



Guía de
SEGURIDAD DIGITAL
PARA MUJERES POLÍTICAS



Guía de
SEGURIDAD DIGITAL
PARA MUJERES POLÍTICAS



Equipo investigador:

Equipo S.O.S Digital:

- Carolina Pérez
- Nayarani Rivera
- Eloisa Larrea
- Lu An Mendez
- Alejandra Torrez

Equipo Oxfam:

Lourdes Montero Justiniano, Directora País Oxfam en Bolivia
Lisbeth España, Coordinadora de Programas
Paola Carballo Cadima, Oficial del Proyecto

Diseño gráfico:

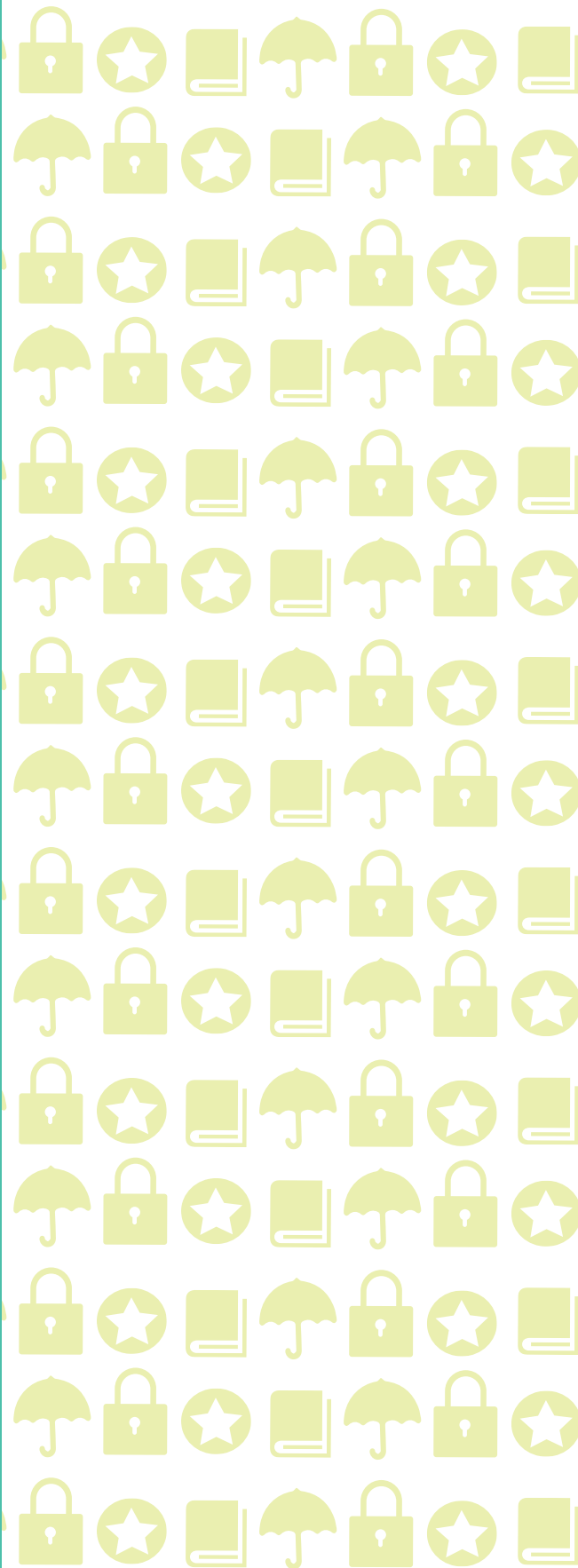
Bien Común Estudio

Edición:

Cecilia Terrazas

Este material es posible gracias al proyecto Recipe cofinanciado por la Unión Europea. Su contenido es responsabilidad exclusiva de los autores y socios en la ejecución y no reflejan necesariamente las opiniones de la Unión Europea.

Bolivia, 2025



contenido

Presentación	5
1. ANTECEDENTES	7
1.1. Objetivos de la guía	8
1.1.2. Objetivos específicos	8
1.1.3. ¿A quién está dirigida esta guía?	9
1.1.4. Algunas consideraciones importantes	9
2. ¿QUÉ ES EL ACOSO Y VIOLENCIA POLÍTICA FACILITADA POR LA TECNOLOGÍA?	10
2.1. ¿Cuáles son los efectos del acoso y violencia política facilitada por la tecnología?	11
2.2. ¿Cuál es el objetivo del acoso y violencia política facilitada por la tecnología?	12
2.3. ¿Cuáles son las formas de violencia más comunes que enfrentan las mujeres políticas en periodos electorales?	13
3. SEGURIDAD DIGITAL PARA MUJERES POLÍTICAS EN EL CONTEXTO ELECTORAL	17
3.1. Seguridad en tu celular y computadora.	17
3.2. ¿Qué es una contraseña segura y por qué es importante no compartirla con nadie?	19
3.3. ¿Qué es un gestor de contraseña y cómo me puede ayudar?	20



3.4.	La importancia de la verificación en dos pasos (2FA)	21
3.5.	¿Qué es el phishing o el engaño digital y por qué debo protegerme de él?	23
3.6.	¿Qué es el cifrado en las aplicaciones de comunicaciones?	26
3.7.	¿Cómo proteger tu privacidad en línea siendo una mujer en la política?	30
3.8	¿Cómo encontrar y/o borrar la información de un celular Android perdido?	34
4.	¿CÓMO RESPONDO A LOS ATAQUES DE ACOSO Y VIOLENCIA POLÍTICA FACILITADOS POR LA TECNOLOGÍA?	36
4.1.	Ley 243 contra el acoso y violencia política hacia las mujeres	36
4.2.	Figuras penales y reporte en plataformas contra la violencia de género facilitada por la tecnología, por tipo de violencia.	37
4.3.	Algunas formas de respuesta auto gestionadas para enfrentar el acoso y violencia política facilitada por la tecnología	46
5.	RECURSOS ÚTILES	48
5.1.	¿Cómo activar la verificación en dos pasos?	48
5.2.	Configuraciones de privacidad en Facebook	58
5.2.1.	Configuraciones de privacidad en Instagram	60
5.2.2.	Configuraciones de privacidad en Tik Tok	62
5.3.	Documentación de agresiones en contextos de violencia de género facilitada por la tecnología en procesos electorales	64
	Modelo de ejemplo para la documentación	65



Presentación

En un mundo cada vez más conectado, las mujeres en política enfrentan una paradoja: mientras las tecnologías amplifican sus voces, también las exponen a riesgos digitales sin precedentes. **El acoso en línea, el hackeo de cuentas, la vigilancia ilegal y las campañas de desinformación** se han convertido en herramientas frecuentes para intimidar, silenciar y socavar su liderazgo. A nivel internacional, según un informe de la Unión Interparlamentaria (UIP, 2023), el 85% de las parlamentarias encuestadas ha sufrido acoso psicológico en redes sociales, y una de cada tres ha considerado abandonar la política debido a amenazas digitales.

En Bolivia, donde la participación política de las mujeres ha crecido significativamente en la última década –con una representación del 55% en la Cámara de Senadores y 47% en la Cámara de Diputados–, persiste una brecha entre avances formales y protección real. El acoso y la violencia política en las redes sociales ha ganado terreno y fuerza contra las mujeres políticas, limitando su ejercicio pleno de liderazgo.

En estudio reciente realizado por Oxfam en Bolivia y Fundación Internet Bolivia, reveló que, durante las elecciones nacionales de 2020, el 60% de las candidatas enfrentaron situaciones de acoso y violencia política facilitada por la tecnología, y el 73% de candidatas se abstuvieron de hacer publicaciones en redes sociales por temor a ser amenazadas o sufrir agresiones.

Entre las formas más recurrentes de violencia digital identificadas se encuentran desde robo de identidad, utilización de cuentas falsas que distorsionan sus discursos hasta filtraciones malintencionadas de información privada, campañas de difamación y desprestigio. Estos ataques, a menudo premeditados, tienen el objetivo de intimidar, desacreditar y silenciar las voces de las mujeres políticas, buscando excluirlas de la esfera pública.

Frente a este escenario, y considerando el contexto actual en Bolivia –donde el marco legal para la sanción del acoso y la violencia de género facilitada por la tecnología es insuficiente y ambiguo, y los recursos técnicos para su prevención y atención aún son limitados–, surge la necesidad de una guía de seguridad digital dirigida especial-



mente a mujeres políticas. Este material busca ofrecer orientaciones conceptuales y herramientas didácticas para desarrollar habilidades de protección y resistencia ante posibles ataques

Esperamos que esta guía sea una herramienta que permita a las mujeres políticas fortalecer sus capacidades de autoprotección, les permita alzar la voz y mantenerse activas en el espacio virtual y espacio público.

Lourdes Montero
Directora País de Oxfam en Bolivia

Cristian León
Director Fundación Internet Bolivia



ANTECEDENTES

En sus inicios, Internet fue visto como una herramienta clave para fortalecer la democracia, ya que facilitaba la comunicación directa entre la ciudadanía y quienes ocupan cargos de toma de decisiones. Sin embargo, con el paso del tiempo, también se ha convertido en un espacio en el que se reproducen y amplifican diversas formas de violencia, particularmente contra las mujeres que participan en política. Además, la agresividad y hostilidad en línea han limitado la capacidad de las mujeres para ejercer su derecho a la participación política en entornos digitales.

Las plataformas digitales, especialmente redes sociales como Facebook, han sido señaladas por fomentar la polarización y el discurso de odio. Sus algoritmos priorizan publicaciones con insultos, ataques y desinformación, y estos tienen mayor alcance, ya que generan reacciones más intensas en el público. Este fenómeno afecta directamente a las mujeres que participan en política, quienes reciben respuestas agresivas y denigrantes cada vez que realizan una publicación.

Una de las estrategias más comunes de violencia política digital es el desprestigio basado en sus capacidades o intelecto. Se cuestiona su formación, su trayectoria y su legitimidad en el cargo, argumentando, por ejemplo, que no cuentan con la preparación suficiente para ocupar puestos de liderazgo. Otra táctica frecuente es el desprestigio con contenido sexual, en el que se las vincula sentimentalmente con figuras de poder, o se difunden imágenes íntimas falsas con el objetivo de afectar su credibilidad y autoridad.

Además, estas tácticas de desprestigio se entrelazan con otras formas de violencia sexual relacionada con las TIC (Tecnologías de la Información y Comunicación), que incluyen manipulación de imágenes y videos con contenido sexual, difusión de material íntimo sin consentimiento y otras estrategias que buscan someter a las mujeres al escarnio público. Este tipo de violencia no es espontáneo, sino que en muchos casos es organizado y estructurado, con el fin de expulsar a las mujeres de la vida política y reforzar una cultura patriarcal que sigue viendo su participación como una anomalía.

El acoso digital y la violencia de género contra las mujeres en política no pueden entenderse como hechos aislados, sino como parte de una problemática estructural. Si bien Bolivia, como muchos países de América Latina, ha logrado una transformación



en la participación política de las mujeres en las últimas décadas, aún persisten percepciones machistas que dificultan su plena inclusión en estos espacios.

Sumado a ello, la polarización política en el país ha exacerbado esta situación. En los casos analizados de violencia digital y física contra mujeres políticas, muchos comentarios justifican las agresiones en función de la afiliación partidaria de la víctima, reforzando la idea de que las mujeres “merecen” ser atacadas si pertenecen a ciertos grupos políticos. Este fenómeno erosiona la calidad democrática y perpetúa un entorno hostil donde las mujeres enfrentan barreras adicionales para ejercer su derecho a la participación política.

Esta guía surge como respuesta a la violencia de género que se ejerce a través de la tecnología contra mujeres que participan en política desde diferentes espacios y roles, entendiendo que la seguridad digital es una herramienta clave para gestionar riesgos en línea, pero que no garantiza que las mujeres dejen de enfrentar violencia y acoso político, ya que este es un problema estructural arraigado en dinámicas de poder desiguales.

“ El acoso digital y la violencia de género contra las mujeres en política no pueden entenderse como hechos aislados, sino como parte de una problemática estructural. ”

1.1. Objetivos de la guía



Esta guía ofrece recomendaciones para que las mujeres políticas puedan estar y ejercer su actividad en Internet de forma más segura. No pretende ofrecer soluciones definitivas a la violencia política digital, sino brindar herramientas y estrategias que ayuden a mitigar riesgos y reducir la exposición a ataques en entornos digitales, especialmente durante los periodos electorales.

1.1.2. Objetivos específicos

- Identificar y analizar los riesgos digitales más comunes que enfrentan las mujeres políticas, especialmente en contextos electorales, basándose en estudios previos y otras guías especializadas.



- Proporcionar orientaciones prácticas y accesibles sobre el entorno digital y medidas de seguridad esenciales que las mujeres políticas deben conocer para protegerse en línea.
- Diseñar herramientas y recursos concretos que les permitan mitigar los riesgos digitales más frecuentes, reducir su exposición a ataques y fortalecer su presencia en espacios digitales de manera más segura.
- Promover un enfoque colectivo de seguridad digital, que no solo brinde soluciones individuales, sino que también fomente la creación de redes de apoyo y estrategias comunitarias de resistencia ante la violencia política digital.

1.1.3. ¿A quién está dirigida esta guía?

Esta guía está dirigida principalmente a mujeres que participan en política, ya sea como candidatas, funcionarias públicas, militantes de partidos, y/o que inciden en el debate público. Está pensada para quienes consideran que se encuentran en riesgo de enfrentar violencia de género facilitada por la tecnología debido a su rol en la vida política, y buscan herramientas para fortalecer su seguridad en el ámbito digital.



1.1.4. Algunas consideraciones importantes

- La tecnología no se rompe, no tengas miedo de intentar, de probar. Recuerda que aprendemos haciendo. Si sientes miedo de aplicar las recomendaciones de esta guía, o necesitas resolver alguna pregunta, puedes escribir a la línea de ayuda del Centro S.O.S. Digital: 62342430.
- Recuerda que todas tenemos ritmos diferentes de aprendizaje.
- No todo sirve para todas. Es importante identificar los riesgos particulares de las personas y sus comunidades; es decir, puede ser que algunos aspectos de esta guía no sean útiles para ti; selecciona los que tengan más sintonía con tu experiencia digital.





¿QUÉ ES EL ACOSO Y VIOLENCIA POLÍTICA FACILITADA POR LA TECNOLOGÍA?¹

El acoso y la violencia política (AVP) son obstáculos para la participación de las mujeres en la vida pública y el ejercicio de sus derechos políticos. Algunas de sus manifestaciones incluyen presiones para que renuncien a sus cargos, difamación pública, discriminación y amenazas, limitando su acceso y permanencia en espacios de decisión.

