14 de Mayo 2026

CANDIDATA EN TERRITORIO DIGITAL

Taller para candidatas indígenas en la era de la inteligencia artificial.

batsil.org

PLAN DE ACCIÓN

Siete secciones para revisar cada semana.
Pega esta hoja donde la veas todos los días. Es recordatorio: el detalle está en el manual del taller.

01

CUENTAS Y CONTRASEÑAS

Que nadie entre a hacerse pasar por mi.
Contraseñas únicas en cada cuenta, verificación en dos pasos activada, cómo recuperar mis cuentas escrito en lugar seguro (no en el celular).

02

PRIVACIDAD EN MIS PERFILES

Quién ve lo que publico
Configuración de privacidad revisada, acuerdo con mi familia sobre qué publican de mi, cuentas de mis hijas e hijos cuidadas.

03

EQUIPO DE RESPUESTA

Si algo pasa no decidir sola
Cuatro personas, con nombre y teléfono: Ancla (a quien llamo primero), técnica (sabe de redes), legal (abogada), cuidado (está fuera de la política).

04

EVIDENCIA DE MIS CUENTAS OFICIALES

Probar cuáles son mis cuentas oficiales si me suplantan
Linktree (o equivalente) con todas mis cuentas, capturas de pantalla con fecha visible, carpeta con mis fotos oficiales autorizadas.

05

PLAN ANTE UN ATAQUE

Tener un guión en frío para ejecutarlo en caliente
1) Documento (capturas con URL y fecha). 2) Llamo a mi persona ancla. 3) Espero dos horas antes de cualquier respuesta pública. 4) No respondo al agresor, no borro evidencia. 5) Si hay contenido íntimo o amenaza física: proceder con la denuncia.

06

INFORMACIÓN PERSONAL PROTEGIDA

Que nadie sepa donde encontrarme
Sin mi dirección ni mi rutina en redes, teléfono y correo de campaña separados de los personales. Lo que publican mis hijos sobre mí, revisado con ellos.

07

MI SALUD Y MI GENTE

Sostenerme como persona, no sólo como candidata.
Una mujer de confianza fuera de la política con quien hablar (amiga, terapeuta, tía...). Permiso para desconectarme sin culpa. Pásale esta información a otra mujer.

Si hoy pasa algo: **079**. Línea de la secretaría de mujeres, gratuita 24/7. Asesoría, acompañamiento y enlace directo cono plataformas digitales.
088 Guardia Nacional. Apoyo técnico especializado y canalización de delitos cibernéticos.

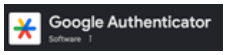
batsil.org

ANEXO A. LISTA DE VERIFICACIÓN PERSONAL DE SEGURIDAD DIGITAL

Esta hoja es tuya, llénala con tus propias palabras y guárdala donde la veas. Marca cada acción con fecha y responsable.

1. **Cuentas y contraseñas**

□ Tengo contraseñas distintas en mis cuentas más importantes (correo, Facebook, Instagram, WhatsApp, banco).
□ Activé verificación en dos pasos en al menos: correo, Facebook, Instagram, WhatsApp.
□ Sé quién, además de mí, conoce mis contraseñas. Esa persona es:



_____

□ Tengo escrito en un lugar seguro (no en el celular) cómo recuperar mis cuentas si pierdo el celular.

2. **Privacidad de mis perfiles**

□ Revisé qué información personal aparece pública en mis redes (teléfono, dirección, escuelas de mis hijos).
□ Configuré mis redes para que solo personas conocidas puedan ver fotos personales y de mi familia.
□ Hablé con mi familia más cercana (hijas, hijos, pareja, mi mamá) sobre lo que sí y lo que no quiero que publiquen sobre mí.
□ Revisé las cuentas de mis hijas e hijos menores: ¿están públicas? ¿Saben lo que sí y lo que no compartir sobre mí?

3. **Equipo de respuesta**

□ Tengo identificada UNA persona de confianza en mi equipo de campaña a quien le aviso primero si algo pasa:

_____

□ Esa persona sabe que tiene esa responsabilidad y aceptó.
□ Tengo el teléfono de mi abogada o defensora pública guardado y a la vista:

_____

□ Tengo el 079 y el 088 guardados en mi celular como contactos.

5. **Evidencia de mis cuentas oficiales**

□ Tengo capturas de pantalla de mis cuentas oficiales (con foto de perfil, número de seguidores, fecha) por si tengo que probar que una cuenta es falsa.
□ Tengo guardadas en una carpeta las fotos oficiales mías que SÍ autoricé públicamente. Las guardé en:

_____

□ Mi equipo sabe cuáles son mis cuentas oficiales reales y cuáles no.
□ Publiqué un mensaje aclarando cuáles son mis cuentas oficiales para que mis simpatizantes lo sepan. (Linktree o equivalente). También funciona muy bien tener una página web, es más difícil clonar una página web que clonar una cuenta de redes sociales.

4. **Plan ante un ataque**

□ Sé cuál es mi primer paso si me atacan: documentar antes de responder.
□ Sé que NO voy a responder en caliente. Voy a llamar primero a mi persona de confianza (sección 3).
□ Sé que tengo derecho a denunciar bajo Ley Olimpia y que la Ley Olimpia cubre también imágenes generadas con IA.
□ Sé a qué Ministerio Público o fiscalía me toca acudir en mi localidad o entidad:

_____

6. **Información personal protegida**

□ Borré o pedí que borren publicaciones antiguas con mi dirección, teléfono personal o lugares donde estoy seguido.
□ Pedí a mi familia y amistades que no etiqueten ubicaciones cuando publican fotos conmigo.
□ Tengo separado un teléfono o cuenta de campaña, distinta de mi teléfono y cuentas personales.
□ Si me hostigan, sé qué hacer con los mensajes: NO los borro, los documento.

