Manual práctico para la prevención, denuncia y protección de las mujeres políticamente activas ante la violencia política digital

ASOCIACIÓN NACIONAL DE REGIDORAS, SÍNDICAS Y ALCALDESAS SALVADOREÑAS

EQUIPO DE DIRECCIÓN Y COORDINACIÓN:
Dirección y coordinación: Junta Directiva y equipo técnico de Andrysas
Equipo consultor: Laura Nathalie Hernández, Ana Cristina Castaneda y Domingo Flores Arriaza

El Manual práctico para la prevención, denuncia y protección de las mujeres políticamente activas ante la violencia política digital ha sido desarrollado por la Asociación Nacional de Regidoras, Síndicas y Alcaldesas Salvadoreñas (ANDRYSAS), con el apoyo del Instituto Nacional Demócrata (NDI), en el marco del Consorcio para el Fortalecimiento de Procesos Electorales y Políticos (CEPPS) y el soporte de la Agencia de los Estados Unidos para el Desarrollo Internacional (USAID), la Entidad de las Naciones Unidas para la Igualdad de Género y el Empoderamiento de las Mujeres (Onu Mujeres) y la Embajada de Canadá en El Salvador.

ANDRYSAS es una asociación pluralista de mujeres funcionarias y ex funcionarias municipales, que promueve una participación creciente y sostenida de mujeres en los Concejos Municipales, el empoderamiento de sus capacidades y su desempeño.

Agradecimientos especiales para las mujeres políticamente activas que brindaron sus aportes desde su experiencia acerca de la situación de violencia que enfrentan a través de las redes sociales y medios digitales. Imagen de portada generada con AI por ImageFusion.

Contenido

Acrónimos

CE: Código Electoral

Centros de llamadas 126: Número telefónico de ISDEMU que proporciona información, orientación e intervención oportuna cuando lo requieran y demanden en cualquier parte del territorio nacional

Convención de Belém do Pará: Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia en contra de la Mujer

FGR: Fiscalía General de la República

ISDEMU: Instituto Salvadoreño para el Desarrollo de la Mujer

LEDIC: Ley Especial contra los Delitos Informáticos y Conexos

LEIV: Ley Especial Integral para una Vida Libre de Violencia para las Mujeres

LIE: Ley de Igualdad, Equidad y Erradicación de la Discriminación contra las Mujeres

OJ: Órgano Judicial

PNC: Policía Nacional Civil

Plataforma 126 Te Orienta: Espacio virtual de ISDEMU en el cual se brinda orientación, apoyo psicológico y social y asesoría legal a mujeres en situaciones de vulnerabilidad

TIC: Tecnología de la información y comunicación

TSE: Tribunal Supremo Electoral

Introducción

La Asociación Nacional de Regidoras, Síndicas y Alcaldesas Salvadoreñas (Andrysas) con el apoyo del Instituto Nacional Demócrata (NDI), en el marco del Consorcio para el Fortalecimiento de Procesos Electorales y Políticos (CEPPS), con el soporte de la Agencia de Estados Unidos para el Desarrollo Internacional (USAID), Onu Mujeres y la Embajada de Canadá, han elaborado el presente "Manual práctico para la prevención, denuncia y protección de las mujeres políticamente activas frente a la violencia política digital" con el objetivo de brindar una herramienta práctica que contribuya a la prevención y protección de las mujeres ante los ataques o manifestaciones de violencia que reciben a través de las redes sociales y medios digitales.

La violencia política digital contra las mujeres es una modalidad de agresión ejercida mediante el uso de las tecnologías de la información y las comunicaciones (TIC 's) y dirigida principalmente hacia mujeres que desempeñan roles activos en la esfera pública, como políticas, activistas y lideresas.

En un informe presentado por Andrysas en mayo del presente año sobre la "Violencia hacia mujeres políticamente activas en el proceso electoral 2024", se evidenció que las redes sociales, los medios digitales y, en general, las TIC's son utilizadas como un arma política contra el ejercicio de los derechos políticos de las mujeres, con el propósito de desincentivar y deslegitimar su participación como candidatas tanto en las elecciones internas de los partidos políticos como en las elecciones generales del país.[1] [2]

Instituciones como ONU Mujeres y el Consejo de Derechos Humanos subrayan que este tipo de violencia no solo refleja las desigualdades de género preexistentes, sino que también contribuye a intensificarlas. A pesar de que la tecnología puede actuar como una herramienta para el empoderamiento de las mujeres, su uso indebido genera barreras significativas que afectan su participación plena y segura en espacios públicos y privados.

En este contexto, el manual se presenta como una herramienta que describe la conceptualización de la violencia política digital, las medidas de seguridad y privacidad, medidas de prevención y medidas de reacción ante los ataques de violencia política, así como los mecanismos de denuncia en las plataformas digitales y las instituciones nacionales competentes en el abordaje de la violencia contra las mujeres.

1. *Andrysas. Informe sobre la violencia en contra de mujeres políticamente activas en El Salvador. Observación de violencia a mujeres políticamente activas en las elecciones internas en 2023;*
2. *Andrysas. Observatorio de violencia contra las mujeres políticamente activas en El Salvador 2023-2024. Balance General: elecciones del 3 de marzo de 2024.*

Objetivo del manual

El propósito de este manual es ofrecer a las mujeres una herramienta de apoyo orientada a la protección y prevención frente a los ataques y manifestaciones de violencia política digital.

Asimismo, busca constituirse en un recurso informativo que aborde conceptos relacionados con la violencia política digital, proporcionando además herramientas prácticas para su identificación, prevención y denuncia en las diversas plataformas digitales disponibles en Internet.

Este manual se presenta como una guía accesible, práctica e informativa, diseñada para brindar asistencia a mujeres que desempeñan cargos de responsabilidad pública o comunitaria en El Salvador, contribuyendo así a su empoderamiento y seguridad en el ámbito digital.

Glosario[3]

Sextorsión: es una forma de amenaza o chantaje mediante el uso de imágenes, videos o información sexual de la víctima como herramienta de coerción.

Ciberacoso: es la intimidación, amenaza o abuso repetido a través de las TIC's como redes sociales, mensajes de texto o correos electrónicos.

Difusión de material o contenido íntimo sin consentimiento: consiste en compartir o difundir imágenes o videos íntimos y sexualmente explícitos de una persona, sin su consentimiento, con el objetivo de humillar, intimidar.

Acoso sexual y de género en línea: son aquellas conductas no deseadas de índole sexual o basadas en el género que se llevan a cabo a través de las TIC's plataformas digitales. Por ejemplo, mensajes ofensivos, imágenes explícitas o comentarios degradantes.

Campañas de desinformación o difamación: consiste en la propagación de noticias falsas o manipuladas, o contenido difamatorio para dañar la reputación y credibilidad de la víctima.

Ciberhostigamiento: es un tipo de ciberacoso más prolongado y dirigido que implica un patrón de intimidación persistente, diseñado para causar miedo o angustia emocional.

Doxing: es la publicación de información personal o confidencial de una persona (por ejemplo: dirección, teléfono, documentos de identidad) sin su consentimiento, con el fin de hostigar o intimidar.

Discurso de odio: comentarios, publicaciones o contenido que incitan a la violencia o discriminación contra individuos o grupos basados en raza, religión, género, orientación sexual, entre otros.

Suplantación de identidad: consiste en hacerse pasar por otra persona en Internet con fines de fraude, acoso o manipulación.

Phishing: es una forma de fraude en la que se utiliza correos electrónicos, sitios web o mensajes falsos para engañar a las personas para que compartan datos personales o financieros, o instale software malicioso

Astroturfing o campañas coordinadas: se caracterizan por la organización y ejecución en masa de "campañas" o "estrategias" acordadas para atacar a una persona, publicación, asociación o página web. Estos ataques son concertados dentro de grupos cerrados, los agresores utilizan perfiles falsos y planean distintas actividades de acoso, que pueden incluir llamadas telefónicas, visitas a domicilio, denuncias policiales o la baja de sus perfiles.

Deepfakes o contenidos sintéticos: son contenidos falsos (videos, audios, fotos) creados o alterados usando inteligencia artificial, y que muestran a una persona expresando algo que no dijeron o hicieron en realidad.

---

3. *Glosario elaborado a partir de conceptos tomados de varias referencias, tales como: Plataforma del Proyecto "acoso.online"; Publicaciones de la organización "Hiperderecho"; Informes de la organización UNODC; Manual sobre violencia en línea de "Pen America". Disponible en: https://onlineharassmentfieldmanual.pen.org/es/violencia-en-linea-glosario/*

Menú Hamburguesa: se le llama de esta manera al ícono que representa en la interfaz de usuario la ubicación de un menú de opciones o de configuración. Se representa con este logo: ☰ y es parte del diseño de aplicaciones de varios tipos incluyendo apps móviles de redes sociales.

URL: Abreviatura en inglés de Universal Resource Alocator, se puede traducir cómo "Localizador Universal de Recursos". Coloquialmente les llamamos "links", y son las direcciones de las páginas web. Compuestas por el nombre de dominio y la ruta, por ejemplo, en la URL www.google.com/docs el dominio sería www.google.com y la ruta sería "/docs".

Autenticación o Verificación en dos pasos: es un método de verificar que una persona usuaria de un sistema sea realmente quien dice ser al solicitarle dos piezas de identificación de diferentes tipos antes de autorizar acceder al sistema o sus recursos. Generalmente los tipos de identificación son: un secreto (por ejemplo, una contraseña o PIN), un objeto cómo una llave o código de un sólo uso, y una identificación biométrica. Se le llama verificación en dos pasos cuándo el método de verificación contiene al menos dos de estos tres tipos de identificación.

Llave de Hardware: un dispositivo similar a una memoria USB que se utiliza para almacenar exclusivamente datos de autenticación para una persona usuaria de algún sistema. Estos dispositivos funcionan de manera similar a llaves, pues requieren interactuar con el sistema (generalmente siendo conectados a un puerto USB o vía Bluetooth o NFC) a un sistema para identificar a su usuario. Estas llaves suelen utilizarse como parte de un mecanismo de verificación de dos pasos.

Hackear/Hacking: coloquialmente conocemos como hackear a la práctica de vulnerar los mecanismos de protección de una cuenta o un recurso digital para hacer uso de él sin autorización, alterar su integridad, o inhibir su disponibilidad.

Gestores de Contraseñas: son aplicaciones cuya utilidad es almacenar de manera segura las credenciales de las personas usuarias, protegiéndolas con criptografía fuerte. También funciona como una manera eficaz de no memorizar ni reutilizar una gran cantidad de contraseñas, pues basta conocer la clave maestra con la que se protegen las demás credenciales para acceder a ellas.

Cifrado de Extremo a Extremo (también llamado Cifrado de punto a punto, o "E2E"): es una técnica que protege los datos comunicados entre dos partes, asegurándose que solamente los participantes en una conversación puedan leer el contenido de los mensajes. El cifrado se diseña de tal manera que sea casi imposible aún para una computadora el romper la clave y acceder a los datos que se transmiten entre las personas participantes.

Identidad Inferida: se le llama así al resultado de determinar relaciones entre diferentes tipos de datos con los que interactuamos (por ejemplo: anuncios, fotos en RRSS, publicaciones, etc) con el fin de identificar de manera individual a la persona usuaria. A pesar de que la identidad inferida no recaba datos sensitivos cómo identificación nacional, pasaporte, u otros, es posible identificar a una persona al cruzar estos datos de identidad inferida con otras fuentes de datos (por ejemplo, datos de la red celular) para identificar a una persona.

Qué es la violencia política digital

Al referirnos a la violencia política digital contra la mujer, estamos relacionando dos modalidades de violencia específicamente ejercida por razones de género: la violencia política y la violencia digital.

La violencia política dirigida a la mujer son todas aquellas acciones u omisiones que pretenden excluir por razón de género y, como resultado de estas, generar un daño individual o colectivo que menoscaba o anula el reconocimiento, goce y ejercicio de sus derechos políticos y civiles en cualquier ámbito de la vida política.[4]

La violencia digital o violencia facilitada por las tecnologías en contra la mujer es todo acto de violencia contra la mujer por razón de género, mediante el uso de tecnologías de la información y la comunicación, tales como, teléfonos móviles y los teléfonos inteligentes, Internet, plataformas de medios sociales o correo electrónico.

