Septiembre de 2026

INTRODUCCIÓN A LA ATENCIÓN A LAS VMD POR GRUPOS DE PARES

Plan de seguridad: mapeo de dispositivos

LA REPO

PLAN DE SEGURIDAD: MAPEO DE DISPOSITIVOS

LUGARES DÓNDE SE ALMACENA TU INFORMACIÓN

Dispositivos físicos a los cuales puedes acceder físicamente:

- Disco duro del ordenador.
- USB, tarjetas SD, mini SD, micro SD.
- Disco duro externo.
- Teléfono móvil.
- Tabletas.
- Dispositivos conectados (tipo Echo, Google Home o Alexa, relojes conectados, cámaras conectadas etc.).
- CDs, DVDs.
- Copias físicas (o "copias en papel") en la oficina o en casa.
- Bandeja de entrada del gestor de correos electrónicos (tipo Outlook o Thunderbird).
- Multimedia: cintas de vídeo, grabaciones de audio, fotografías, etc.

Información que tienes en "cuentas y plataformas" custodiados por terceros. Acceder solo ingresando tus credenciales:

- Correos electrónicos.
- Cuentas en redes sociales.
- "La nube": Dropbox, Google Drive, SkyDrive, etc.
- Cuentas bancarias.
- Sitios de compra en línea.
- Cuentas administrativas (seguridad social, impuestos, otras).
- Páginas webs propias.

CÓMO RELLENAR LA TABLA

TIPOS DE INFORMACIÓN O DATOS QUE SE ALMACENAN EN CADA UNO DE ESTOS LUGARES

- Correos electrónicos (con la abogada, psicóloga, trabajadora social, personas de tu círculo, entorno militancia y activismo, redes de apoyo...).
- Denuncias.
- Trabajos académicos.
- Documentos con contraseñas.
- Datos de contacto, como bases de datos de clientes, etc.
- Informes/investigaciones.
- Cuentas/hojas de cálculo.
- Vídeos, Audios, Imágenes.
- Mensajes privados en tus aplicaciones de mensajería instantánea, etc.

NIVEL DE SENSIBILIDAD

Indica si esta información tiene un nivel de sensibilidad alta, mediana o baja. Para evaluarlo, pregúntate cuál sería el impacto que tendría en tu vida si esa información desapareciera o si alguien no autorizado accediera a ella.

COPIA DE SEGURIDAD/DONDE

A continuación, pregúntate si existe una copia o resguardo de estos datos en algún otro lugar. Si lo hay, apunta en la tabla dónde está esa copia. Puedes aprovechar este momento para destacar la diferencia entre las copias maestras y los duplicados.

AMENAZAS

Listado de las posibles amenazas, indicadores de comportamiento anómalo que temes, que has podido detectar o que podrían comprometer tu información:

- Pérdida de copia de seguridad.
- No tiene copia de seguridad.
- Contraseñas flojas o que no has cambiado en mucho tiempo.
- Uso de la misma contraseña en varias cuentas.
- Posible vigilancia en redes sociales.
- Infección por malware.
- Instalación de un software espía en tus dispositivos.
- Hardware viejo, apagones eléctricos, sobrecalentamiento.
- Acceso no autorizado por terceros malintencionados.
- Notificaciones de intentos de iniciar sesión en esa cuenta.

MEDIDAS DE SEGURIDAD

Indica buenas prácticas generales de "higiene digital" o acciones preventivas para mitigar riesgos identificados previamente que quieras emprender.

- ➔ Usar antivirus.
- ➔ Desinstalar apps no conocidas y/o que no usas nunca.
- ➔ Hacer copias de seguridad.
- ➔ Proteger con contraseñas seguras y/o implementar doble autentificación.
- ➔ Borrar archivos de forma segura.
- ➔ Cifrar tu información.
- ➔ Hacer un restablecimiento de fábrica.
- ➔ Usar diferentes cuentas de correo o redes sociales para comunicarte o en ámbitos (laboral, activismo, contactos externos...).

MI MAPA DE DISPOSITIVOS Y CUENTAS

Rellena una fila por cada lugar donde guardas información (un dispositivo, una cuenta, una plataforma...).

Lugares	Tipos de información	Nivel de sensibilidad	Copia de seguridad/Donde	Amenazas	Medidas de Seguridad

EJEMPLO DE REFERENCIA

Lugares	Tipos de información	Nivel de sensibilidad	Copia de seguridad/Donde	Amenazas	Medidas de Seguridad
Disco externo de respaldos	Fotografías personales	Alto	No	Guardado en mi casa	Disco cifrado y bajo llave

Ejemplo extraído de la documentación de Fembloc "Mapeo de información (cuentas y dispositivos)"

docs.fembloc.cat/dispositivos-plataformas-violencia-machista-mapeo-informacion-ex-pareja.html