web. Los smartphones tienen ya construido en ellos una aplicación buscadora para el mismo propósito.

- **Netiquette:** Esta categoría hace alusión a normas de comportamiento (de ahí la mezcla y abreviatura con la palabra "etiqueta" en la red) es el conjunto de las mejores prácticas y las cosas que se deben evitar cuando se utiliza el Internet, especialmente en comunidades tales como foros o grupos en línea. Es más de un conjunto de convenciones sociales que tienen como objetivo hacer que las interacciones en línea sean constructivas, positivas y útiles. Los ejemplos incluyen: publicar fuera de tema, insultar a la gente, enviar o publicar spam, etc.

- **Network sniffing:** Del inglés "Husmear en línea". Esta es una técnica que utiliza un programa de software para monitorizar y analizar el tráfico de red. Esto se puede utilizar legítimamente, para detectar los problemas y mantener un flujo de datos eficiente. Sin embargo, también puede ser utilizado maliciosamente hacia datos que se transmiten a través de una red.

- **Nombre del dominio:** La dirección, en letras, de un sitio web o servicio de Internet. Por ejemplo: ssd.eff.org, facebook.com, hiperderecho.org.

O:

- **Ofuscación:** En la seguridad cibernética, la ofuscación es una táctica utilizada para hacer un código de ordenador oscuro o claro, por lo que los seres humanos o ciertos programas de seguridad (como antivirus tradicional) no pueden entenderlo. Mediante el uso de código ofuscado, los criminales cibernéticos hacen más difícil para los especialistas en seguridad cibernética leer, analizar y aplicar ingeniería inversa a su malware, evitando que para encontrar una manera de bloquear el malware y suprimen la amenaza.

- **Offline Attack:** Del inglés "Ataque fuera de línea". Este tipo de vulneración puede ocurrir cuando un atacante logra obtener acceso a datos a través de medios sin conexión, como las escuchas, mediante la penetración de un sistema y el robo de información confidencial o mirando por encima del hombro de alguien y la obtención de las credenciales a los datos secretos.

P:

- **Penetración:** En la seguridad cibernética, la penetración se produce cuando un atacante malintencionado haya podido burlar a las defensas de un sistema y los datos confidenciales adquirir de ese sistema.

- **Phishing:** Esta es una técnica maliciosa utilizada por los ciberdelincuentes para obtener

información sensible (datos de tarjetas de crédito, nombres de usuario y contraseñas, etc.) de los usuarios. Los atacantes se hacen pasar por una entidad de confianza para cebar las víctimas para que confíe en ellos y revelar sus datos confidenciales. Los datos recogidos a través de phishing se pueden utilizar para el robo financiero, robo de identidad, para obtener acceso no autorizado a las cuentas de la víctima oa las cuentas que tienen acceso, a la víctima de chantaje y más.

- **Privacidad:** Cuando hablamos de seguridad digital, la noción de "privacidad" nos refiere al conjunto de configuraciones a nuestra disposición en nuestros dispositivos y aplicaciones. Estas permitirán que habilitemos o deshabilitemos, según nuestra elección, determinadas configuraciones y, con ellas, nuestras posibilidades de mostrarnos en Internet y cómo permitimos que se use nuestra información en espacios online.

- **Proxy basada en la red:** Un sitio web que le deja acceder a sus usuarios a otros sitios web cerrados o censurados. Generalmente, un proxy basado en la web le deja a usted una dirección web (o URL) dentro de la página, y luego entonces la vuelve a mostrar en la página proxy. Esta es más fácil de usar que la mayoría de los otros servicios de circunvalar la censura.

Q:

- **Q de... ¿Qué puedo hacer para potenciar mi seguridad digital?** La respuesta es seguir leyendo y relacionándome con definiciones útiles sobre tecnología y entorno de Internet. Más información significa mayor poder para la toma de decisiones

R:

- **Ransomware:** Es un tipo de malware (software malicioso) que encripta todos los datos en un PC o dispositivo móvil, bloqueando el acceso del titular de los datos a ella. Después de que ocurra la infección, la víctima recibe un mensaje en el cual se le indica que a cambio de una cierta cantidad de dinero (por lo general, en bitcoins), la persona podrá acceder a la clave de descifrado. Por lo general, también hay un límite de tiempo para efectuar el pago del rescate. No hay garantía de que si la víctima paga el rescate, esta persona efectivamente reciba la clave de descifrado.