En una sociedad cada vez más conectada digitalmente, una de las problemáticas más alarmantes es la violencia digital o violencia de género facilitada por la tecnología, la cual se manifiesta, potencia, agrava o amplifica a través del uso de TIC's y otras herramientas digitales.[5] Al ejercerse a través de medios digitales como las redes sociales, correos electrónicos, mensajes de texto, u otras plataformas en línea puede adoptar diversas formas, por ejemplo, acoso en línea, ciberacoso, ofensas, sextorsión, y distribución no consensuada de imágenes íntimas, discurso que incita al odio; deslegitimación haciendo referencia a su cuerpo, conocimiento, o experiencia en la política; difamación; amenazas; intimidación o troleo; rastreo o vigilancia a través de redes sociales, entre otras.

De conformidad con nuestra legislación,[6] al ejercer violencia digital pueden ocurrir 3 tipos de violencia:

1. **Violencia Psicológica y Emocional:** es toda conducta directa o indirecta que ocasione daño emocional, disminuya el autoestima, perjudique o perturbe el sano desarrollo de la mujer; ya sea que esta conducta sea verbal o no verbal, que produzca en la mujer desvalorización o sufrimiento, mediante amenazas, exigencia de obediencia o sumisión, coerción, culpabilización o limitaciones de su ámbito de libertad, y cualquier alteración en su salud que se desencadene en la distorsión del concepto de sí misma, del valor como persona, de la visión del mundo o de las propias capacidades afectivas, ejercidas en cualquier tipo de relación.

4. *La normativa salvadoreña reconoce la violencia política en el artículo 10 de la LEIV; y la LEDIC hace referencia al acoso a través de las TIC's como una forma de intimidación haciendo uso de tecnologías digitales (artículo 32).*
5. *UN Women. Technology-facilitated violence against women.*
6. *Art. 9 de la Ley Especial Integral para una Vida Libre de Violencia de El Salvador.*

2. **Violencia sexual:** es toda conducta que amenace o vulnere el derecho de la mujer a decidir voluntariamente su vida sexual, comprendida en ésta no sólo el acto sexual sino toda forma de contacto o acceso sexual, genital o no genital, con independencia de que la persona agresora guarde o no relación conyugal, de pareja, social, laboral, afectiva o de parentesco con la mujer víctima
3. **Violencia simbólica:** Son mensajes, valores, iconos o signos que transmiten y reproducen relaciones de dominación, desigualdad y discriminación en las relaciones sociales que se establecen entre las personas y naturalizan la subordinación de la mujer en la sociedad.

En los siguientes apartados hemos preparado recomendaciones para que puedas configurar tu seguridad y privacidad como medida para la prevención de la violencia política digital, o tomes acción frente a la violencia política digital y conozcas paso a paso cómo denunciar en redes sociales o plataformas digitales.

Medidas de seguridad y privacidad

Las redes sociales y aplicaciones de mensajería, tales como Facebook, Instagram, WhatsApp, TikTok, y Equis(X), antes Twitter, ofrecen diferentes configuraciones de seguridad para proteger las cuentas, sin embargo, a menudo estas configuraciones no están activadas por defecto y no se incentiva o instruye a la persona usuaria a activarlas. Adicionalmente, estas plataformas usualmente tienen configuraciones que permiten controlar algunas de sus funciones comúnmente utilizadas en actividades de acoso y hostigamiento.

En este apartado se muestra cómo habilitar estas configuraciones para proteger su seguridad y privacidad, además de gestionar el riesgo de potenciales ataques de acoso y hostigamiento.

Se han clasificado estas configuraciones y medidas en dos grupos:

- Medidas de Prevención
- Medidas de Recuperación

MEDIDAS DE PREVENCIÓN Y MEDIDAS DE REACCIÓN

Las medidas preventivas son acciones y cambios en las configuraciones de las cuentas y de las RRSS que hacemos para gestionar el riesgo de sufrir un incidente de violencia digital, y tratar de atenuar las consecuencias si perdemos acceso a nuestras cuentas en plataformas digitales.

Las medidas reactivas, son acciones que iniciamos una vez sufrimos el incidente, con el objetivo de recuperar, en la medida de lo posible, el acceso y operación normal de nuestras cuentas, o en su defecto reducir lo más posible el daño que pueda causar el incidente en nuestras vidas.

MEDIDAS DE PREVENCIÓN

Protege tu cuenta

Configura la privacidad y seguridad de tus cuentas.

Identifica en la plataforma los botones para acceder a los ajustes o configuración. Suelen estar en los menús de hamburguesa, opciones, o configuración representados por estos íconos:

También son accesibles a través de una URL específica que puedes abrir ya sea en una computadora (que es lo recomendable) o en tu dispositivo móvil.

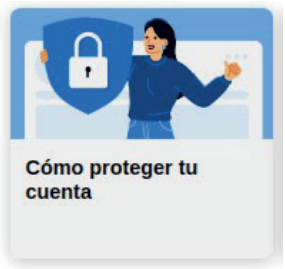
Facebook / Instagram

Autenticación en dos pasos y ajustes de privacidad

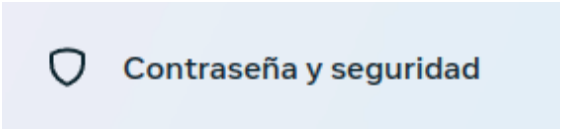
La verificación en dos pasos consiste en que, para iniciar sesión en un dispositivo nuevo, es necesario un código de un sólo uso contenido en una app gestora de contraseñas. Las alertas de inicio de sesión envían una notificación vía email o notificación push a un dispositivo de confianza cada vez que se inicia sesión en un dispositivo nuevo.

Los ajustes de seguridad en Facebook se encuentran en el asistente que podemos encontrar en el link: https://www.facebook.com/privacy/checkup/

Recuerda que, si vinculas tu cuenta de Instagram o Threads con tu cuenta de Facebook, puedes aplicar estos ajustes de seguridad y privacidad a ambas cuentas en el centro de cuentas.



En la sección “cómo proteger tu cuenta” de Facebook encontrarás el asistente para activar la verificación en dos pasos, y las alertas de inicio de sesión. El asistente te llevará al centro de cuentas, en dónde debes ir a la sección “contraseña y seguridad”.



Códigos de recuperación

Los códigos de recuperación son un mecanismo para recuperar acceso a tu cuenta en caso de que pierdas tu contraseña o los dispositivos que utilizas para la verificación en dos pasos. Selecciona “métodos adicionales” y genera códigos de recuperación.

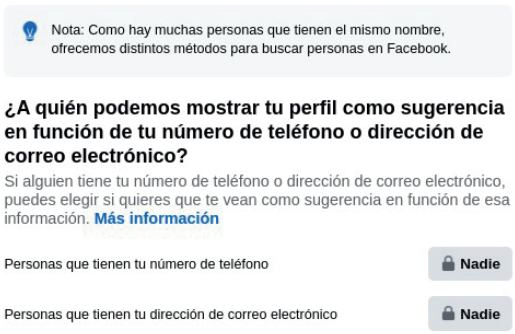
Guarda los códigos de recuperación en tu app de gestor de contraseñas preferida. También puedes apuntarlos en un archivo en una computadora de confianza, o incluso en un papel guardado en un lugar seguro o con gente de absoluta confianza.

Revisa que el número de teléfono que esté seleccionado para mandar un mensaje de texto de recuperación sea el tuyo, elimina cualquier número que ya no utilices o que no reconozcas. Revisa los dispositivos de confianza y elimina TODOS los que ya no utilices o que no reconozcas.

Cómo pueden buscarte las personas en Facebook

Sigue el asistente para restringir cómo otras personas usuarias pueden interactuar con tu cuenta. Por ejemplo, podrás elegir que sólo los amigos de tus amigos te puedan enviar solicitud de amistad.

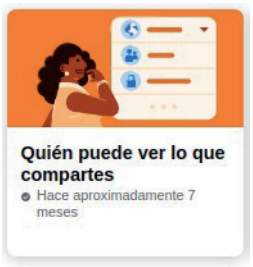
Importante: Evita que las personas que tengan tu número de teléfono o emails en sus contactos te encuentren en Facebook cambiando las opciones a “Nadie”.



Importante: Evita que tu perfil aparezca en Google y otros motores de búsqueda desactivando la opción que lo permite.

.

Quién puede ver lo que compartes en Facebook



Sigue el asistente para reducir quién puede ver tu email o teléfono asociados a tu perfil. Puedes seleccionar “Solo yo” para que no sean visibles.

Reduce la visibilidad de información que te pueda identificar (cómo tu cumpleaños, lista de amigos/seguidores, lugar de trabajo/estudios) seleccionando “Amigos” o “Solo yo”.

Revisa la audiencia de tus publicaciones e historias futuras. Cambiarla a “Amigos” evitará que las vea gente desconocida. Limita también las publicaciones anteriores

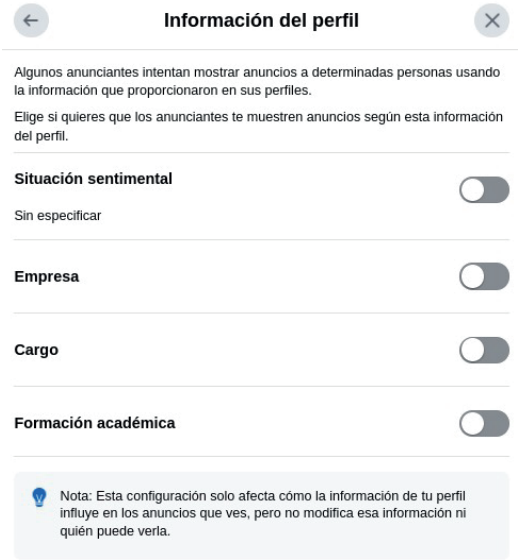
Tu configuración de datos en Facebook

Importante: Elimina las apps y sitios web con acceso a tu cuenta que no utilices o que no reconozcas.

Si alguna app o sitio web antiguo fuera comprometido, esto reduce el riesgo que tu información podría quedar expuesta.

Tus preferencias de anuncios en Facebook

Sigue el asistente para desactivar el compartir información de tu perfil con personas y empresas que puedan publicar anuncios.



Restringe quién puede ver tus interacciones con anuncios seleccionando “Solo yo”

Whatsapp

Verificación en dos pasos

Abre los “Ajustes” y toca en “Cuenta”, luego en “Verificación en dos pasos”. Toca en “Activar o Configurar PIN”.

Ingresa un PIN de 6 dígitos, asegúrate de ser un número que recuerdes muy bien. Si olvidas tu PIN, tendrás que esperar 7 días antes de poder cambiarlo

Opcional: puedes configurar un email para restablecer la verificación en dos pasos. Toca en Añadir dirección de correo electrónico. Asegúrate que tienes acceso a este correo, pues ahí se enviarán instrucciones para restablecer la autenticación en dos pasos si pierdes acceso a tu cuenta.

Dispositivos vinculados

Asegúrate que los dispositivos vinculados a tu cuenta sean solamente tuyos.

En Android toca el ícono “Más Opciones”. En iPhone abre los “Ajustes”. Toca en “Dispositivos Vinculados” y revisa la lista de dispositivos, y asegúrate que sólo estén dispositivos que sean tuyos. Si no reconoces un dispositivo, eliminarlo de inmediato.

OJO: en los dispositivos vinculados se sincronizan todos los chats y contactos se sincronizan. Por eso es importante que sólo tengas vinculados dispositivos de tu propiedad.

Privacidad de tus estados

Configura la privacidad de tus estados para que sólo sean visibles por quien tú decidas. Sigue estos pasos:

Abre la pestaña de “Novedades o Estados” y luego toca en el botón de menú “Más”. Se ve así:

Toca en “Privacidad de estados”. Puedes seleccionar la audiencia para tus estados. Puedes escoger “Mis contactos”, “Mis Contactos Excepto”, o “Sólo Compartir con…”.

Privacidad de tu cuenta

Configura la privacidad de tu cuenta y elige quién puede ver tu hora de “Última Vez” y “Estado en Línea”, “Foto del Perfil”, “Sección Info.” o “Actualizaciones de Estado”, o quién puede añadirte a grupos.

Sigue estos pasos:

Abre los “Ajustes” y luego toca en “Privacidad”. Puedes seleccionar la audiencia que verá tu información aquí.

