45 AÑOS Empoderando a niñas y mujeres
GESMujer

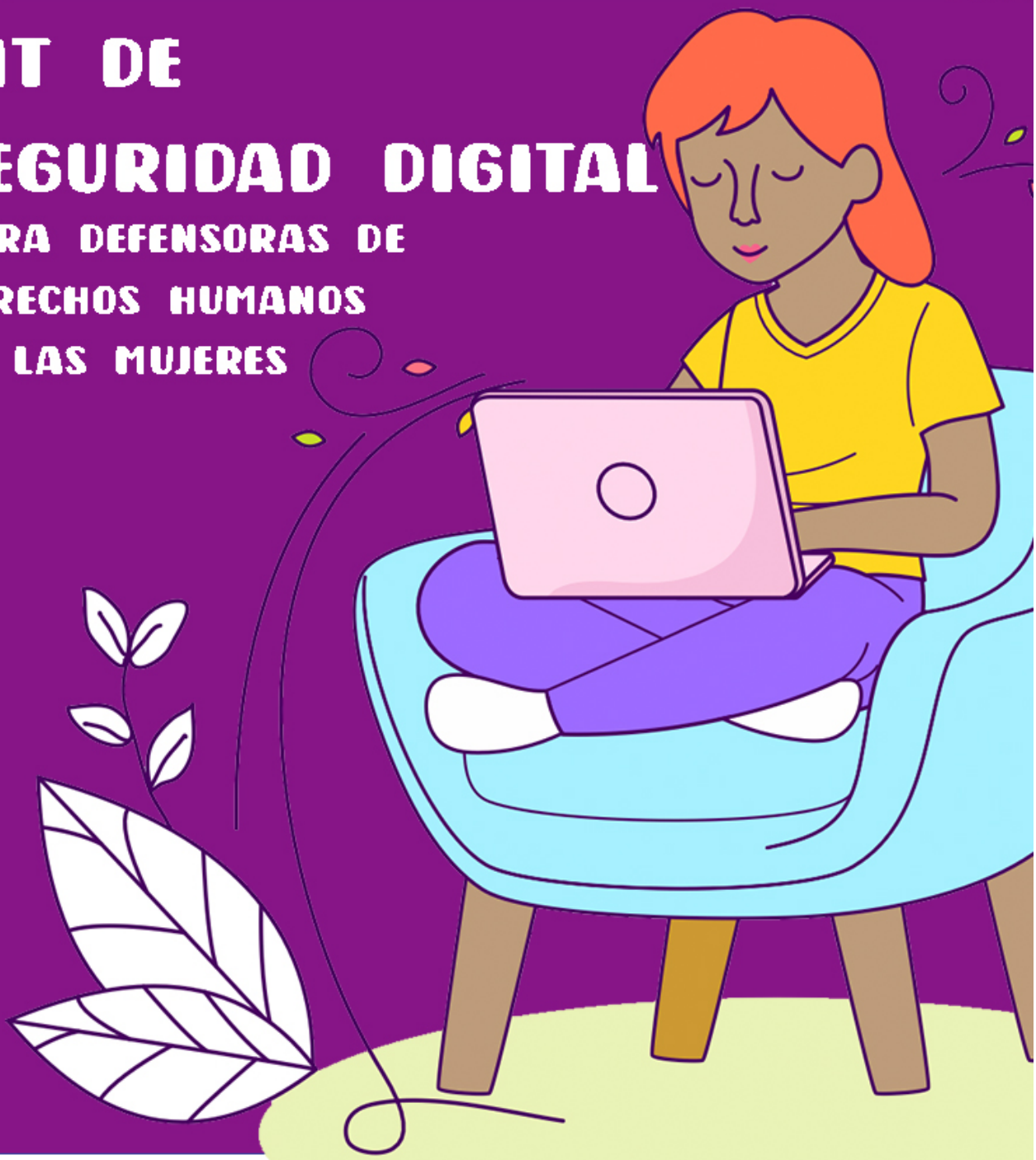
Freedom House

PROGRAMA DE BIENESTAR GESMUJER

El mundo que soñamos

KIT DE SEGURIDAD DIGITAL

PARA DEFENSORAS DE DERECHOS HUMANOS DE LAS MUJERES



¡La seguridad digital también es parte del autocuidado!

www.gesmujer.org

45 AÑOS Empoderando a niñas y mujeres
GESMujer

Freedom House

PROGRAMA DE BIENESTAR GESMUJER

El mundo que soñamos

KIT DE SEGURIDAD DIGITAL

PARA DEFENSORAS DE DERECHOS HUMANOS DE LAS MUJERES

El Grupo de estudios sobre la mujer Rosario Castellanos A.C., pone a disposición de las defensoras de derechos humanos y toda persona interesada un Kit de seguridad digital, fue elaborado como parte del proyecto: Programa de bienestar de autocuidados GESMujer "El mundo que soñamos", financiado por la Fundación Freedom House; su contenido es responsabilidad del Grupo de estudios sobre la mujer Rosario Castellanos y no necesariamente refleja el punto de vista de Freedom House.