Aunque la tecnología digital ha revolucionado la participación política al facilitar la comunicación con la ciudadanía, la difusión de propuestas y la denuncia de abusos, también ha dado lugar a nuevas formas de agresión como el acoso y la violencia política facilitada por la tecnología (AVP -FT), que se refiere al uso de herramientas digitales para hostigar, difamar, amenazar o desacreditar a mujeres que participan en política, con el objetivo de silenciarlas y limitar su participación.

Este tipo de violencia se manifiesta a través de ataques en redes sociales, difusión de información falsa, manipulación de imágenes o videos, y otras estrategias que buscan socavar la credibilidad de las mujeres, manteniéndolas en posiciones de subordinación, y restringiendo su derecho a la participación política y su libertad de expresión.

“...se refiere al uso de herramientas digitales para hostigar, difamar, amenazar o desacreditar a mujeres que participan en política, con el objetivo de silenciarlas y limitar su participación.”



¹ Oxfam Bolivia y Fundación InternetBolivia.org (2024). Entre la impunidad y la polarización: acoso y violencia política facilitada por la tecnología en Bolivia. Disponible en <https://internetbolivia.org/publicacion/entre-la-polarizacion-y-la-impunidad-acoso-y-violencia-politica-facilitada-por-la-tecnologia-en-bolivia/>



2.1. ¿Cuáles son los efectos del acoso y violencia política facilitada por la tecnología?

El acoso y la violencia política facilitada por la tecnología (AVP -FT), no solo afectan la vida digital de las mujeres en política, sino que tienen repercusiones profundas en su bienestar emocional, su participación política y su vida social. Aunque muchas veces se minimiza su impacto bajo la idea de que “lo que sucede en Internet no es real”, la realidad es que sus efectos son tangibles y pueden ser devastadores.²

Tabla No. 1	
Impactos en la salud mental y emocional • Estrés y ansiedad constante: Las víctimas viven en un estado de alerta permanente debido a las amenazas y agresiones en línea. • Depresión y pérdida de motivación: La violencia digital puede generar desmotivación para continuar con su labor política. • Aislamiento social y digital: Muchas mujeres optan por reducir su presencia en redes o incluso retirarse del ámbito político. • Necesidad de atención psicológica: Un alto porcentaje de mujeres que han enfrentado este tipo de violencia requiere apoyo terapéutico.	Impactos en la participación política • Deslegitimación de su liderazgo: Se cuestiona su capacidad y derecho a ocupar cargos políticos. • Desgaste y distracción: En lugar de enfocarse en su trabajo, deben dedicar tiempo y energía a enfrentar agresiones. • Miedo y autocensura: La violencia genera temor por su seguridad y la de sus familias, llevándolas a evitar ciertos temas o debates. • Desincentivo para la participación: Muchas mujeres deciden no postularse a cargos públicos por temor a ser atacadas.
Impactos económicos • Costos legales y médicos: Buscar justicia o apoyo psicológico implica gastos adicionales. • Reducción de productividad: El impacto emocional puede afectar su desempeño laboral y político. • Riesgo de pérdida de empleo: Algunas mujeres abandonan sus cargos o son presionadas para renunciar.	Impactos en la democracia • Debilitamiento del debate público: Se limita la participación de mujeres en discusiones políticas. • Normalización de la violencia: Al no haber consecuencias para los agresores, la violencia se perpetúa. • Pérdida de representación: Menos mujeres en política significa una democracia menos inclusiva.

2 Paz Peña (2022). Guía Práctica Contra la violencia política de género digital. Trabajo y Justicia Social.



Es importante reconocer que el AVP-FT no es un problema individual, sino colectivo y estructural, pues afecta la democracia en su conjunto. Por ello, protegerse digitalmente es fundamental, pero también es clave exigir que las plataformas y las instituciones tomen medidas para prevenir y sancionar estas agresiones.

“ Es importante reconocer que el AVP-FT no es un problema individual, sino colectivo y estructural, pues afecta la democracia en su conjunto. ”

2.2. ¿Cuál es el objetivo del acoso y violencia política facilitada por la tecnología? ³

- Deslegitimar el liderazgo femenino: A través de ataques en línea, se cuestiona y desacredita el derecho de las mujeres a ejercer funciones políticas, afectando su credibilidad y autoridad como líderes.
- Invadir la privacidad de las mujeres: Se incrementa la presión para que compartan más información personal, aumentando su vulnerabilidad y el costo de participar en espacios públicos y digitales.
- Distracción de su trabajo político: Las amenazas y abusos constantes desvían la atención de sus responsabilidades, obligándolas a dedicar tiempo y recursos para enfrentar los ataques, en lugar de centrarse en su labor política.
- Generar temor por su seguridad: El acoso digital crea sensación de inseguridad, lo que obliga a las mujeres a implementar medidas adicionales para protegerse a sí mismas y a su entorno (amigos/as, familia, etc.)
- Desincentivar la participación política: Las agresiones en línea buscan desmotivarlas para que no postulen a cargos públicos ni participen en el debate político, limitando su capacidad para contribuir al desarrollo democrático.
- El AVP - FT busca restar poder a las mujeres percibidas como rivales. Desde una lógica machista, se recurre a ataques contra su vida privada con el objetivo de debilitarlas, reducir su influencia y frenar su participación política. Algunas personas consideran que, para recuperar o mantener el poder, deben eliminar a sus oponentes, y lo hacen dañando su integridad personal.

3 Paz Peña (2022). Guía Práctica Contra la violencia política de género digital. Trabajo y Justicia Social.



2.3. ¿Cuáles son las formas de violencia más comunes que enfrentan las mujeres políticas en periodos electorales?

Tabla No 2		
Tipo de violencia	Definición	Ejemplo
Abuso de datos personales usando TIC	Se usa la tecnología para obtener, compartir o manipular información personal sin permiso. - Suplantación y robo de identidad: Alguien se hace pasar por otra persona en redes o plataformas digitales. - Obtención de información personal no consentida: Roban o acceden a datos privados sin autorización, como contraseñas, dirección o conversaciones. - Publicación no autorizada de datos personales, fotos o videos personales: Compartir sin permiso información, dirección de su domicilio, número de teléfono, poniendo en riesgo la privacidad.	Las mujeres en política son frecuentemente víctimas del uso indebido de su información personal con el objetivo de intimidarlas o desacreditarlas. En muchos casos, se filtran sus datos de contacto, direcciones o información sobre sus familias, exponiéndolas al acoso y las amenazas. Además, se crean perfiles falsos que difunden mensajes en su nombre, lo que distorsiona su imagen pública y afecta negativamente su credibilidad.
Violencia sexual relacionada con las TIC	Cuando la tecnología se usa para afectar la intimidad y la seguridad de una persona de manera sexual. - Obtención de imágenes íntimas sin consentimiento: Tomar o grabar a alguien sin su permiso en situaciones privadas. - Difusión de imágenes íntimas sin consentimiento: Compartir fotos o videos íntimos sin autorización, dañando la reputación y seguridad de la persona. - Extorsión: Amenazar con publicar imágenes íntimas o información personal para obtener algo a cambio. - Edición de imágenes o videos con contenido sexual: Modificar fotos o videos para hacer que alguien parezca estar en una situación sexual que no ocurrió.	El uso de imágenes íntimas como herramienta de ataque es una táctica recurrente contra mujeres políticas. En muchos casos, se difunden fotografías manipuladas para hacerlas parecer parte de contenido sexual, o se filtran imágenes privadas obtenidas sin su consentimiento. Estos ataques buscan socavar su autoridad y reducir su trayectoria profesional a su vida privada, instalando la idea de que su presencia en la política está ligada a favores sexuales y no a su capacidad.



Tipo de violencia	Definición	Ejemplo
Acoso	Actos de acoso y violencia política basada en género mediante el uso de tecnologías de la información y la comunicación u otras herramientas digitales. Son agresiones constantes en línea que buscan intimidar, molestar o dañar a alguien. • Insultos reiterados: Mensajes ofensivos repetidos con la intención de lastimar. • Monitoreo y acecho: Vigilar y seguir cada movimiento de una persona en redes o incluso en la vida real a través de la tecnología. • Monitoreo y acecho a familiares: Involucrar a seres queridos en el acoso para generar más presión. • Expresiones racistas y discriminatorias: Comentarios ofensivos basados en raza, género, orientación sexual u otros aspectos personales. • Amenazas: Advertencias de daño físico, psicológico o social a una persona. • Comentarios sobre apariencia física y sexualización: Críticas o mensajes incómodos sobre el cuerpo o la imagen de alguien. • Ataques por adscripción político-ideológica: Agresiones por pertenecer o apoyar una ideología, partido o causa.	Las mujeres en política enfrentan ataques sistemáticos en redes sociales que buscan silenciarlas o cuestionar su autoridad. Desde insultos constantes sobre su físico y vestimenta, hasta amenazas directas contra ellas y sus familias. Muchas son monitoreadas de manera obsesiva, con personas analizando cada palabra o decisión para encontrar motivos de crítica. También reciben mensajes discriminatorios que las descalifican por su género, su origen o su afiliación política, creando un ambiente hostil que busca expulsarlas del espacio público.
Acceso o control no autorizado	Cuando alguien ingresa o manipula cuentas o sistemas sin permiso. • Crackeo: Acceder sin autorización a cuentas, dispositivos o sistemas, muchas veces para robar información o dañar.	Algunas mujeres políticas han perdido el control de sus redes sociales y correos electrónicos tras ser crackeadas, lo que permitió acceder a información privada que luego fue divulgada fuera de contexto o manipulada. En otros casos, las cuentas intervenidas fueron utilizadas para publicar mensajes falsos, generando confusión y dañando su credibilidad.



Tipo de violencia	Definición	Ejemplo
Afectaciones de canales de expresión o censura	Estrategias para silenciar voces en internet. • Ataque por actores individuales: Cuando una sola persona hostiga o intenta silenciar a alguien con mensajes, comentario u otros. • Ataque masivo y coordinado por actores grupales: Varias personas se organizan para atacar de manera sistemática, con el objetivo de bajar publicaciones, que la persona atacada cierre sus cuentas, etc. • Eliminación de publicaciones, páginas y perfiles por denuncia o iniciativa en redes sociales: Se usan reportes falsos o "normas de la comunidad"⁴ de plataformas para borrar contenido.	Muchas mujeres políticas han sido víctimas de campañas organizadas para hacer desaparecer sus publicaciones o incluso sus perfiles en redes sociales. Grupos coordinados reportan masivamente su contenido hasta lograr que sea eliminado bajo el argumento de que infringe normas de una u otra plataforma. Otras veces, enfrentan campañas de acoso masivo que las obligan a retirarse de espacios digitales por seguridad y salud mental, limitando su derecho a expresarse y a participar en el debate público.
Campañas de difamación y desprestigio	Estrategias para dañar la imagen de alguien a través de mentiras y ataques. • Actos que dañan la reputación o credibilidad de una persona: Difundir rumores falsos o información distorsionada. • Desinformación de género: Compartir noticias o datos manipulados para reforzar estereotipos de género y desacreditar a mujeres y diversidades. • Desprestigio con base en sus capacidades o intelecto: Insinuar que alguien no es competente o que logró algo por razones ajenas a su esfuerzo. • Desprestigio con contenido sexual: Vincular la vida privada de alguien o con cuestiones sexuales para deslegitimarla.	El objetivo de las campañas de difamación contra las mujeres en la política es dudar de su autonomía y habilidades. A menudo las vinculan con hombres poderosos dentro de los partidos políticos, sugiriendo que las mujeres solo pueden llegar a cargos importantes gracias a su relación con ellos. De esta forma, se busca poner en duda su capacidad para tomar decisiones por sí mismas y se intenta hacer pública su vida privada para desacreditarlas.

4 Las "normas de la comunidad" en las plataformas digitales son un conjunto de reglas que establecen lo que está permitido y lo que no dentro de una red social, foro o servicio en línea.



Tipo de violencia	Definición	Ejemplo
Brecha digital	La desigualdad en el acceso, uso y las habilidades con respecto a la tecnología. • Acceso a Internet: No todas las personas pueden conectarse con la misma facilidad. • Acceso a dispositivos: No todas tienen celulares, computadoras u otros equipos para participar en el mundo digital. • Habilidades digitales: Algunas personas tienen menos conocimientos sobre cómo usar la tecnología, lo que limita sus oportunidades.	Algunas mujeres políticas de pueblos indígenas enfrentan mayores barreras para desarrollar habilidades digitales, lo que amplía la brecha de oportunidades políticas en comunidades que ya se encuentran en situación de vulnerabilidad.
Omisiones por parte de actores con poder regulatorio	Cuando instituciones o autoridades no hacen lo necesario para proteger a las mujeres en el entorno digital. • Violencia institucional: Falta de respuesta o negligencia de las instituciones ante denuncias de violencia digital. • Violencia en acceso a servicios: Dificultades para acceder a plataformas, ayuda legal o apoyo por parte de entidades oficiales.	Cuando las mujeres políticas denuncian violencia digital, muchas veces las autoridades minimizan sus casos o no les brindan protección efectiva. La falta de regulación clara con una tipificación específica y de mecanismos de respuesta permiten que las agresiones continúen sin sanción para los agresores, ni mecanismos de reparación para las víctimas.

Elaboración propia basada en el informe: “Entre la impunidad y la polarización: acoso y violencia política facilitada por la tecnología en Bolivia”. Oxfam Bolivia y Fundación InternetBolivia.org (2024). Disponible en <https://internetbolivia.org/publicacion/entre-la-polarizacion-y-la-impunidad-acoso-y-violencia-politica-facilitada-por-la-tecnologia-en-bolivia/>





3. SEGURIDAD DIGITAL PARA MUJERES POLÍTICAS EN EL CONTEXTO ELECTORAL

¿Qué es la seguridad digital holística?

La seguridad digital nos permite construir una vida digital priorizando el bienestar, especialmente de aquellas personas que suelen enfrentar constantes vulneraciones en los espacios digitales. Abarca tres aspectos fundamentales: la protección física, el bienestar mental y los autocuidados, y la seguridad en el entorno digital. Este enfoque es esencial porque reconoce que lo que vivimos en Internet es tan real como en el mundo físico.⁵

Se dice que es holística porque abarca la seguridad de una persona como un todo, y no solo la parte digital. Considera cómo lo que hacemos en línea afecta nuestra seguridad física y emocional, y viceversa.

¿Por qué la seguridad digital es importante para las mujeres candidatas?

La seguridad digital es clave en un contexto electoral para proteger a las mujeres candidatas de amenazas en línea. Incluye prevenir el acoso y la violencia política facilitada por la tecnología, cuidar su bienestar mental, proteger su identidad, reputación y datos personales, y crear espacios seguros en internet. Esto les permite participar en política con mayor confianza, reducir riesgos y saber cómo responder ante situaciones de AVP – FT.

