

4. Desigualdades y violencias de género en entornos digitales.

Los entornos digitales forman parte de la vida cotidiana. Las redes sociales, las aplicaciones de mensajería, los videojuegos en línea, las plataformas educativas, los servicios de empleo, las herramientas de videollamada, los medios de comunicación digitales y los sistemas de inteligencia artificial se utilizan para relacionarse, informarse, trabajar, estudiar, participar en la comunidad y acceder a servicios. Estos espacios amplían las oportunidades de comunicación y participación, aunque también pueden reproducir desigualdades ya presentes en la sociedad y generar formas específicas de discriminación y violencia.

La **violencia digital de género** comprende conductas ejercidas a través de internet, dispositivos, aplicaciones, redes sociales o tecnologías de comunicación que causan o pueden causar daño psicológico, sexual, económico, social o reputacional a las mujeres. Puede incluir acoso, amenazas, vigilancia, control de dispositivos, suplantación de identidad, difusión no consentida de contenido íntimo, extorsión sexual, ataques a la reputación y otras prácticas dirigidas a limitar la autonomía o la participación de una persona. La Delegación del Gobierno contra la Violencia de Género señala que estas conductas pueden ejercerse mediante nuevas tecnologías, redes sociales e internet, y que deben entenderse como formas de violencia con efectos reales sobre la libertad y la seguridad de las mujeres.

La dimensión digital no convierte estas situaciones en menos graves. La velocidad de difusión, la posibilidad de almacenar y reenviar contenidos, la permanencia de la información en línea, la geolocalización, el acceso a datos personales y la dificultad para eliminar determinadas publicaciones pueden ampliar el daño y prolongarlo en el tiempo. La Agencia Española de Protección de Datos destaca que la viralización, la accesibilidad a través de buscadores y la dificultad de retirada de contenidos crean riesgos específicos, especialmente en casos de divulgación no consentida de información sensible o imágenes íntimas, vigilancia digital, daños reputacionales, sextorsión y acoso sexual en línea.

El análisis de las desigualdades digitales debe incluir dos planos relacionados. Por una parte, es necesario estudiar las barreras que dificultan a determinadas mujeres acceder, comprender y utilizar tecnologías digitales en condiciones de autonomía. Por otra, deben identificarse las conductas de discriminación, acoso, control o violencia que pueden producirse en estos espacios. La intervención con perspectiva de género requiere atender a ambos elementos, ya que una mujer que carece de competencias digitales, recursos técnicos o privacidad para utilizar un dispositivo puede encontrarse en una situación de mayor vulnerabilidad ante la exclusión o la violencia.

El entorno digital como espacio de participación y desigualdad

Las tecnologías digitales pueden facilitar el acceso a información, formación, empleo, participación ciudadana, redes de apoyo y recursos públicos. Una mujer que vive en una zona rural puede realizar una consulta administrativa sin desplazarse. Una persona con movilidad reducida puede participar en una reunión telemática. Una asociación puede difundir una campaña de sensibilización a través de redes sociales. Una trabajadora puede acceder a formación en línea compatible con determinados horarios.

Estas oportunidades dependen de que las personas cuenten con conexión, dispositivos, competencias digitales, tiempo disponible y condiciones de seguridad. La **brecha digital de género** se refiere a las desigualdades que pueden existir entre mujeres y hombres en el acceso, uso, formación, confianza y aprovechamiento de la tecnología. Esta brecha no se limita a disponer de un teléfono móvil o de conexión a internet. También incluye la posibilidad de utilizar herramientas

digitales con autonomía, proteger la privacidad, identificar riesgos, participar en debates públicos y acceder a oportunidades laborales o formativas.

Una mujer puede disponer de un dispositivo, pero compartirlo con otras personas de su hogar. Puede tener conexión limitada, depender de otra persona para realizar trámites digitales o carecer de un espacio privado desde el que consultar información sensible. Estas circunstancias son especialmente relevantes cuando se trata de recursos relacionados con empleo, ayudas económicas, salud sexual, conciliación, violencia de género o apoyo psicológico.