Las herramientas que contiene el Kit de seguridad digital, fueron co-creadas por defensoras de derechos humanos de diferentes organizaciones y colectivas a través de sesiones de talleres dentro y fuera de GESMujer: CANICA de Oaxaca, A.C., Red de abogadas indígenas en Oaxaca, Red de Periodistas Oaxaqueñas y Sikanda A.C.

Coordinadora:
María del Rosario Martínez Miguel.

Elaboró:
Soledad Venegas Nava.

Elementos de diseño:
Galindo David Fercano Velasco.

Junio 2023.

Grupo de estudios sobre la mujer Rosario Castellanos A.C.
Tercera privada de Guadalupe Victoria No. 107
Colonia Libertad, Oaxaca, C.P. 68090.
Teléfono: (951) 5166810
Email: contacto@gesmujer.org
www.gesmujer.org

¡La seguridad digital también es parte del autocuidado!

Quiero saber más...

www.gesmujer.org/autocuidado

45 AÑOS Empoderando a niñas y mujeres

GESMujer

Freedom House

PROGRAMA DE BIENESTAR GESMUJER

El mundo que soñamos

KIT DE SEGURIDAD DIGITAL

PARA DEFENSORAS DE DERECHOS HUMANOS

VIOLENCIA DIGITAL

La violencia digital contra defensoras de derechos humanos se refiere a los actos de violencia, acoso, intimidación y abuso que ocurren en el ámbito digital dirigidos específicamente hacia las mujeres defensoras de derechos humanos, activistas y líderes de movimientos sociales. Este tipo de violencia se manifiesta a través de diversas formas, como el acoso en línea, la difamación, la discriminación, la publicación no consensuada de información personal, la divulgación de imágenes íntimas sin consentimiento (conocido como porno venganza"), el hackeo de cuentas, la suplantación de identidad y la difusión de rumores y mentiras con el objetivo de desacreditar y socavar la labor de las defensoras y el movimiento feminista.

¿Cómo afecta a las defensoras?

La violencia digital contra defensoras tiene como objetivo silenciar y desalentar a las mujeres que se expresan en línea, buscan el cambio social y defienden los derechos humanos. Estos actos pueden tener un impacto significativo en la vida personal y profesional de las defensoras, generando estrés, ansiedad, miedo e incluso llevándolas a abandonar su trabajo y activismo.

¿Qué puedo hacer para prevenir?

- Conciencia sobre la violencia digital. Protege tu información personal.
- Limita la cantidad de información personal que compartes.
- Contraseñas seguras y autenticación de dos factores.
- Bloquea y denuncia: Aprende cómo bloquear y denunciar a usuarios que te estén acosando o difundiendo contenido ofensivo.
- Mantén la evidencia: Si experimentas violencia digital, guarda capturas de pantalla, correos electrónicos, mensajes o cualquier otra prueba que puedas recopilar.
- Busca apoyo: No enfrentes la violencia digital sola. Busca el apoyo de personas de confianza, como amistades, familiares o colegas.
- Denuncia ante las autoridades.

Fuente: Guía ciberseguras
https://socialtic.org/wp-content/uploads/2017/12/GuiaEstrategias

Quiero saber más...

¡La seguridad digital también es parte del autocuidado!

www.gesmujer.org/autocuidado

45 AÑOS Empoderando a niñas y mujeres
GESMujer

Freedom House

PROGRAMA DE BIENESTAR GESMUJER

El mundo que soñamos

KIT DE SEGURIDAD DIGITAL
PARA DEFENSORAS DE DERECHOS HUMANOS

LEY OLIMPIA.. LA DENUNCIA.

Recuerda que el autocuidado es fundamental. Si sientes que tu seguridad está en riesgo, considera tomar un descanso de las redes sociales o buscar asesoramiento profesional para manejar el impacto emocional de la violencia digital.

También te recomendamos que actives tu red de apoyo, procura recibir acompañamiento psicológico y legal con perspectiva de género.

Fuente: Ley Olimpia http://ordenjuridico.gob.mx/violenciagenero/LEY%20OLIMPIA.pdf

La Ley Olimpia

Reforma
Artículos
249 y 250

"Delitos contra la intimidad sexual"

La Ley Olimpia, publicada en el Periódico Oficial el 24 de agosto de 2019. Es la reforma al Código Penal de la Ley General del Estado de Oaxaca. La Ley sanciona con hasta ocho años de cárcel a aquella persona que "por cualquier medio divulgue, comparta, distribuya, publique y/o solicite imágenes, audios o videos de una persona desnuda parcial o totalmente de contenido íntimo, erótico o sexual, ya sea impreso, grabado o digital, sin el consentimiento de la víctima".

La Denuncia la puedes hacer en la Fiscalía y de manera virtual en la polícia cibernetica de manera anónima en el siguiente link: https://sspo.gob.mx/?page_id=38

¿Cómo hacer una denuncia por violencia digital?