3.1. Seguridad en tu celular y computadora.

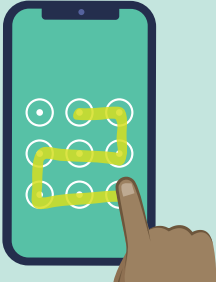
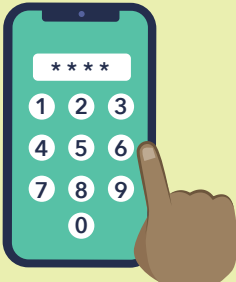
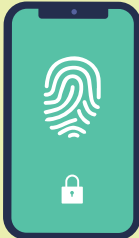
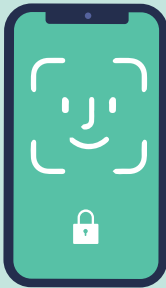
El primer paso para proteger tu información es asegurarte de que tu celular tenga un buen método de bloqueo. Hoy en día los teléfonos son herramientas esenciales en la

5 Hiperderecho. [Seguridad digital con enfoque holístico](https://hiperderecho.org/tecnorestencias/2020/09/seguridad-digital-enfoque-holistico/#:~:text=En%20este%20sentido%2C%20la%20seguridad%20digital%20hol%C3%ADstica,se%20ven%20constantemente%20vulneradas%20en%20espacios%20virtuales.). Disponible: <https://hiperderecho.org/tecnorestencias/2020/09/seguridad-digital-enfoque-holistico/#:~:text=En%20este%20sentido%2C%20la%20seguridad%20digital%20hol%C3%ADstica,se%20ven%20constantemente%20vulneradas%20en%20espacios%20virtuales.>



vida personal y profesional, y en una campaña electoral se convierten en un centro de comunicación, organización y estrategia.

Desde redes sociales hasta aplicaciones de mensajería y correo electrónico, los celulares almacenan mucha información importante. Como candidata, tu información está en riesgo de robo o acceso no autorizado, por tanto, **PROTEGER TU DISPOSITIVO ES CLAVE PARA EVITAR FILTRACIONES, SUPLANTACIÓN DE IDENTIDAD, O QUE ALGUIEN ACCEDA A TUS CUENTAS SIN PERMISO.**

Tabla No. 3	
1. Dibujar un Patrón Este método, aunque sencillo y rápido, es el menos seguro. Cualquier persona que observe tu pantalla podría replicar el patrón. Además que las formas de patrón que se pueden crear son bastante limitadas. 	2. Código Numérico Un PIN de 4 dígitos es mejor que un patrón, pero aún así, es vulnerable. Se recomienda utilizar un código de al menos 6 dígitos o, preferiblemente, una combinación alfanumérica, es decir una contraseña para mayor seguridad. 
3. Huella Digital Este sistema es cómodo y relativamente seguro. Sin embargo, dado que nuestras huellas pueden quedar marcadas en superficies, hay posibilidades de que alguien las use para vulnerar el acceso al dispositivo. Se recomienda combinar este método con un PIN o contraseña segura. 	4. Reconocimiento Facial Aunque es una opción avanzada, la seguridad depende de la calidad del software. En algunos casos, fotos o videos pueden engañar a los sensores de reconocimiento facial. 

TE RECOMENDAMOS QUE UTILICES UN PIN O CONTRASEÑA COMO MÉTODO DE BLOQUEO DE TU CELULAR.



3.2 ¿Qué es una contraseña segura y por qué es importante no compartirla con nadie?



Una contraseña segura es una clave que usas para proteger tu cuenta en Internet. Debe ser difícil de adivinar, por eso es importante que combine letras (mayúsculas y minúsculas), números y símbolos. Además, debe ser lo suficientemente larga, preferiblemente de al menos 12 caracteres.

¿Por qué no compartirla?

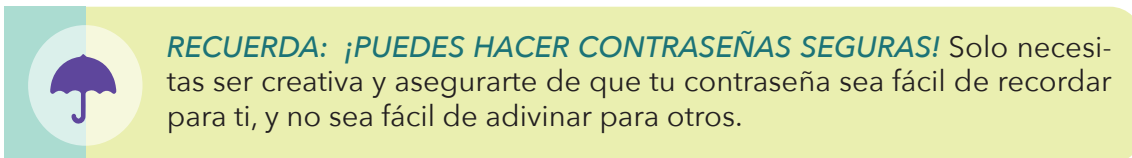
Es esencial no compartir tu contraseña con nadie, ni siquiera con personas de confianza, porque quien tenga acceso a tu contraseña podría entrar a tus cuentas personales y manipular información importante. **EN EL CASO DE LAS MUJERES QUE HACEN POLÍTICA, ESTO PODRÍA PONER EN RIESGO SU SEGURIDAD PERSONAL Y PROFESIONAL**, especialmente en un contexto electoral donde la privacidad y la protección de los datos son clave. Mantener tus contraseñas privadas ayuda a proteger tu identidad, tu información personal y tu trabajo político de posibles ataques y acoso digital.

Recomendaciones para crear contraseñas seguras

- ✓ Usa palabras aleatorias: En lugar de usar nombres o fechas fáciles de adivinar, puedes combinar palabras que no tengan relación entre sí. Por ejemplo, “luna-piedra-zapato” o “flor-cielo-cuento”.
- ✓ Aprovecha tus canciones o poemas favoritos: Elige una frase de tu canción o poema favorito y conviértela en tu contraseña. Por ejemplo, “Para bailar esto es una bomba” puede convertirse en “P4r4b41l4r3st03sunab0mb4”. Agrega mayúsculas, números y símbolos para hacerla más segura.
- ✓ Hazla larga: Cuanto más larga sea la contraseña, más difícil será de adivinar. Trata de usar al menos 12 caracteres.
- ✓ No uses información personal: Evita incluir cosas como tu nombre, apellido o fechas de nacimiento, ya que son fáciles de encontrar para los atacantes; sobre todo si existe mucha información tuya en Internet.



- ✓ Crea frases fáciles de recordar: Puedes formar contraseñas a partir de frases completas que solo tú entiendas, por ejemplo, "MeGustaLeerLibrosEnElMinibus" o "tuEnvidiaesMiPasion".
- ✓ No la compartas con nadie, ni con tu equipo de trabajo, y asegúrate de cerrar tus sesiones cuando abras tus redes sociales en computadoras ajenas, como oficinas o cafés internet.



3.3. ¿Qué es un gestor de contraseña y cómo me puede ayudar?

Uno de los desafíos más comunes de las contraseñas seguras es poder recordarlas todas, ya que se recomienda no usar la misma contraseña en todas tus cuentas.

Para hacer más fácil esto existen los gestores de contraseñas. Son herramientas que permiten administrar y guardar de forma segura las contraseñas; funcionan como una caja fuerte digital, y así no necesitas recordar todas, pero siempre tendrás acceso a ellas cuando las necesites.

Existen algunos gestores de contraseñas que son muy fáciles de usar como:

1. Bitwarden

- Código abierto y auditado.
- Tiene una versión gratuita completa.
- Se puede usar en navegador, móvil y escritorio.

<https://bitwarden.com/>

2. KeePassXC

- Totalmente offline, no depende de la nube.
- Funciona en Windows, Linux y macOS.
- Usa bases de datos cifradas (.kdbx).

<https://keepassxc.org/>



3.4. La importancia de la verificación en dos pasos (2FA)



Existe una forma de evitar que alguien acceda a tus cuentas en línea, incluso si roban tu contraseña, se trata de la verificación en dos pasos (2FA).

¿Qué es la verificación en dos pasos?

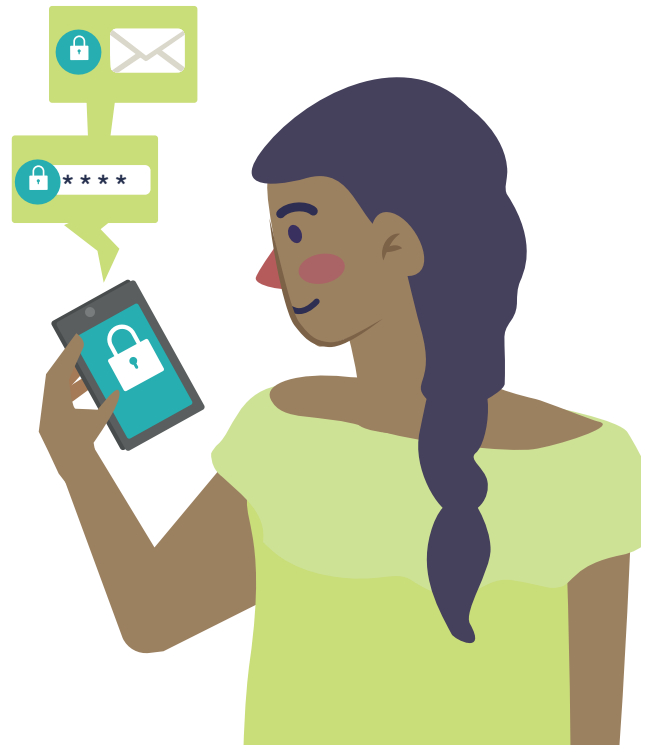
Es un mecanismo de seguridad adicional para proteger tus cuentas en línea. Como su nombre indica, hay ***DOS PASOS PARA INICIAR SESIÓN EN TUS CUENTAS: EL PRIMERO ES TU USUARIO Y CONTRASEÑA, Y EL SEGUNDO ES UN CÓDIGO ÚNICO*** que se genera solo una vez.

La verificación en dos pasos (2FA) es como una puerta con dos cerraduras. La primera cerradura es tu contraseña, que es como una clave común. Pero, si alguien llega a robarla, no podrá acceder a tu cuenta, porque se necesita la segunda cerradura (el código único que recibes) para abrirla. Incluso si tienen la primera clave, necesitarán la segunda para poder entrar. De esta forma, tienes una capa extra de seguridad, como un guardia adicional que asegura que nadie entre sin tu permiso.

¿Cómo se obtiene el código único de verificación en dos pasos?

Los códigos de verificación en dos pasos se pueden obtener de diferentes maneras:

- SMS: Recibes un código único a tu número de teléfono por mensaje de texto.
- Aplicación: Usas una aplicación en tu celular que genera códigos que cambian cada 30 o 60 segundos. Esta es la opción más recomendada porque implica mayor seguridad.



- Notificación en el celular: Recibes una notificación en tu teléfono donde te preguntan si autorizas o no el acceso a tu cuenta.

Dependiendo de cómo tengas configurada la verificación en dos pasos, cuando se te pida el código único, solo necesitas revisar tus SMS, abrir tu aplicación de códigos, o solo una de estas opciones para acceder a tu cuenta.

¿Dónde puedo activar la verificación en dos pasos?

Puedes activar la verificación en dos pasos (2FA) en las configuraciones de seguridad de la mayoría de las cuentas en línea, como Google, Facebook, Instagram y otras plataformas.

¿Por qué las mujeres candidatas en contextos electorales deben usar contraseñas seguras y activar la verificación en dos pasos?



Porque están expuestas a ataques digitales que buscan vulnerar su seguridad, afectar su reputación y obstaculizar su participación política. Por tanto, **PROTEGER SUS CUENTAS EN LÍNEA CON CONTRASEÑAS SEGURAS Y LA VERIFICACIÓN EN DOS PASOS (2FA) ES FUNDAMENTAL PARA EVITAR ACCESOS NO AUTORIZADOS Y POSIBLES ATAQUES.**

Riesgos de no proteger sus cuentas:

- Suplantación de identidad: Un atacante podría tomar el control de sus cuentas y publicar información falsa en su nombre.
- Filtración de información sensible: Pueden acceder a mensajes privados, datos personales y estratégicos que podrían ser usados en su contra.
- Campañas de desprestigio: Alguien con acceso a sus cuentas podría difundir contenido dañino o manipular su información para afectar su imagen pública.

3.5. ¿Qué es el phishing o el engaño digital y por qué debo protegerme de él?

El phishing es un tipo de engaño digital en el que atacantes intentan hacerte caer en una trampa para robar información personal, como contraseñas, datos bancarios o acceso a tus cuentas. Lo hacen haciéndose pasar por instituciones, plataformas o personas de confianza para engañarte y lograr que entregues tu información sin darte cuenta.



¿Cómo intentan engañarte?

- Enviando correos electrónicos falsos: Mensajes que parecen venir de bancos, redes sociales o servicios digitales, pero en realidad contienen enlaces maliciosos.

Por ejemplo:

Una candidata recibe un correo electrónico, aparentemente enviado por una entidad electoral, en el que se le informa sobre la necesidad de actualizar sus datos para evitar la inhabilitación de su candidatura. El mensaje incluye un enlace que simula ser el sitio oficial, pero al ingresar, se solicita su usuario y contraseña de Facebook. Al proporcionar esta información, los atacantes obtienen acceso a su cuenta y comienzan a publicar contenido en su nombre.

- Mensajes de texto o llamadas sospechosas: Te piden que verifiques tu cuenta o descargues un archivo que puede ser peligroso.

Por ejemplo:

Una persona recibe un mensaje de texto de un número desconocido que dice: *"Se ha detectado un intento de acceso a su cuenta de redes sociales. Para verificar su identidad y evitar el cierre, haga clic en este enlace e ingrese sus credenciales."* Si sigue el enlace y proporciona su información, los atacantes toman el control de sus redes.



- Páginas web falsas: Sitios que imitan plataformas legítimas para que ingreses tu usuario y contraseña.

Por ejemplo:

Durante la campaña electoral, una candidata recibe un mensaje de WhatsApp con un enlace a un supuesto portal de noticias locales que ofrece entrevistas exclusivas a candidatas. Cuando accede y completa un formulario con datos personales y contraseñas de sus cuentas, la información es robada por los atacantes.

- Archivos o enlaces maliciosos: Documentos o links que, al abrirlos, pueden infectar tu dispositivo con virus.

Por ejemplo:

Una candidata recibe un correo con un documento adjunto titulado *“Encuestas internas de intención de voto”*. Al abrirlo, su computadora se infecta con un virus que permite a los atacantes espiar su actividad y acceder a información confidencial sobre su campaña.

Recuerda que existen dos tipos de “engaños digitales” o phishing:

- El dirigido: Este tipo de ataque es más sofisticado y está dirigido a una persona o grupo específico. Los atacantes investigan a su víctima y personalizan el engaño para hacerlo más creíble.
- El general: Este tipo de ataque se envía de forma masiva sin un objetivo específico. Los atacantes envían correos, mensajes o enlaces falsos a muchas personas con la esperanza de que algunas caigan en la trampa.

¿Por qué debo protegerme del phishing o del engaño digital?