Puedes seleccionar la audiencia para tu foto de perfil, última vez en línea, acerca de quién puede agregarte a grupos, y tus contactos.

Puedes restringir la audiencia a “Todos, Mis contactos, Mis contactos, excepto… o Nadie”.

También puedes bloquear el acceso a la aplicación con PIN o con FaceID/huella digital.

Mensajes que desaparecen

Para reducir el riesgo que alguien que comprometa tu cuenta, robe o decomise tu dispositivo lea tus conversaciones sensitivas, configura los mensajes que desaparecen.

Abre los “Ajustes” y luego toca en “Privacidad”. Toca en “Duración Predeterminada” y luego selecciona una duración.

Puedes hacer que los mensajes desaparezcan al cabo de 24 horas, 7 días o 90 días después de que sean leídos.

Si necesitas guardar una conversación importante antes que desaparezca, puedes tocar en la foto del contacto o grupo, y luego tocar en “Exportar Chat”.

Twitter (X)

Autenticación en dos fases

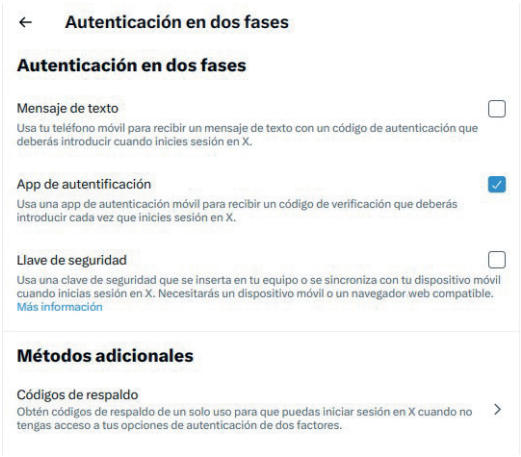
Entra en la dirección https://x.com/settings y revisaremos las configuraciones de seguridad y privacidad.

Abre el apartado “Tu Cuenta” y luego entra en la sección “Cambia tu contraseña”. Puedes guardarla en tu gestor de contraseñas.

Abre el apartado “Seguridad y Acceso” a la cuenta y abre la sección de “Autenticación en

Dos Fases". Marca la opción "App de autenticación" y desmarca la opción de "Mensaje de Texto".

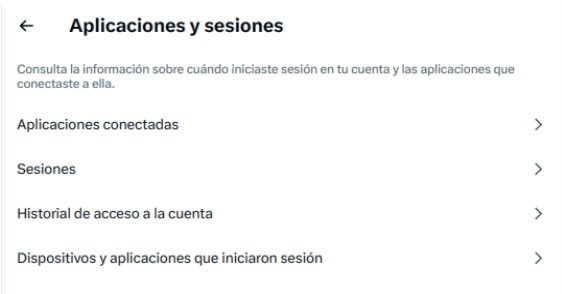
En la sección "Métodos Adicionales", abre el apartado "Códigos de respaldo". Guarda los códigos en tu gestor de contraseñas.



Aplicaciones y sesiones conectadas

Abre el apartado "Seguridad y Acceso" a la cuenta y abre la sección de "Aplicaciones y Sesiones". Abre el apartado "Aplicaciones Conectadas" y remueve las apps y sitios web que no utilices o que no reconozcas.

Abre el apartado "Sesiones" y remueve las sesiones en dispositivos viejos o que no reconozcas. Ten cuidado de no remover la sesión que aparece marcada como "Activa Ahora".



Delegar cuenta

Abre el apartado "Seguridad y Acceso" a la cuenta y abre la sección de "Cuentas Conectadas". Remueve las cuentas que no reconozcas o que ya no tengas acceso.

Abre el apartado "Delega". Revisa las cuentas que te han delegado y también las cuentas en "Miembros" en los que has delegado, elimina todas las cuentas que no reconozcas o que ya no tengas acceso.

Si no quieres que alguien más administre tu cuenta desde su perfil de X/Twitter, o administrar la cuenta de alguien más con la tuya, desactiva el switch que indica "Permitir que otros te inviten a su cuenta".

Datos de Ubicación

Abre el apartado "Privacidad y Seguridad" y abre la sección de "Tus posts". Abre la sección "Añadir Información de Ubicación" a tus posts, y quita la selección de la caja. Luego haz clic en "Eliminar toda la Información de Ubicación" incluida en tus posts.

Silenciar y bloquear

Abre la sección "Silenciar y Bloquear". Puedes bloquear y silenciar cuentas, y elegir palabras o frases que quieras silenciar para no ver esos posts. Abre "Notificaciones Silenciadas". Puedes silenciar notificaciones de distintas categorías.

Mensajes Directos

Abre el apartado “Privacidad y Seguridad” y abre la sección de “Tus Posts”. Abre la sección “Mensajes Directos”.

Elige quién puede enviarte mensajes directos. Las opciones son “Todos, Usuarios verificados, o Nadie”. Activa la caja que dice “Filtrar mensajes de baja calidad”.

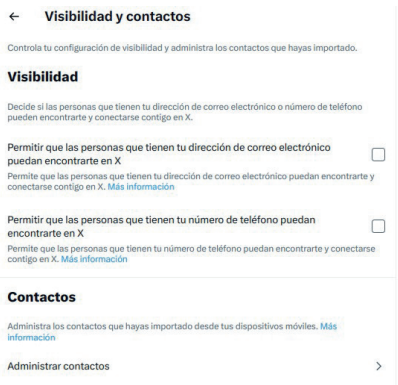
Esto suele filtrar muchos mensajes de troles y spam. Si gustas, activa o desactiva la caja de “Mostrar Confirmaciones de Lectura” para que otros usuarios sepan cuándo leíste sus mensajes.

Visibilidad y Contactos

Abre el apartado “Privacidad y Seguridad” y abre la sección de “Tus posts”. Abre la sección “Visibilidad y Contactos”.

Desmarca las opciones “Permitir que las personas que tienen tu dirección de correo electrónico puedan encontrarte en X” y “Permitir que las personas que tienen tu número de teléfono puedan encontrarte en X”.

En el apartado “Contactos”, abre la sección “Administrar Contactos”. Haz clic en “Eliminar todos los Contactos”.

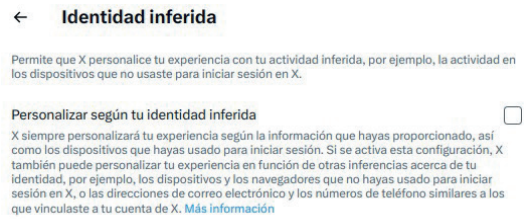


Privacidad de datos

Abre el apartado “Privacidad y Seguridad” y abre la sección de “Preferencias de Anuncios” y desmarca la caja con “Anuncios Personalizados”.

Abre la sección “Identidad Inferida” y desmarca la caja con “Personalizar” según tu identidad inferida. Abre la sección “Datos compartidos con Socios Comerciales” y desmarca la caja con “Permitir el intercambio de Información Adicional con Socios Comerciales”.

Abre la sección “Información de Ubicación” y desmarca la caja con “Personalizar según los ugares donde estuviste”. Abre la sección de “Grok” y desmarca la caja con “Permite que tus posts, así como tus interacciones, entradas y resultados con Grok, se utilicen para entrenamiento y perfeccionamiento”.



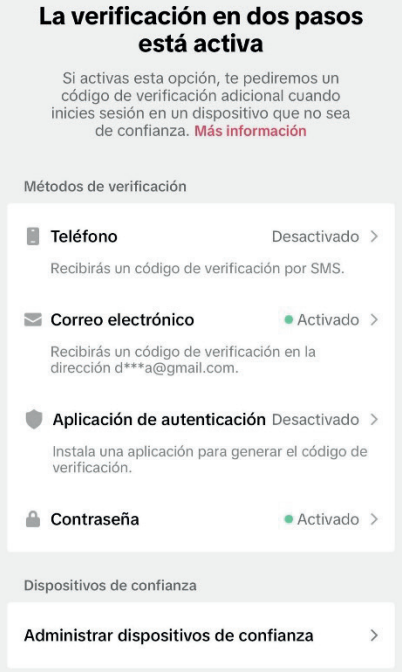
Tiktok

Asegúrate que sólo tus dispositivos tengan una sesión iniciada.

Ingresa en “Ajustes y Privacidad” en el menú hamburguesa, luego en “Seguridad y permisos”, luego en “Tus dispositivos”.

Elimina todos los dispositivos que no reconozcas. Luego, toca en “Permisos de aplicaciones y servicios”. Elimina todas las apps que no reconozcas.

Activa la verificación en dos pasos en esta sección también.

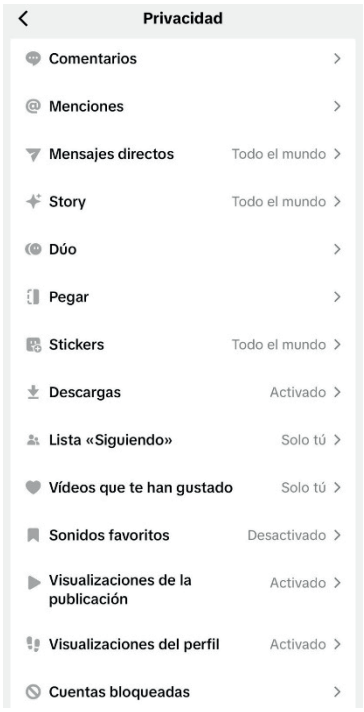


Configuración de Privacidad

Sigue estos pasos para que regules quién puede interactuar con tu cuenta y ver cierta información de tu perfil. Así evitas mensajes y otras interacciones no deseadas.

Configura quién puede comentar, mencionarte y enviar mensajes privados.

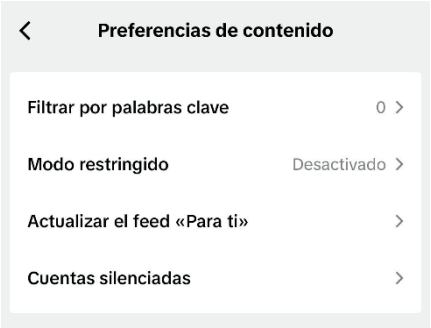
Ingresa en “Ajustes y Privacidad” en el menú hamburguesa, luego en Privacidad, y luego en la sección respectiva para comentarios, menciones, mensajes directos, story, duo, y pegar. Según la actividad, puedes escoger entre “Todo el mundo”, “personas que sigues”, “amigos”, o “nadie”.



Filtrando el contenido que ves

Puedes filtrar ciertas palabras y frases para evitar interactuar con contenido no deseado.

Puedes establecer filtros por palabras clave, para evitar ver contenido de odio u otro tipo. Ingresa en “Ajustes y Privacidad” en el menú hamburguesa, luego en “Preferencias de Contenido”. Puedes agregar palabras clave para filtrar el contenido que se identifique con ellas, y también puedes silenciar cuentas sin bloquearlas.

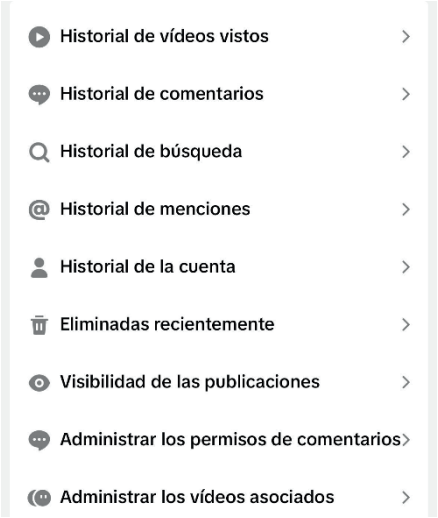


Configuración de Comentarios

Sigue estos pasos para configurar quién puede interactuar con comentarios en tus publicaciones.

Puedes activar y desactivar los comentarios para videos específicos y cambiar la visibilidad de varios posts a la vez.

Ingresa en “Ajustes y Privacidad” en el menú hamburguesa, luego en “Centro de Actividades”, luego en “Administrar los permisos de comentarios”, y en “Visibilidad de las publicaciones”. Selecciona las publicaciones que quieres configurar en cada sección.