- Realizar un registro de los incidentes o de los ataques en un documento.
- Crear captura de pantalla, guardar los enlaces y/o imágenes, recopilar información sobre las personas/agresor(es).
- Crear una bitácora, es decir una documentación (hojas de cálculo o documento de texto) con información relevante como: fecha, hora, tipo de ataque/incidente, plataforma, url, captura de como pantalla y contenido. Puede ser narrado/escrito como testimonio de los sucesos.
- Registrar incluso con notas sobre el nivel de riesgo que se percibe y acciones de seguimiento.
- Se recomienda a compañarse en todo momento con personas aliadas de la red de apoyo, abogadas con perspectia de género.
- Una vez todo el registro poder acudir a la fiscalia y hacer la denuncia y darle seguimiento.

Fuente: Guía ciberseguras
https://socialtic.org/wp-content/uploads/2017/12/GuiaEstrategias

Quiero saber más...

¡La seguridad digital también depende de ti!

www.gesmujer.org/autocuidado

45 AÑOS Empoderando a niñas y mujeres
GESMujer

Freedom House

PROGRAMA DE BIENESTAR GESMUJER

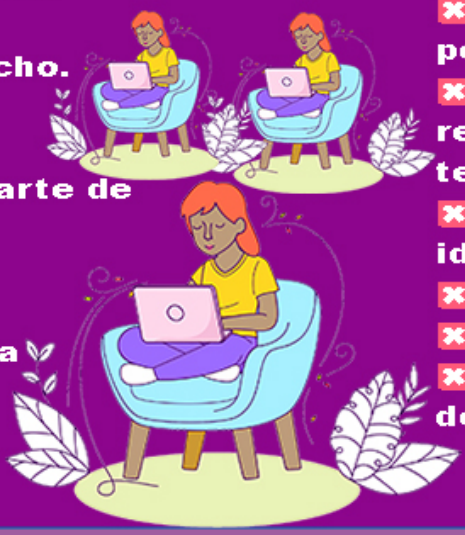
El mundo que soñamos

KIT DE SEGURIDAD DIGITAL

PARA DEFENSORAS DE DERECHOS HUMANOS

TIPOLOGÍA DE LA VIOLENCIA DIGITAL CONTRA LAS MUJERES

- Acceso o control no autorizado.
- Monitoreo y acecho.
- Amenazas.
- Desprestigio.
- Omisiones por parte de actores con poder regulatorio.
- Control y manicupalción de la información.
- Expresiones discriminatorias.



- Difusión de información personal o íntima.
- Abuso sexual relacionado con la tecnología.
- Suplantación y robo de identidad.
- Acoso.
- Extorsión.
- Afectaciones a canales de expresión.

Ten en cuenta que...

Lo que compartimos, tanto en redes sociales y plataformas digitales llevan una carga de información privada, que de forma inconsciente, muchas veces, no tenemos cuidado de la información que publicamos y esa información, es un medio ideal para perpetuar la violencia digital por personas con un objetivo claro, "hacer daño".

Otro punto que considerar es, la información en dispositivos, no es segura, está expuesta a robo, extravío o descomposturas de equipos, el peligro, está ahí, a la mano de posibles personas agresoras, quienes te vigilan, controlan o monitorean, todo lo que haces dentro y fuera de Internet,

Aquí encuentras la guia completa.
https://genderit.org/es/resources/13-formas-de-agresion-en-linea-contra-las-mujeres

Quiero saber más...

¡La seguridad digital también depende de ti!

www.gesmujer.org/autocuidado

45 AÑOS Empoderando a niñas y mujeres
GESMujer

Freedom House

PROGRAMA DE BIENESTAR GESMUJER

El mundo que soñamos

KIT DE SEGURIDAD DIGITAL
PARA DEFENSORAS DE DERECHOS HUMANOS

TIPOLOGÍA DE LA VIOLENCIA DIGITAL

RECOMENDACIONES

La tipología de la violencia digital nos permite identificar los peligros existentes, como Defensoras de derechos humanos, conocer esta tipología ayuda a tener un panorama con mayor claridad, del tipo de violencia que sufre una persona y qué hacer para ayudarle.

Te recomendamos darle mantenimiento a los dispositivos limpieza periódica, guarda información importante en Bóveda Digital, como contraseñas de tus cuentas personales, bancos, plataformas, correos y sistemas de comunicación y diversión.
Recomendamos uso de antivirus, invierte en original un pirata no es seguro que te proteja, al contrario te vulnera tu equipo e información.
Las contraseñas son solo tuyas, el acceso a las plataformas y redes sociales, son tu extensión de tu vida, no puedes dar el acceso a otra persona.
Utiliza métodos de doble factor para recibir notificaciones ante cualquier amenaza de hackeo o violación a tu seguridad digital.

Aquí encuentras la guía completa
https://genderit.org/es/resources/13-formas-de-agresion-en-linea-contra-las-mujeres

Navegar por internet de forma segura

Te recomendamos navegar de forma segura, eliminando los datos que se guardan en los navegadores, sobre todo, si son equipos públicos o colectivos. Borra el historial del navegador, no guardes contraseñas menos si no es tu equipo, instala un bloqueador de anuncios o software malisioso, instala antivirus en tus dispositivos, ayduan a biquear ataques o software daniño como spam, troyanos, fishing, spyware, entre otros.
Puedes usar para navegar el modo INCÓGNITO, o utiliza DuckDuckGo.
Otro tip, es la información que guardas en discos duros, o en la nube, ponle clave de acceso, ya que por descuido puede ser vulnerada, lo mismo para entrar a carpetas, archivos computadoras y teléfonos celulares y tu WhatsApp.