Las mujeres candidatas en contextos electorales pueden ser blanco de ataques digitales diseñados para robar información estratégica, acceder a cuentas personales o incluso manipular su imagen pública. Un ataque de phishing puede poner en riesgo su seguridad, la de su equipo y la de su campaña.

¿Cómo protegerse del phishing o del engaño digital?

- Desconfía de mensajes inesperados que pidan información personal o te presionen para actuar rápido.
- Verifica los enlaces antes de hacer clic. Pasa el cursor sobre ellos y revisa que la URL sea la oficial.
- No descargues archivos de remitentes desconocidos. Activa la verificación en dos pasos (2FA) para que, aunque alguien consiga tu contraseña, no pueda acceder a tus cuentas.
- Recuerda que este tipo de engaño juega con la urgencia y usualmente tienen el objetivo de generar miedo, estrés o ansiedad para que reacciones sin pensar.

La mejor defensa contra el phishing es la prevención. Si algo parece sospechoso, verifícalo antes de actuar.

¿Cómo identificar si una URL es oficial y evitar sitios falsos?

Los atacantes usan sitios web falsos para engañar y robar tu información. Antes de hacer clic en un enlace o ingresar tus datos en una página, sigue estos pasos para verificar si es una URL oficial.

- Observa con atención la dirección web (URL)
- Antes de hacer clic en un enlace, revisa que la URL (dirección web) sea la correcta.



Algunas señales de advertencia incluyen:

- **Errores ortográficos o caracteres extraños:**

URL oficial: www.bancoejemplo.com

URL falsa: www.banco-ejempl0.com o www.bancoejemplo.seguro.net



- **Dominios sospechosos o añadidos:**

Los sitios oficiales suelen terminar en **.com**, **.gob**, **.org** o el dominio propio de la institución.

Cuidado con URLs que terminan en **.net**, **.xyz**, **.info** cuando esperas un sitio de confianza.

- **Revisa si la URL usa "https://"**

Las páginas seguras usan "https://" al inicio de la dirección web. Busca el candado en la barra de direcciones:

Seguro: **https://www.ejemplo.com** (con candado)

No seguro: **http://www.ejemplo.com** (sin candado)

Pero ojo: Aunque una página tenga "https://", eso no garantiza que sea legítima. **SIEMPRE REvisa EL DOMINIO COMPLETO.**

3.6. ¿Qué es el cifrado en las aplicaciones de comunicaciones?

Imagina que envías una carta muy importante a una amiga. Para asegurarte que nadie más la lea en el camino, la guardas en una caja fuerte con un candado especial. Solo tu amiga tiene la llave para abrirla.

Eso es exactamente lo que hace el cifrado de extremo a extremo (E2EE) en las aplicaciones de mensajería. Cuando envías un mensaje, este se convierte en un código secreto que solo el destinatario puede descifrar. Solo tú y la persona con la que hablas tienen la "llave" para abrir el mensaje.

¿Por qué es importante?

- Protege tu privacidad: Nadie más puede leer tus mensajes, ni siquiera la aplicación.
- Evita espionaje: Aunque alguien intercepte el mensaje, verá solo un código sin sentido.
- Si eres candidata, el cifrado protege tus conversaciones de ataques o filtraciones.



Tabla No. 4				
Aplicaciones que tienen el cifrado de extremo a extremo y otras opciones de seguridad				
	Signal	WhatsApp	Telegram	Facebook Messenger
Cifrado de extremo a extremo	Si	Si	Solo activando la opción de chat secreto	x
Autodestrucción de mensajes: Es una función que permite que los mensajes se eliminen automáticamente después de un tiempo determinado, garantizando mayor privacidad y seguridad en las conversaciones.	Si	Si Sin embargo, los mensajes temporales pueden ser reenviados, o respaldados por copias de seguridad si estos aún no desaparecen	Sí Solo en chat secreto	Sí Disponible en el modo efímero o con temporizador en el chat secreto
Bloqueo de capturas de pantalla	Sí No está habilitado por defecto. Su uso es para evitar que software espía tome capturas de tus chats, no para evitar que la otra persona lo haga	No	Sí Sólo en chat secreto. Nota: Al agregar un código de desbloqueo a la aplicación se habilita una opción para evitar capturas de pantalla en cualquier chat	Sí Sólo en chat secreto. Nota: Al agregar un código de desbloqueo a la aplicación se habilita una opción para evitar capturas de pantalla en cualquier chat
Es de código abierto ⁶	Si	No	Parcialmente	No

Fuente: Protege.La - Seguridad y privacidad en apps de mensajería.
 Disponible en: <https://protege.la/wp-content/uploads/2022/02/tabla-apps-mensajeria-2022.pdf>

Los grupos de WhatsApp, Telegram o cualquier otra plataforma de mensajería pueden ser útiles para la organización de campañas, pero también representan un riesgo si incluyen personas desconocidas o si son públicos.



Pueden ser peligrosos porque:

- No tienes control sobre quién ve la información. Una persona ajena podría ser añadida sin tu conocimiento.
- Pueden filtrar datos personales o estratégicos. Información sobre tu campaña o equipo puede terminar en manos equivocadas.
- El contenido puede usarse en tu contra. Capturas de pantalla o mensajes sacados de contexto pueden ser utilizados para desinformación o ataques.

¿Cómo protegerte?

- Usa grupos cerrados con personas de confianza.
- Si es necesario compartir información delicada, hazlo en chats privados y con cifrado de extremo a extremo. Signal es una muy buena opción.
- Revisa quién administra los grupos y limita quién puede agregar participantes.
- Borrar mensajes antiguos con información que ya no sea relevante.



No reenvíes mensajes sin verificar su origen

En una campaña electoral, **LA DESINFORMACIÓN Y LAS NOTICIAS FALSAS PUEDEN USARSE COMO ARMA EN TU CONTRA**. Un simple reenvío puede amplificar un mensaje falso y afectar tu reputación.

¿Cómo identificar información dudosa?

- Mensajes con urgencia o alarmismo, por ejemplo: "¡Comparte esto antes de que lo borren!"
- Contenido sin fuente confiable o con enlaces sospechosos.
- Errores ortográficos o cambios en los nombres de instituciones oficiales.



¿Qué hacer antes de reenviar un mensaje?

- Verifica en fuentes oficiales (sitios web gubernamentales, medios de comunicación reconocidos).
- Pregunta a la persona que lo envió de dónde lo obtuvo.
- Si el mensaje es sobre ti o tu campaña, consulta con tu equipo antes de compartirlo.
- Evita reacciones impulsivas. Una mala información puede desviar la atención de tu mensaje político.

Usa mensajes temporales en conversaciones sensibles

Para proteger tus comunicaciones y evitar filtraciones, usa la opción de mensajes que desaparecen, esto se puede configurar en aplicaciones como WhatsApp, Signal y Telegram.

¿Por qué es útil esta función?

- Reduce el riesgo de que mensajes sean utilizados en tu contra.
- Evita que conversaciones estratégicas queden almacenadas en dispositivos de otras personas.

¿Cómo activarlos?

- WhatsApp: Ve al chat ➡ Toca el nombre del contacto ➡ Activa "Mensajes temporales" y elige el tiempo de duración.
- Signal: Abre el chat ➡ Toca los tres puntos arriba ➡ Activa "Mensajes que desaparecen" y selecciona el tiempo.
- Telegram: Usa los "Chats secretos" ➡ Configura el tiempo de autodestrucción del mensaje.



Importante:

LOS MENSAJES TEMPORALES NO EVITAN CAPTURAS DE PANTALLA. Comparte solo con personas de confianza.

No uses esta función para información que necesites conservar. Úsala solo para conversaciones estratégicas o confidenciales.

3.7. ¿Cómo proteger tu privacidad en línea siendo una mujer en la política?

La privacidad es un derecho que permite a las personas decidir quién accede a su información en redes sociales. En un contexto electoral, las candidatas pueden ser investigadas y atacadas en Internet, utilizando información pública para desacreditarlas, agredirlas, acosarlas o violentarlas. Por lo tanto, es crucial presentar estrategias para proteger su privacidad en línea.

“ La privacidad es un derecho que permite a las personas decidir quién accede a su información en redes sociales. ”

¿Por qué es importante separar la vida pública de la personal?

Una estrategia clave para cuidar tu privacidad en Internet es **MANTENER PERFILES SEPARADOS EN REDES SOCIALES**, es decir, una cuenta personal donde sea posible dar una imagen relajada y cotidiana a las personas más allegadas y de confianza, y otra cuenta pública, enfocada a la carrera política donde se pueda hacer campaña y pronunciamientos oficiales.



Tabla No. 5	
Cuenta Personal	Cuenta Pública
• Es posible publicar o comentar cosas personales, actividades, intereses y contenido más relajado o de entretenimiento. • Solo tienen acceso personas cercanas y conocidas, amistades, familia. • Se configura la privacidad para que el público en general NO tenga acceso a: datos personales, publicaciones, mensajes, imágenes, lista de amistades, etiquetas.	• Las publicaciones solo están relacionadas con la imagen política, campañas u pronunciamientos oficiales. • Tiene acceso al público en general, incluso es posible publicitar el perfil buscando llegar a más audiencia. • Se debe configurar de tal forma que no contenga datos personales o sensibles. • Se puede verificar en la red social para que cuentas falsas no se hagan pasar por la cuenta oficial. Si necesitas apoyo para verificar tu cuenta puedes escribir a la línea de ayuda del Centro S.O.S. Digital: +591 62342430

Configuraciones en la privacidad para cuentas personales

Muchas veces plataformas como Facebook o Tik Tok no tienen una forma sencilla de configurar la privacidad, pero están obligadas a proporcionar medios para **DECIDIR QUÉ INFORMACIÓN COMPARTIR Y CON QUIENES COMPARTIRLA**.

Tabla No. 6		
¿Cómo ingresar a las configuraciones de privacidad en las redes sociales?		
Facebook: • Abre la app de Facebook. • Toca el menú (en Android / Perfil en iPhone). • Selecciona Configuración y privacidad. • Selecciona Configuración. • Selecciona Privacidad para ajustar quién puede ver tu información y publicaciones.	Instagram: • Abre la app de Instagram. • Ve a tu perfil y toca el menú (en la esquina superior derecha). • Selecciona Configuración y privacidad. • Ajusta la privacidad de tu cuenta, la visibilidad de tus historias y quién puede enviarte mensajes.	WhatsApp: • Abre la app de WhatsApp. Toca los tres puntos (en Android) / Configuración (en iPhone). • Ve a Privacidad. Configura quién puede ver tu foto de perfil, estados, última conexión y más.



Twitter/X

- Abre la app de Twitter/X.
- Toca tu foto de perfil y selecciona Configuración y soporte > Configuración y privacidad.
- Entra en Privacidad y seguridad.
- Ajusta quiénes pueden ver tus tweets y cómo interactúan contigo.

TikTok

- Abre la app de TikTok.
- Ve a tu perfil y toca las tres líneas (=) en la esquina superior derecha.
- Selecciona Configuración y privacidad.
- Ajusta la privacidad de tu cuenta, comentarios y quién puede enviarte mensajes.

En las configuraciones de privacidad de tus **cuentas personales** es importante revisar:

- **Datos personales:** Muchos de los datos en los perfiles de redes sociales son públicos por defecto, como el nombre completo, fecha de nacimiento, lugar de residencia y hasta las fotos. Es mejor que esta información no sea visible para todos. Es posible configurar el perfil para que sólo los contactos puedan ver estos datos o incluso para que nadie pueda verlos.
- **Quién ve tu perfil:** Asegúrate de saber quién puede ver tu perfil o encontrarlo en las redes sociales. También es posible decidir si las publicaciones son visibles para todos y todas o sólo para contactos.
- **Control de los comentarios y mensajes:** Es posible elegir quién puede dejar comentarios en las publicaciones, quién puede enviarte mensajes o publicar en el perfil. Esto es de mucha ayuda para evitar que personas desconocidas se contacten contigo o con alguien de tu familia.
- **Cuenta restringida:** Una cuenta restringida es mucho más segura, ya que ninguna persona que no sea un contacto puede ver, acceder a tu información, ni a tu foto de perfil o portada.
- **Filtro de etiquetas o menciones:** Es posible configurar quienes pueden etiquetar o mencionar tu perfil en otras publicaciones, también es posible activar una alerta para saber cuándo se crea una etiqueta y verificar antes de aceptarla.

En **cuentas públicas** las configuraciones de privacidad son diferentes, se recomienda tomar en cuenta las siguientes configuraciones:



- **Datos personales:** En una cuenta pública se recomienda omitir datos que no deben ser de conocimiento público, es mejor solo colocar datos relevantes; y no poner el resto de datos, o que no sean visibles.
- **Control de comentarios y mensajes:** En caso de que la cuenta reciba comentarios ofensivos o mensajes no apropiados, es posible configurarla para evitar recibirlos, ya sea temporalmente o indefinidamente.
- **Sobre la moderación de comentarios:** En caso de que se esté atacando una cuenta, es posible moderar los comentarios de las publicaciones tal cual se indican en los siguientes enlaces:
 - [Modo profesional de Facebook.](#)
 - [Modo control de comentarios TikTok](#)
- En caso de Instagram se debe hacer la eliminación de comentarios de forma manual o activar la privacidad de la cuenta para evitar que personas que no te sigan puedan comentar.
- **Página y no perfil:** Se recomienda también considerar el uso de una página de Facebook en lugar de un perfil, ya que ésta permite mayor control sobre el contenido que verán los seguidores y el uso de publicidad.
- **Grupo y no perfil:** Es posible también hacer uso de un grupo de Facebook, cuya ventaja es poder filtrar a las personas que forman parte del mismo, y de esa forma evitar el acoso en esta red social.
- **Verificación de los perfiles:** Se recomienda solicitar la verificación de la cuenta, cuya función principal es asegurar su autenticidad, evitar la suplantación de identidad y dar mayor credibilidad.

¿Cómo activar la verificación en redes sociales para cuentas públicas?

En muchas redes sociales es posible pedir que tu cuenta sea verificada. Esto sirve para demostrar que la cuenta es realmente tuya. Para lograrlo, debes cumplir algunos requisitos, como enviar documentos que prueben quién eres, como el carnet de identidad u otros requisitos dependiendo de cada red social. Una vez que revisen tus documentos y aprueben la verificación, verás una marca, como una palomita, jun-



to al nombre de tu cuenta. Tener una cuenta verificada ayuda a evitar que alguien se haga pasar por ti, te difame o te ataque, y también le da más confianza y seriedad a tu imagen, sobre todo si eres una figura pública, como en el caso de la política.