- **Riesgo:** En seguridad digital, con "riesgo" nos referimos a la posibilidad de que alguna amenaza se concrete.

S:

- **Sistema operativo:** Con esta categoría, nos referimos al conjunto de órdenes y programas que permiten la operación de otros programas en una computadora. Windows, Android y Apple OS X, iOS son ejemplos todos de un sistema de operación.

- **Software libre de código abierto:** El software de fuente abierta o software libre es un software que puede ser distribuido de forma gratuita de forma que permite que otros lo modifiquen y rehacer desde cero. Mientras que este se conoce como un "Software Libre", este no es necesariamente gratis o libre como diciendo libre de costo: los programadores de FLOSS pueden solicitar donaciones o cobrar por apoyo o copias. Linux es un ejemplo de un programa de fuente abierta como los son Firefox y Tor.

- **Spam:** Está compuesto de correos electrónicos no solicitados u otros tipos de mensajes enviados a través de Internet. El spam se utiliza a menudo para enviar malwares y difundir links que busquen vulnerar a través de phishing, por lo que nunca se debe abrir, responder o descargar archivos adjuntos de los mensajes de spam.

T:

- **Tarjeta SIM:** Esta es una pequeña tarjeta removible que puede ser introducida en un teléfono móvil para poder proveer servicio a una compañía particular de teléfono móvil. Las tarjetas SIM (del inglés "subscriber identity module" o módulo de identidad de suscriptor) también pueden guardar números de teléfonos y mensajes de textos.

- **TOR:** Llamado así por sus siglas, "The Onion Router" en inglés o "El enrutador cebolla". Se trata de un proyecto y navegador cuyo objetivo principal es el desarrollo de una red de comunicaciones distribuida de baja latencia y superpuesta sobre Internet. De este modo, el encaminamiento o ruta de transferencia de los mensajes intercambiados en sus usuarios y usuarias no revelará su identidad o, mejor dicho, su dirección IP. Esto le provee de un carácter de anonimato a nivel de red. En esa línea, mantiene la integridad y el secreto de información que viaja por ella.

- **Troyano:** Se denomina caballo de Troya, o troyano, a un malware que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.

U:

- **U de... ¡unámonos contra la violencia digital de género!** Cada unx de nosotrxs, como usuarixs o activistas, podemos incidir en la creación de una Internet en la que todxs podamos ser quienes queremos ser.

V:

- **Verificacion 2 pasos:** Recuerda, piensa en "Algo que tú sabes y algo que tú tienes." Los sistemas de registros que solo requieren un nombre de usuario y una clave corren el riesgo de ser penetrados cuando alguien puede obtener (o adivinar) esta información. Los servicios que ofrecen verificación de 2 pasos también requieren que tú proveas una confirmación por separado que diga que eres la persona que dices ser El segundo factor puede ser un código secreto desechable, un número generado por un programa que corra en un dispositivo móvil, o un dispositivo que lleves y que puedas usarlo para confirmar quién eres tú.

- **Virus:** Un virus informático es un tipo de software malicioso con la capacidad de autorreplicación. Necesita la intervención humana para entrar en un dispositivo o programa y puede copiarse a sí mismo en otros programas informáticos, archivos de datos, o en ciertas secciones de su ordenador, como el sector de arranque del disco duro. Una vez que esto sucede, estos elementos se infectarán. Los virus informáticos están diseñados para ordenadores daño y sistemas de información y pueden propagarse a través de Internet, a través de las descargas maliciosas, archivos adjuntos de correo electrónico infectados, los programas maliciosos, archivos o documentos. Los virus pueden robar datos, destruir la información, registrar las pulsaciones del teclado y más.

- **VPN comercial:** Una Red Privada Virtual comercial es un servicio privado que ofrece retransmitir de forma segura sus comunicaciones por Internet a través de su propia red. La ventaja de esto es que todos los datos que envíes y recibas están ocultos de las redes locales, por lo que es más seguro contra los delincuentes cercanos, los proveedores de servicios de Internet locales no confiables o cualquier otra persona que potencialmente esté espiando en tu red local. Una VPN puede estar alojada en un país extranjero, lo que resulta útil tanto para proteger las comunicaciones de un gobierno local como para eludir la censura nacional. La desventaja es que el tráfico se descifra al final de la VPN comercial. Esto significa que debe confiar en que la VPN comercial (y el país en el

que se encuentra) no espiará su tráfico.

