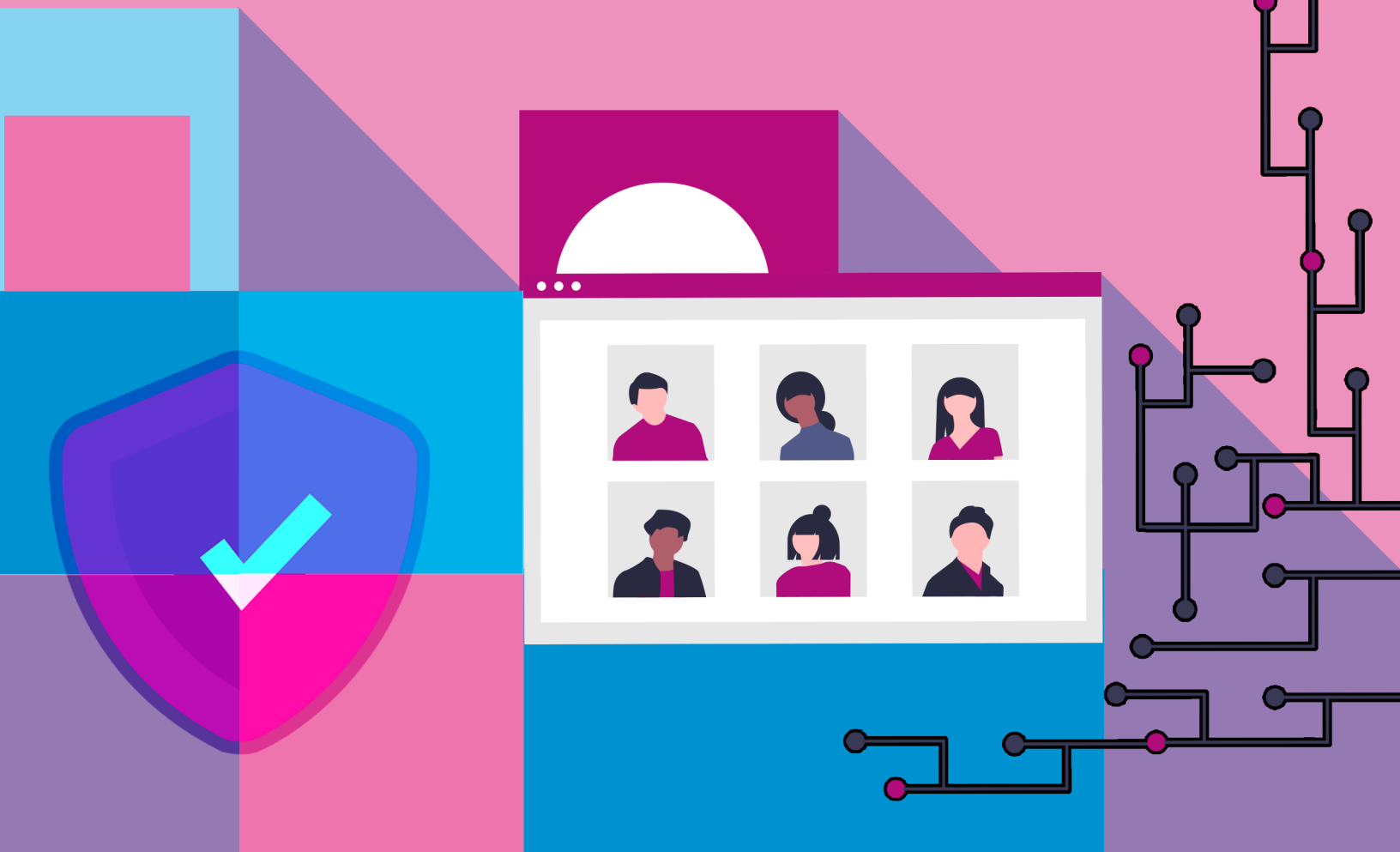
# GUIA PARA PROTOCOLOS DE SEGURIDAD DIGITAL Y FÍSICA PARA ORGANIZACIONES Y COLECTIVOS



## Contenido

# GLOSARIO

- **HISTORIAL DE NAVEGACIÓN:** lista de sitios web que visitas, generalmente registrados por defecto por tu seguridad.

- **CIFRADO O CONEXIÓN DE EXTREMO A EXTREMO:** se trata de un sistema de comunicación en dónde solamente les usuaries que se están comunicando, pueden leer los mensajes.

- **TORRE DE CELULARES:** estructura que aloja antenas y equipo de telecomunicaciones que permite la comunicación entre celulares.

- **HTTPS:** protocolo que crea conexiones cifradas entre los dispositivos y sitios web. En tu navegador debe de aparecer, previo a la dirección de la página web, https://ladirecciondelsitioweb.com

- **URL:** es la dirección única asignada a cada recurso que se encuentra en línea.

- **DIRECCIÓN IP:** es la numeración única con la que se puede identificar cada dispositivo

- **PROVEEDOR DE SERVICIOS DE INTERNET:** empresa que provee servicio de conexión de internet.

- **ROUTER:** dispositivo que conecta y dirige el tráfico de internet.

- **WIFI:** tecnología que habilita conectividad de red a través de señales de radio (inalámbricas). Lo que hace posible la conexión entre dispositivos.

- **CÓDIGO ABIERTO:** es el código con el que fue programado la aplicación, programa o sitio web y que fue creado con el fin de que cualquier persona pueda modificarlo, distribuirlo y auditarlos sin ningún problema de forma gratuita. Además, que la mayoría de aplicaciones o programas de código abierto, siguen parámetros en donde se respeta los datos e información de sus usuaries.

- **CÓDIGO CERRADO:** a diferencia del código abierto, el código cerrado busca regalías de casi todo lo que ofrecen o tienen contenido gratuito limitado. No permiten que su código sea modificado y no ofrece mayor información sobre los datos que recolecta sobre sus usuaries.

- **GENERADOR DE CONTENIDOS:** son toda aquella persona, empresa, medios y organizaciones, que crean contenidos para que esté disponible en la web.

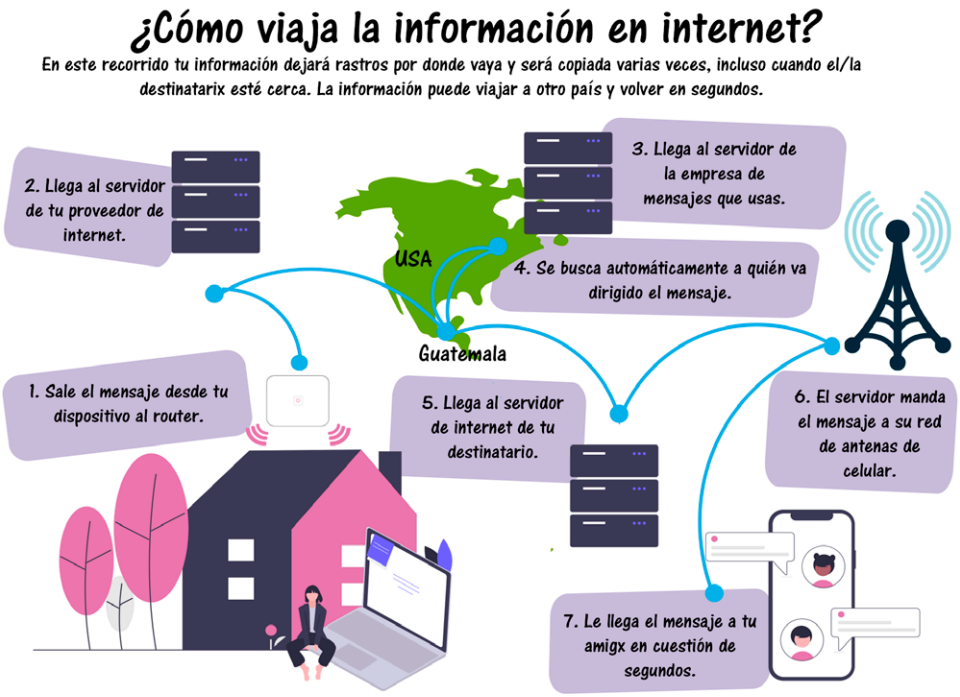
- **GEOLOCALIZADOR:** el geolocalizador permite tener la ubicación geográfica real de cada dispositivo. Esta ubicación se realiza aunque no esté encendido en el dispositivo.