La desigualdad digital puede verse agravada por otros factores sociales. Las mujeres mayores, las mujeres que viven en zonas rurales, las mujeres con discapacidad, las mujeres migrantes, las mujeres con bajos ingresos, las mujeres que tienen responsabilidades intensivas de cuidado o las mujeres que se encuentran en una situación de violencia pueden experimentar barreras añadidas. La perspectiva interseccional permite reconocer que no todas las mujeres acceden a la tecnología desde las mismas condiciones.



Nota

El acceso a una herramienta digital no garantiza su uso autónomo, seguro y útil. La intervención debe analizar si las personas destinatarias pueden comprender la información, proteger sus datos, participar sin temor y utilizar los recursos disponibles sin depender de terceros.

Dimensiones de la brecha digital de género

La brecha digital se manifiesta de maneras diversas. Para diseñar actuaciones de comunicación e información inclusivas, resulta útil diferenciar sus principales dimensiones.

Dimensión	Manifestación	Posible efecto
Acceso material	Falta de dispositivos propios, conexión insuficiente o dependencia de equipos compartidos.	Dificultad para acceder a trámites, cursos, ofertas de empleo o recursos comunitarios.
Competencias digitales	Escaso conocimiento para utilizar aplicaciones, formularios, plataformas o sistemas de seguridad.	Mayor dependencia de otras personas y menor autonomía en la gestión de información.
Tiempo disponible	Responsabilidades de cuidado, jornadas laborales extensas o falta de espacios personales.	Menor posibilidad de formarse, participar en redes o realizar gestiones digitales.
Seguridad y privacidad	Uso de dispositivos controlados, contraseñas compartidas o falta de privacidad en el hogar.	Riesgo de vigilancia, control, exposición de datos o acceso no autorizado a información personal.
Confianza y participación	Miedo a equivocarse, recibir ataques o exponerse públicamente.	Menor presencia de mujeres en debates, comunidades digitales o espacios de representación.
Accesibilidad	Plataformas poco adaptadas a personas con discapacidad sensorial, física o cognitiva.	Exclusión de recursos, formación y canales de participación.

Representación	Escasa presencia de mujeres como referentes en ámbitos tecnológicos y digitales.	Menor identificación con estudios, profesiones y actividades relacionadas con la tecnología.
-----------------------	--	--

Estas dimensiones pueden acumularse. Por ejemplo, una mujer mayor que vive sola en un entorno rural puede tener dificultades de conectividad, menor experiencia digital y acceso limitado a apoyo técnico. Una mujer que convive con una persona que ejerce violencia puede disponer de un teléfono, pero no contar con privacidad para buscar recursos o contactar con servicios de ayuda. La evaluación de estas circunstancias debe formar parte del diagnóstico comunicativo y comunitario.

Características de la violencia en línea

La tecnología puede convertirse en una herramienta de control, vigilancia, intimidación o difusión de contenidos dañinos. Algunas características propias del entorno digital pueden intensificar el impacto de la violencia.

La **inmediatez** facilita que un mensaje ofensivo, una imagen íntima o un dato personal se difunda en pocos minutos. La **viralidad** permite que muchas personas accedan al contenido, lo descarguen, lo reenvíen o lo reproduzcan en otros canales. La **persistencia** hace que una publicación pueda permanecer disponible durante un periodo prolongado, incluso después de que la persona afectada haya solicitado su retirada. La **replicabilidad** implica que un archivo puede copiarse y compartirse en múltiples espacios. La **deslocalización** permite que la agresión continúe fuera del ámbito escolar, laboral, familiar o comunitario.

También influye la posibilidad de utilizar perfiles anónimos o falsos. Una persona agresora puede enviar mensajes desde cuentas diferentes, crear perfiles simulados, difundir rumores sin identificarse o utilizar herramientas tecnológicas para ocultar su identidad. Estas dinámicas pueden aumentar la sensación de inseguridad y dificultar que la persona afectada limite el contacto.