Google/Youtube

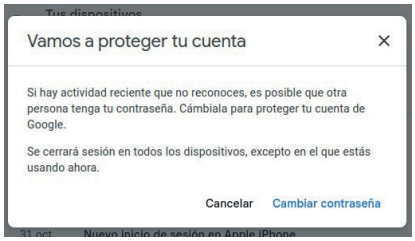
Revisión de Seguridad

Entra en la dirección https://myaccount.google.com/security-checkup revisaremos las configuraciones de seguridad y recuperación de tu cuenta.

Abre el apartado Tu cuenta y luego entra en la sección Cambia tu contraseña.
Puedes guardarla en tu gestor de contraseñas.

Abre el apartado Actividad relacionada con la seguridad reciente y revisa que las actividades que aparecen te sean familiares. Si no reconoces alguna actividad, puedes cambiar tu contraseña haciendo clic en ¿Ves alguna actividad que no reconoces?

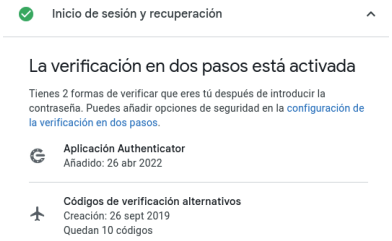
En la sección Inicio de Sesión y Recuperación, abre la Configuración de la verificación en dos pasos para poder activarla. Ten a la mano tu gestor de contraseñas para escanear un código QR, y de manera opcional: tu teléfono y una llave de seguridad si la tienes.



Verificación en dos pasos

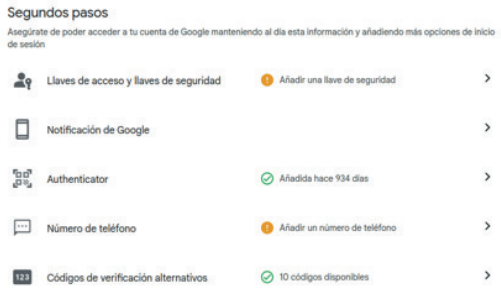
En esta sección puedes activar la verificación en dos pasos.

En esta sección puedes configurar la verificación en dos pasos. Te recomendamos utilizar una app como Bitwarden, Google Authenticator o Contraseñas en iOS para escanear el código QR y completar el proceso.



Abre el apartado Códigos de Verificación Alternativos para generar códigos de emergencia en caso de que pierdas acceso a tu app dónde se generan tus códigos, o a tus dispositivos vinculados con tu cuenta Google. Guarda los códigos en un lugar seguro, por ejemplo, en un gestor de contraseñas, un archivo en una computadora de confianza, o incluso un papel cuidado por gente de absoluta confianza.

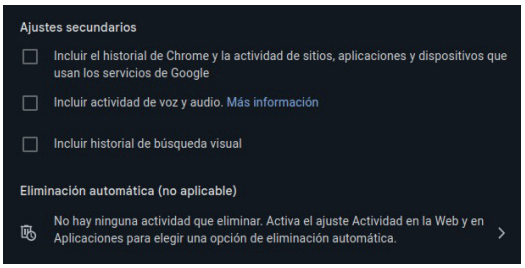
Opcional: En la sección “Llaves de Seguridad”, puedes vincular tu cuenta de Google a una llave de Seguridad USB, NFC o Bluetooth si tienes una.



Revisión de Privacidad

Entra en la dirección https://myaccount.google.com/privacycheckup revisaremos las configuraciones de privacidad y uso de tus datos.

En la sección “Actividad web y aplicaciones”, haz clic en “Desactivar” para dejar de guardar un historial de uso de tu actividad en la web y aplicaciones. Desactiva todos los ajustes secundarios y borra tu actividad guardada. Las opciones se ven así:



Personalización de Colección de tus datos

Puedes limitar los datos tuyos que Google recolecta y muestra a sus anunciantes y clientes.

En el apartado “Revisa cómo se personalizan tus anuncios”, busca la sección “Mi centro de anuncios” y haz clic para desactivar los anuncios personalizados.

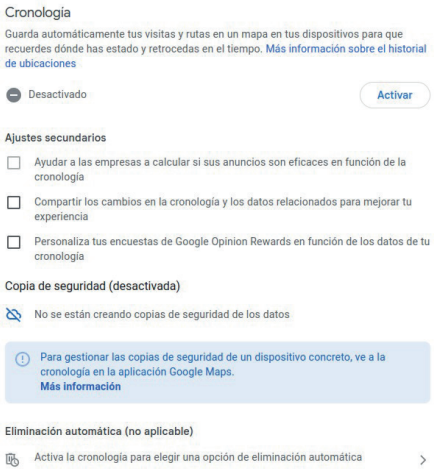
En el apartado “Revisa qué información del perfil ven los demás”, busca tu foto de perfil y nombre y haz clic en ella. Aquí puedes cambiar el nombre que aparece en tu cuenta y tu foto de perfil. Puedes restringir otros datos como género, fecha de nacimiento, y otros datos adicionales que tengas agregados en tu cuenta.

Historial de Ubicación

Entra en la dirección https://myaccount.google.com/data-and-privacy y busca la sección “Configuración del Historial”.

Busca el apartado de “Cronología”. Puedes ubicarla con este logo:

Haciendo clic sobre este apartado, desactiva la Cronología, desactiva todos los “Ajustes Secundarios”, y también elimina la “Copia de Seguridad” (esta es una copia de tu historial de ubicaciones).
Ve la siguiente imagen para una referencia:



Privacidad en YouTube

Tu cuenta de YouTube comparte la configuración de “Privacidad y Seguridad de Google”. Si utilizas YouTube mayoritariamente para ver videos, puedes entrar en https://www.youtube.com/account_privacy para configurar la privacidad de tus suscripciones.

Telegram

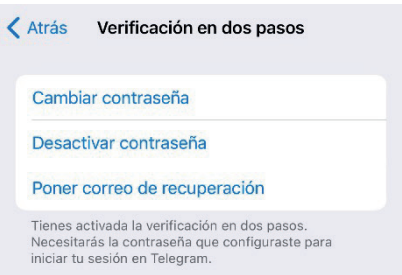
Protege tu cuenta

Entra en la sección de Ajustes en la App, Telegram en el menú Hamburguesa en Android, o en el logo de configuración en iOS.

Dentro de “Ajustes”, entra en “Privacidad y seguridad”. Toca en “Verificación en dos pasos” y activa la verificación. Te pedirá escribir una contraseña, asegúrate de guardarla en tu gestor de contraseñas.

Opcional: puedes establecer un email de recuperación en caso de que olvides tu contraseña, ten cuidado que sea un correo que sólo tú tengas acceso.

Toca en “Autoeliminar mensajes” y configura cuánto tiempo tardan los mensajes de tus chats y grupos en auto eliminarse. Recuerda que los chats en Telegram no están cifrados por defecto, por eso es importante evitar compartir información sensible por ellos.



Protege la privacidad de tu identidad y tus datos

Recuerda que, por defecto, los otros usuarios, y miembros y administradores de grupos y canales pueden ver tu número de teléfono. Protege tu identidad al utilizar Telegram siguiendo estos pasos.

Dentro de “Ajustes”, entra en “Privacidad y seguridad”. En la sección “Privacidad”, cambia la visibilidad de tu número de teléfono. Puedes elegir entre todos, mis contactos, o nadie. Restringe quién puede encontrarte por tu número de teléfono a sólo “Mis contactos”. Así tu número de teléfono no será público.

Restringe otros detalles de tu perfil cómo ver la hora de tu última vez en línea, foto de perfil, biografía, fecha de nacimiento. Igual que con el número de teléfono, puedes elegir entre todos, mis contactos, o nadie.

Ojo: Para todas estas configuraciones, puedes configurar excepciones.
Ejemplo: puedes compartir tu número con “Nadie”, excepto un contacto de confianza.

Configuraciones para prevenir el acoso y hostigamiento

Telegram es frecuentemente utilizada por grupos criminales y lleva un riesgo aumentado de acoso y hostigamiento. Protege tu cuenta de estas conductas con estas configuraciones:

Dentro de “Ajustes”, entra en “Privacidad y seguridad”. En la sección “Privacidad”, cambia la privacidad de “Mensajes reenviados”. Esto hace que, si alguien reenvíe un mensaje tuyo, este mensaje no lleve un link a tu cuenta de usuario. Puedes elegir entre todos, mis contactos, o nadie.

Restringe también los usuarios que puedan hacerte llamadas. Puedes elegir entre “todos”, “mis contactos”, o nadie. También configura que las llamadas siempre sean peer-to-peer (es decir, sin intermediarios) seleccionando “Siempre”.

Restringe quién puede enviarte invitaciones a grupos y canales. Puedes elegir entre “todos”, “mis contactos”, o “nadie”.

Ojo: Para todas estas configuraciones, puedes configurar excepciones.
Ejemplo: puedes compartir tu número con “Nadie”, excepto un contacto de confianza.

Dispositivos vinculados

Entra en la sección de “Ajustes” en la App, Telegram en el menú hamburguesa en Android, o en el logo de configuración en iOS.

Dentro de Ajustes, entra en “Privacidad y seguridad”. Toca en “Verificación en dos pasos” y activa la verificación. Te pedirá escribir una contraseña, asegúrate de guardarla en tu gestor de contraseñas.

Opcional: puedes establecer un email de recuperación en caso de que olvides tu contraseña, ten cuidado que sea un correo que sólo tú tengas acceso.

Toca en “Autoeliminar mensajes” y configura cuánto tiempo tardan los mensajes de tus chats y grupos en auto eliminarse. Recuerda que los chats en Telegram no están cifrados por defecto, por eso es importante evitar compartir información sensible por ellos.

MEDIDAS DE REACCIÓN

Facebook

¿Tu cuenta fue hackeada?
Ingresa al asistente de recuperación de cuentas https://www.facebook.com/hacked

- Sigue las instrucciones para recuperar tu cuenta. Puede que necesites tener a la mano lo siguiente:
  - Tu gestor de contraseñas con tu contraseña anterior
  - Tus códigos de recuperación
  - Un dispositivo (computadora, smartphone o tablet) en donde hayas iniciado sesión anteriormente
  - Acceso a por lo menos uno de los emails de recuperación de tu cuenta de Facebook

Ojo: ten mucho cuidado si recibes correos para recuperar tu cuenta que tu no has solicitado, puede ser que alguien esté intentando comprometer tu cuenta usando estos mecanismos de recuperación. No abras ningún link, y revisa los pasos de Prevención y Preparación desde la app o el sitio web de Facebook.

¿No quieres exponer ningún detalle de tu perfil con alguien que no esté en tus contactos o lista de amigos?
Cómo “restringir” tu perfil de Facebook: Al restringir tu perfil, solamente tu foto de perfil, portada, hasta 5 detalles que hayas configurado como públicos en tu biografía, los álbumes de fotos que hayas compartido, y tus publicaciones de Marketplace seguirán siendo públicas. No puedes restringir tu perfil si está en modo “Profesional”, debes desactivar este modo antes de restringirlo.

Haz clic en el botón de tres puntos “. . .” bajo tu foto de perfil.

Luego haz clic sobre “Restringir perfil”.

Puedes desactivar la restricción en cualquier momento con el mismo menú.

Instagram

¿Tu cuenta fue hackeada?
Ingresa al asistente de recuperación de cuentas https://www.instagram.com/hacked
Sigue las instrucciones para recuperar tu cuenta. Puede que necesites tener a la mano lo siguiente:

- Tu gestor de contraseñas con tu contraseña anterior.
- Tus códigos de recuperación.
- Un dispositivo (computadora, smartphone o tablet) en donde hayas iniciado sesión anteriormente.
- Acceso a por lo menos uno de los emails de recuperación de tu cuenta de Facebook.

Ojo: es posible que Instagram te solicite realizar un proceso de verificación que involucra enviar fotografías o video de tu rostro. Puedes encontrar más información de este proceso en este link.

Ojo: ten mucho cuidado si recibes correos para recuperar tu cuenta que no has solicitado, puede ser que alguien esté intentando comprometer tu cuenta usando estos mecanismos de recuperación. No abras ningún link, y revisa los pasos de Prevención y Preparación desde la app o el sitio web de Facebook.

¿Estás recibiendo muchos comentarios ofensivos, de acoso, o con incitación al odio?
Sigue estos pasos para bloquear comentarios de gente específica, o apagarlos en todos los posts y reels de tu perfil público de Instagram.