También es importante mencionar que, en general, no es posible transferir una cuenta verificada a otra. Las cuentas verificadas no pueden cambiar el nombre de la cuenta o transferir esa verificación a una cuenta diferente. Y qué muchas veces la solicitud de verificación es denegada sin muchas explicaciones por parte de las plataformas.⁶

“ En muchas redes sociales es posible pedir que tu cuenta sea verificada. Esto sirve para demostrar que la cuenta es realmente tuya. ”

3.8 ¿Cómo encontrar y/o borrar la información de un celular Android perdido?

Android es un sistema operativo para celulares y otros dispositivos móviles que pertenece a Google. Debido a esto, existen herramientas como **Encontrar mi dispositivo** y el **borrado remoto**, que permiten ubicar, bloquear o borrar un celular en caso de pérdida o robo.

Encontrar mi dispositivo

Esta función permite ver la ubicación del celular en un mapa, hacerlo sonar incluso si está en silencio, y bloquearlo para evitar que otra persona lo use.

Pasos para rastrear un celular:

1. Entra a google.com/android/find desde otro celular o computadora, o busca en Google **“Encontrar mi dispositivo Android”** y selecciona el primer resultado.



6 Paz Peña (2022). Guía Práctica Contra la violencia política de género digital. Trabajo y Justicia Social.



2. **Inicia sesión con tu cuenta de Google** (debe ser la misma que usabas en el celular perdido). Es necesario recordar el correo y la contraseña.
3. Si tienes varios dispositivos, selecciona el que quieres rastrear en la parte superior de la pantalla.
4. En el mapa, aparecerá la última ubicación conocida del celular.
5. Puedes elegir entre tres opciones:
 - **Reproducir sonido:** El celular sonará por cinco minutos aunque esté en silencio.
 - **Bloquear dispositivo:** Puedes cerrar sesión en tu cuenta de Google y mostrar un mensaje en la pantalla con un número de contacto.
 - **Borrar dispositivo:** Borra toda la información del celular (esto es irreversible).



Borrado remoto

Si no se puede recuperar o rastrear el celular, esta opción permite ***BORRAR DE FORMA REMOTA TODOS LOS DATOS DEL DISPOSITIVO PARA PROTEGER LA INFORMACIÓN PERSONAL.*** Una vez hecho esto, ya no se podrá rastrear el celular con "Encontrar mi dispositivo."

Pasos para borrar un celular de forma remota:

1. Sigue los pasos anteriores para acceder a **Encontrar mi dispositivo**.
2. Selecciona la opción **"Borrar dispositivo"**.
3. Confirma la acción. El celular se restablecerá a su estado de fábrica en el momento que se conecte a internet.

Debemos tomar en cuenta que para que estas funciones sean efectivas, el celular debe estar encendido y con acceso a internet.





¿CÓMO RESPONDO A LOS ATAQUES DE ACOSO Y VIOLENCIA POLÍTICA FACILITADOS POR LA TECNOLOGÍA?

En Bolivia no existe normativa específica para responder a la violencia facilitada por la tecnología. Sin embargo, si existe normativa que protege el derecho a vivir una libre de violencia para mujeres y otros delitos penales, que se pueden usar para denunciar el acoso y violencia política facilitada por la tecnología.

4.1. Ley 243 contra el acoso y violencia política hacia las mujeres

De acuerdo a la Ley 243, las mujeres candidatas o electas y en función política pública, tienen cuatro caminos para realizar una denuncia por acoso y violencia política:

Tabla No. 7	
Vía Constitucional	• Acción de Libertad: En caso de persecución o privación de libertad como forma de amenaza. • Acción de amparo constitucional: Cuando se restringe el ejercicio actividades y derechos políticos. • Acción de protección de la privacidad: Cuando se ha vulnerado la intimidad personal, familiar o se dañado la reputación de una mujer. • Acción de cumplimiento: Cuando la Constitución Política del Estado no fue respetada.
Vía Electoral	La denuncia puede ser presentada de forma verbal o escrita por la candidata, una mujer electa o en función pública, por sus familiares, o por una persona natural o jurídica, ante la Secretaría o los Tribunales Electorales Departamentales, así como en las oficinas regionales del SERECI. Los Tribunales Electorales Departamentales tienen la obligación de brindar apoyo y asesoría legal a las personas denunciante. En este procedimiento no se requiere la presencia de una abogada ni un acta formal de denuncia. La persona denunciante solo necesita acudir a las oficinas mencionadas y realizar la denuncia de forma verbal. Esta será redactada por el Secretario de Cámara y deberá ser firmada por la persona denunciante. Además, puede solicitar protección de identidad para que su nombre no sea revelado a terceros.



Vía Administrativa	Si se conoce a la persona atacante, se puede denunciar ante la misma institución a la que pertenece la persona agresora o grupo agresor. Se buscarán sanciones administrativas o disciplinarias de acuerdo al procedimiento dispuesto en la norma vigente.
Vía Penal	Los delitos de acoso político y/o violencia política pueden ser denunciados ante la FELCV o el Ministerio Público. Si la vida de la persona agredida está en riesgo, se deben otorgar medidas de protección.

4.2. Figuras penales⁷ y reporte en plataformas contra la violencia de género facilitada por la tecnología, por tipo de violencia.

Abuso de datos personales usando TIC



Definición: Uso de las tecnologías de la comunicación e información para obtener, compartir o manipular información personal sin permiso.

Cómo reportar en las plataformas:

- **Retirar información personal de google:** Se debe entrar a la página de [soporte de Google](#) y llenar el formulario de Solicitud de retiro de información personal.
- **Formulario de infracción de privacidad:** Activar un vpn para que se rastree el IP en un país extranjero. 1) Abrir el [formulario de violación de privacidad](#) de facebook, llenar los datos que se pide con las direcciones url de las publicaciones que difunden información personal. 2) Abrir el [formulario de violación de privacidad](#) de Instagram 3) Abrir la [página de denuncia](#) de Tiktok, busca la opción de “Informar sobre un problema de privacidad o ejercer mis derechos sobre datos”, llenar el [formulario de violación a la privacidad](#) de Tiktok.
- **Suplantación y robo de identidad:** Existen formularios para denunciar una cuenta falsa que usa información personal de alguien más para hacerse pasar por la persona, a continuación se compartirá el formulario de [Facebook](#), [Instagram](#), [Tiktok](#).

7 Rivera, N (2025) Guía para acompañantes de la sociedad civil frente a casos de violencia de género facilitada por la tecnología VG FT. AGETIC. ONU MUJERES.



- **Denunciar contenido por derechos de autor:** Las herramientas para reportar derechos de autor pueden ser útiles para bajar contenido que incluya fotos personales propias que son de nuestra propiedad o autoría. Si las fotos han sido obtenidas de nuestras redes sociales o de nuestras cuentas, es importante no borrar dichas fotos. Para hacer la denuncia, se observan diferentes indicaciones en este [enlace](#). Es importante que se tome en cuenta que estas denuncias no son anónimas.

Cómo realizar una denuncia legal:

- **Suplantación y robo de identidad:** En el caso que una persona use información personal o fotos para crear una página falsa que suplante la identidad de otra persona, se puede hacer la denuncia por:
 - Artículo 198°. Falsedad material.
 - Artículo 199°. Falsedad ideológica.
 - Artículo 200°. Falsificación de documento privado.
- **Recolección y/o publicación no autorizada de datos personales:** En caso que se publique información privada o personal de una mujeres candidatas, electas, designadas o en el ejercicio de funciones político- públicas. Se puede hacer la denuncia en el marco de la ley 243 por medio de las siguientes vías.
 - **Vía Administrativa:** Cuando el o la agresora pertenezcan a una institución dependiente del gobierno, se puede hacer la denuncia en la misma institución para abrir un proceso disciplinario.
 - **Vía Penal:** Se puede denunciar bajo los artículos 148 Bis y 148 Ter ante el Ministerio Público.



Violencia sexual relacionada con las TIC



Definición: Cuando la tecnología se usa para afectar la intimidad y la seguridad de una persona de manera sexual.

Cómo reportar en las plataformas:

- **Reportar fotos o videos con contenido íntimo en redes sociales:** Entra a la publicación y busca los tres puntos que están a un costado de la publicación, busca la opción de *Reportar* y elige la opción *Creo que es ofensiva*, luego busca la opción *Desnudos o actividad sexual*
- **Reportar fotos o videos con contenido íntimo en páginas pornográficas:** Todas las páginas pornográficas tienen un servidor que les vende el espacio. Si se han publicado fotos íntimas sin consentimiento en una de estas páginas, se debe buscar la página de contacto de la página y/o las políticas de uso de la misma página. Con esta información se debe escribir una correo indicando que se es dueño de las fotos y no ha dado consentimiento para su difusión en dicha página y que se solicita que se retire la foto o video o se tomarán medidas legales por infracción de derechos de autor. Varias páginas pornográficas ya cuentan con formularios para retirar contenido que infrinjan los derechos de autor.
- **Prevenir la difusión en caso de extorsión:** En caso que las fotos no se hayan difundido, pero se esté amenazando con la difusión, se puede crear una huella Hash de la foto, para que la misma sea reconocida y retirada con rapidez, en caso que llegasen a publicarla. Existe una organización que apoyan con la creación de Huellas Hash: Crear caso en <https://stopncii.org/> (mayores de 18 años). Aplicable sólo si la persona tiene acceso a las fotos o videos íntimos. Esta herramienta aplica sólo si la persona tiene fotos o videos íntimos. Sirve para sacar una huella digital a las mismas y poder ser identificadas y bajadas rápidamente si se suben a plataformas de redes sociales (Facebook, instagram, Tik tok, bumble, onlyfans, tricks, pornhub y snap inc, click sale, red gifts, yubo)
- **Formulario de violación de la privacidad:**
 - [formulario de violación de privacidad](#) de Instagram.
 - Abrir la [página de denuncia](#) de Tiktok, busca la opción de "Informar sobre un problema de privacidad o ejercer mis derechos sobre datos", llenar el [formulario de violación a la privacidad](#) de Tiktok.



- **Formulario de infracción a los derechos de autor:** Las herramientas para reportar derechos de autor pueden ser útiles para bajar contenido que incluya fotos personales propias que son de nuestra propiedad o autoría. Si las fotos han sido obtenidas de nuestras redes sociales o de nuestras cuentas, es importante no borrar dichas fotos. Para hacer la denuncia, se observan diferentes indicaciones en este [enlace](#). Es importante que se tome en cuenta que estas denuncias no son anónimas.

Cómo realizar la denuncia:

- **Difusión de imágenes íntimas sin consentimiento:** Cuando se difunde, comparte o distribuye fotos o vídeos íntimos sin el consentimiento de la persona, se puede denunciar bajo el tipo penal de pornografía, tal como indica el **artículo 323 bis** del Código Penal de Bolivia. Es necesario tomar en cuenta que, si bien este tipo de violencia incluye imágenes editadas o generadas por IA, el tipo penal no contempla estos casos.

También se puede hacer una demanda constitucional bajo la forma de **Habeas Data** se refiere al derecho que tiene toda persona de conocer, actualizar y rectificar la información que se haya recogido sobre ella en archivos y bancos de datos, tanto públicos como privados, y de exigir su supresión o confidencialidad si la información es falsa o discriminatoria. Este mecanismo puede ser empleado para solicitar que se baje las fotos o vídeos íntimos de páginas de internet bolivianas.

- La Acción de Protección de Privacidad, también conocida como habeas data, es un recurso constitucional en Bolivia establecido en el **Artículo 130 de la Constitución Política del Estado**. Este mecanismo permite a las personas proteger sus derechos fundamentales relacionados con la privacidad, la honra, la imagen, la intimidad y la autodeterminación.



- **Sextorsión en línea:** Cuando se amenaza o se extorsiona a una persona bajo la amenaza de difundir sus fotos o videos íntimos, se puede denunciar bajo el delito de **Artículo 333. Extorsión.**
- **Afectaciones a la indemnidad sexual:** En casos de manipulación o coerción a adultas para que participen en actividades sexuales a través de TIC, aprovechándose de su vulnerabilidad o confianza, se puede hacer la denuncia bajo los siguientes tipos penales:
 - Artículo 320°. Corrupción de mayores.
 - Artículo 342°. Engaño a personas incapaces.

Acoso



Definición: Actos de acoso y violencia política basada en género mediante el uso de tecnologías de la información y la comunicación u otras herramientas digitales.

Cómo reportar en las plataformas:

- **Registrar el acoso:** Es de suma importancia que se registre los actos de acoso antes de realizar cualquier otra acción de manera que se tenga la siguiente información: Captura de pantalla, fecha y hora de publicación, nombre de cuenta o teléfono de origen, enlace url de la publicación.
- **Reportar contenido ofensivo:** Las publicaciones, mensajes, o contenidos reiterados amenazantes, ofensivos e insultantes pueden ser reportados directamente, seleccionando la opción de Reportar, que se encuentra en el ícono de tres puntos a lado de la publicación. Para mayor información, se puede usar los siguientes enlaces:
 - [Facebook.](#)
 - [Instagram.](#)
 - [TikTok.](#)
 - [Snapchat.](#)





- **Bloquear agresores:**

- En whatsapp: Elige el chat ofensivo, amenazante o intimidante y selecciona los tres puntos del costado y elige la opción Reportar, esto permitirá que Whatsapp lea los últimos 5 mensajes intercambiados y bloqueará al contacto para que no pueda mandarte nuevos mensajes.
- En redes sociales: Entra al perfil de la persona que te está acosando, busca los tres puntos a un costado. Selecciona la opción de bloquear cuenta.

Cómo realizar la denuncia:

- **Ciberacoso:** Ante el hostigamiento o intimidación de una persona a través de medios digitales, como redes sociales, mensajes de texto o correos electrónicos, con la intención de causar daño emocional o psicológico, se puede hacer la denuncia bajo los siguientes tipos penales:
 - Artículo 312 quater. Acoso sexual.
 - Artículo 272 bis. Violencia familiar o doméstica. En su vertiente de violencia psicológica.
 - Denuncia por violencia política: Tal como indica el artículo 8 de la ley 243, se considera violencia política los actos que presionen o induzcan a las autoridades electas o designadas a presentar renuncia al cargo, o que se obliguen mediante la fuerza o intimidación a las autoridades electas o designadas en el ejercicio de sus funciones político - públicas, suscribir todo tipo de documentos y/o avalar decisiones contrarias a su voluntad, al interés público o general.



- **Monitoreo y acecho:** Ante las acciones que buscan seguir de cerca las actividades en línea de una persona sin su consentimiento para controlarla o intimidarla, se puede denunciar bajo los siguientes tipos penales:
 - Artículo 271°. Lesiones graves y leves, en su vertiente de daño psicológico.
- **Coacción digital:** Ante los mensajes o comunicaciones que expresan la intención de causar daño físico, emocional o reputacional a una persona con el fin de cambiar su actitud, se puede hacer la denuncia bajo los tipos penales siguientes:
 - Artículo 333°. Extorsión.
 - Artículo 293°. Amenazas.