En determinados casos, la violencia digital se combina con violencia presencial. El control del teléfono, las contraseñas, la ubicación o las conversaciones puede formar parte de un patrón más amplio de dominación. La revisión de dispositivos, la exigencia de acceso a redes sociales o la imposición de enviar fotografías y ubicaciones no constituyen muestras de afecto. Son prácticas de vigilancia que pueden limitar la autonomía y la libertad de las mujeres.

Marco de protección frente a las violencias sexuales digitales

La legislación española reconoce expresamente que las violencias sexuales pueden producirse en el ámbito digital. La **Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual** incluye dentro de su ámbito las violencias sexuales cometidas mediante tecnologías y presta especial atención a la difusión de actos de violencia sexual, la pornografía no consentida y la extorsión sexual a través de medios tecnológicos. La norma también establece que las políticas de prevención y sensibilización deben actuar en ámbitos como el educativo, laboral, digital, publicitario y mediático.



Legislación

Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual.

Esta norma garantiza la protección integral de la libertad sexual e incorpora de forma expresa las violencias sexuales cometidas en el ámbito digital, incluidas determinadas conductas de difusión no consentida y extorsión mediante tecnologías.

La respuesta profesional debe evitar reducir cualquier conflicto en línea a una cuestión técnica o privada. Cuando existe control, intimidación, chantaje, difusión no consentida de contenido íntimo, amenazas sexuales o ataques dirigidos a limitar la participación de una mujer por razón de género, es necesario valorar la situación desde una perspectiva de derechos, seguridad y posible violencia.

La intervención debe ajustarse a las competencias de cada servicio. Una profesional del ámbito social, educativo, comunitario o laboral puede detectar indicios, escuchar sin culpabilizar, registrar la información necesaria, activar protocolos internos, orientar sobre recursos disponibles y derivar a servicios especializados cuando la situación lo requiera. La valoración jurídica de los hechos y la adopción de medidas procesales corresponden a los órganos competentes.

Formas de violencia y discriminación digital

Las manifestaciones de violencia digital pueden ser muy diversas. Algunas se producen de forma puntual; otras forman parte de un patrón continuado de control, humillación, intimidación o aislamiento. La siguiente clasificación permite identificar conductas frecuentes.

Manifestación	Descripción	Ejemplo
Ciberacoso	Envío reiterado de mensajes ofensivos, humillantes, intimidatorios o degradantes.	Recibir insultos continuos por publicar una opinión en una red social.
Control digital	Vigilancia de dispositivos, contraseñas, redes sociales, ubicación o contactos.	Exigir acceso al teléfono o activar la geolocalización de forma permanente.
Amenazas en línea	Mensajes destinados a generar miedo, intimidación o silenciamiento.	Amenazar con difundir datos personales o imágenes privadas.
Sextorsión	Chantaje mediante imágenes, vídeos o conversaciones de contenido sexual.	Exigir dinero, nuevas imágenes o encuentros a cambio de no difundir contenido íntimo.
Difusión no consentida de contenido íntimo	Publicación o reenvío de imágenes, audios o vídeos privados sin autorización.	Compartir fotografías íntimas recibidas en un contexto de confianza.
Suplantación de identidad	Creación o uso de perfiles falsos para dañar, manipular o engañar.	Abrir una cuenta con el nombre de una mujer para publicar mensajes ofensivos.

EDITORIAL TUTOR FORMACIÓN

Doxing	Difusión de datos personales, domicilio, teléfono, lugar de trabajo u otra información identificativa.	Publicar la dirección de una mujer para promover ataques contra ella.
Ataques a la reputación	Difusión de rumores, montajes, mensajes falsos o contenidos descontextualizados.	Compartir información manipulada para desacreditar a una profesional.
Acoso sexual digital	Comentarios, imágenes, propuestas o mensajes de carácter sexual no deseados.	Enviar de forma insistente contenidos sexuales a través de mensajería.
Discurso de odio sexista	Mensajes que degradan, atacan o promueven hostilidad contra mujeres o colectivos concretos.	Comentarios que cuestionan la presencia de mujeres en política, ciencia o deporte.
Violencia mediante inteligencia artificial	Uso de herramientas tecnológicas para crear, modificar o difundir contenido dañino.	Generar una imagen sexualizada falsa de una mujer y difundirla como si fuera real.