- En tu perfil, toca en el menú hamburguesa, es el que se ve así:

- Toca en “Configuración” y luego toca en “Comentarios”.
- Puedes bloquear a usuarios específicos, permitir que solo comenten tus seguidores, tus seguidores y a quienes sigues, o nadie.
- Puedes prohibir los comentarios solamente en una publicación específica tocando el botón de menú que se ve así en la publicación:

- Luego toca en “No permitir comentarios”
- Tendrá un icono parecido a este:

Whatsapp

Bloquear mensajes de desconocidos

Si te encuentras en una situación en dónde recibes muchos mensajes de cuentas de desconocidos, puedes activar esta opción para bloquear mensajes de desconocidos temporalmente.

En Android toca el ícono “Más Opciones”, en iPhone abre los “Ajustes”. Luego toca en “Privacidad”.

Luego toca en “Avanzada”. Activa la opción “Bloquear mensajes de cuentas desconocidas”.

Ojo: WhatsApp bloqueará los mensajes de cuentas desconocidas cuando sean muy numerosos. Durante este período, tus contactos pueden enviarte mensajes con normalidad. El bloqueo de mensajes se detiene cuando la cantidad de mensajes vuelve a la normalidad.

Dispositivo robado o decomisado

Si tu dispositivo fue robado o decomisado, completa los pasos de esta lista.

- Solicita un chip nuevo a tu compañía de celular, y utilízalo en otro dispositivo para vincular tu cuenta.
- Debes tener a la mano tu PIN para registrar la cuenta
- Al vincular el dispositivo, se cerrará la sesión en todos los demás dispositivos.
- Puedes asegurarte revisando en “Ajustes” y luego en “Dispositivos vinculados” que no haya más dispositivos que el tuyo asociados a tu cuenta.

Ojo: si olvidas tu PIN, tendrás que esperar 7 días para poder volver a vincular tu cuenta.

Twitter (X)

¿Tu cuenta fue hackeada?

Ingresa al asistente de recuperación de cuentas https://help.x.com/es/forms/account-access/regain-access

- Sigue las instrucciones para recuperar tu cuenta. Puede que necesites tener a la mano lo siguiente:
  - Tu gestor de contraseñas con tu contraseña anterior
  - Tus códigos de recuperación
  - Un dispositivo (computadora, smartphone o tablet) en donde hayas iniciado sesión anteriormente
  - Acceso a por lo menos uno de los emails de recuperación de tu cuenta de Facebook

Ojo: ten mucho cuidado si recibes correos para recuperar tu cuenta que tu no has solicitado, puede ser que alguien esté intentando comprometer tu cuenta usando estos mecanismos de recuperación. No abras ningún link, y revisa los pasos de Prevención y Preparación desde la app o el sitio web de X/Twitter.

¿Estás recibiendo posts dónde etiquetan a tu usuario en fotos ofensivas o violentas? ¿Estás recibiendo notificaciones de menciones en contenido de odio o violencia?

Entra en la dirección https://x.com/settings y restringiremos estas interacciones.

- Entra en el apartado “Privacidad y Seguridad”.
- Ve a la sección “Audiencia, contenido multimedia y etiquetas”.
- Ve a la sección “Etiquetado de fotos” y desactiva el Switch para que no puedan etiquetarte en fotos.
- Entra en la sección “Silenciar y Bloquear”
- Para añadir palabras silenciadas, haz click en el signo +
- Puedes ingresar palabras o frases, especificar si se aplica el filtro a personas que sigues o a todos, y definir una duración del filtro.

Google

Para recuperar tu cuenta de Google en caso de que sea comprometida, ten a la mano al menos una de las siguientes cosas:

- Un dispositivo donde hayas iniciado sesión antes
- El teléfono asociado a tu cuenta de Google
- Tu app gestora de contraseñas, o autenticador para la verificación de dos pasos
- Tus códigos de recuperación

Entra a este link y sigue los pasos: https://accounts.google.com/signin/recovery

Si tienes dudas sobre cómo proceder, sigue este asistente para verificar que pasos seguir: https://support.google.com/accounts/troubleshooter/2402620

Telegram

¿Tu cuenta fue hackeada o tu teléfono robado/confiscado?

Si tienes un dispositivo vinculado desde el que puedes acceder a tu cuenta, puedes cerrar todas las demás sesiones.

- Ve a “Ajustes”, luego a “Dispositivos”
- Toca en cerrar todas las demás sesiones

También puedes borrar remotamente tu cuenta utilizando una computadora y un dispositivo vinculado.

- Entra al enlace: https://my.telegram.org/auth
- Introduce tu número de teléfono.
- Introduce el código que recibiste en tu dispositivo vinculado.

Ojo: tu cuenta, y todo su contenido serán eliminados permanentemente.

Telegram es una app de mensajería que NO ofrece cifrado de extremo a extremo, por lo que los contenidos de los chats y grupos pueden ser leídos por las autoridades si Telegram se los proporciona. Además, el gobierno ha restringido previamente el acceso a Telegram.

¿CÓMO DENUNCIAR LA VIOLENCIA POLÍTICA DIGITAL?

Las redes sociales y plataformas digitales deben ser espacios digitales seguros. Denunciar contenidos inapropiados o abusivos en redes sociales es fundamental para mantener un ambiente digital seguro y respetuoso.

Las principales redes sociales y aplicaciones de mensajería, tales como Facebook, Instagram, WhatsApp, TikTok, y Twitter (X), ofrecen mecanismos de denuncia de violencia digital que infrinjan sus políticas. La denuncia de contenidos que representan violencia digital permite identificar a cuentas o perfiles que ejercen violencia contra las mujeres en la política; es también una medida de prevención para que otras mujeres no sean víctimas de violencia digital.

¿Qué acciones puedes tomar frente a la violencia política digital?

1. Denunciar o Reportar
2. Bloquear

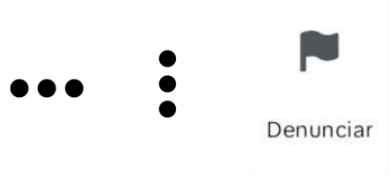
Una primera acción es denunciar o reportar. Cada plataforma o red social ofrece diversas opciones para denunciar o reportar publicaciones, comentarios, perfiles, o mensajes que representen violencia digital como, por ejemplo, lenguaje de odio, acoso, desinformación, amenazas, uso de datos personales sin autorización, entre otros tipos de violencia digital; la mayoría de las plataformas garantiza la confidencialidad de las denuncias, emite un informe sobre la denuncia, y proporciona actualizaciones sobre la denuncia.

Una segunda acción es el bloqueo. Puedes bloquear usuarios para evitar interacciones no deseadas, o para limitar el acceso a tu información, publicaciones o perfil. También puedes bloquear contenidos para que la plataforma no te muestre contenidos específicos o provenientes de una cuenta en particular. A diferencia de la denuncia, al bloquear, la plataforma no revisa si el comportamiento del usuario infringe sus normas y políticas, o si representan violencia digital; es decir, no es un mecanismo para poner alto a los usuarios abusivos o para evitar la difusión de contenidos que son violencia digital.

A continuación, se presenta una guía paso a paso para denunciar y bloquear contenidos o cuentas en plataformas digitales más utilizadas por las mujeres en la política en El Salvador.

DENUNCIAR O REPORTAR

Identifica en la plataforma los botones para denunciar o reportar. Suelen estar representados por tres puntos o por una bandera. Al hacer clic en el botón o ícono con los tres puntos o la bandera, se desplegará un menú con varias opciones.



Facebook

Reportar una publicación, comentario o "video en vivo"

Paso 1. Identifica la publicación o comentario que deseas denunciar, o visita el perfil de la cuenta o página que desea reportar. Haz clic en el ícono de tres puntos.

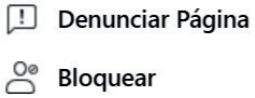
Paso 2. Selecciona la razón de la denuncia (por ejemplo, acoso, violencia).

Paso 3. Sigue los pasos adicionales. Envía la denuncia.

Bloquear a un usuario o página

Paso 1. Visita el perfil o página que deseas bloquear. Haz clic en los tres puntos.

Paso 2. Selecciona "bloquear" y confirma.



Instagram

Reporta una publicación, un en vivo o "live", o comentario

Paso 1. Identifica la publicación o comentario que deseas denunciar o visita el perfil que deseas reportar. Haz clic en el ícono de tres puntos, y luego en la opción "Reportar".

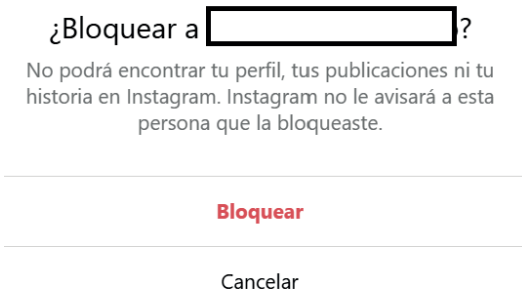
Paso 2. Selecciona el motivo de la denuncia (por ejemplo, acoso, violencia).

Paso 3. Sigue los pasos adicionales. Envía la denuncia.

Bloquear, reportar o restringir una cuenta

Paso 1. Visita el perfil o página que deseas bloquear. Haz clic en los tres puntos.

Paso 2. Selecciona “bloquear” y confirma.



Whatsapp

Reportar a un contacto, estatus de whatsapp o contenidos (fotografías, video)

Paso 1. Toca el nombre o número en la parte superior del chat para abrir la información del contacto que deseas reportar, o selecciona el estatus o contenido a reportar.

Paso 2. Haz clic en el ícono de tres puntos, luego en “Más”. Selecciona la opción “Reportar”.

Paso 3. Confirma el reporte, y si deseas, bloquea al contacto.

Bloquear a Contacto

Paso 1. Toca el nombre del contacto o número en la parte superior del chat para abrir la información del contacto que deseas reportar.

Paso 2. Haz clic en el ícono de tres puntos, luego en “Más.

Paso 3. Confirma el bloqueo, y si deseas, reporta al contacto.

Twitter (X)

Reportar perfil, publicación, lista, momentos, espacio en X (“Space”) o comentario

Paso 1. Identifica el contenido o visita el perfil del usuario que deseas denunciar. Haz clic en el ícono de tres puntos.

Paso 2. Selecciona la opción “Denuciar”.

Paso 3. Selecciona la razón de la denuncia (por ejemplo, abuso, discurso violento, privacidad).

Paso 4. La plataforma podría solicitar que identifiques publicaciones abusivas o dañinas, y otra información.

Bloquear a Contacto

Paso 1. Visita el perfil que deseas reportar, o desde un comentario hecho por el perfil que desees denunciar y haz clic en el ícono de tres puntos.

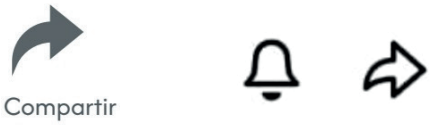
Paso 2. Haz clic en el ícono de bloqueo.

Paso 3. Confirma el bloqueo.

Tik Tok

Denunciar una cuenta o contenido (video, sesión LIVE, mensaje, hashtag, comentario).

Paso 1. Identifica el video, haz clic en el botón con una flecha para “compartir”; o mantén presionado el video o el comentario por denunciar. Otra opción es visitar el perfil que se quiere denunciar, y hacer clic en el botón de compartir, y seleccionar la opción que corresponda.



Paso 2. Selecciona el incono con la bandera para “Denunciar”.

Paso 3. Selecciona la razón de la denuncia (por ejemplo, odio y acoso, información falsa, violencia, etc.).

Paso 4. Sigue los pasos adicionales. Envía la denuncia.

Denunciar una cuenta perfil

Paso 1. Visita el perfil que deseas reportar y haz clic en el botón con una flecha para “compartir”.

Paso 2. Haz clic en el ícono con la bandera “Denunciar”.

Paso 3. Selecciona el motivo “denunciar cuenta”.

Paso 4. Indica la razón de la denuncia (por ejemplo, suplantación de identidad, contenido inapropiado, entre otros).

Paso 5. Sigue los pasos adicionales.

Telegram

Reportar a un contacto o grupo

Paso 1. Abre el chat o grupo donde se presenta el acoso.

Paso 2. Toca el nombre del contacto y selecciona la opción para Reportar.

Paso 3. Haz clic en el ícono de tres puntos, luego en “Más”, selecciona la opción “Reportar”.

Paso 4. Elige el tipo de abuso que corresponda (acoso, contenido inapropiado, etc.)