# CAPÍTULO I: BÁSICO DE INTERNET

## 1. ¿CÓMO FUNCIONA LA INTERNET Y CÓMO VIAJA NUESTRA INFORMACIÓN?

¿Te has preguntado alguna vez por dónde pasa un mensaje o correo electrónico antes de llegar a su destino? ¿Cómo funciona Internet? ¿Hasta dónde llega nuestra información? ¿Le llegará solo al destinatarix?

Internet no es algo que sucede como arte de magia, para que haya conexión entre un dispositivo y otro se necesita de una infraestructura que ayudarán a que se establezca estas conexiones. Además, hay muchas empresas que brindan diferentes servicios para hacer que el mensaje que enviemos vaya de un punto a otro.




La infraestructura que se necesitará para que esto sea posible es:

1. Servidores
2. Data centers
3. Proveedores de internet (en el caso de Guatemala Tigo y Claro)
4. Cables terrestres-submarinos
5. Empresas de contenidos digitales
6. Puntos de entrada o acceso (routers o datos)
7. Infraestructura a nivel de usuario.

Todo lo que se encuentra en la red es posible porque:

1. Hay generadores de contenidos
2. Conexiones de punto a punto entre servidores que alojan contenidos y servicios.
3. Cibernautas
4. Servicios (cada red social, páginas webs, chats, videos, etc)

# 2. METADATOS, HUELLAS O SOMBRAS DIGITALES.

Los metadatos se definen como "los datos de los datos", es la huella que dejamos al enviar un mensaje de texto, hacer una navegación en internet o hacer una llamada. Durante esta parte reflexionaremos sobre nuestros rastros digitales.

Los metadatos pueden ser:

- Intencionales y visibles, eso quiere decir que nosotres estamos conscientes que los generamos.

- Invisibles e involuntarios, es todo aquel rastro que se queda mientras estamos navegando o usando nuestros dispositivos digitales y de los cuales no sabemos que se queda un rastro de nuestra actividad en el mismo.

Tipos de metadatos más comunes:

- Número de teléfono
- Direcciones de correo electrónico
- Nombres de usuarixs
- Número de IP de tu dispositivo (número que identifica un dispositivo en una red)
- Datos de geolocalización
- Fecha y hora
- Información sobre el dispositivo que usas (especificaciones técnicas)
- Asuntos de correos
- Direcciones URL.

**Descarga estas herramientas:**

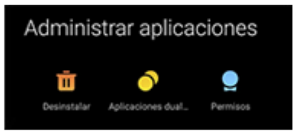
- **MetadataRemover: Con esta app puedes eliminar metadatos de tus archivos (ubicación, hora, etc.)**

- **Obscuracam: proteje la identidad en fotografías y elimina los metadatos.**

# 3. ¿CÓMO HACER UNA DATA DETOX?


Vamos a la opción de configuración o ajustes.


Buscamos la opción de administrar aplicaciones.




Seleccionamos desinstalar


Por último seleccionamos las aplicaciones que ya no utilicemos y seleccionamos desinstallar

Como paso extra puedes instalar CC Cleaner para eliminar basura residuos y de las aplicaciones.

Este paso consiste en hacer un conteo de todas las aplicaciones que tenemos instaladas en nuestro dispositivo y vamos eliminando todas aquellas apps que hemos dejado de usar y solo ocupan espacio en nuestro teléfono.

**Nota: ¡Cuidado!** Hay varias aplicaciones que trae el teléfono son para que funcione correctamente. Solo debes de desinstalar aquellas que tú hayas descargado e instalado y ya no uses (también pueden ser aquellas apps como "ideas claro", "google fit", etc).

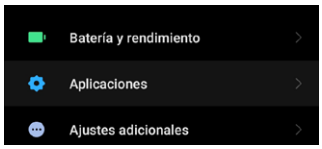
# 4. QUITAR PERMISOS A LAS APPS.

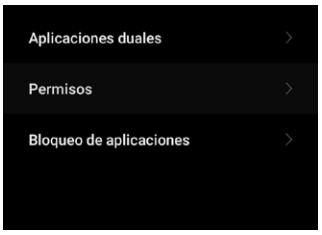
Esta actividad nos ayudará a reducir el riesgo de fuga de información. Hay aplicaciones que mantienen permanentemente encendido el micrófono, cámara y ubicación, entre otros. Estas opciones la mayoría de apps no lo necesitan, pero tratan que se hacernos pensar que si no están activas la aplicación "no podrá funcionar".

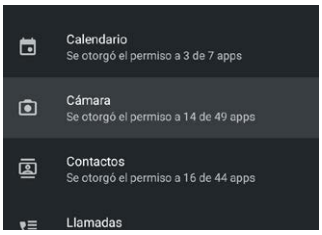
## ¿Cómo encuentro los permisos en mi celular?

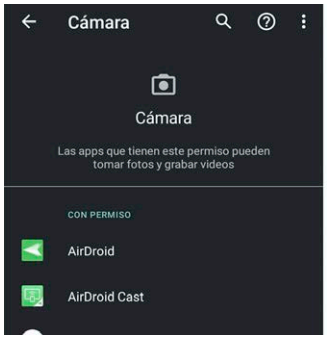
Sigue estos pasos. La mayoría de teléfonos celulares tienen la misma ruta para encontrarlo.

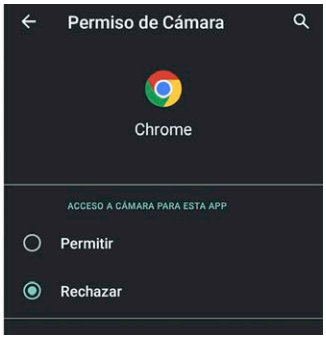
- Ajustes
- Aplicaciones
- Gestor de permisos/ Permisos
- Te aparecerá un listado, esos son los permisos que usan las aplicaciones. Debes de elegir una por una y revisar si las apps que nos aparecen realmente necesitan ese acceso para su funcionamiento.
- Si no necesita el acceso a esa función una de las aplicaciones, la seleccionas y le das "rechazar o no permitir". Y ¡Listo!


**Nota: ¡Cuidado!** Al igual que en la data detox, debes de tener cuidado de verificar bien a qué le quitarás el acceso. Trata de centrarte en aquellas aplicaciones que tu hayas descargado, como juegos, redes sociales, chats y las apps de google (fotos, fit, calendar, etc).