La Agencia Española de Protección de Datos identifica como ejemplos de violencia digital el acoso en redes sociales, la sextorsión, el seguimiento mediante aplicaciones espía, la suplantación de identidad, los ataques a la reputación y las amenazas a través de redes sociales o mensajería instantánea.

Control digital y vigilancia en relaciones afectivas

El **control digital** puede presentarse de forma gradual y normalizarse como una muestra de interés o confianza. Pedir de manera insistente la ubicación, exigir fotografías para comprobar dónde se encuentra una persona, revisar conversaciones, imponer la entrega de contraseñas o exigir respuesta inmediata a los mensajes son conductas que limitan la autonomía.

En relaciones afectivas, estas prácticas pueden comenzar con peticiones aparentemente informales. Con el tiempo, pueden transformarse en vigilancia constante, aislamiento de amistades, supervisión de contactos, acceso a correos electrónicos, control de horarios o amenazas de difusión de información privada. La persona agresora puede utilizar aplicaciones de geolocalización, cuentas compartidas, dispositivos vinculados, copias de seguridad o perfiles falsos para mantener el control.

Los mensajes de prevención deben evitar culpabilizar a la persona afectada por haber compartido una contraseña, una fotografía o información personal. El control es responsabilidad de quien lo ejerce. La intervención debe centrarse en identificar la conducta, valorar el riesgo y facilitar apoyo seguro.

Algunas señales de alerta pueden ser las siguientes:

- Exigencia de enviar ubicación o fotografías de manera constante.
- Necesidad de responder inmediatamente a mensajes o llamadas.
- Revisión del teléfono, redes sociales o correos electrónicos.
- Imposición de eliminar contactos o dejar de seguir a determinadas personas.
- Presión para compartir contraseñas.
- Uso de dispositivos o aplicaciones para conocer movimientos y actividades.
- Amenazas de publicar conversaciones, fotos o datos personales.
- Creación de perfiles falsos para vigilar, provocar o controlar.

- Revisión de historial de navegación o de aplicaciones instaladas.
- Críticas, insultos o castigos cuando la persona no está disponible en línea.



Nota

Compartir una contraseña o una ubicación no debe entenderse como una prueba de confianza obligatoria. La privacidad forma parte de la autonomía personal y debe respetarse en cualquier relación.

Acoso, amenazas y silenciamiento de mujeres en espacios públicos digitales

Las mujeres que participan activamente en redes sociales, medios digitales, política, divulgación, deporte, cultura, ciencia o activismo pueden recibir ataques dirigidos a su apariencia, vida personal, sexualidad, maternidad o presencia pública. Estos mensajes no suelen centrarse en las ideas expresadas, sino en desacreditar, humillar o expulsar a la mujer del espacio de debate.



El acoso, las amenazas y los comentarios sexistas en línea pueden afectar al bienestar y limitar la participación de las mujeres en los espacios públicos digitales.

El ataque puede proceder de una persona concreta o de múltiples cuentas. En ocasiones adopta la forma de campañas coordinadas, difusión de insultos, comentarios sexualizados, amenazas, publicaciones manipuladas o envío masivo de mensajes. La finalidad puede ser provocar miedo, desgaste emocional, autocensura o abandono de la participación pública.

El Ministerio de Igualdad ha señalado que los ataques sexistas en redes pueden centrarse en la apariencia de las mujeres y no en sus ideas, con un efecto disciplinante que reduce su presencia en el espacio digital y empobrece el debate público.

Esta violencia puede afectar especialmente a mujeres que ocupan posiciones visibles o cuestionan estereotipos de género. También puede dirigirse contra mujeres jóvenes, periodistas, creadoras de contenido, representantes políticas, docentes, investigadoras, deportistas, sindicalistas, activistas o profesionales que trabajan en sectores masculinizados.