Acceso o control no autorizado



Definición: Cuando alguien ingresa o manipula cuentas o sistemas sin permiso.

Cómo reportar en las plataformas:

- **Reportar cuentas crackeadas o robadas:** En los casos que se pierda el acceso de una cuenta, se puede usar los siguientes enlaces para tratar de recuperarlos.
 - [Centro de ayuda Facebook.](#)
 - [Centro de ayuda Instagram.](#)
 - [Centro de ayuda Tiktok.](#)
- Una medida de precaución que puede ayudar a responder a estos ataques de forma rápida, es activar las alertas de inicio de sesión en nuestro correo o número de teléfono.
- **Recuperación de correo electrónico:** Para recuperar una cuenta robada de gmail, usa el siguiente enlace de [recuperación de cuenta.](#)



- **Eliminar cuenta de red social o contenido del dispositivo robado:** En caso que no se pueda recuperar la cuenta se reporta la cuenta hackeada como cuenta falsa que suplanta identidad con el siguiente formulario <https://www.facebook.com/help/contact/295309487309948>. También se puede rastrear, bloquear y borrar contenido del celular robado con el siguiente link <https://myaccount.google.com/find-your-phone>.

Cómo realizar la denuncia:

- **Crackeo:** Acceso no autorizado a sistemas informáticos, cuentas en servicios digitales, generalmente mediante el uso de software malicioso o técnicas de piratería.
 - Artículo 363 bis. Manipulación informática.
 - Artículo 363 ter. Alteración, acceso y uso indebido de datos informáticos.

Afectaciones de canales de expresión o Censura



Definición: Estrategias para silenciar voces en internet.

Cómo reportar en las plataformas:

- **Solicitar revisión de suspensión de cuentas:** En los casos que una cuenta haya sido suspendida se puede solicitar una revisión en los siguientes enlaces:
 - [Revisión en Facebook](#).
 - [Revisión en Instagram](#).
- **Solicitar apoyo:** Se puede solicitar apoyo a organizaciones especializadas en derechos digitales, como Access Now, en el siguiente enlace: <https://www.access-now.org/help-es/#contact-us>



Campañas de difamación y desprestigio



Definición: Estrategias para dañar la imagen de alguien a través de mentiras y ataques.

Cómo reportar en las plataformas:

- **Formularios de reporte de difamación:** Para hacer la denuncia por difamación se requiere que se guarde los enlaces url de las publicaciones difamatorias y llenar los siguientes formularios de [facebook](#) e [Instagram](#).
- **Reportar contenido difamatorio:** En tiktok, se puede denunciar contenido difamatorio entrando a la publicación difamatoria, seleccionando los tres puntos al costado, selecciona Reportar, luego selecciona Reportar Contenido ilegal, y selecciona Difamación.



Cómo realizar la denuncia:

- **Difamación:** Ante la difusión de información falsa que perjudica la reputación de una persona en plataformas digitales, blogs o correos electrónicos, se puede denunciar bajo los siguientes tipos penales:
 - Artículo 282°. Difamación.
 - Artículo 284°. Ofensa a la memoria de los difuntos.
 - Art. 285°. Propalación de ofensas.
- **Calumnia:** Ante la acusación falsa a alguien de un delito o conducta inapropiada, con la intención de dañar su honor, se puede denunciar bajo los siguientes tipos penales:



- Artículo 283°. Calumnia.
- Artículo 284°. Ofensa a la memoria de los difuntos.
- Artículo 285°. Propalación de ofensas.
- **Injuria:** Ante las publicaciones y afirmaciones o comentarios que ofenden o menoscaban el honor de una persona, generalmente a través de expresiones despectivas o insultantes en medios digitales, se puede hacer la denuncia bajo el siguiente tipo penal:
 - Artículo 287°. Injuria.

Es importante tomar en cuenta que estos delitos son de orden privado, por lo que no se requiere una investigación por parte de la fiscalía. La denuncia se presenta directamente ante el juez de sentencia, lo que significa que la persona afectada debe conocer la identidad del agresor.

“ Es importante tomar en cuenta que estos delitos son de orden privado, por lo que no se requiere una investigación por parte de la fiscalía. ”

4.3. Algunas formas de respuesta auto gestionadas para enfrentar el acoso y violencia política facilitada por la tecnología

- ✓ **No respondas al acosador:** Los agresores en línea buscan provocarte para que reacciones impulsivamente. **Ignorarlos** puede evitar que la situación empeore. **No interactuar es una forma efectiva de cortar el conflicto.**
- ✓ **Haz un pronunciamiento público si lo necesitas:** Si te sientes en peligro o crees que es importante dejar constancia, **comunica públicamente lo que está ocurriendo**. Esto puede ayudarte a **protegerte, visibilizar el problema y dejar antecedentes**.
- ✓ **Rodéate de personas de confianza:** Es clave tener un grupo de apoyo que te dé contención emocional y práctica. **Un círculo cercano te ayudará a manejar mejor lo que estás viviendo y a tomar decisiones con más claridad.**



- ✓ **Organízate con otras compañeras:** La unión hace la fuerza. **Conectarte con quienes han pasado por lo mismo** puede ayudar a crear respuestas colectivas más fuertes. **Juntas pueden denunciar e intervenir de forma más efectiva.**

- ✓ **Crea un protocolo en tu partido o grupo:** Tener un plan claro para enfrentar el acoso y la violencia política digital dentro de tu espacio político es una respuesta sólida. **Ese protocolo debe incluir pasos concretos ante cada caso y asegurar una acción coordinada.**

- ✓ **Espacios para compartir y escuchar:** Crear lugares donde se puedan contar experiencias y brindar apoyo mutuo es muy importante. **Estos espacios fortalecen la empatía y permiten construir soluciones entre todas.**

- ✓ **Acércate a organizaciones que puedan ayudarte:** Existen muchas organizaciones, locales e internacionales, que trabajan contra el acoso y la violencia política. **Pueden darte recursos, asesoría legal y respaldo. No dudes en contactarlas.**

- ✓ **No hay una sola forma de responder:** Cada caso es distinto. **Lo que sirve a una persona puede no servir a otra.** Lo importante es **adaptar las estrategias a cada situación y siempre cuidar tu seguridad y bienestar.**



“ Tener un plan claro para enfrentar el acoso y la violencia política digital dentro de tu espacio político es una respuesta sólida. ”





RECURSOS ÚTILES

En esta sección se presentan algunos tutoriales para ingresar a las opciones de configuración en distintas redes sociales, que permitirán dar mayor seguridad a las cuentas y modificar las opciones de privacidad acorde a las necesidades de cada caso; además de una estrategia para documentar posibles agresiones que puedan darse en el contexto electoral.

5.1. ¿Cómo activar la verificación en dos pasos?

Tutorial Google



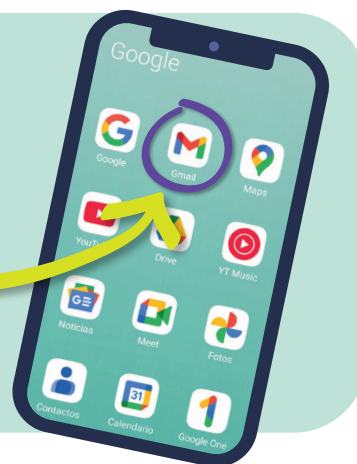
Mira el video tutorial
escaneando el QR



1 Para activar la **verificación en dos pasos** de Google primero ingresamos a la aplicación **Gmail**.

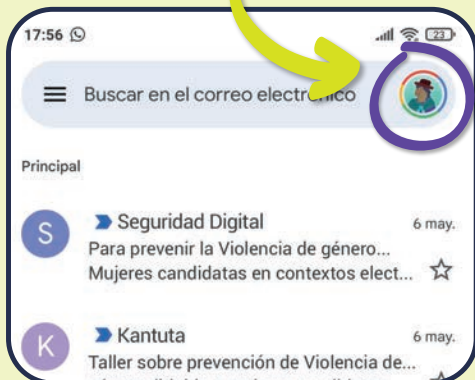
Mira el video
tutorial

La verificación en dos pasos es esencial para cuidar tu cuenta de personas que busquen acceder a ella sin tu consentimiento, recuerda que una cuenta Google es muy importante, porque muchas veces guarda información muy importante que puede permitir el acceso a más cuentas. A continuación, se indican los pasos y recomendaciones para activarla.



2

Una vez dentro de la App de **Gmail** buscamos nuestra **foto de perfil** en la esquina superior derecha e ingresamos allí.

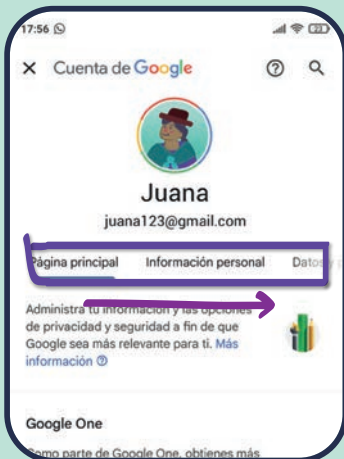


3

Veremos una pantalla con el nombre y correo, y abajo un botón de **"Cuenta de Google"** ahora ingresamos allí.

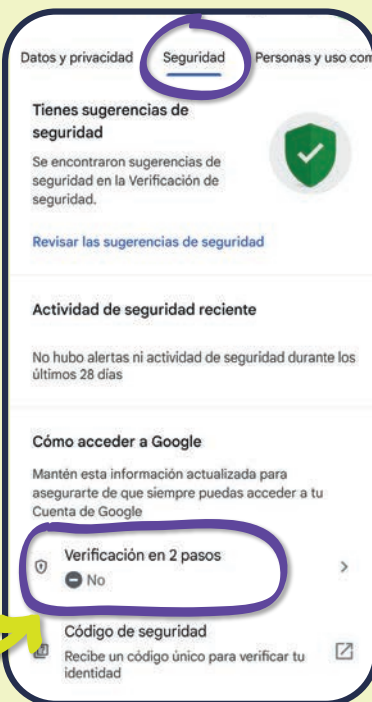
4

En la cuenta de Google veremos varias opciones. Deslizaremos hacia la derecha buscando **"Seguridad"**.



5

Una vez en la opción de **seguridad**, veremos en la parte inferior **"Verificación en 2 pasos"**



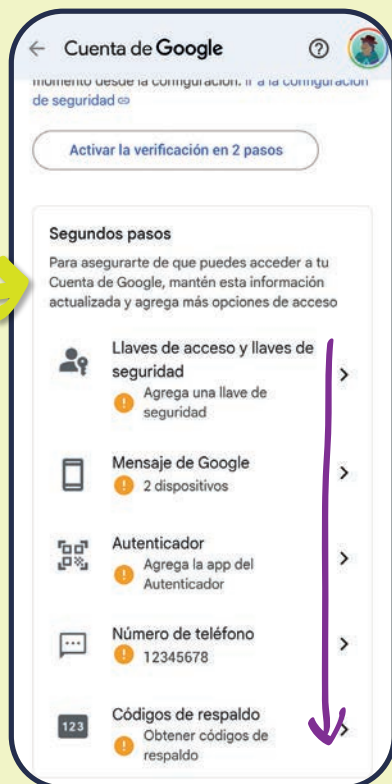
6

Una vez dentro de "Verificación en 2 pasos", deslizaremos hacia abajo para ver todas las opciones.



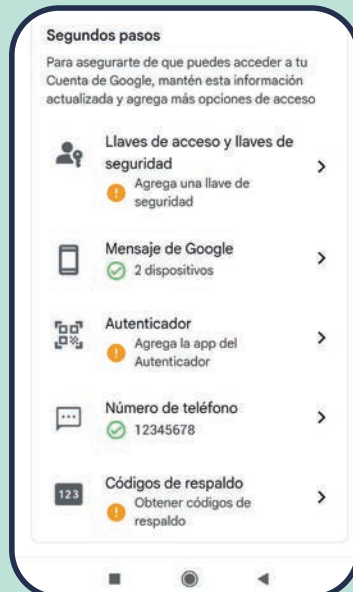
Nota. Cada una de las opciones tiene sus propios pasos a seguir.

Sigue las instrucciones que aparecen en pantalla en cada opción.



7

Se recomienda elegir al menos **dos opciones diferentes**.



8

Una vez activada tendremos una verificación y cada vez que ingresemos a la cuenta nos pedirá la contraseña y una de las opciones activadas.



Nota. Recuerda cerrar sesión de tu cuenta de google cada vez que uses un dispositivo que no es de confianza.



Tutorial Instagram

Una cuenta de Instagram suele estar vinculada a Facebook, por lo que, si una persona externa tiene acceso, es posible que tenga acceso a Facebook también, así que te recomendamos cuidar ambas cuentas con la verificación en dos pasos. Para activarla seguimos los siguientes pasos:

Mira el video tutorial escaneando el QR



1 Primero ingresamos a nuestra aplicación de **Instagram**.

Mira el video tutorial



2 En tu página de perfil presiona las **tres líneas** de la esquina superior derecha (menú de opciones).

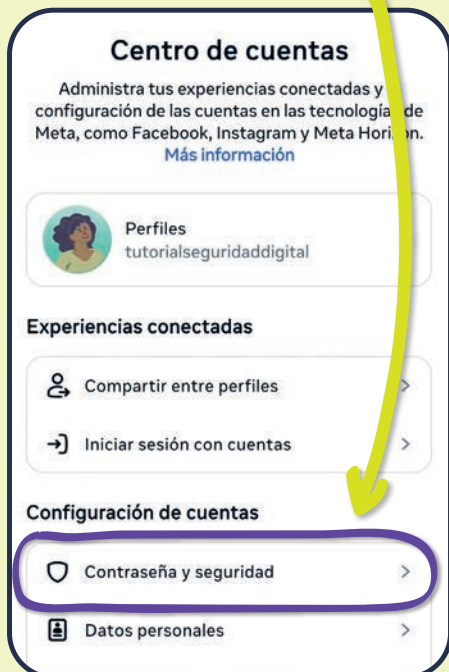


3 Ingresamos en la primera opción "**Centro de cuentas**".



4

Dentro de las opciones busca y selecciona **"Contraseña y seguridad"**.



Contraseña y seguridad

Inicio de sesión y recuperación

Administra tus contraseñas, preferencias de inicio de sesión y métodos de recuperación.

- Cambiar contraseña
- Autenticación en dos pasos**
- Inicio de sesión guardado

Controles de seguridad

Revisa los problemas de seguridad mediante comprobaciones en las apps, los dispositivos y los correos electrónicos enviados.