# CAPÍTULO II: VIOLENCIAS EN LÍNEA

Las violencias que sufrimos en las calles no están ajenas a las violencias que vivimos mientras estamos conectadas/es a internet. Últimamente en épocas de pandemia estas violencias han aumentado. Estar conectadas y navegar no debería representar un peligro para nosotras, por lo tanto, internet es también un territorio en disputa.

## 1. ¿CÓMO SABER QUE ESTOY SIENDO VIOLENTADE EN ESPACIOS DIGITALES?

- Incomodidad
- Amenazas
- Vigilancia

### Algunos tipos de violencias

- Compartir imágenes sin consentimiento

Está bien que queramos compartir imágenes nuestras con otres con quienes tenemos un acuerdo previo. Pero en ocasiones las personas con quienes compartimos nuestras imágenes envían, sin nuestro consentimiento, nuestras fotografías a otros, usualmente a grupos formados mayoritariamente por hombres.

Buenas prácticas: antes de enviar tus fotos procura eliminar metadatos y ocultar tatuajes, rostros, cicatrices, etc cualquier parte o señal que indiquen que eres tu. Trata de que no se vea tu espacio (habitación, casa o que indique tu ubicación).

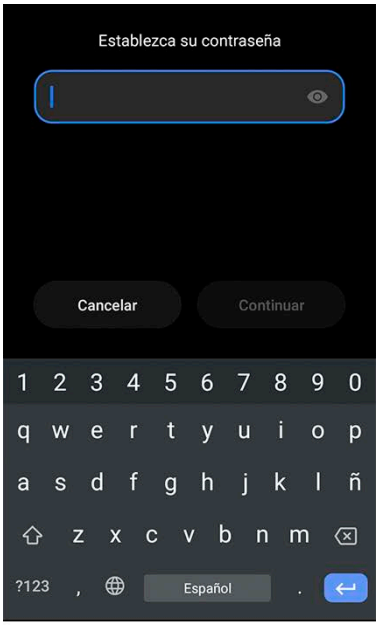
- Control de nuestras plataformas digitales

Suele suceder en parejas o personas cercanas a nosotres, estas personas creen que "deben" de tener acceso a nuestras plataformas digitales, pero no es así. Los espacios digitales son parte de nuestra privacidad.

Buenas prácticas: mantén tu dispositivo y acceso a las aplicaciones con clave. Hoy en día la mayoría de dispositivos permiten tener contraseñas para cada aplicación.

**En el caso que filtren alguna fotografía tuya ingresa a este enlace para que tu imagen no pueda seguir siendo localizada en línea:**

**Algunas rutas que puedes seguir para resguardar tu información:**

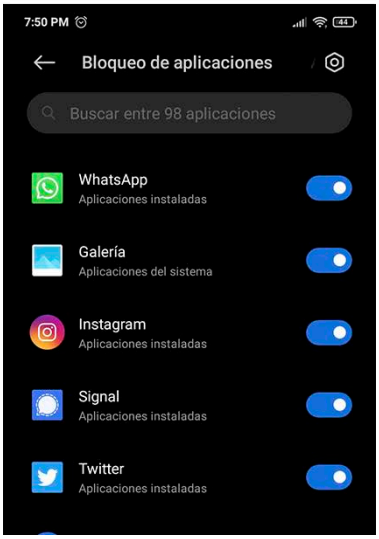



a) Pasos para contraseña de bloqueo de pantalla.

- Ajustes
- Seguridad
- Gestor de contraseñas
- Contraseña de bloqueo de pantalla

b) Pasos para contraseña de apps

- Ajustes
- Seguridad
- Bloqueo de apps
- Entrar en la tuerquita (esquina superior derecha de la pantalla)
- Tipo de contraseña
- PIN personalizado / regresamos a la pantalla anterior
- Agregar PIN / cambiar PIN
- Agregar pregunta de recuperación




c) Agregar apps que necesiten contraseña para su ingreso (será el PIN que colocamos en el paso anterior)

- Ajustes
- Seguridad
- Bloqueo de aplicaciones
- Agregamos todas las aplicaciones que queramos, sugerimos que sean todas o al menos que estén, chats, correos, lista de contactos, app del banco y redes sociales.

- Acoso en línea

Es un hostigamiento que pueden ser desde “Que linda foto”, “Que bonita eres”, “Soy fotógrafo y quisiera hacerte unas fotos desnuda”; llegar hasta a los insultos, si el acosador no es correspondido. También es acoso cuando somos atacadas porque apoyamos o somos partes de los diferentes movimientos feministas, antiracistas, LGBTIQ+,etc. Usualmente estos tipos de acoso se dan a través de las redes sociales personales, de la organización o colectivas a las que pertenecemos

El acoso puede darse desde distintos canales, pero usualmente en perfiles personales en redes sociales, páginas que administramos, etc.

Buenas prácticas: bloquea y reporta al acosador. La mayoría de plataformas y redes sociales tienen opciones para reportar estos tipos de violencias. Aunque sabemos que esto no garantiza que las violencias desaparezcan, sí hará que desaparezca su perfil y se tardará un poco en crear una cuenta nueva. Esto te dará tiempo para cambiar tus datos y privacidad de tu perfil.

Los bloqueos y reportes deben de ser masivos. Busca tu red de apoyo más cercano para que te ayuden a hacer estos reportes.

**Nota:** cada una de estas violencias deben de ser documentadas, con capturas de pantalla, anotar el nombre del usuario, hora día y cualquier otro dato que pueda proporcionarte información sobre el perfil desde donde hacen el acoso. Estos datos nos servirá para saber si existe un patrón de comportamiento, si es alguien cercano o si es un troll sin nada que hacer. De cualquier manera, ningún tipo de violencia la debemos tomar a la ligera. Además, en el caso que decidas hacer una denuncia, llevarás varias pruebas y datos que pueden apoyar a la investigación.

- Discurso de odio

El discurso de odio incita a la violencia y va desde expresiones escritas, verbales o visuales, de discriminación, acoso, amenzas o violencia contra una persona o grupo por motivo de su género, discapacidad, orientación sexual, etnia o creencia religiosa

Al igual que el anterior es necesario documentar porque en algunos casos, la violencia pasa de lo virtual a lo físico.

Buenas prácticas: documentar todo lo que nos sea enviado:

- Documentar
- Reportar y bloquear
- Cambiar

## 2. MI PRIVACIDAD EN GOOGLE Y FACEBOOK.

Hoy en día, la mayoría contamos con una o varias redes sociales y varios momentos de nuestras vidas las compartimos por estos canales. Sin embargo, esta es una forma muy fácil de saber quién eres, quiénes son tus amiges más cercanos, familiares, qué te gusta, hasta apodos.

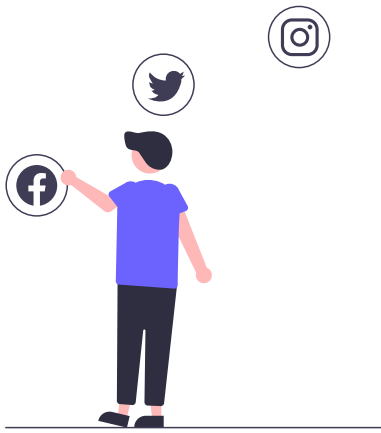
¿CÓMO NOS PROTEGEMOS?