La respuesta institucional debe incluir políticas de moderación, protocolos frente a ataques, mecanismos de denuncia, protección de datos y apoyo a las personas afectadas. Las organizaciones que utilizan redes sociales deben establecer criterios claros sobre comentarios discriminatorios, amenazas, difusión de datos personales y contenidos que puedan vulnerar la dignidad de las personas.

Violencia sexual digital y difusión no consentida de contenido íntimo

La difusión no consentida de imágenes, vídeos, audios o conversaciones de carácter íntimo constituye una forma grave de vulneración de la privacidad y de la libertad sexual. Puede ocurrir después de una relación afectiva, durante una situación de chantaje, mediante acceso no autorizado a dispositivos, en grupos de mensajería o a través de plataformas de contenido.

El consentimiento para crear una imagen o compartirla con una persona concreta no equivale al consentimiento para difundirla, reenviarla, almacenarla en otro espacio o utilizarla para chantajear. La responsabilidad corresponde a quien divulga, amenaza con divulgar o colabora en la difusión.

La **sextorsión** se produce cuando una persona utiliza contenido íntimo o sexual para exigir dinero, nuevas imágenes, encuentros, silencio, obediencia o cualquier otra conducta. Puede afectar a mujeres adultas, adolescentes y niñas. La amenaza puede mantenerse durante un periodo prolongado y generar miedo, aislamiento, ansiedad y dificultades para acudir a servicios de apoyo.

La Ley Orgánica 10/2022 presta atención específica a la pornografía no consentida, la difusión de actos de violencia sexual y la extorsión sexual mediante medios tecnológicos.

En este tipo de situaciones, el acompañamiento profesional debe ser respetuoso y evitar preguntas que culpabilicen a la persona afectada. Comentarios como “¿por qué enviaste esa imagen?” trasladan la responsabilidad a quien ha visto vulnerada su intimidad. La actuación debe centrarse en la protección, la reducción de daños, la preservación de información relevante y la activación de recursos especializados cuando sea necesario.

Suplantación de identidad, ataques reputacionales y exposición de datos

La **suplantación de identidad** consiste en utilizar el nombre, la imagen, los datos o la cuenta de otra persona para generar confusión, perjudicarla o manipular su entorno. Puede incluir la creación de perfiles falsos, el uso de fotografías sin autorización, el envío de mensajes en nombre de la víctima o la publicación de contenidos que simulan proceder de ella.

Los **ataques reputacionales** incluyen rumores, publicaciones falsas, descontextualización de mensajes, montajes, campañas de desprestigio y difusión de información personal. Pueden tener consecuencias graves en la vida laboral, educativa, comunitaria o familiar de la persona afectada. Una profesional puede recibir comentarios falsos que cuestionen su competencia; una estudiante puede ser objeto de rumores sexuales; una activista puede sufrir campañas de difamación para limitar su presencia pública.

El **doxing** se refiere a la divulgación de datos personales como domicilio, teléfono, lugar de trabajo, información familiar, ubicación o datos identificativos. Esta práctica puede aumentar el riesgo de acoso presencial, amenazas, hostigamiento a familiares o pérdida de seguridad en la vida cotidiana.

Las entidades deben ser especialmente cuidadosas con la publicación de fotografías, nombres, ubicaciones, agendas y datos de contacto. Una imagen tomada durante una actividad comunitaria puede revelar información sensible sobre la presencia de una mujer en un recurso de apoyo, una

asociación o un servicio especializado. La difusión de estos contenidos debe realizarse con criterios de privacidad, consentimiento y evaluación de riesgos.

Inteligencia artificial, manipulación de imágenes y contenido sintético

Las herramientas de inteligencia artificial generativa permiten crear o modificar imágenes, audios y vídeos de manera rápida. Estas posibilidades pueden utilizarse con fines creativos, educativos o profesionales, aunque también pueden emplearse para producir contenidos falsos, sexualizados, humillantes o descontextualizados.

Los **contenidos sintéticos** pueden incluir imágenes manipuladas, voces imitadas, audios falsos o vídeos que hacen parecer que una persona ha dicho o realizado algo que nunca ocurrió. En los casos más graves, estas herramientas pueden utilizarse para crear imágenes íntimas falsas o sexualizadas de mujeres, menores o personas en situación de especial vulnerabilidad.