Quiero saber más...

¡La seguridad digital también depende de ti!

www.gesmujer.org/autocuidado

PROGRAMA DE BIENESTAR GESMUJER

El mundo que soñamos

KIT DE SEGURIDAD DIGITAL

PARA DEFENSORAS DE DERECHOS HUMANOS

USO DE LA CONTRASEÑA 1

¿Qué es?

Una contraseña es una combinación de letras, números y símbolos que se utiliza para proteger la seguridad y la privacidad.

Estas contraseñas deben ser robustas y difíciles de adivinar para evitar posibles ataques cibernéticos o violaciones de la información.

¿Cómo puedo utilizarla?

Recuerda que la seguridad de la contraseña es solo una medida de protección. También es importante utilizar medidas adicionales de seguridad, como la autenticación de dos factores, mantener tus dispositivos actualizados y estar atenta a posibles intentos de phishing o ataques cibernéticos.

¿Cómo mejorar su uso?

- **Longitud**: Utiliza contraseñas que tengan al menos 8 caracteres. Cuanto más larga sea la contraseña, más difícil será de romper.
- **Complejidad**: Combina letras (mayúsculas y minúsculas), números y símbolos especiales. Utiliza una combinación de caracteres que no sea fácilmente adivinable.
- **Evita información personal:** No utilices información personal como tu nombre, fecha de nacimiento o palabras comunes relacionadas contigo. Estas son fáciles de adivinar o descubrir mediante ataques de fuerza bruta o ingeniería social.
- **Evita secuencias o patrones obvios:** No utilices secuencias numéricas como "123456" o patrones de teclado como "qwerty". Estas son contraseñas débiles y fáciles de adivinar.
- **No reutilices contraseñas:** Utiliza contraseñas únicas para cada cuenta o plataforma que utilices. Si reutilizas contraseñas y una cuenta se ve comprometida, todas las demás también estarán en riesgo.
- **Actualiza regularmente:** Cambia tus contraseñas periódicamente, al menos cada 3-6 meses, para mantener la seguridad de tus cuentas.

Fuente: Ciberseguras. "Violencia contra las mujeres + seguridad", 2027..
Link: https://socialtic.org/wp-content/uploads/2017/12/GuiaEstrategias_Ciberseguras.pdf

Quiero saber más...

¡La seguridad digital también es parte del autocuidado!

www.gesmujer.org/autocuidado

45 AÑOS Empoderando a niñas y mujeres

GESMujer

Freedom House

PROGRAMA DE BIENESTAR GESMUJER

El mundo que soñamos

KIT DE SEGURIDAD DIGITAL

PARA DEFENSORAS DE DERECHOS HUMANOS

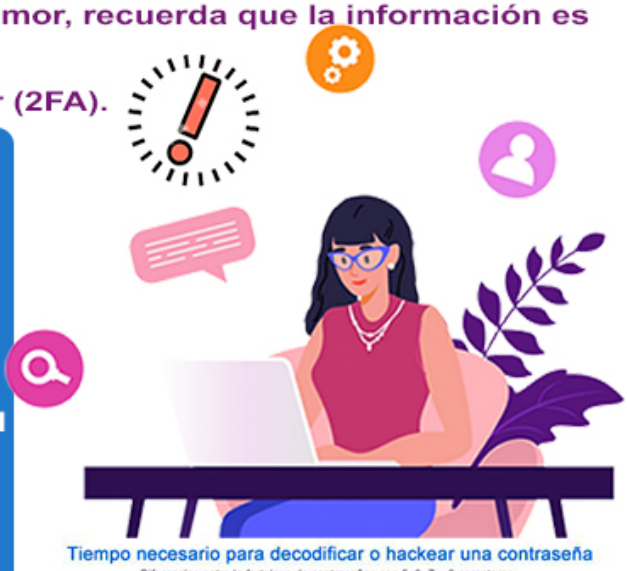
CONTRASEÑA, TE RECOMENDAMOS...

- Existen sitios web que te piden contraseñas de ocho caracteres, sin embargo te recomendamos que elijas al menos 15 o una frase que logres combinar con letras, números y símbolos.
- Evita que la contraseña esté relacionada con tu información personal, como tu nombre apellido o fecha de nacimiento.
- Utiliza números, símbolos y letras mayúsculas y minúsculas en orden aleatorio.
- No utilizar secuencias de letras o números.
- No usar la misma contraseña para varias cuentas.
- No compartir tus contraseñas, ni por amor, recuerda que la información es tuya y puedes ser vulnerada.
- Utiliza el autentificador de doble factor (2FA).

Puedes usar un software para generar contraseñas aleatorias, te recomendamos: Https://passwordsgenerator.net/

Guarda tus contraseñas, hay opciones gratuitas para gestionar contraseñas.

Véase el llavero de icloud para iphone o el de google en android.
También puedes usar una bóveda digital como KeePass o 1Password, las consigues en tu tienda de aplicaciones de tus dispositivos móviles, y te ayudan incluso en tus equipos de cómputo.
Estos son gestores seguros para las Contraseñas y que perfectamente pueden servir.