Facebook: para saber cómo proteger nuestras información en las plataformas que más usamos, en este caso facebook, es importante que nos preguntemos:

¿Qué y cómo ven mi perfil otres usuaries? ¿Qué información está pública?

Es importante que revises en la configuración de tu cuenta los siguientes aspectos:

- Privacidad
- ¿Quién puede ver tus publicaciones?
- ¿Quién puede encontrarte?
- Etiquetado
- Información fuera de Facebook
- Cerrar otras sesiones



Buenas prácticas:

- Hacer un perfil diferente para el activismo.
- Si ingresas desde un navegador, revisa que la URL sea HTTPS y tenga el candadito verde al inicio de la dirección para saber que es segura.
- Hacer verificación de dos pasos. Esto nos alertará si otres quieren acceder a nuestro perfil desde otros dispositivos.

Google: esta es una de las plataformas de mayor recolección de datos. Casi toda la información pasa por elles. Pero no son los únicos. Sin embargo, aunque nos

ofrecen diferentes servicios para "facilitarnos la vida", existen otras plataformas alternativas que nos dan el mismo servicio y protegen nuestra información.

## Herramientas y buenas prácticas

- Celulares y Google: en esta parte vamos a desligar varias opciones que no necesitan nuestro teléfono para funcionar. Te dejamos acá la ruta que puedes seguir, para la mayoría de teléfonos es la misma o parecida.

Rutas:

1. Ajustes_Google_anuncios_cancelar anuncios personalizados.
2. Ajustes_Google_autocompletar_apagar usar autocompletar con google
3. Ajustes_Google_activar encontrar mi dispositivo

- Migrar correos: la mayoría de nosotres contamos con una cuenta en gmail, pero como hemos visto, no son del todo seguros. Exiten otras alternativas de correos que son seguros y que no recolectan información, podemos sugerir Riseup (https://riseup.net/) en el caso de este correo, necesitas que alguien que ya tenga cuenta con elles, te envíe un código de invitación para crear tu propia cuenta. Tutanota (https://tutanota.com/es/) y Protonmail (https://protonmail.com/).

- Motores de búsqueda y buscadores: los que te mostramos acá son alternativos a Chrome. Aunque algunas páginas que busques no sean las primeras en aparecer, funcionan exactamente igual que Chrome, pero estos buscadores son seguros y sabemos que no se quedarán tu información.

- Envío de documentos seguros:

1. Riseup share: solo debes de cargar el documento, imagen o audio (deben de tener un peso determinado), cuando haya cargado copias el link y lo envías al destinatario.

2. Disroot: funciona similar a riseup share, pero acá podemos colocar el tiempo que puede estar vigente el link.

Para más información sobre cómo puedes proteger tu teléfono, te dejamos este enlace en el que puedes encontrar un kit de data detox para celulares:

Alternativas de navegadores de internet para celulares:

MozillaFirefox

DuckDuckGo

Firefox Focus

RiseUp

Disroot

## 3. CHATS SEGUROS

¿Qué debemos de tomar en cuenta para usar un chat?

Para saber si el chat que usamos para comunicarnos es seguro, es importante que tenga las siguientes opciones:

- Opción de bloqueo (PIN o contraseña).
- Tenga opción para activar la verificación de dos pasos.
- Cifrado de extremo a extremo.

Información sobre algunos de los chats más utilizados

- Whatsapp: código cerrado, esto quiere decir que no permite que sea auditado y que se verifique si realmente cumple lo que ofrecen respecto a la privacidad en las comunicaciones entre sus usuaries. Si tiene verificación de dos pasos, no tiene opción de chat secreto y descarga imágenes, audios y videos automáticamente a tu dispositivo.

- Telegram: tiene código abierto, se puede cifrar, tiene verificación de dos pasos, clave de acceso y cifrado de extremo a extremo.

- Signal: tiene código abierto, está cifrado, clave acceso, bloqueo de capturas de pantalla y opción de autodestrucción de mensajes.

- Messenger: código cerrado, verificación de dos pasos, es parte de facebook.

## 4. CONTRASEÑAS SEGURAS

Todas las redes y algunas paginas que visitamos nos solicitan tener unx usuarix y contraseña, pero ¿recuerdas todas las contraseñas? ¿usas la misma contraseña para todo o la mayoría de plataformas?

Tener una contraseña diferente es algo muy importante para proteger tu información y evitar que terceros accedan fácilmente a tus plataformas.

Características para tener una contraseña segura:

- Que sea extensa
- Compleja
- No usar frases literales
- Nada personal
- Secreta
- Utiliza una contraseña por servicio
- Que sea fresca.

**Keepass**

¿Cómo puedo recordar todas las contraseñas?

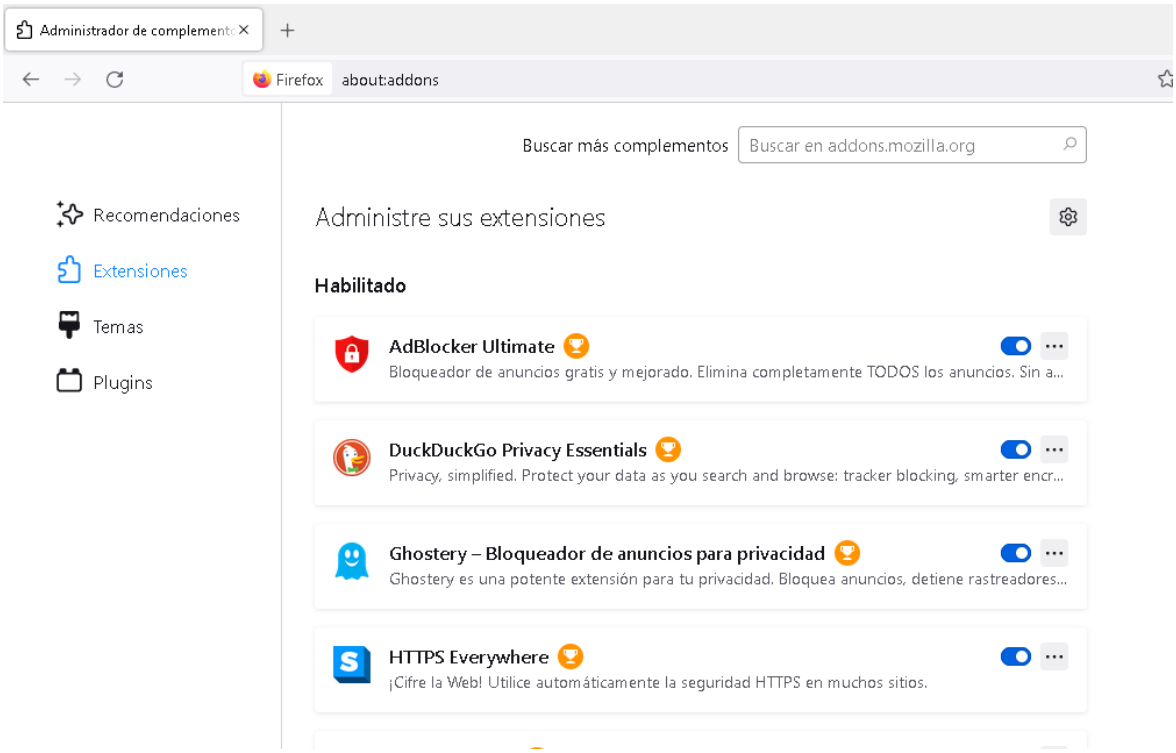
Sabemos que no podríamos memorizar todas las contraseñas para cada plataforma, es por eso que te recomendamos usar un llavero virtual que te facilitará usar contraseñas diferentes y estar seguras. Keepass es una buena plataforma que puedes instalar y solo tienes que memorizar una contraseña.