- Dónde iniciaste sesión
- Alertas de inicio de sesión
- Correos electrónicos recientes
- Comprobación rápida de seguridad

5

En el menú de seguridad tenemos la opción **"Autenticación en dos pasos"**. Selecciónala para continuar.

tutorialseguridaddigital • Instagram

Agrega seguridad adicional a tu cuenta

La autenticación en dos pasos protege tu cuenta con un código adicional que debes ingresar cuando inicias sesión en un dispositivo que no reconocemos. [Más información](#)

Elige un método de seguridad

- App de autenticación**
Recomendado • Te recomendaremos que descargues una app si no tienes ninguna. La app generará un código que deberás ingresar al iniciar sesión.
- SMS o WhatsApp**
Enviaremos un código al número de celular que elijas.

Siguiente

6

Elige la opción de tu preferencia y selecciona **"Siguiente"** para continuar.

Sigue las instrucciones que aparecen en pantalla en cada opción.



7

Una vez **activada** nuestra autenticación de dos pasos, tendremos esta notificación.



Tutorial Facebook

La verificación en dos pasos es esencial para cuidar tu cuenta de personas que busquen acceder a ella sin tu consentimiento. Para activar la verificación en dos pasos de Facebook seguimos los siguientes pasos:

Mira el video tutorial
escaneando el QR

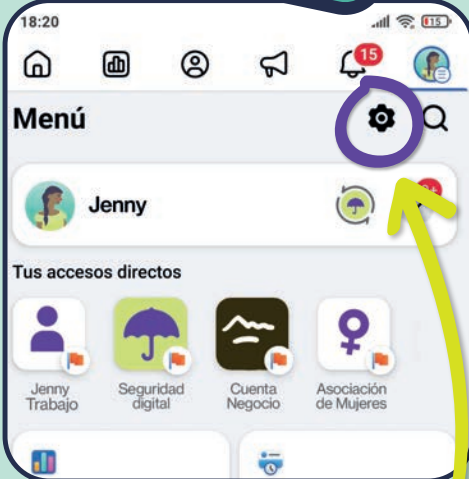


1 Primero ingresamos a
nuestra aplicación de
Facebook.

Mira el video
tutorial



2 Dentro de la aplicación de Facebook
encontraremos **tres líneas o una
pequeña** bajo la foto de perfil,
entramos ahí.

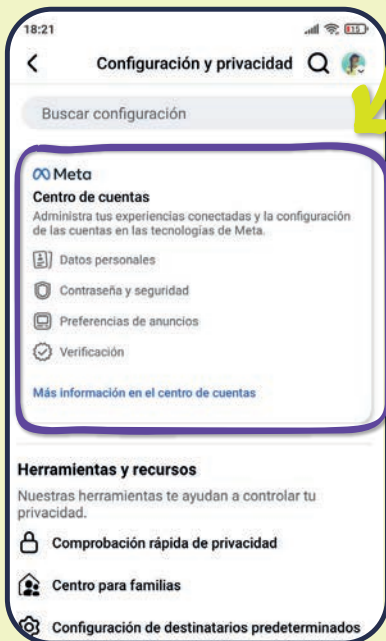


3 En este apartado, en la esquina superior
derecha veremos el ícono (tuerca) de
configuraciones e ingresamos allí.



4

Dentro de las configuraciones lo primero que veremos es el **Centro de Cuentas de Meta** e ingresamos allí.



5

Dentro del Centro de Cuentas veremos la configuración de cuentas y allí está **"Contraseña y seguridad"**.



6

En Contraseña y seguridad ingresamos a **Autenticación en dos pasos**



Autenticación en dos pasos

Elige una cuenta para configurar la autenticación en dos pasos.



7

Dentro de **Autenticación en dos pasos** veremos una lista de cuentas, elegiremos la que queramos configurar.



8

Cuando actives la autenticación en dos pasos, se te solicitará que elijas uno de los tres métodos de seguridad, **se recomienda activar al menos una**.

Sigue las instrucciones que aparecen en pantalla.



Nota. Cuando actives la autenticación en dos pasos se te pedirá que guardes el navegador o el dispositivo móvil que estás usando, para poder ingresar directamente a tu cuenta.

No hagas clic en **Guardar este navegador** si estás usando una computadora pública a la que otras personas pueden acceder.

Cómo obtener códigos de inicio de sesión

SMS o WhatsApp

Enviaremos un código al *****42. >

Métodos adicionales

Consulta cómo iniciar sesión de forma segura aunque los otros métodos no estén disponibles. >

Agrega un método de respaldo

App de autenticación

Recomendado • Te recomendaremos que descargues una app si no tienes ninguna. La app generará un código que deberás ingresar al iniciar sesión. >

Llaves de seguridad

Usa llaves de seguridad físicas para proteger tu cuenta del acceso no autorizado. Tendrás que tener esta llave contigo para iniciar sesión desde un dispositivo no reconocido. >



Mira el video tutorial escaneando el QR

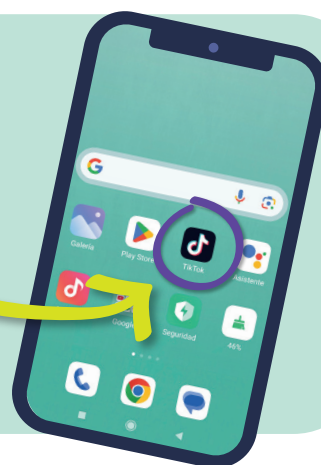


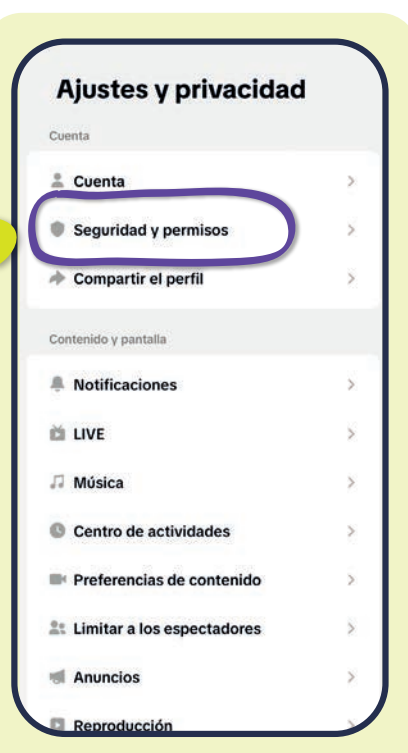
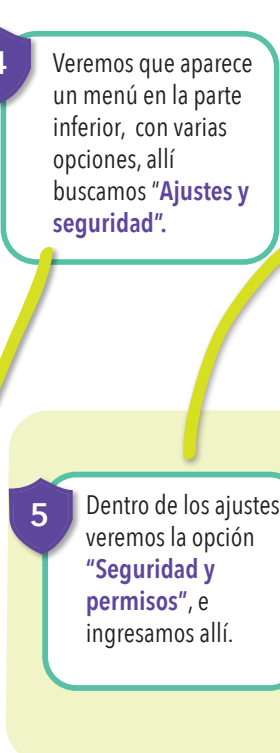
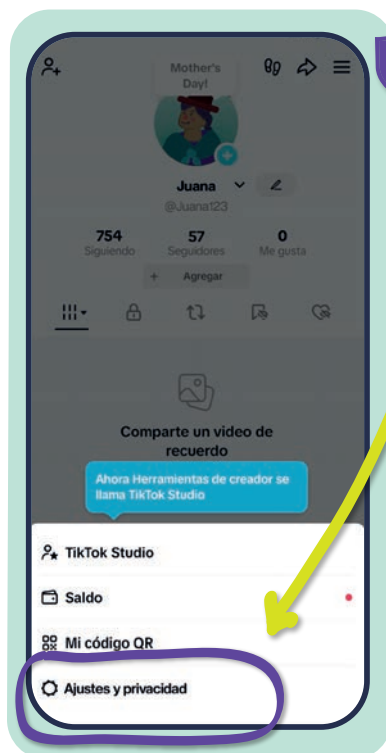
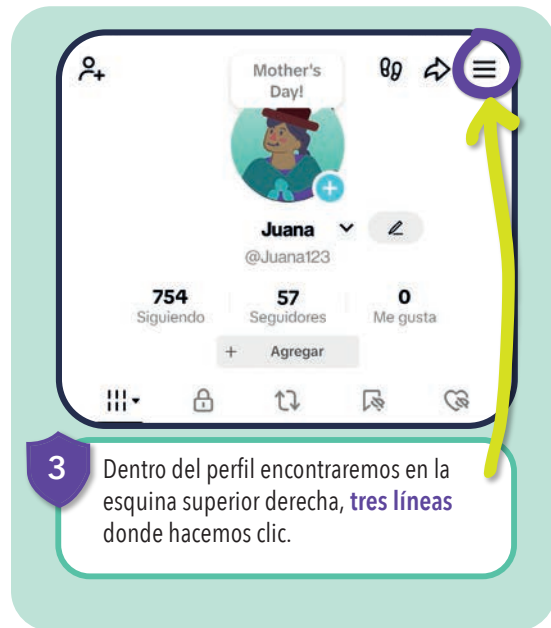
1

Para activar la **verificación en dos pasos** primero ingresamos a la aplicación **Tik Tok**.



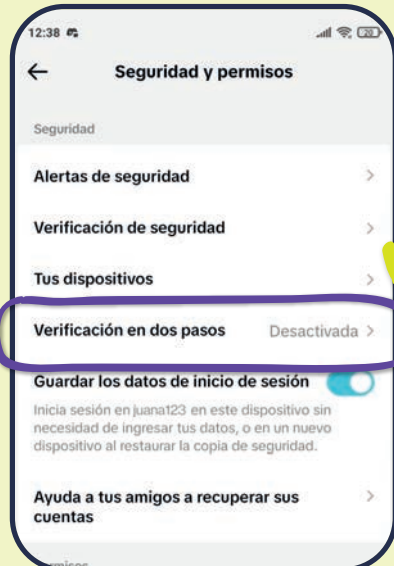
Mira el video tutorial





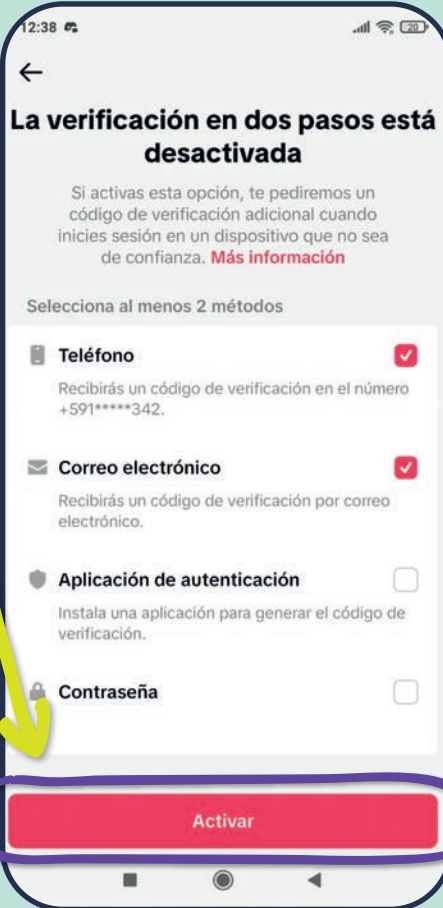
6

Aquí encontraremos el apartado de **"Verificación en dos pasos"**, como vemos esta desactivada.



7

En esta sección podemos ver varias opciones para configurar la verificación. **Seleccionamos al menos una y pulsamos activar.**



La verificación en dos pasos está activa

Si activas esta opción, te pediremos un código de verificación adicional cuando inicies sesión en un dispositivo que no sea de confianza. **Más información**

Métodos de verificación

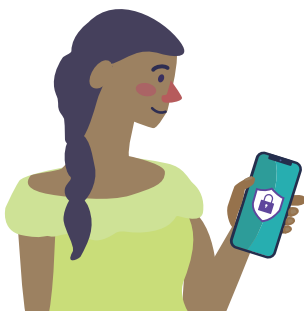
- ☒ **Teléfono** * Activado >
Recibirás un código de verificación en el número +591*****342.
- ☒ **Correo electrónico** * Activado >
Recibirás un código de verificación en la dirección j*****3@gmail.com
- ☒ **Aplicación de autenticación** * Activado >
Consulta la aplicación de autenticación para ver el código de verificación.
- ☒ **Contraseña** * Activado >

8

Una vez configurados todos los pasos y luego de presionar activar, veremos que todas las opciones seleccionadas aparecen como **activado**.



5.2. Configuraciones de privacidad en Facebook



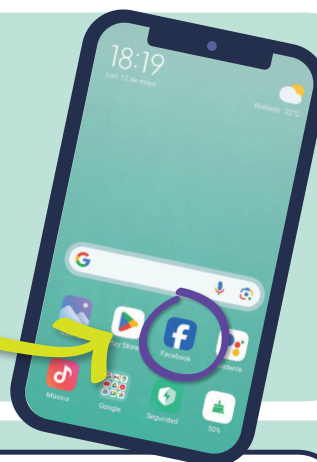
Dentro de las configuraciones de privacidad tenemos muchas opciones, es importante que sean revisadas a profundidad para encontrar la mejor forma de configurar para cada caso particular. Para revisar las configuraciones de privacidad en Facebook seguimos los siguientes pasos:

Mira el video tutorial
escaneando el QR

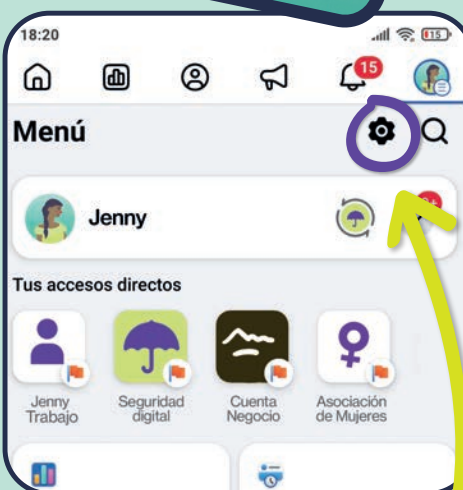


1 Para revisar las **configuraciones de privacidad** el primer paso es ingresar a nuestro **Facebook**.

Mira el video tutorial



2 Dentro de la aplicación de Facebook encontraremos **tres líneas o una pequeña** bajo la foto de perfil, entramos ahí.

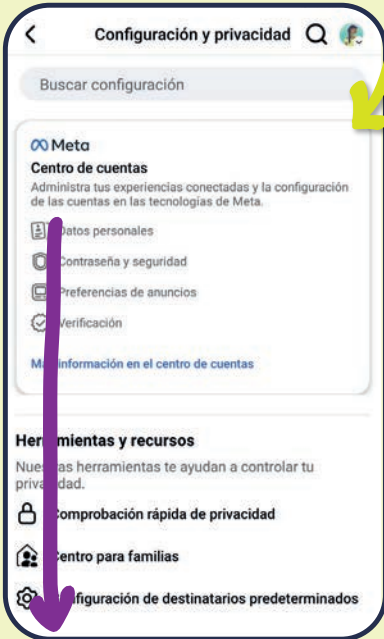


3 En este apartado, en la esquina superior derecha veremos el ícono (tuerca) de **configuraciones** e ingresamos.



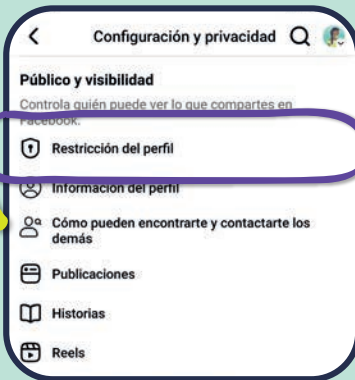
4

Dentro de las configuraciones deslizaremos hacia abajo buscando la opción llamada **"Público y privacidad"**



5

Restringir el perfil nos ayudará a que personas que no son contactos no puedan ver nada del perfil.