Tiempo necesario para decodificar o hackear una contraseña

Diferencias entre la fortaleza de contraseñas con 5, 6, 7 u 8 caracteres.
Usando números, letras, letras con mayúsculas y minúsculas, combinando lo anterior y por ultimo agregando símbolos.

38172 Al instante	manue Al instante	MaNue 4 segundos	MaN72 9 segundos	MaN7* 1 minuto
381723 Al instante	manuel 3 segundos	MaNuel 3 minutos	MaN723 9 minutos	MaN72* 2 horas
3817239 Al instante	manuela 1 minuto	MaNuelA 3 horas	MaN723e 10 horas	MaN72*@ 8 dias
38172395 10 segundos	manuelas 35 minutos	MaNuelAB 6 dias	MaN723eB 25 dias	MaN72*@& 2 años

norfipc.com

Fuente: Ciberseguras. "Violencia contra las mujeres + seguridad", 2027..
Link: https://socialtic.org/wp-content/uploads/2017/12/GuiaEstrategias_Ciberseguras.pdf

QUIERO SABER MÁS...

¡LA SEGURIDAD DIGITAL TAMBIÉN ES PARTE DEL AUTOCUIDADO!

www.gesmujer.org/autocuidado

45 AÑOS Empoderando a niñas y mujeres
GESMujer

Freedom House

PROGRAMA DE BIENESTAR GESMUJER

El mundo que soñamos

KIT DE SEGURIDAD DIGITAL
PARA DEFENSORAS DE DERECHOS HUMANOS

GHOSTING

El término "ghosting" se utiliza comúnmente en el contexto de las relaciones personales, de pareja o en grupos y colectivas, y se refiere a cuando una persona termina abruptamente una relación sin ninguna explicación o sin dar señales claras de su intención de terminar, aplicando la "Ley del hielo", dedicandose solo a observar y no dar explicaciones, afectando emocionalmente a las personas.

TiPOS de GhOSTiNG

Minighosting: Deja de contestar algunos mensajes o los contesta mucho tiempo después.

Ghosting pasivo: sigue reaccionando a las historias en las redes sociales o dando like a las publicaciones.

Ghosting intermitente: cuando la persona desaparece, y semanas o meses después reaparece reaccionando a publicaciones o historias.

EL Ghosting se ve así:

Te ignora durante unos días y luego te habla como si nada hubiera pasado.

Un día te responde normal y al otro de modo cortante.

La persona desaparece sin dar explicación.

Te deja en visto o ignora.

Puede bloquearte de las redes sociales.

No contesta tus mensajes o llamadas.

Fuente: Pinzón Salcedo E. "El Ghosting como fenómeno de ruptura en las relaciones de pareja", 2019. Consultado en http://hdl.handle.net/11371/2304

QUIERO SABER MÁS...

¡LA SEGURIDAD DIGITAL TAMBIÉN DEPENDE DE TI!

www.gesmujer.org/autocuidado

45 AÑOS Empoderando a niñas y mujeres
GESMujer

Freedom House

PROGRAMA DE BIENESTAR GESMUJER

El mundo que soñamos

KIT DE SEGURIDAD DIGITAL
PARA DEFENSORAS DE DERECHOS HUMANOS

ANTE EL GHOSTING, TE RECOMENDAMOS:

ESTARTEGÍAS DE AUTOCUIDADO

1. **Mantén la calma y respétate a ti misma:** Si has sido ghosteada, es importante mantener la calma y no dejarse llevar por la frustración o la angustia. Reconoce que mereces ser tratada con respeto y no te mereces ser ignorada sin explicación.

2. **Dale tiempo a la situación:** Aunque pueda ser difícil, dale tiempo a la situación y evita bombardear a la persona que te ghosteó con mensajes o intentos desesperados de contacto.

3. **Enfócate en tu bienestar:** Concéntrate en cuidarte a ti misma y en tu bienestar emocional.

4. **Busca apoyo:** No enfrentes el ghosting sola. Busca apoyo emocional en amistades cercanas, familiares o incluso en grupos de apoyo en línea. Compartir tus sentimientos y hablar sobre la experiencia puede ayudarte a procesar lo sucedido.

5. **Dedica tiempo a actividades que disfrutes:** Mantén una rutina saludable y cultiva relaciones positivas en tu vida.

6. **Dale espacio:** Es posible que la otra persona necesite espacio o esté pasando por algo personal que la haya llevado a tomar esa decisión.

Fuente: Pinzón Salcedo E. "El Ghosting como fenómeno de ruptura en las relaciones de pareja", 2019. Consultado en http://hdl.handle.net/11371/2304

QUIERO SABER MÁS...