**Puedes descagar un manual y un tutorial para Keepass haciendo click aquí**

# 5. SEGURIDAD PARA COMPUTADORAS

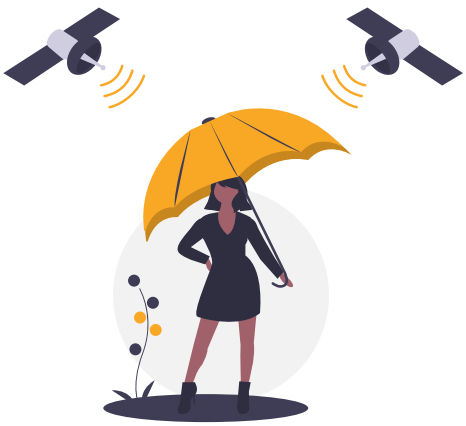
Instalación de complementos para nuestro motor de búsqueda:

- Descargar Firefox en la computadora
- Buscar en la parte superior derecha (tres rayas horizontales)
- Buscar complementos
- En el espacio de búsqueda, colocar los siguientes complementos: DuckduckGo, Ghostery, Adblock, Privacy Badger y HTTPS Everywhere. Cada uno de estos complementos ayudarán a detener rastreadores o cookies que se puedan colar en tus navegaciones y hacer que tus navegaciones sean más seguras.




## Virtual Privacy Network (VPN)

Puedes usar las siguientes plataformas de VPN que son gratuitas y seguras para proteger tu ubicación y no puedan conocer desde qué parte del mundo estás navegando.



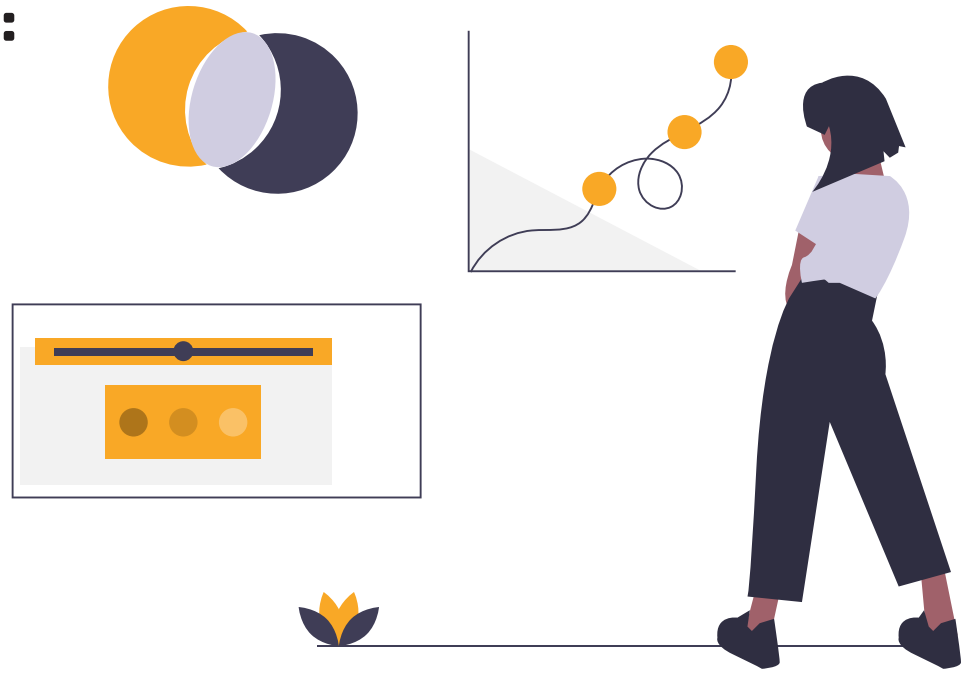
Tor para computadora

Tunnelbear para computadora

Tor para celular

Tunnelbear para celular

# CAPÍTULO III: MAPEO DE RIESGOS



## 1. LÍNEA DE TIEMPO

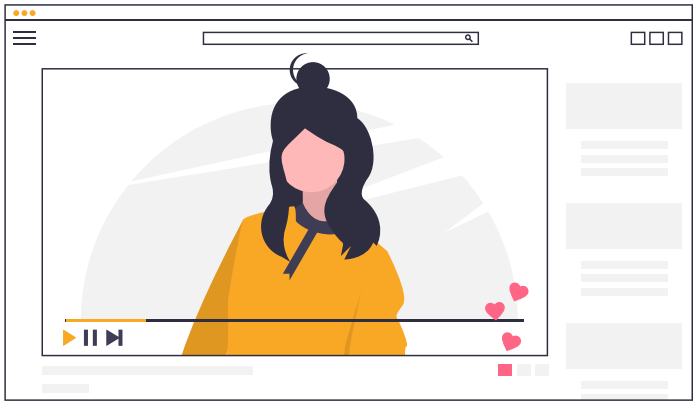
La idea de crear una línea de tiempo es identificar cuáles han sido los riesgos, amenazas y mitigación que hemos implementado para cuidarnos, cuáles han funcionado, cuáles ya no son viables y cuáles podemos implementar.

| ¿Cuándo pasó? | Amenaza | Riesgo | Mitigación |
|---|---|---|---|
| 2006 | Asesinatos, conflictos internos por conformar o no la organización.<br>Falta de reconocimiento de la organización por parte de las autoridades y la sociedad. | Alto | Denuncias<br>Incidencia<br>Organización |
| 2009 | No existía un espacio físico y nadie quería alquilar a la organización.<br>No se tenía ningún tipo de financiamiento. | Alto | Investigación<br>Buscar el reconocimiento internacional |
| 2011 | Contra-movimiento | | |
| 2012 | Ataque por parte de los medios de comunicación a causa de un incidente personal en la catedral. | Alto | |
| 2016 | Se pierde apoyo de las agencias internacionales.<br>Asesinatos y exilio. | Alto | Implementación del área jurídica |
| 2018 | Con el crecimiento de redes sociales crecen los discursos de odio y agresiones en redes sociales. | Alto | Discurso de sensibilización<br>Comunicados<br>Alianzas con otras organizaciones<br>Se mejora la seguridad a través de cámaras y el alquiler de oficinas en un edificio. |
| 2021 | Crecen las agresiones en redes sociales.<br>Iniciativas de ley 5272 y 5940 que son completamente anti derechos y son impulsadas por diputados un discurso ultra conservador. | Alto | |

# 2. ¿QUIÉNES ESTAMOS EXPUESTES?

Vamos a identificar qué tipo de perfil tiene cada persona que es parte de la colectiva/organización para así tener claro quién o quiénes están más expuestxs riesgos.