La Agencia Española de Protección de Datos ha advertido sobre los riesgos asociados a la generación y difusión de imágenes de terceras personas mediante inteligencia artificial, incluyendo la sexualización, el contenido íntimo sintético, la atribución de hechos no reales con consecuencias reputacionales y la descontextualización de imágenes.

La detección puede resultar compleja porque los contenidos manipulados pueden parecer verosímiles. Por ello, es importante desarrollar competencias de verificación y evitar compartir materiales de origen dudoso. La intervención profesional debe valorar el posible daño, proteger a la persona afectada y activar los mecanismos de retirada o denuncia que correspondan.

Sesgos algorítmicos y desigualdad de oportunidades

Los algoritmos intervienen en la información que aparece en buscadores, redes sociales, plataformas de empleo, servicios de publicidad, recomendaciones de contenido y sistemas de selección automatizada. Estos sistemas utilizan datos, reglas y modelos de clasificación para ordenar, recomendar o priorizar determinados contenidos.

Los **sesgos algorítmicos** pueden producirse cuando los datos de partida contienen desigualdades históricas o cuando las decisiones de diseño reproducen estereotipos de género. Un sistema puede mostrar con mayor frecuencia ofertas de empleo técnico a hombres, recomendar contenidos relacionados con cuidados o belleza a mujeres, asociar determinados perfiles con menor capacidad de liderazgo o limitar el alcance de campañas informativas dirigidas a determinados grupos.

Estas situaciones pueden ser difíciles de detectar porque el funcionamiento técnico suele ser poco transparente para las personas usuarias. La intervención con perspectiva de género debe plantear preguntas sobre quién diseña los sistemas, qué datos se emplean, qué criterios se utilizan para clasificar a las personas y qué grupos pueden quedar excluidos.

La siguiente tabla recoge algunos ámbitos en los que pueden aparecer sesgos:

Ámbito digital	Riesgo de desigualdad	Ejemplo de revisión
Plataformas de empleo	Recomendación desigual de ofertas según perfiles previos.	Comprobar si mujeres y hombres reciben información sobre los mismos sectores y puestos.
Publicidad digital	Segmentación basada en estereotipos o comportamientos históricos.	Revisar si una campaña de formación tecnológica se dirige también a mujeres.

EDITORIAL TUTOR FORMACIÓN

Redes sociales	Priorización de contenidos polémicos, ofensivos o polarizadores.	Analizar la difusión de mensajes sexistas y las medidas de moderación.
Sistemas de selección	Valoración automatizada de currículos con datos sesgados.	Revisar criterios utilizados y posibles efectos sobre candidaturas femeninas.
Plataformas educativas	Recomendación diferenciada de itinerarios o recursos.	Comprobar si se reproducen expectativas de género en la orientación formativa.
Herramientas de inteligencia artificial	Generación de imágenes o textos que reproducen roles tradicionales.	Analizar la representación de mujeres y hombres en respuestas, imágenes y ejemplos.

La revisión de estos sistemas debe formar parte de las políticas de igualdad de organizaciones que utilizan herramientas digitales para seleccionar personal, difundir información, gestionar servicios o relacionarse con la ciudadanía.

Adolescencia, socialización digital y prevención

La adolescencia es una etapa especialmente relevante para la socialización de género y el aprendizaje de relaciones afectivas. Las redes sociales, aplicaciones de mensajería, plataformas de vídeo y videojuegos pueden ser espacios de expresión, amistad, creatividad y participación. También pueden convertirse en escenarios de presión estética, control en parejas jóvenes, ciberacoso, sexualización, difusión de imágenes o discursos que normalizan comportamientos de dominación.



La educación digital y afectivo-sexual ayuda a prevenir riesgos como el ciberacoso, la presión estética o el control en las relaciones adolescentes.