¡LA SEGURIDAD DIGITAL TAMBIÉN DEPENDE DE TI!

www.gesmujer.org/autocuidado

45 AÑOS Empoderando a niñas y mujeres

GESMujer

Freedom House

PROGRAMA DE BIENESTAR GESMUJER

El mundo que soñamos

KIT DE SEGURIDAD DIGITAL

PARA DEFENSORAS DE DERECHOS HUMANOS

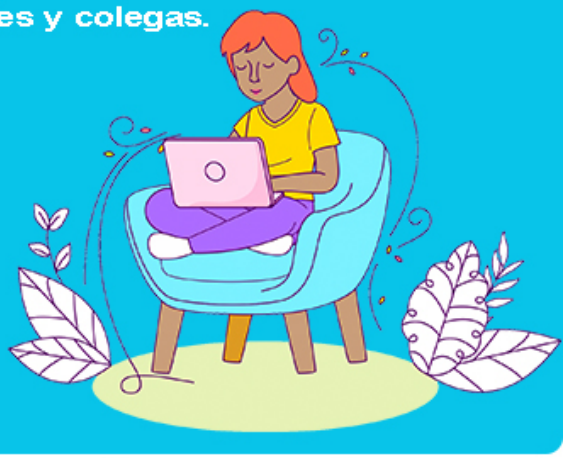
LA GEOLOCALIZACIÓN

La violencia con la geolocalización se refiere a la utilización de la información de ubicación de una persona, obtenida a través de servicios de geolocalización en dispositivos móviles o mediante el seguimiento en línea, para amenazar, acosar o atacar a defensoras de derechos humanos y activistas.

Esta forma de violencia digital puede tener un impacto significativo en la seguridad y el bienestar de las defensoras, ya que amenaza su privacidad, su integridad física y emocional, y puede generar un clima de temor y desconfianza. También limita la capacidad de las defensoras para llevar a cabo su trabajo y dificulta la participación activa en movimientos y protestas sociales.

¿Cómo afecta?

Es importante destacar que la violencia con la geolocalización también puede tener consecuencias indirectas al afectar la seguridad de las personas que rodean a la defensora, como familiares, amistades y colegas.



¿Cómo puedo protegerme?

Para hacer frente a la violencia con la geolocalización, es fundamental tomar medidas de seguridad digital, como desactivar los servicios de geolocalización en las aplicaciones y configuraciones del dispositivo móvil, revisar y ajustar las opciones de privacidad en las redes sociales y evitar compartir información de ubicación sensible en plataformas públicas. Además, es importante recibir capacitación en seguridad digital y contar con redes de apoyo y asesoramiento para responder adecuadamente en caso de amenazas o ataques.

Fuente: Genderit.org. https://genderit.org/es/articles/defender-los-territorios-digitales-sin-dejar-huella

Quiero saber más...

¡La seguridad digital también depende de ti!

www.gesmujer.org/autocuidado

PROGRAMA DE BIENESTAR GESMUJER

El mundo que soñamos

KIT DE SEGURIDAD DIGITAL
PARA DEFENSORAS DE DERECHOS HUMANOS

GEOLOCALIZACIÓN-RECOMENDACIONES

Configurar la geolocalización y mantener la privacidad de la información puede ayudar a proteger la seguridad y evitar exponerse innecesariamente. Aquí algunos consejos:

Configuración de dispositivos

En los dispositivos iOS (iPhone/iPad): Ve a "Ajustes" > "Privacidad" > "Servicios de ubicación". Aquí, puedes desactivar la geolocalización globalmente o administrarla por aplicación.

En dispositivos Android: Ve a "Ajustes" > "Ubicación" o "Privacidad y seguridad" > "Ubicación". Aquí, puedes desactivar la geolocalización globalmente o ajustarla por aplicación.

Configuración en Redes sociales

Revisa la configuración de privacidad de cada red social que utilices. Puedes encontrar opciones para desactivar la geolocalización en publicaciones, etiquetas de ubicación y compartir tu ubicación en tiempo real.

Considera desactivar la opción de "ubicaciones en segundo plano" para las aplicaciones de redes sociales, lo cual limitará la capacidad de la aplicación de rastrear tu ubicación constantemente.

Mensajería instantánea

En aplicaciones de mensajería instantánea como WhatsApp o Telegram, revisa las opciones de privacidad y desactiva la función de compartir tu ubicación en tiempo real.

Wifi y Bluetooth

Desactiva la función de Wi-Fi y Bluetooth cuando no los estés utilizando. Esto puede ayudar a evitar que terceros rastreen tu ubicación a través de redes inalámbricas o dispositivos cercanos.

Fuente: Genderit.org. https://genderit.org/es/articles/defender-los-territorios-digitales-sin-dejar-huella

Quiero saber más...

¡La seguridad digital también depende de ti!

www.gesmujer.org/autocuidado

45 AÑOS Empoderando a niñas y mujeres
GESMujer

Freedom House

PROGRAMA DE BIENESTAR GESMUJER

El mundo que soñamos

KIT DE SEGURIDAD DIGITAL
PARA DEFENSORAS DE DERECHOS HUMANOS

DOXING

El Doxing es una forma de violencia en línea que implica la divulgación maliciosa de información personal y privada con la intención de causar daño, acosar o intimidar a las defensoras. Esta práctica puede exponer datos sensibles como direcciones, números de teléfono, información familiar, lugares de trabajo y otra información personal sin el consentimiento de la persona afectada.