- Comunicación
- Creación de contenidos
- Gestión de proyectos
- Encargades de la seguridad
- Defensoras y defensores de derechos
- Finanzas y manejo de presupuestos
- Manejo de contactos
- Gestor o gestora de relaciones estratégicas
- Manejo de redes sociales
- Lideresa/líder de la colectiva/organización
- Administrativa

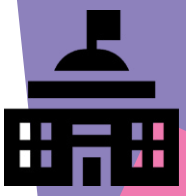


# 4. CONOCIENDO A NUESTRE VECINE.

Los adversarios son actores cuyo interés es opuesto al nuestro y van a buscar contrarrestar nuestras acciones. Todo adversario tiene sus propias percepciones y estrategias.

Entender a nuestros adversarios nos ayudará a mejorar la planificación y decidir qué acciones de protección o mitigación puede realizarse al verse vulnerada tu seguridad.

## Identificando a nuestro adversario ¿Cuáles son los más comunes?



**1. Actor Estatal:** persona, dependencia u organización que está actuando en nombre de un gobierno.

- Capacidad: recursos y programas dedicados para la interceptación de comunicaciones y vigilancia. Equipos y herramientas de alta capacidad para cumplir con sus objetivos. Además, puede tener/tienen contactos con igual o más poder que elles. Pueden actuar en conjunto con otros adversarios como delincuentes informáticos, grupos armados, fuerzas de seguridad, netcenters, etc.

**2. Grupos armados:** Organizaciones reconocidas dedicadas al hurto, chantaje u otro tipos de actividades criminales en la región donde se realizan las actividades.

- Capacidad: Variable según el lugar donde se ejecutan las actividades.

**3. Fuerzas de seguridad:** todos aquellos grupos estatales que deben o deberían dar seguridad a la ciudadanía (Policía Nacional Civil, ejército). También están la seguridad privada, usualmente contratados por empresas, organizaciones y transporte.

- Capacidad: tiene mayor libertad de movilizarse (sobretodo ahora en la pandemia). Poseen armas "legales". Trabajan en conjunto con grupos armados y actores estatales (en la mayoría de ocasiones).

**4. Delincuencia común:** Personas o organizaciones dedicadas al hurto, chantaje u otro tipos de actividades criminales en la región donde se realizan las actividades.

- Variable según el lugar donde se ejecutan las actividades.

**5. Ubicación:** lugar en donde se encuentra ubicada la organización o sede de nuestro colectivo.

- Capacidad: depende de la ubicación geográfica de la organización y colectivo (país, departamento, zona, municipio, comunidad, etc). Y la ubicación específica (dirección exacta). Estos datos ayudarán a saber más sobre el contexto que tiene cada colectiva/organización y qué les rodea (quién es nuestre vecine).

**6. Naturaleza: Condiciones climáticas.**

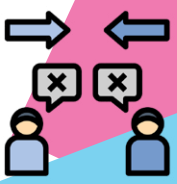
- Capacidad: dependerá de la ubicación geográfica y física de la organización y las actividades e implementos que cada uno tiene (equipo, computadoras, proyectores, celulares, etc)

**7. Empleado descontento:** Empleado que se siente descontento o desconexión con la organización. Puede ser por diferencias con la gerencia, percepción de mal pago, diferencias ideológicas etc. Pueden ser empleados fijos o consultores.

- Capacidad: conocimiento de los procesos internos de la organización/colectivas, sus actividades, debilidades y fortalezas. Tiene acceso permanente a las instalaciones, a sus recursos y quienes lo manejan.

**8. Opositor ideológico:** Personas o grupos opuestos a la razón de ser de la organización. Sus creencias religiosas o políticas los hacen estar motivados para afectar específicamente a la organización o persona. Pueden ser iglesias, partidos políticos o sus seguidores.

- Capacidad: variables según la organización y su objeto social.



**9. Competencia:** Organizaciones que compiten en el mismo sector por los mismos tipos de proyectos y financiación.

- Capacidad: Conocimiento de las propuestas de la organización, sus medios de financiamiento, proyectos y actividades pasadas. En algunos casos cuentan con personas quienes hayan pertenecido anteriormente a la organización.

**10. Trolls:** Persona que busca causar controversias, a través de mensajes en redes sociales o acoso directo a las personas.

- Capacidad: Variable según la organización. Es muy común que se les lea en redes sociales después de alguna marcha o acción pública.

**11. Delincuente informático:** Persona que busca lucrarse a través de sus actividades delictivas en internet. Se lucra vendiendo cuentas de servicios en internet o fraude bancario. No tiene una preferencia por las personas a quien ataque, lo hace por facilidad de ataque al blanco.

- Capacidad: Tiene leves conocimientos técnicos, usa herramientas libres o las consigue de forma ilegal.

**12. Sript Kiddie:** Persona sin conocimientos técnicos que ejecuta herramientas o explota vulnerabilidades de forma automatizada.

- Capacidad: Su conocimiento se limita a la ejecución de herramientas encontradas en internet.

# 4. AMENAZAS, RIESGOS, VULNERABILIDADES Y CAPACIDADES

## RIESGOS

Los riesgos normalmente se conocen como la exposición a una situación donde hay posibilidad de sufrir daño o estar en peligro. Cuando se dice que alguien o algo está en riesgo, es porque se considera que está en desventaja frente a algo más.

## AMENAZAS

Son todas aquellas acciones de origen natural o provocado intencionalmente por alguien, para generar un peligro hacia nosotres. Se refiere entonces, una declaración o intención de hacernos daño.

## VULNERABILIDADES

Son factores que hacen más probable que las amenazas se materialicen o provoquen un daño mayor. Mientras mayor sean nuestras vulnerabilidades con las tecnologías (y fuera de ellas/físicas), nuestros riesgos serán mayores.

Es toda aquella característica o circunstancias propias, que pueden potenciar el efecto de ese peligro.

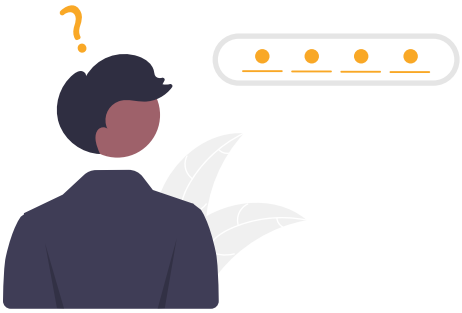
## CAPACIDADES

Son las habilidades y recursos que contamos para mejorar nuestra seguridad. Mientras más capacidades tengamos, menores serán los riesgos.

$$\text{Riesgos} = \frac{\text{Amenazas x Vulnerabilidad}}{\text{Capacidades}}$$

## AMENAZAS MÁS COMUNES

Aunque las amenazas y riesgos pueden variar, dependiendo de varios factores, acá dejamos las amenazas más comunes.



**a. Pérdida de información:** se refiere a situaciones en las que algún documento importante es eliminado y perdemos el acceso al mismo. Existen diferentes formas de perder información. Puede ser debido al mal manejo o daño de las unidades de almacenamiento, virus en los dispositivos o acceso no autorizado a nuestras nubes.

- **Riesgos:** pérdida de información importante para la colectiva/organización (contratos, pagos, depósitos, informes, etc).
- **Buenas prácticas:** respalda tu información de forma constante. Puedes guardarla en unidades de almacenamiento y cifrarlas.

**b. Exposición crítica de información:** Es cuando se ha filtrado algún tipo de dato o información sensible que puede poner en riesgo a quienes trabajan en la organización o personas cercanas. Esta amenaza también hace referencia a la publicación de información íntima no consentida.