Paso 5. Envía la denuncia. Telegram revisará el caso.

Bloquear a Contacto

Paso 1. Ve a la opción “Contactos” para ver tus contactos para abrir la información del contacto que deseas reportar.

Paso 2. Selecciona el contacto que deseas bloquear, presionando el nombre del usuario o su imagen de perfil.

Paso 3. Presiona el menú de tres puntos y escoge la opción “Bloquear”.

Paso 4. Confirma el Bloqueo, y si deseas reporta al contacto.

Youtube

Denunciar video, imagen o título

Paso 1. Haz clic en los tres puntos verticales a un lado del video.

Paso 2. Haz clic en la bandera para “Denunciar”.

Paso 3. Selecciona la opción que corresponda (por ejemplo, hostigamiento o acoso, contenido sexual, contenido que incite al odio, etc.).

Paso 4. Sigue las instrucciones para completar la denuncia.

Google, Gmail, Drive

Reportar o bloquear un correo, foto u otro contenido

Paso 1. Accede a tu cuenta de cuenta de correo de Google (Gmail) o alguna otra aplicación de Google, y ve al contenido que quieras reportar o al usuario que quieras bloquear.

Paso 2. Haz clic en los tres puntos verticales para "Reportar" o Bloquear.

Paso 3. Selecciona la opción que corresponda. En caso de que sospeches de un correo que pueda ser Phishing, selecciona la opción "Reportar Phishing" la cual encontrarás bajo un símbolo de anzuelo.

Paso 4. Sigue las instrucciones para completar la denuncia o bloqueo, según sea el caso.

CONSEJOS ADICIONALES

Denuncia
La denuncia es importante para que las plataformas tomen medidas contra los comportamientos abusivos.

Consulta las políticas de cada plataforma
Cada red social o plataforma tiene sus propias políticas y normas comunitarias.

Configura la privacidad y seguridad
Revise el apartado de este manual "Medidas de Prevención" sobre las opciones para limitar quién puede interactuar con su cuenta, ver o comentar en sus publicaciones.

Solicita soporte adicional
En casos graves, algunas plataformas ofrecen soporte adicional o recursos para víctimas de acoso.

Normativa nacional e internacional aplicable a la violencia política digital

NORMATIVA NACIONAL	Código Electoral
	Código Penal
	Ley Especial contra los Delitos Informáticos y Conexos (LEDIC)
	Ley Especial Integral para una Vida Libre de Violencia para las Mujeres (LEIV)
NORMATIVA INTERNACIONAL	Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia en contra de la Mujer
	Declaración sobre la Violencia y el Acoso Político contra las Mujeres.
	Mecanismos de seguimiento Convención Belém Do Pará.

Autoridades competentes en El Salvador

AUTORIDAD	COMPETENCIA	DISPOSICIÓN LEGAL
Isdemu 1-2-6 y sitio web "126 Te Orienta"	Número telefónico y espacio virtual[7] que brinda orientación, apoyo psicológico y social y asesoría legal a mujeres en situaciones de vulnerabilidad.	Artículo 12 y 13 de la LEIV
Fiscalía General de la República	Fiscalía Adjunta para la Mujer, Niñez, Adolescencia y otros grupos vulnerables es la responsable de investigar y persecución penal para delitos basados en violencia de género.	Artículo 25, 56 de la LEIV. Artículo 19 Reglamento especial de la Fiscalía General de la República.
Órgano Judicial	Por medio de Juzgados Especializados de Instrucción para una Vida Libre de Violencia y Discriminación para las Mujeres; Juzgados Especializados de Sentencia para una Vida Libre de Violencia y Discriminación para las Mujeres; Cámara Especializada para una Vida Libre de Violencia y Discriminación para las Mujeres. Responsables de sancionar los tipos penales relacionados con la violencia y discriminación de género.	Artículo 56-A de la LEIV. Decreto no. 286 del 25 de febrero de 2016[8].
PNC	Auxiliar y proteger de forma oportuna y adecuada a las mujeres que enfrentan hechos de violencia.	Art. 25 numeral 5 , y artículo 57 literal l) de la LEIV.
Tribunal Supremo Electoral	Responsable de la prevención y atención de las mujeres por violencia política en razón de su género. Autoridad responsable en proporcionar información, orientación y asesoría jurídica en forma oportuna y gratuita a las mujeres que denuncien violencia política ante el Tribunal. Encargada de sancionar por medio de la vía administrativa la propaganda electoral prohibida.	Artículo 10-A de la LEIV. Sección 6.1. del Protocolo para la Prevención y Atención de las mujeres víctimas de violencia política en El Salvador. Artículo 173 y 249 del Código Electoral.

7. *https://126teorienta.gob.sv/welcome/*
8. *El decreto crea los Juzgados y Tribunales Especializados para una Vida Libre de Violencia y Discriminación para las Mujeres en los municipios de San Salvador, Santa Ana y San Miguel. (Publicado en el Diario Oficial el 4 de abril de 2016).*

Evidencia digital

Para poder abonar al proceso judicial de una denuncia por acoso, hostigamiento, u otros delitos por medio de evidencia digital, esta evidencia debe ser guardada siguiendo un concepto llamado “Cadena de Custodia”.

Cuando decimos que una evidencia se ha guardado siguiendo una debida cadena de custodia, quiere decir que se ha documentado cada movimiento de los artefactos que componen esta evidencia.

Normalmente en un proceso legal, hay muchas personas que tienen que ver o hacer análisis de la evidencia, por eso es necesario que la persona o personas encargadas de apoyarnos en nuestro caso estén conscientes de su importancia y también que estén capacitadas para mantener la cadena de custodia. Cómo mínimo, la persona representante legal y/o perito informático deben estar familiarizados con el concepto de cadena de custodia y hacerse responsables de que se mantenga.

TIPOS DE EVIDENCIA DIGITAL. ¿CÓMO PODEMOS GUARDARLA?

Evidencia digital en plataformas de acceso público

Decimos que una plataforma es de acceso público, cuándo para ver estas publicaciones no requieren que una persona tenga una cuenta en dicha plataforma para accederla.

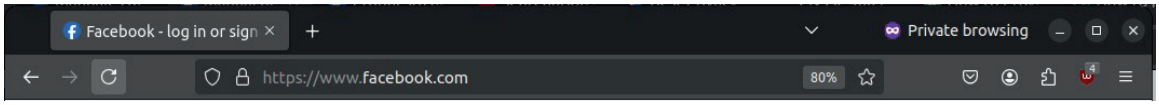
Ejemplo: tweets en Twitter/X, o post públicos en Facebook o Instagram.

Una manera de verificar si una publicación en Facebook es de acceso público, es copiar el link de la publicación y abrirlo una ventana de navegación privada.

Puedes abrir una ventana privada utilizando los siguientes métodos para los navegadores más comunes:

Google Chrome / Chromium:
En una ventana normal, presiona al mismo tiempo las teclas Control, Mayúsculas y N. Esto abre una ventana de navegación en modo incógnito. Esta ventana se ve así:

Mozilla Firefox:
En una ventana normal, presiona al mismo tiempo las teclas Control, Mayúsculas y P. Esto abre una ventana de “Navegación Privada”. Esta ventana se ve así:



Microsoft Edge:

En una ventana normal, presiona al mismo tiempo las teclas Control, Mayúsculas y N. Esto abre una ventana de navegación en modo “InPrivate”. Esta ventana se ve así:

Si puedes ver la publicación en estos modos de navegación privada, sin iniciar sesión en la plataforma o red social, entonces eso quiere decir que la publicación es de acceso público.

¿CÓMO GUARDAR O ARCHIVAR EVIDENCIA DE PUBLICACIONES DE ACCESO PÚBLICO?

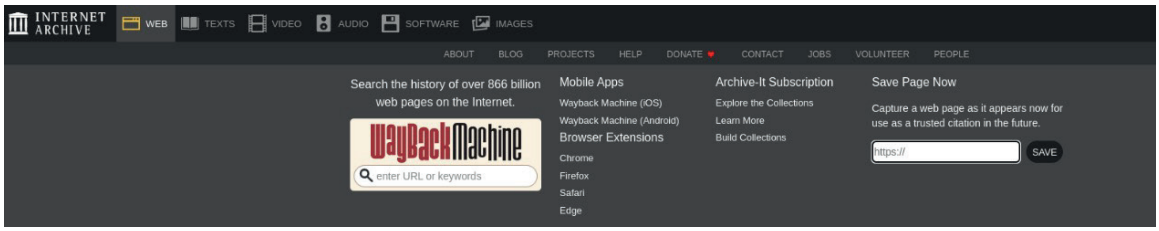
Existen sitios web dedicados a archivar copias de sitios y plataformas web de acceso público, son de uso gratuito y por ser neutrales, es posible utilizarlos para almacenar copias de publicaciones que queramos utilizar como evidencia digital. Los sitios de mayor uso y confiabilidad son “Internet Archive” y “Archive Today”. A continuación, están los pasos para guardar copias en línea descargables utilizando estos sitios.

Internet Archive

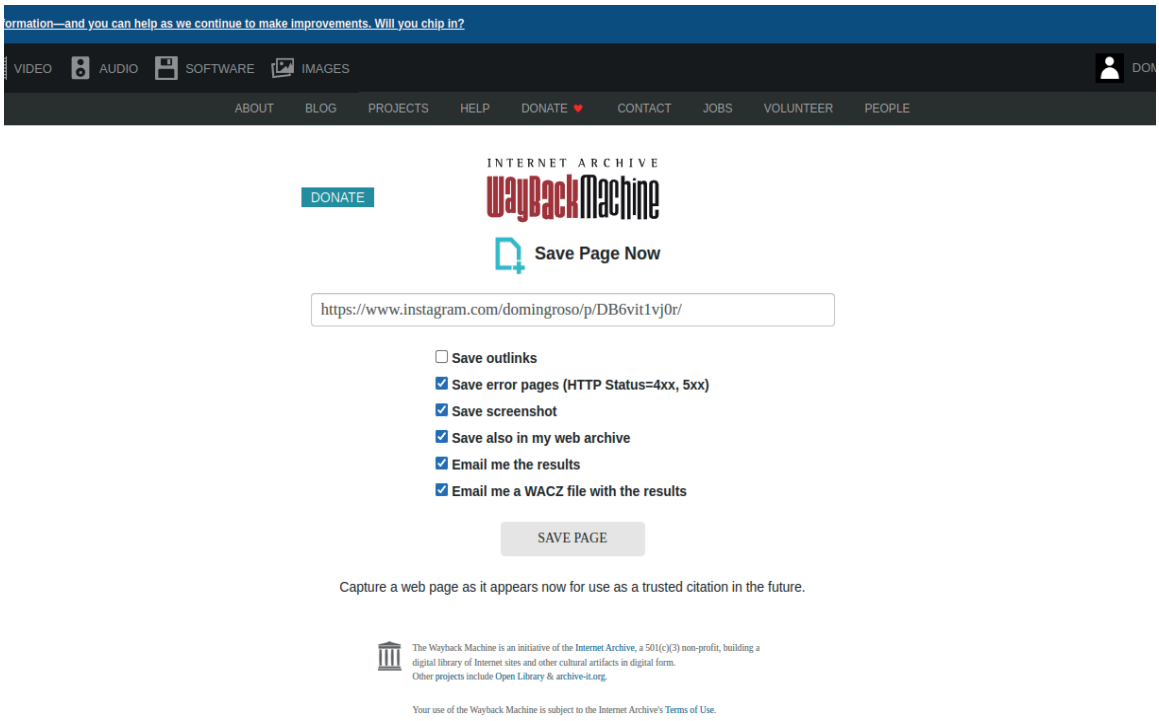
Debes ingresar en la página https://web.archive.org

Aunque es opcional para archivar páginas, es muy recomendable registrar una cuenta en esta página, pues así nos puede enviar por correo una copia de las páginas que archivemos. Regístrate con un correo electrónico o una cuenta google en https://archive.org/account/signup