Fuente: 13 formas de violencia digital contra las mujeres.
https://luchadoras.mx/internetfeminista/13-formas-violencia-linea-las-mujeres/

CONSECUENCIAS

El doxing puede tener consecuencias graves para las defensoras, ya que puede poner en peligro su seguridad física, exponerlas a acosadores o permitir que sus datos personales sean utilizados de manera perjudicial.
También puede afectar su capacidad para llevar a cabo su trabajo de defensa de derechos y generar un ambiente de miedo e intimidación.

Medidas de seguridad

- Configuración de privacidad: Revisa y ajusta cuidadosamente la configuración de privacidad en tus cuentas en línea y en las redes sociales. Limita la cantidad de información personal visible para el público y controla quién puede ver y acceder a tu perfil y contenido.
- Minimiza la información personal en línea: Evita publicar datos sensibles como tu dirección, número de teléfono u otra información personal que pueda ser utilizada en tu contra.
- Monitoreo de actividad en línea: Si notas actividad sospechosa o inusual, como cambios no autorizados en tu perfil o inicio de sesión desde ubicaciones desconocidas, toma medidas inmediatas para asegurar tus cuentas y notificar a la plataforma.
- Educación y concientización: Mantente informada sobre las prácticas de seguridad en línea y las tácticas utilizadas por los doxers para proteger tu privacidad y seguridad en línea.
- Denuncia y busca apoyo: Si eres víctima de doxing, denuncia el incidente a las autoridades pertinentes y a la plataforma en la que se llevó a cabo.

Quiero saber más...

¡La seguridad digital también es parte del autocuidado!
www.gesmujer.org/autocuidado

45 AÑOS Empoderando a niñas y mujeres
GESMujer

Freedom House

PROGRAMA DE BIENESTAR GESMUJER

El mundo que soñamos

KIT DE SEGURIDAD DIGITAL
PARA DEFENSORAS DE DERECHOS HUMANOS

DOXING
Medidas de seguridad

Configuración de privacidad: Revisa y ajusta cuidadosamente la configuración de privacidad en tus cuentas en línea y en las redes sociales. Limita la cantidad de información personal visible para el público y controla quién puede ver y acceder a tu perfil y contenido.

Minimiza la información personal en línea: Evita publicar datos sensibles como tu dirección, número de teléfono u otra información personal que pueda ser utilizada en tu contra.

Monitoreo de actividad en línea: Si notas actividad sospechosa o inusual, como cambios no autorizados en tu perfil o inicio de sesión desde ubicaciones desconocidas, toma medidas inmediatas para asegurar tus cuentas y notificar a la plataforma.

Educación y concientización: Mantente informada sobre las prácticas de seguridad en línea y las tácticas utilizadas por los doxers para proteger tu privacidad y seguridad en línea.

Denuncia y busca apoyo: Si eres víctima de doxing, denuncia el incidente a las autoridades pertinentes y a la plataforma en la que se llevó a cabo.

Fuente: 13 formas de violencia digital contra las mujeres.
https://luchadoras.mx/internetfeminista/13-formas-violencia-linea-las-mujeres/
Imagén. https://www.freepik.es/vector-gratis/ilustracion-abstracta-doxing_20892037

Quiero saber más...

¡La seguridad digital también es parte del autocuidado!
www.gesmujer.org/autocuidado

45 AÑOS Empoderando a niñas y mujeres
GESMujer

Freedom House

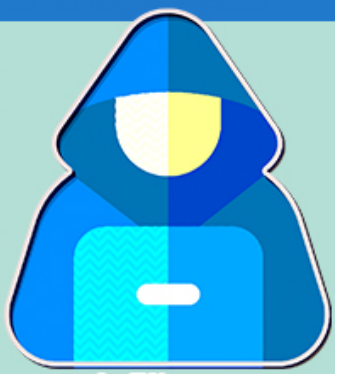
PROGRAMA DE BIENESTAR GESMUJER

El mundo que soñamos

KIT DE SEGURIDAD DIGITAL
PARA DEFENSORAS DE DERECHOS HUMANOS

SUPLANTACIÓN DE IDENTIDAD

Se refiere al uso no autorizado de la identidad de una defensora en línea, ya sea a través de la creación de perfiles falsos o el uso indebido de sus cuentas en redes sociales. Esto puede ser utilizado para difamar, enviar mensajes perjudiciales o realizar actividades ilegales en nombre de la defensora.



La suplantación de identidad también puede ser utilizada para infiltrarse en redes y comunidades en línea donde las defensoras están activas, con el objetivo de obtener información sensible o socavar la confianza en la defensora y sus compañeras de lucha.

Para hacer frente a la suplantación de identidad, es importante tomar precauciones como mantener seguras las contraseñas de tus cuentas en línea, utilizar medidas de autenticación de dos factores, estar atenta a cualquier actividad sospechosa en tus cuentas y reportar de inmediato cualquier perfil falso o suplantación de identidad que identifiques.