- Riesgos: interceptación de contraseñas, mensajes, correos, videos y fotografías, ubicación o cualquier otra forma de ubicarnos a través de nuestra información personal.

- Buenas prácticas: antes de publicar algo, es necesario que nos preguntemos ¿quién quiero que tenga acceso a esta información? Es muy importante que mejoremos nuestra privacidad en redes sociales y cuentas de servicios. Utiliza mensajería con cifrado de extremo a extremo y utiliza correos que estén cifrados por defecto, como Protonmail.

c. Confiscación e inspección de dispositivos: es la "revisión legal" de nuestros dispositivos. Se puede interpretar como un robo, ya que bajo la lógica de legal pueden acceder a nuestra información.

- Riesgos: pueden realizar una copia y/o clonación del dispositivo, instalar algún software espía o intentar acceder a nuestra información.

- Buenas prácticas: si vas a viajar, realiza un respaldo de tu información. Borra la información sensible en tus dispositivos, el acceso a tus cuentas personales y laborales.

d. Monitoreo y vigilancia: Las empresas de telecomunicaciones y proveedores de servicios en línea, gobiernos y hackers maliciosos, pueden fácilmente hacer un rastreo de nuestra actividad en línea para distintos fines comerciales o políticos.

- Riesgos: ubicación, claves, información personal, actividades, información laboral,etc.

- Buenas prácticas: si usarás el wifi de algún aeropuerto, navega con una VPN, revisa tu información en redes, permisos de apps y utiliza navegadores que no guarden tu información y activa complementos.

e. Suplantación de identidad: nos referimos al uso de técnicas para la suplantación de credenciales o hacerse pasar por otra persona (creación de cuentas falsas).

- Riesgos: acceso a datos personales, imágenes y rasgos (como nos dirigimos con lxs demás). Acceso a contactos importantes.

- Buenas prácticas: contraseñas fuertes para todas tus cuentas, bloqueo de pantalla y apps con contraseña de código y no con patrones. Y realizar la verificación de dos pasos.

f. Ataque de fuerza bruta: Es el intento forzado de ingresar a una cuenta o servidor. Normalmente el atacante puede intentar adivinar las credenciales de acceso (Cuenta/usuarie y contraseña) o bien desarrollar ataques sofisticados con diccionarios para descifrarlas.

- Riesgos: información almacenada en el servidor de la organización o colectiva (acceso a la página web, contenido, correos, etc).

- Buenas prácticas: contraseñas fuertes para redes sociales, correos, cuentas de banco, etc. Además, agregar verificación de dos pasos. Y al momento de pérdida o robo de tus dispositivos, cambiar contraseñas y cerrar sesiones de redes sociales en los dispositivos que ya no tengas acceso.

g. Phishing: Es el uso de correos y/o mensajes falsos, a veces también llamadas o interacciones directas, que buscan engañar a la víctima al hacerse pasar por entidades o personas en las que confía y así, ésta acceda a brindar información importante.

- Riesgos: correos electrónicos, usuarixs y contraseñas de banco, servicios en línea en los cuales te brindan un link para que abras tu sesión y coloques una nueva contraseña.

- Buenas prácticas: desconfía de correos o mensajes que tengan al menos una de las siguientes características: 1) tiene errores ortográficos y/o gramaticales de forma deliberada. 2) el contenido es vago. 3) adjuntan archivos o extensiones extrañas . 4) incluye enlaces extraños que no son HTTTPS. 5) el remitente es desconocido o está mal escrito.
Y por último, consulta siempre con fuentes oficiales.

h. DDOS: El Ataque de Denegación de Servicios (DDoS) consiste en mantener la red ocupada consumiendo el ancho de banda con mensajes constantes que alteran la normalidad de la prestación de servicio.

- Riesgos: acceso a routers, red de computadoras.

- Buenas prácticas: revisar que las páginas web inicien con https. Revisar la velocidad de tu red wifi (https://fast.com/es/)

i. Acoso: Es la práctica de hostigar de manera continua y sistemática a la víctima pese a que ésta ha pedido a la persona agresora que cese su práctica. Para las víctimas es normalmente difícil establecer el límite entre simplemente comentarios o mensajes y acoso.
El acoso puede darse por correo, por mensajes directos o bien comentarios en publicaciones de la víctima en diferentes plataformas de redes sociales.

- Riesgos: abandono de algunas o todas las plataformas. miedo y algunas agresiones pueden llegar a ser físicas.

- Buenas prácticas: bloquear al agresor, no interactuar, documentar y denunciar.

j. Sniffing: el atacante intenta detectar la ruta de comunicación entre la víctima, quien remite, y quien recibe o distribuye la información (empresa que brinda el servicio de internet). El atacante sólo busca encontrar información, no interactuar con ella o modificarla.

- Riesgos: datos personales, rutinas de la persona que está siendo interceptada, lista y contacto de las personas con las que más interactúa, usuarixs y claves de acceso.

- Buenas prácticas: utiliza VPN, buscadores seguros, buenas contraseñas, lenguaje cifrado.

k. Malware: Es un software malicioso que hackers maliciosos instalan en los dispositivos sin que les usuaries se den cuenta. Pueden usarlos para espiar y registrar lo que haces, cambiar funcionalidades, extraer información, etc.

- Riesgos: Información personal, privacidad, acceso a cámara y micrófono, imágenes, páginas webs que visitas, usuarixs y contraseñas de cuentas.

- Buenas prácticas: instalar antivirus y Ccleaner.

# 5. ¿POR QUÉ ES IMPORTANTE HACER UN INVENTARIO DE NUESTRO EQUIPO?

Una forma de identificar tus vulnerabilidades es entendiendo qué buscas proteger. Por eso, es preciso que tengas consciencia de qué tipo de información es la más crítica para tí, en caso de que llegaras a perderla.

AUDITORIA INTERNA

| Dispositivo/ Equipo | Cantidad | No. Indentificación | Información | | | | Observaciones |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |

# 6. FORMAS DE AFRONTAR LAS AMENAZAS Y RIESGOS

Se crearán diferentes escenarios para saber cómo afrontar cada uno.
Para hacerle frente a cada incidente de seguridad, es necesario tener un protocolo o rutas a seguir para no actuar a ciegas y poder detener cada amenaz y riesgos que puedan sufrir nuestra información, instalaciones o nosotrxs mismxs.

## ¿Qué es un incidente de seguridad digital?

Es cuando hay un acceso o intento de acceso, uso, divulgación, modificación o destrucción no autorizada de la información.

Estos incidentes también pueden ser físicas hacia las instalaciones de cada organización/colectivo y al personal.

## PROTOCOLOS A SEGUIR PARA CADA INCIDENTE

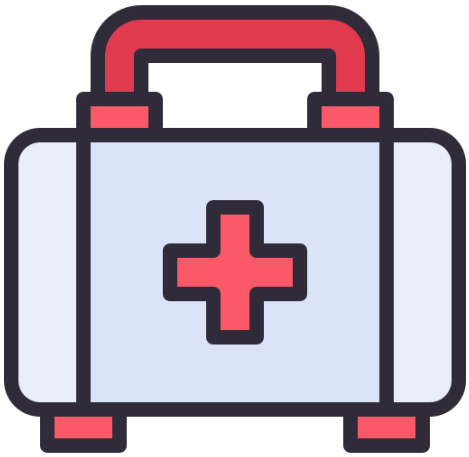
a. Preparación
b. Detección y análisis
c. Contención
d. Erradicación y Recuperación
e. Actividades post incidente

## ACCIONES PREVIO A QUE OCURRA UN INCIDENTE

**Preparación:** prevenir las amenazas. Son todas aquellas actividades que vamos a realizar cuando sabemos que existe una amenaza y así reducir la probabilidad de que ésta ocurra.