- **Vulnerabilidad:** Una vulnerabilidad es un agujero en la seguridad informática, que deja el sistema abierto a los daños causados por los atacantes cibernéticos. Se busca que las vulnerabilidades sean resueltas tan pronto como estas se descubren, es decir, antes de que un delincuente cibernético se aproveche de estas y haga uso de las mismas.

W:

- **Worm:** De "gusano" en inglés. Un "worm" informático es uno de los tipos más comunes de malware. Es similar a un virus, con la diferencia en su manera de extensión: los gusanos tienen la capacidad de propagarse de forma independiente y auto-replicarse de forma automática mediante la explotación de vulnerabilidades del sistema operativo, mientras que los virus dependen de la actividad humana con el fin de propagación. Por lo general, un usuarix lo "atrapa" a través de correos electrónicos masivos que contienen archivos adjuntos infectados. Los gusanos también pueden incluir "cargas" que los ordenadores anfitriones, comúnmente diseñados para robar datos, así como borrar archivos y/o enviar documentos por correo electrónico.

X:

- **XMPP:** Es un estándar abierto de mensajería instantánea - Google usa XMPP para Google Talk; Facebook la ofrecía, pero dejó de hacerlo. Los servicios de mensajería instantánea independientes no corporativos normalmente usan XMPP. Los servicios como WhatsApp tienen su propio protocolo cerrado y secreto.

Y:

- **Y de... Y, ahora, ¿Qué más necesito para ser una persona experta en seguridad digital?** ¡No te olvides de revisar bien el kit con el que viene este anexo!

Z:

- Como te imaginarás, ¡encontrar palabras con Z ha sido un reto! Si bien aquí te presentamos unas cuantas que muy probablemente no significarán algún riesgo para ti, consideramos que de todos modos podría servirte a manera de conocimientos extra con los cuales estar en nivel Experto sobre vocabulario de seguridad digital... Eso, además de unas cuantas recomendaciones sobre la plataforma Zoom.

Así, si jugaras a tutti frutti de seguridad digital,
ganarías incluso con la letra Z
¡No dejes de activarlas!

- **Zero day:** Conocido como "día cero" o "ataque Hora Cero" son ataques que utilizan vulnerabilidades en los programas informáticos mediante que los criminales cibernéticos han descubierto y los fabricantes de software aún no han parcheado, al no conocer sobre la existencia de esas vulnerabilidades. Por ese motivo, estos suelen llevarse a cabo antes de que las compañías de software de seguridad tomen conciencia de ellos. A veces, estos son descubiertos por los proveedores de seguridad o investigadores y se mantienen privados hasta que la empresa parcha dichas las vulnerabilidades.

- **ZeuS/ Zbot:** ZeuS, también conocido como Zbot, es un caballo de Troya - o, simplemente, troyano-, que infecta a los usuarios de Windows e intenta recuperar la información confidencial que almacenan los ordenadores infectados. Una vez instalado, también intenta descargar archivos de configuración y actualizaciones de Internet. Su propósito es robar datos privados de las víctimas, así como la información del sistema, contraseñas, datos bancarios u otros detalles financieros.

- **Zombie:** Un ordenador zombie es uno conectado a Internet, que en apariencia está operando con normalidad, pero puede ser controlado por un hacker que tiene acceso remoto al mismo y envía comandos a través de un puerto abierto. Principalmente, los zombies se utilizan para realizar tareas maliciosas, tales como la difusión de ataques de correo no deseado u otros datos a otros equipos infectados o lanzamiento de DoS (denegación de servicio) sin que el propietario sea consciente de ello.

- **Zoom:** Lo más importante que debes recordar a la hora de conectarte a una videollamada Zoom es que tienes a tu disposición una serie de configuraciones de privacidad que puedes aprovechar De todas maneras, como último tip, te hacemos presente que hay más de una plataforma con la cual puedes realizar videollamadas. Entre ellas, te recomendamos 3 junto con unas **recomendaciones para reuniones seguras.**
  - Google Meet.
  - Jitsi
  - Microsoft Teams