Si sospechas o descubres que alguien está suplantando tu identidad en línea o la de otra persona, es importante tomar medidas para denunciarlo. Aquí hay algunos pasos que puedes seguir:

- Documentar la evidencia
- Denunciar en la plataforma en línea
- Dar aaviso a contactos y seguidor@s
- Realizar la denuncia ante las autoridades
- Actualiza y cambia contraseñas

Fuente: Guía ciberseguridad
https://www.gob.mx/cms/uploads/attachment/file/555226/Gui_a_de_Ciberseguridad_SCT_VF.pdf:

Quiero saber más...

¡La seguridad digital también depende de ti!

www.gesmujer.org/autocuidado

45 AÑOS Empoderando a niñas y mujeres
GESMujer

Freedom House

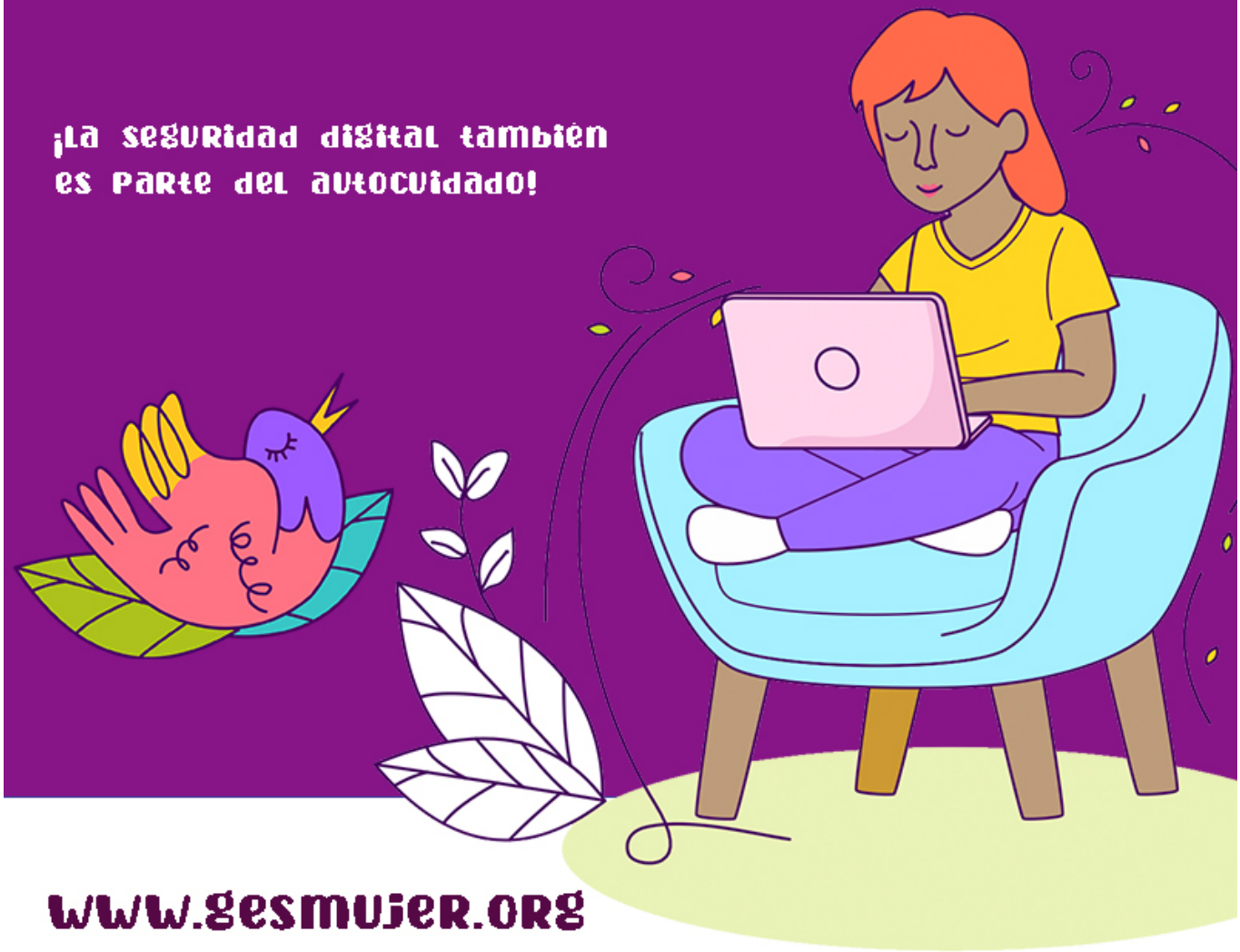
PROGRAMA DE BIENESTAR GESMUJER

El mundo que soñamos

Con la llegada de nuevas tecnologías cada día, es importante estar alerta para identificar las violencias contra las mujeres y cuerpos feminizados, por ello estar capacitándose sobre el uso y nuevas herramientas y estrategias de autocuidado digital es una buena forma de transitar en el ciberespacio de manera segura.

No estás sola, muchas mujeres ciberfeministas también están encontrando y compartiendo mecanismos y herramientas para fortalecer la seguridad digital.

Agradecemos que tú también compartas este Kit de seguridad digital para defensoras de derechos humanos de las mujeres entre las colectivas y tu círculo cercano, es de gran ayuda para minimizar los riesgos de la violencia digital, recuerda que el ciberespacio también es nuestro.



www.gesmujer.org