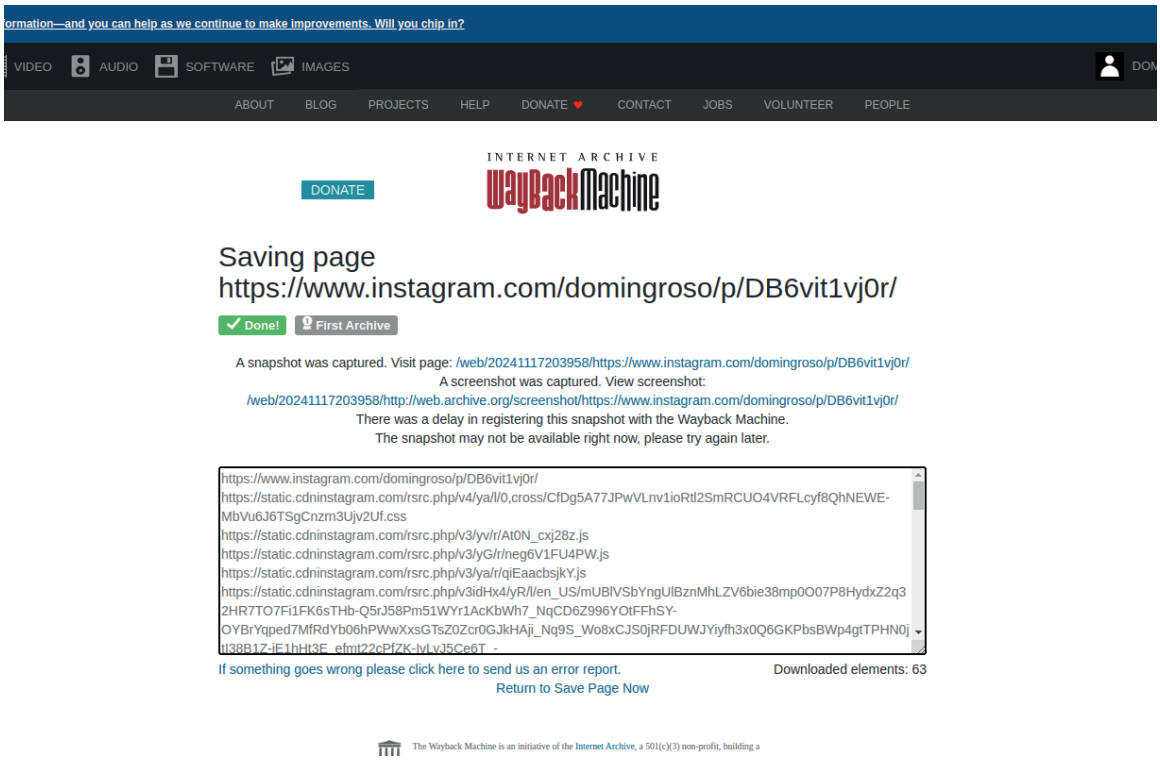
Completa el proceso e inicia sesión, luego para archivar la página sigue estos pasos:



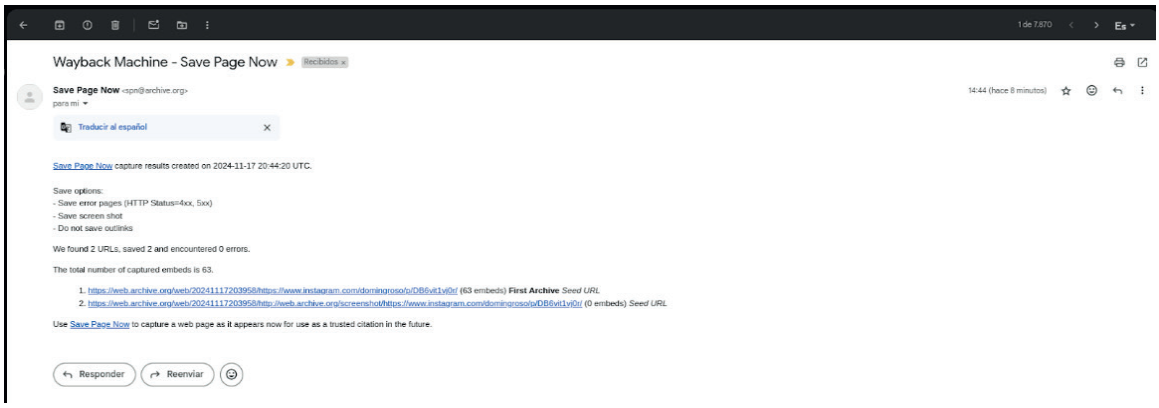
- Haz clic en el menú “web” junto al logo del Internet Archive. En este menú, en la parte derecha busca el recuadro Save page now y pega la dirección de la página que quieres archivar. Es necesario que copies y pegues la URL completa, para este ejemplo copiamos la dirección de un post público de Instagram con su URL completa: https://www.instagram.com/domingroso/p/DB6vit1vj0r/
- Selecciona las opciones que se muestran si quieres que se envíen a tu correo copias de lo que se va a archivar. Es recomendable que lo hagas pues los adjuntos de estos correos quedan en tu posesión aún si la página está fuera de servicio o si el contenido que archivaste es borrado. Sin embargo, cabe mencionar que el servicio de envío por email puede no estar disponible (en el caso de la copia que se guardó para esta demostración, no estaba disponible).



- Una vez hagas clic en “Save page” el proceso inicia y al terminar te mostrará un reporte como: este:



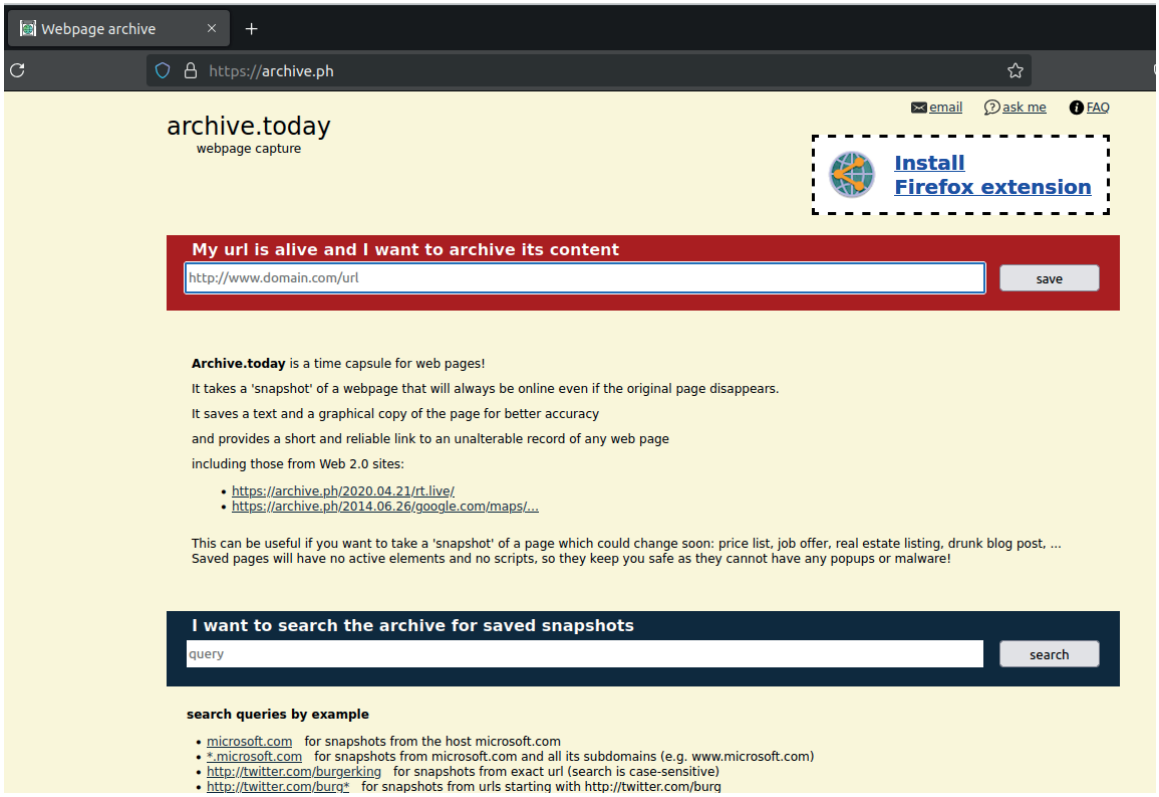
Revisa en tu bandeja de entrada dónde encontrarás una notificación con las URL de las páginas guardadas para futura referencia:



Archive Today

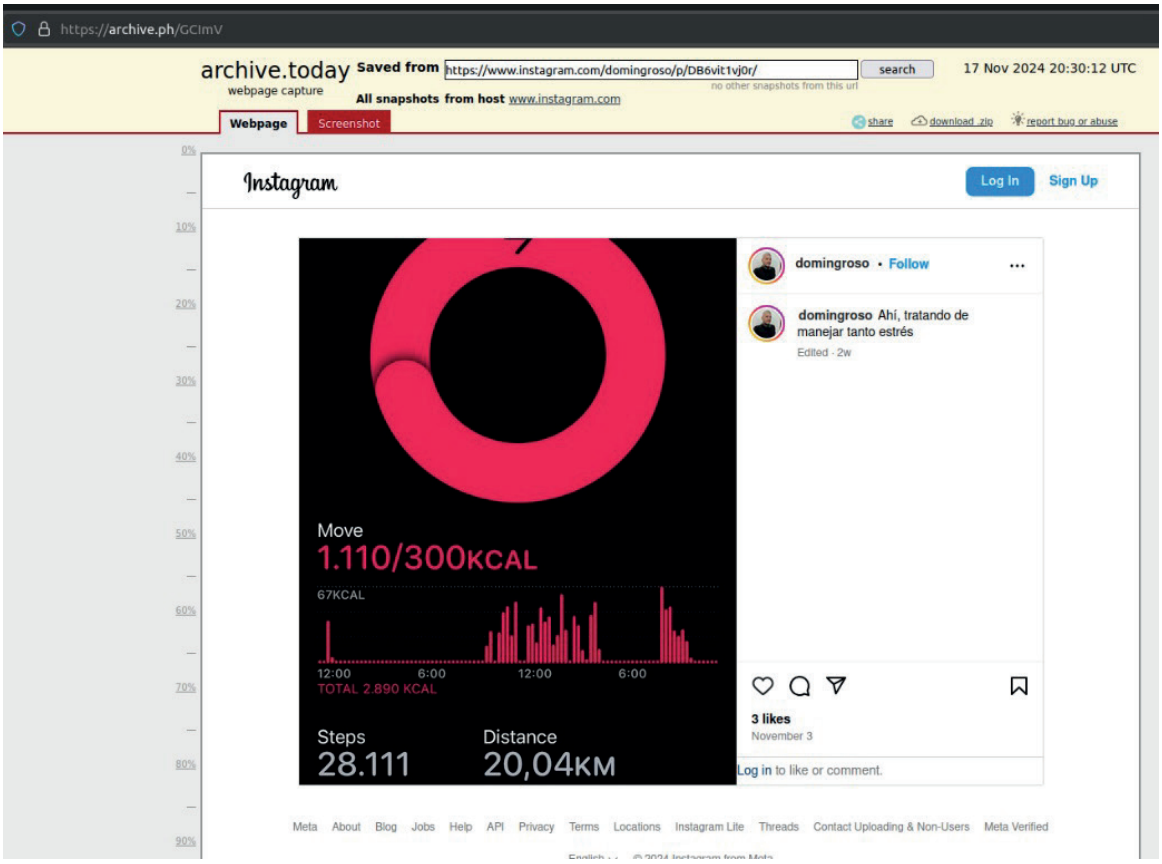
"Archive Today" es una página con un servicio de archivo mucho más simple. No requiere crear una cuenta y es de acceso público. Sigue estos pasos para guardar archivos de contenido de acceso público:

- Ingresa a la página en https://archive.ph



- Copia y pega la URL del contenido que quieras archivar en la sección en el recuadro rojo que lee “My url is alive and I want to archive its content”
- Al hacer clic en “Save”, inicia el proceso de guardado. Muestra una página de progreso similar a esta:

- Al finalizar el proceso, verás un reporte con los resultados similares a la siguiente. Toma nota de la URL que se genere pues con esta URL podrás ingresar a la copia de archivo que acabas de generar:



- Debes anotar la URL que guardaste en este servicio, ya que para acceder al archivo que se generó de esta debes introducirla en el recuadro azúl oscuro en la página de inicio:

- Al hacer clic en “Search” te mostrará las copias existentes de esta URL, incluyendo la que tu hiciste. Identificarla puede ser difícil, pero es posible hacerlo utilizando la URL que guardaste a la hora de hacer la copia del archivo.