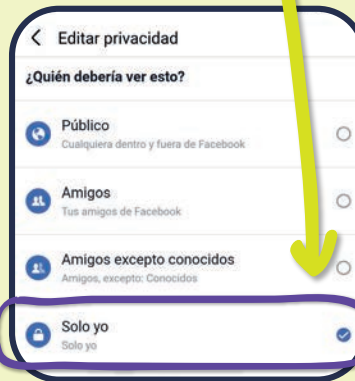
6

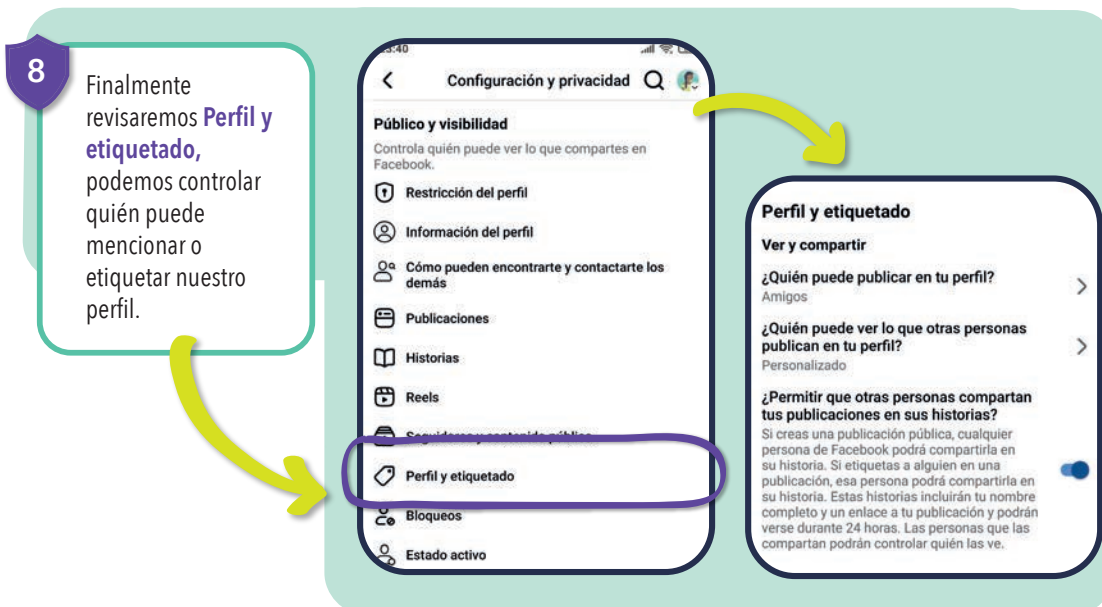
En la **información del perfil** debemos cambiar toda la información que no queramos que sea visible a **"sólo yo"**.



7

En **cómo pueden encontrarte y contactarte los demás**, podemos cambiar quién nos puede enviar mensajes y solicitudes de amistad.

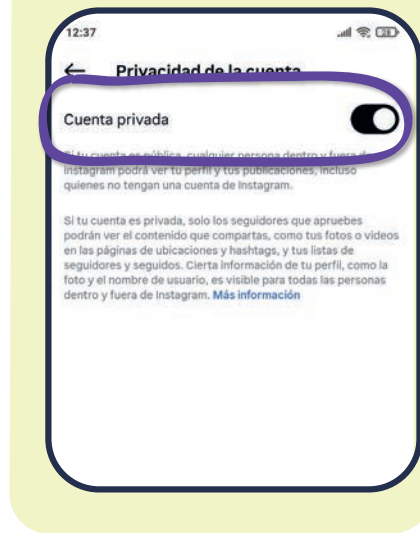
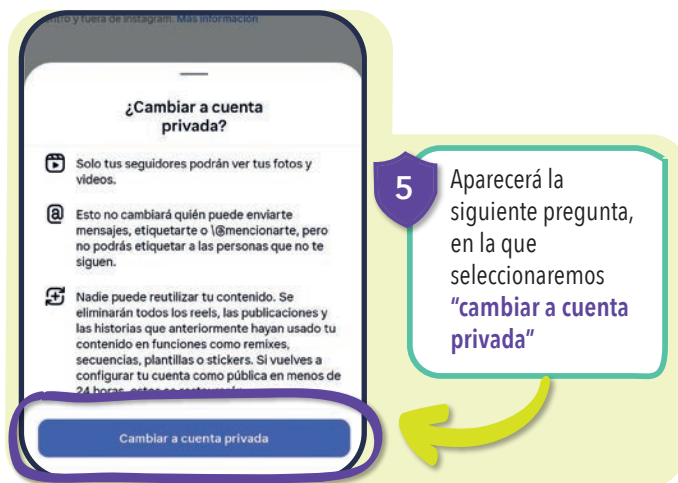
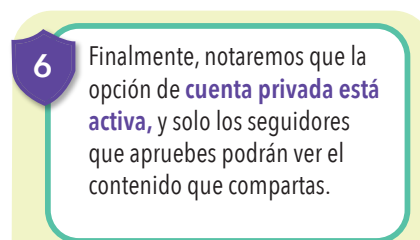
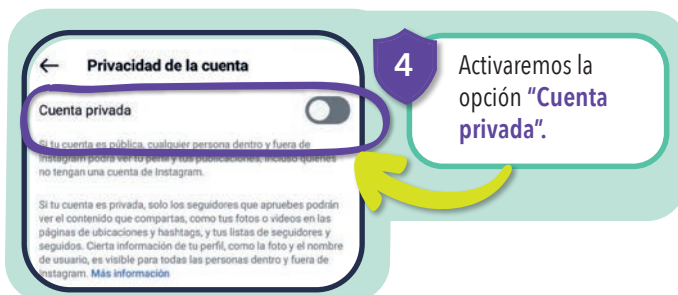
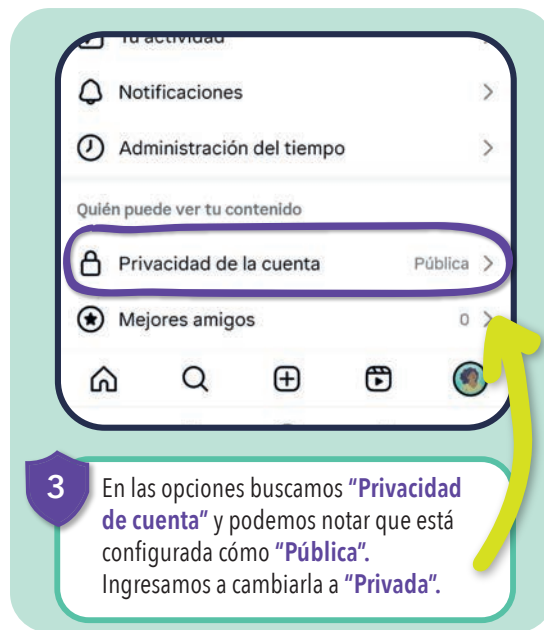




5.2.1. Configuraciones de privacidad en Instagram

En el caso de Instagram, es recomendable tener una cuenta privada, pero también es posible revisar qué publicaciones son visibles, así como las historias e información del perfil. Para revisar las configuraciones de privacidad en esta red seguimos los siguientes pasos:







5.2.2. Configuraciones de privacidad en Tik Tok

En Tik Tok las opciones de privacidad son más limitadas, pero de la misma forma tienes la opción de colocar la cuenta como privada y de crear contenido exclusivo para personas que paguen una suscripción, ocultar publicaciones, comentarios y restringir los mensajes. Para revisar las configuraciones de privacidad en Tik Tok seguimos los siguientes pasos:

Mira el video tutorial
escaneando el QR



1

Para empezar, ingresaremos a nuestra aplicación de **Tik Tok**.

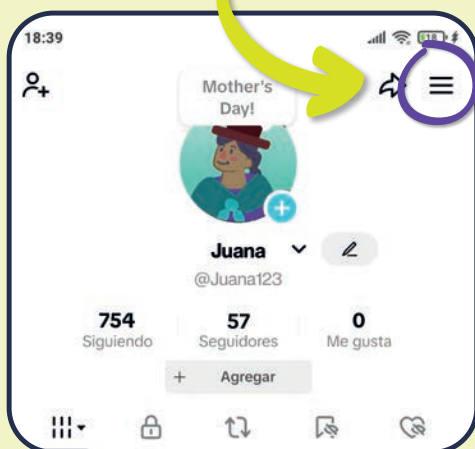


Mira el video
tutorial



2

Dentro de la aplicación ingresamos a nuestro **perfil**. Allí veremos tres líneas en la parte superior, las cuales seleccionaremos.



Comparte un video de
recuerdo

Ahora Herramientas de creador se
llama TikTok Studio

TikTok Studio

Saldo

Mi código QR

Ajustes y privacidad

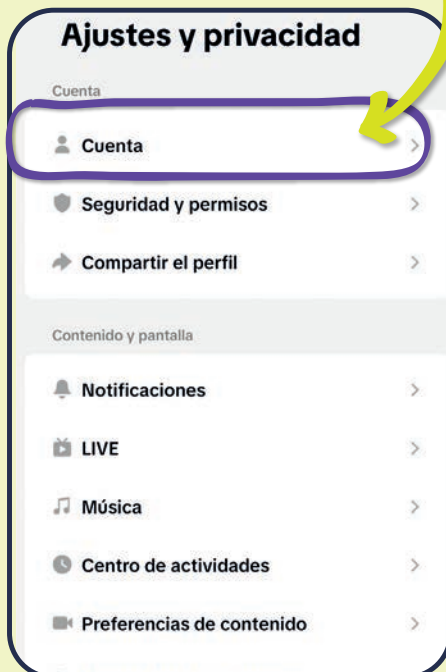
3

Aparecerán algunas opciones,
seleccionamos "**Ajustes y privacidad**".



4

Dentro de ajustes y privacidad ingresamos a la opción **"Cuenta"**.



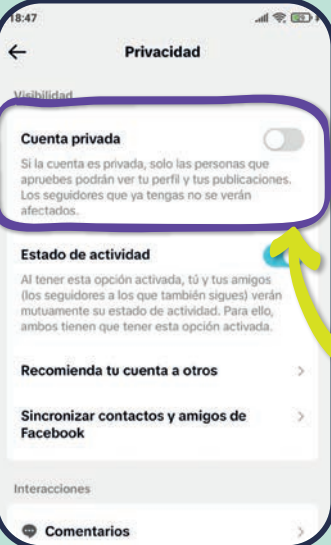
18:47

Cuenta



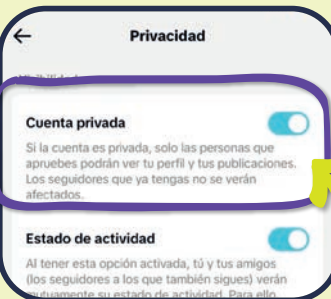
5

En el menú de cuenta buscamos y seleccionamos la opción **"Privacidad"**.



6

Observaremos que la opción de **"Cuenta privada"** está desactivada, por lo que procederemos a activarla al seleccionarla.



7

Finalmente veremos que la opción de **"Cuenta privada"** se activará. Ahora solo los usuarios que tu apruebes podrán ver el contenido que compartas.



5.3. Documentación de agresiones en contextos de violencia de género facilitada por la tecnología en procesos electorales⁸

La documentación consiste en crear un registro detallado con enlaces, fechas, capturas de pantalla y descripciones de incidentes de violencia de género ocurridos en plataformas tecnológicas durante procesos electorales. Este registro ayuda a entender la situación, guardar evidencia, medir la gravedad de los hechos y generar información útil para investigaciones, análisis de tendencias y visibilización de esta violencia en el contexto electoral.

La forma más común de hacerlo es usando hojas de cálculo. A continuación, se indican algunos campos esenciales que deben ser registrados:

Campos recomendados para la documentación:

- Fecha de inicio: El momento en que se produce el primer incidente.
- Descripción del ataque: Detalles sobre el tipo de violencia (acoso, difamación, amenazas, etc.).
- Medio por el cual se realizan los ataques: Plataformas o canales utilizados (redes sociales, correos electrónicos, mensajes directos, etc.).
- Información del agresor (si se conoce): Detalles sobre la identidad del agresor o los posibles sospechosos.
- Registros visuales de la agresión: Capturas de pantalla o grabaciones de los incidentes.
- Enlaces a los perfiles y publicaciones: Direcciones web que enlacen directamente al contenido ofensivo.
- Observaciones: Cualquier otro dato relevante o contexto sobre el ataque.

8 <https://acoso.online/site2022/wp-content/uploads/2020/09/documentacion-difusion-de-imagenes.pdf>



Modelo de ejemplo para la documentación

Fecha de inicio	Descripción del ataque	Medio por el cual se realizan los ataques	Información sobre los posibles agresores	Registros visuales	Enlaces recabados	Observaciones



Esperamos que esta guía se convierta en una herramienta para las mujeres políticas y que, en un contexto altamente polarizado y confrontacional, fortalezca sus capacidades de autoprotección, les permita alzar la voz y mantener su participación en la vida política.



Esperamos que esta guía sea útil



FRENTE A LA VIOLENCIA DIGITAL,
NOS ORGANIZAMOS.



ESCRÍBENOS A LA LÍNEA DE APOYO

+591 **62342430**



Signal



Telegram



WhatsApp



RECIPE

Recentring The Civic Internet
Through Partner Engagement



Cofinanciado por
la Unión Europea



INTERNET
BOLIVIA
.ORG



OXFAM