- Análisis de riesgos (temas del 1 al 4 de este capítulo).
- Higiene de los dispositivos
- Entrenamiento y capacitaciones

## DURANTE EL INCIDENTE



**Detección y análisis:** En esta etapa buscamos identificar la/s amenazas. Acá nos enfocaremos en los vectores de ataques más comunes. Un vector de ataque es el método que utiliza una amenaza para atacar un sistema.

- Buscamos indicadores de compromisos, es toda aquella información relevante que describe un incidente de ciberseguridad, mediante el análisis de sus patrones y comportamientos (señales que nos indica si ha ocurrido o no un incidente).

- Priorizar. Puede que tengamos más de un incidente de seguridad ocurriendo al mismo tiempo, se debe de tener la capacidad de distinguir cuáles son prioritarios y así ir resolviendo.

- Notificar a las personas encargadas de cada área y organizaciones adecuadas. En el caso de haber un equipo de informática o quienes estén a cargo.

**Contención:** acá lo que queremos es detener la amenaza. Debemos de tener o crear una estrategia para evitar que la amenaza se propague a otros espacios o sistemas, o bien, afecte a otras personas. Se buscará reducir el impacto del incidente y que no afecte la operación normal de otros servicios.
La estrategia que utilicemos dependerá de la amenaza.

Erradicación: luego de contener la amenaza, necesitamos eliminarla y tapar cualquier agujero de seguridad que permitió o causó el incidente.

- Aislar el causante de la amenaza (en caso de que sea un virus, quitar el dispositivo infectado y pasar antivirus a todos los demás dispositivos con los que tuvo contacto).

**Recuperación:** toda vez se haya erradicado la amenaza, volvemos a la normalidad. Regresamos todos los sistemas a su operación normal. Pero es necesario mantener el monitoreo de los sistemas y dispositivos, para estar seguros que la amenaza fue erradicada, porque es probable que no esté erradicada por completo.

Actividades post incidente: por último, vamos a documentar las lecciones aprendidas. Es muy importante esta parte para tener un punto de referencia para incidentes futuros.

- Identificamos puntos débiles que deben ser reforzados, similar a la fase de preparación.
- Auditorias
- Entrenamiento y capacitación del personal y revisión periódica de nuestro equipo.

# BIBLIOGRAFÍA:


1. ¿CÓMO VIAJA INTERNET?

- https://www.youtube.com/watch?v=u1xxZ8r2rRc
- https://www.laquimerafeminista.com/que-es-eso-de-la-internet-feminista/
- https://holistic-security.tacticaltech.org/
- https://www.academia.edu/32199540/Violencia_contra_las_mujeres_en_red_vigilancia_y_el_derecho_a_la_privacidad

2. METADATOS:

- Manual Completo - Gender and Tech Resources (tacticaltech.org)
- Corto animación: ¿Qué son los rastros digitales? https://myshadow.org/es
- https://myshadow.org/es/digital-traces-content-and-metadata
- https://www.pikaramagazine.com/2018/11/defenderlos-territorios-digitales-sin-dejar-huella/
- https://www.mediafire.com/file/3i1hv5f5kgx88n6/Seguridad_Digital_-_Sin_Miedo.pdf/file
- Corto sobre Metadatos: https://www.youtube.com/watch?v=iKccR3E6jn4
- El caso de Malte Spitz: https://www.ted.com/talks/malte_spitz_your_phone_company_is_watching?language=es

3. VIOLENCIA DE GÉNERO EN LÍNEA:

- https://luchadoras.mx/internetfeminista/toolkit/
- https://luchadoras.mx/informe-onu/
- https://luchadoras.mx/internetfeminista/violencia-digital/
- 5 claves para evitar el acoso online: https://www.youtube.com/watch?v=fH5tsWEi4co
- https://securityplanner.consumerreports.org/tool/more-anonymity-security-help
- https://securityplanner.consumerreports.org/tool/how-to-remove-stalkerware
- https://acoso.online/gt/
- Privacidad, mi vida con Google y Facebook.

Qué les estamos permitiendo hacer con nuestro contenido: https://myshadow.org/es/lost-in-small-print

4. CONTRASEÑAS SEGURAS

- https://www.tedic.org/el-caos-de-las-contrasenas/

5. MAPEO DE RIESGOS

- https://eldesarmador.org/07-analisis-de-riesgos.html
- https://riesgosdigitales.asuntosdelsur.org/cursos/modelado-de-riesgos/lessons/introduccion/
- https://www.inredh.org/archivos/pdf/defensores.pdf



# R E C U R S O S

1. NUESTROS METADATOS
- https://play.google.com/store/apps/details?id=apps.syrupy.metadatacleaner&hl=es_GT&gl=US
- https://play.google.com/store/apps/details?id=org.witness.sscphase1&hl=es_GT&gl=US
- https://play.google.com/store/apps/details?id=com.piriform.ccleaner&hl=es_GT&gl=US

2. HERRAMIENTAS PARA NUESTRA COMPUTADORA
- https://datadetoxkit.org/en/alternative-app-centre/

3. PRIMERO AUXILIOS DIGITALES/QUÉ HACER PARA DIFERENTES TIPOS DE VIOLENCIAS
- https://www.digitaldefenders.org/es/kit-de-primeros-auxilios-digitales/
- https://digitalfirstaid.org/es/

4. HERRAMIENTAS PARA TELÉFONO Y ACOSO
- https://securityplanner.consumerreports.org/tool/more-anonymity-security-help
- https://securityplanner.consumerreports.org/tool/how-to-remove-stalkerware
- https://securityplanner.consumerreports.org/tool/get-help-with-online-harassment
- https://freedom.press/training/your-smartphone-and-you-handbook-modern-mobile-maintenance/
- https://securityplanner.consumerreports.org/tool/encrypt-your-android-phone
- https://protege.la/

5. CAJAS DE HERRAMIENTAS
- https://securityinabox.org/es/
- https://iheartmob.org/resources/
- https://www.tallpoppy.com/resources
- https://www.tedic.org/respaldo-de-datos-protegiendo-lo-mas-importante-de-tu-organizacion/
- http://sinmiedo.com.co/
- https://www.accessnow.org/issue/digital-security/page/2/?lang=spanish
- https://seguridadigital.org/
- https://seguridaddigital.github.io/segdig/
- https://derechosdigitales.org/microseguridaddigital/otras_iniciativas.html
- https://farodigital.org/

6. LECTURAS:
- https://internews.org/resource/digital-rights-and-the-arts/
- https://safetag.org/guides/Safetag_full_guide.pdf
- https://safetag.org/guide-builder/
- https://www.civicert.org/
- https://www.rarenet.org/resources/
- https://www.frontlinedefenders.org/en/resource-publication/physical-emotional-and-digital-protection-while-using-home-office-times-covid
- https://www.accessnow.org/issue/digital-security/page/2/?lang=spanish
- https://holistic-security.tacticaltech.org/
- https://derechosdigitales.org/microseguridaddigital/otras_iniciativas.html