EVIDENCIA DIGITAL EN PLATAFORMAS DE ACCESO LIMITADO

Decimos que una plataforma es de acceso limitado, cuándo para ver estas publicaciones se requiere una o más de las siguientes condiciones:

Que la persona usuaria tenga una cuenta en dicha plataforma para acceder al contenido.
Que el contenido solamente sea accesible a través del software o app de dicha plataforma
Que el contenido sólo pueda ser visto por un número limitado de personas usuarias de la plataforma, ósea que sea compartido de forma privada.

Ejemplo: Mensajes privados o directos en Instagram, publicaciones en grupos de Facebook, canales o chats de grupo en Telegram, mensajes directos en WhatsApp.

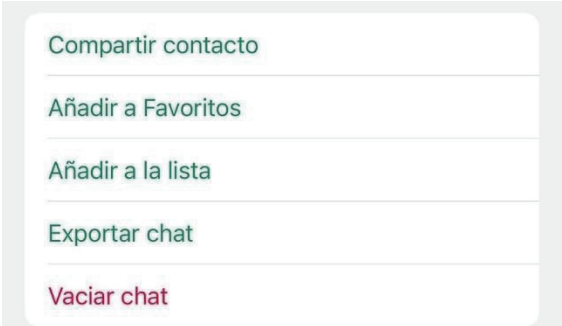
¿Cómo guardar evidencia digital de plataformas de acceso limitado?

Whatsapp

WhatsApp permite exportar el contenido de chats individuales, y enviarlos por correo o guardarlos en un archivo zip de manera local en el dispositivo.

Para exportar un chat, es necesario entrar al perfil del contacto o grupo cuyo chat queremos exportar.

Abajo, hay que tocar en la opción “Exportar chat”



Luego, debemos elegir si incluir o no los archivos multimedia. Tengamos en cuenta que, si el chat contiene muchos archivos multimedia, es posible que no se pueda enviar por correo electrónico, revisa las restricciones de tu proveedor. También tienes la opción de subirlo a Google Drive, iCloud u otro proveedor de almacenamiento.

Al terminar este paso, podrás seleccionar por qué medio quieres compartir el archivo. El archivo se guarda en formato zip y si lo envías por correo, se enviará desde uno de los correos que tengas configurado en tu dispositivo.

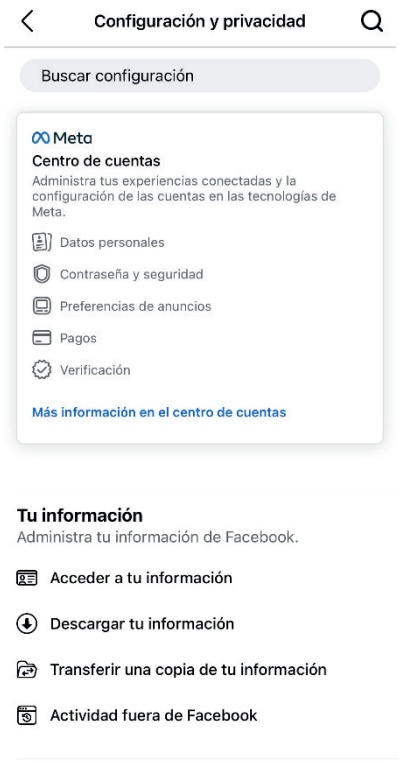
Para preservar la cadena de custodia, una vez tengas el archivo zip con el respaldo de tu correo, entrégalo a las personas encargadas de tu representación legal que estén a cargo de la colección de evidencia digital.

Facebook / Instagram

Para extraer evidencia digital de acceso limitado de Instagram y Facebook, debes solicitar descargarla. La solicitud se hace desde el centro de cuentas para ambas plataformas.

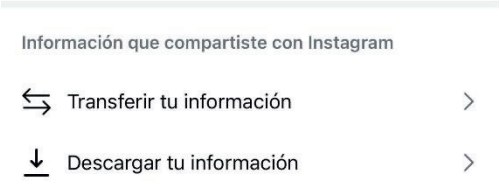
Para iniciar el proceso en Facebook debes abrir buscar el logo del engrane para abrir los ajustes de “Configuración y Privacidad” en tu perfil, y abrir el centro de cuentas.

Luego, en el centro de cuentas, busca la sección “Tu información” y toca en “Descargar tu información”.

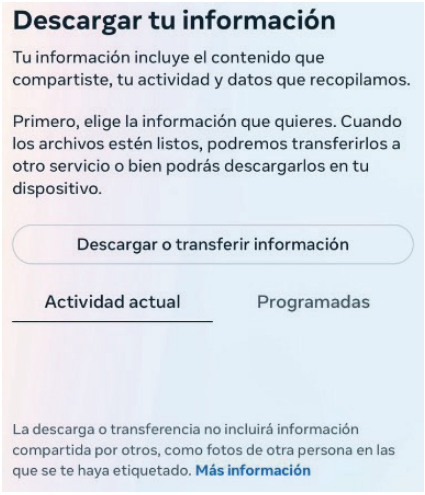


Sigue el siguiente proceso para Instagram:

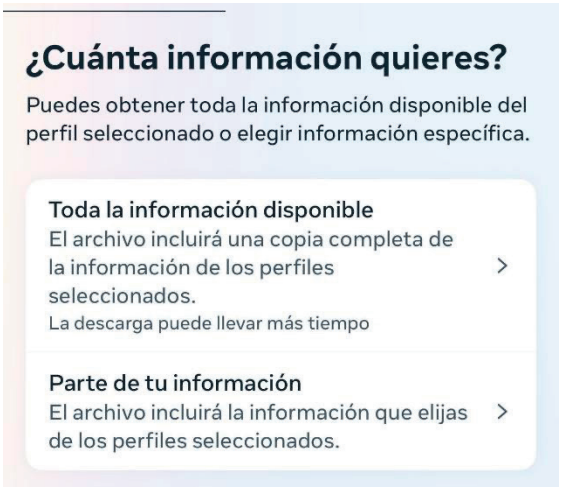
En la pestaña de tu perfil, abre “Ajustes” en el menú hamburguesa. Luego, toca en “Tu Actividad” y busca la sección “Información que compartiste con Instagram” y toca en “Descargar Información”.



Luego elige “Descargar o transferir Información”

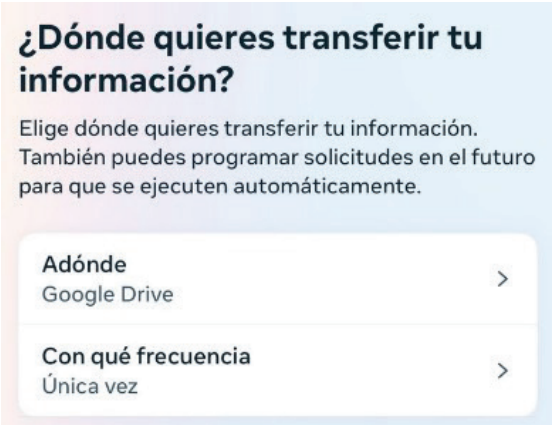


En el siguiente paso, elige “Descargar parte de la información” si quieres exportar una pieza de evidencia digital específica. Por ejemplo, si quieres descargar sólo los mensajes privados.



Luego deberás elegir la información que deseas descargar. En este caso, descargaremos los mensajes:

Luego, es necesario especificar si la información se descarga al dispositivo local o si se transfiere a otra ubicación. Dependiendo del tamaño de las conversaciones y de si incluyen archivos multimedia como videos, el archivo puede ocupar mucho espacio y llenar el almacenamiento del dispositivo. Por lo que es recomendable enviarlos a Google Drive u otro servicio de almacenamiento.



Finalmente, en esta sección podrás elegir el rango de fechas de la información que deseas transferir, y un correo electrónico al que deseas que se envíe una notificación cuándo termine el proceso.

Referencias

Acoso. Online. “Guía práctica para tratar casos de pornografía no consentida en recintos educacionales bajo estándares de derechos humanos y equidad de género”. Disponible en: ://acoso.online/site2022/wp-content/uploads/2018/12/Guia-Practica-Establecimientos-Educacionales_AcosoOnline_2018.pdf

ANDRYSAS. “Informe de resultados. Observación de violencia a mujeres políticamente activas en las elecciones internas en 2023”. Disponible en: https://andrysas.org.sv/wp-content/uploads/2024/02/Informe_Violencia_politica.pdf

ANDRYSAS. “Balance General: elecciones del 3 de marzo de 2024”. Disponible en: https://andrysas.org.sv/wp-content/uploads/2024/03/BALANCE-GENERAL-ELECCIONES-03-DE-MARZO-DE-2024.pdf

ANDRYSAS. “Balance General: elecciones del 4 de febrero de 2024”. Disponible en: https://andrysas.org.sv/wp-content/uploads/2024/02/BALANCE-GENERAL-ELECCIONES-04-DE-FEBRERO.pdf

Hiperderecho. Proyecto “Tecnoresistencias” (agosto, 2020). Disponible en: https://hiperderecho.org/tecnoresistencias/2020/08/acoso-coordinado/

Heinrich Boll Stiftung. Feminism and Gender Democracy. “Análisis comparativo del Marco legal actual en Latino América para combatir la violencia de genero digital y apoyar el liderazgo de las mujeres en la vida pública”. Disponible en: https://fundacionmultitudes.org/marcos-legales-en-latino-america-para-combatir-la-violencia-de-genero-digital-y-apoyar-el-liderazgo-de-las-mujeres-en-la-vida-publica/#

Cultivando Género. “Guía de resistencia digital entre amigas en la red no navegas sola”. Disponible en: https://vita-activa.org/recursos-resources/

OEA. “La violencia de género en línea contra las mujeres y niñas. Guía de conceptos básicos, herramientas de seguridad digital y estrategias de respuesta”. (2021). Disponible en: https://www.oas.org/es/sms/cicte/docs/Manual-La-violencia-de-genero-en-linea-contra-las-mujeres-y-ninas.pdf

OEA. “Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención Belém Do Pará. Disponible en: https://lac.unwomen.org/sites/default/files/2022-11/MUESTRA%20Informe%20Violencia%20en%20linea%202.1%20%282%29_Aprobado%20%28Abril%202022%29_0.pdf

ONU Mujeres. “Violencia de género en línea hacia mujeres con voz pública. Impacto en la libertad de expresión”. (2022). Disponible en: https://lac.unwomen.org/sites/default/files/2023-03/Informe_ViolenciaEnLinea-16Mar23.pdf

ONG Derechos Digitales. “Que no quede huella que no que no”. Disponible en:https://derechosdigitales.org/wp-content/uploads/que-no-quede-huella.pdf

Pen América. “Manual contra el acoso en línea”. Disponible en: https://onlineharassmentfieldmanual.pen.org/es/violencia-en-linea-glosario/

UNFPA. Bodyright. What is technology-facilitated gener-based violence? Disponible en: https://wcaro.unfpa.org/en/publications/brochure-what-technology-facilitated-gender-based-violence-0#:

UN Women, WHO. Technology-facilitated violence against women: taking stock of evidence and data collection (2023). Disponible en: https://www.unwomen.org/en/digital-library/publications/2023/04/technology-facilitated-violence-against-women-taking-stock-of-evidence-and-data-collection

Constitución de la República de El Salvador.

Código Electoral de El Salvador

Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia en contra de la Mujer

Ley especial integral para una vida libre de violencia para las mujeres (LEIV) de El Salvador.

Ley especial contra los delitos informáticos y conexos de El Salvador.

Documentación oficial de WhatsApp con respecto a privacidad y seguridad. Disponible en: https://faq.whatsapp.com/1920866721452534

Centro de ayuda de privacidad y seguridad de Instagram. Disponible en: https://help.instagram.com/196883487377501

Información sobre el “Centro de Cuentas”. Disponible en: https://www.facebook.com/help/943858526073065

Documentación sobre privacidad de herramientas de Google. Disponible en: https://support.google.com/docs/answer/10381817?hl=en

Documentación de seguridad de Telegram. Disponible en: https://telegram.org/blog/sessions-and-2-step-verification

Manual práctico para la prevención, denuncia y protección de las mujeres políticamente activas ante la violencia política digital

ASOCIACIÓN NACIONAL DE REGIDORAS, SÍNDICAS Y ALCALDESAS SALVADOREÑAS