7. **Mi salud y mi gente**

□ Sé que la violencia digital me puede afectar emocionalmente, y eso no es debilidad.
□ Tengo identificada UNA persona con la que voy a hablar si los ataques me están afectando:

_____

□ Sé que tengo derecho a tomar distancia de las redes por unas horas o días, y que eso no es perder la campaña.
□ Le voy a contar a UNA mujer más lo que aprendí hoy. Su nombre:

_____

Cuando termines

Pega esta hoja donde la veas todos los días. La seguridad digital no es algo que se hace una vez: es algo que se revisa cada semana, igual que se revisa la campaña.

ANEXO B. DIRECTORIO DE EMERGENCIA Y REPORTE

Quién	Cómo contactar	Para qué
Secretaría de las Mujeres	079 (24/7)	Asesoría, acompañamiento, enlace con plataformas digitales gracias al acuerdo de marzo 2026.
Guardia Nacional	88	Apoyo técnico especializado y canalización de delitos cibernéticos.
Emergencia general	911	Riesgo físico, amenazas inmediatas, doxing con dirección expuesta.
Policía Cibernética	Buscar línea de tu estado o Ciudad de México: 55 5242 5100	Ataques digitales, suplantación, hostigamiento, fraudes.
Ministerio Público / Fiscalía	Local, según tu entidad	Denuncia formal por Ley Olimpia y delitos relacionados.
Frente Nacional para la Sororidad	Redes sociales: @FNSororidad	Acompañamiento de Defensoras Digitales que han pasado por lo mismo.
INE - UTIVPMRG	55 5628 4200 ext. respectiva	Violencia política contra mujeres en razón de género (incluida la digital).
Conami	conami.mx Fb @mujeresindigenasconamimexico	Lucha y defensa de los derechos de mujeres y pueblos indígenas.
Bats'il	batsil.org hola@batsil.org	Herramientas de ciberseguridad e IA para mujeres indígenas y afrodescendientes.

Cómo reportar en cada plataforma

Facebook / Instagram (Meta): Tres puntos sobre la publicación: "Reportar" → "Acoso" o "Imágenes íntimas sin consentimiento". Para suplantación, ir a "Centro de Ayuda" → "Reportar cuenta falsa que se hace pasar por mí".

TikTok: Mantener pulsado el video → "Reportar". Para perfil falso: ir al perfil → tres puntos → "Reportar" → "Cuenta falsa".

WhatsApp: Si recibes contenido violento de un número: pulsar el contacto → "Reportar contacto" + "Bloquear". Guarda capturas de pantalla antes de bloquear.

YouTube (Google): Bandera bajo el video → "Reportar" → "Acoso" o "Contenido sexual no consensuado". Captura de pantalla antes de reportar.

X (antes Twitter): Tres puntos → "Reportar publicación". X no firmó el acuerdo de marzo 2026, las respuestas pueden tardar más.

Antes de reportar, documenta

1. Captura la publicación con la URL visible en pantalla.
2. Captura el perfil de la persona o cuenta atacante.
3. Anota fecha y hora exactas.
4. Si es un video o audio, descárgalo si puedes (no siempre es posible, pero inténtalo).
5. Guarda todo en una carpeta especial donde vayas acumulando evidencia con fechas.

GLOSARIO

Término	Significado
Algoritmo	Las reglas automáticas con las que una plataforma decide qué te muestra y qué oculta. Es decisión de la empresa, no de un humano que esté revisando.
CEDAW	Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer. Tratado internacional de la ONU. México lo firmó.
Ciberacoso	Acoso, hostigamiento o amenazas a través de medios digitales. Puede ser de una persona o de muchas coordinadas.
Deepfake	Video, audio o imagen falsa generada por inteligencia artificial donde una persona aparece haciendo o diciendo cosas que nunca hizo o dijo.
Doxing	Publicar datos personales de alguien (dirección, teléfono, lugar de trabajo, escuela de sus hij@s) con la intención de ponerla en riesgo.
Hostigamiento coordinado	Cuando muchas cuentas atacan al mismo tiempo a una persona. Frecuentemente las cuentas son falsas o están automatizadas.
IA Inteligencia artificial	Programas de computadora que generan textos, imágenes, audios o videos respondiendo a instrucciones (prompts). ChatGPT, Claude, Gemini son ejemplos.
Imagen íntima no consensuada	Foto o video de carácter íntimo o sexual difundido sin el permiso de la persona retratada. Es delito bajo Ley Olimpia, incluso si fue generada o modificada con inteligencia artificial.
Ley Olimpia	Conjunto de reformas a leyes federales y estatales en México que sancionan la violencia digital de carácter sexual contra mujeres.
Suplantación de identidad	Crear cuentas falsas con el nombre, foto y datos de otra persona para hacerse pasar por ella.
UMA	Unidad de Medida y Actualización. Es la base con la que se calculan multas en México.
Verificación en dos pasos	Función de seguridad que pide, además de tu contraseña, un segundo código que llega a tu celular. Evita que te hackeen aunque te roben la contraseña.
Violencia política de género	Acciones u omisiones dirigidas contra una mujer por su condición de mujer, que limitan su participación política. Puede ser física, simbólica, sexual o digital.