La prevención debe abordar los mensajes que presentan el control como una prueba de amor, la disponibilidad permanente como una obligación o la vigilancia digital como una forma aceptable de relación. El Ministerio de Igualdad identifica el control del móvil y de las redes sociales como una de las señales que conviene detectar en relaciones adolescentes nocivas.

La educación afectivo-sexual y digital debe incluir contenidos sobre consentimiento, privacidad, respeto a los límites, corresponsabilidad, gestión de conflictos, seguridad de las cuentas, verificación de contenidos y prevención de la violencia. También debe promover la reflexión sobre los modelos de feminidad y masculinidad que circulan en redes, videojuegos, publicidad y contenidos audiovisuales.

La Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia, sitúa la prevención, la educación y la detección precoz entre sus prioridades y establece medidas de protección y recuperación frente a situaciones de violencia que afecten a niñas, niños y adolescentes.

Las acciones preventivas deben dirigirse a toda la comunidad educativa y social. El alumnado necesita herramientas para identificar riesgos y pedir ayuda. Las familias requieren información sobre privacidad, acompañamiento y señales de alerta. El profesorado y el personal profesional deben conocer los protocolos de actuación. Los grupos de iguales pueden desempeñar un papel importante para no reenviar contenido dañino, apoyar a la persona afectada y comunicar situaciones de riesgo.

Consecuencias de la violencia digital de género

Las consecuencias de la violencia digital pueden afectar a la salud emocional, las relaciones sociales, la participación pública, la vida laboral, la trayectoria educativa y la seguridad física de las personas afectadas. El daño puede aumentar cuando el contenido se difunde ampliamente, cuando la agresión se prolonga en el tiempo o cuando se combina con violencia presencial.

Entre los efectos que pueden aparecer se encuentran los siguientes:

- Miedo, ansiedad, tristeza, vergüenza o sensación de pérdida de control.
- Aislamiento de amistades, familia, actividades comunitarias o espacios digitales.
- Abandono de perfiles sociales, formación, empleo o participación pública.
- Dificultades de concentración, descanso o rendimiento académico y laboral.
- Daño reputacional y deterioro de relaciones profesionales o familiares.
- Necesidad de cambiar de número de teléfono, cuentas, rutinas o lugares de residencia.
- Riesgo de exposición de datos personales y localización física.
- Dependencia de la persona agresora o aumento de la vigilancia.
- Revictimización cuando el entorno cuestiona, minimiza o difunde el contenido.
- Pérdida de confianza en instituciones, recursos o canales de denuncia.

La AEPD señala que la violencia en línea puede generar daños físicos, psicológicos y económicos, y que las mujeres se ven especialmente afectadas por estas formas de agresión.

La intervención debe evitar interpretar el abandono de redes sociales como una solución suficiente. Retirarse de los espacios digitales puede ser una decisión temporal de autoprotección, aunque también puede limitar el acceso a información, redes de apoyo, oportunidades laborales y participación social. La responsabilidad principal debe recaer en quien ejerce la violencia y en los sistemas que permiten su difusión, no en la persona afectada.

Discriminación múltiple e interseccional en línea

Las desigualdades digitales pueden intensificarse cuando el género se combina con otros factores. Una mujer migrante puede recibir ataques racistas y sexistas. Una mujer con discapacidad puede ser objeto de infantilización, amenazas o explotación de su imagen. Una mujer trans puede encontrar barreras en formularios, perfiles o sistemas de verificación de identidad. Una mujer mayor puede sufrir fraudes, mensajes paternalistas o exclusión de recursos digitalizados. Una mujer rural puede tener dificultades de conectividad y acceso a servicios especializados.

El enfoque interseccional exige evitar la idea de que todas las mujeres experimentan los mismos riesgos o disponen de las mismas herramientas de protección. Las campañas de prevención y los protocolos de intervención deben ser accesibles, comprensibles y adaptados a diferentes situaciones.

La Ley Orgánica 10/2022 establece que las políticas de protección deben tener especialmente en cuenta a las víctimas afectadas por factores superpuestos de discriminación, como discapacidad, edad, origen, orientación sexual, identidad sexual, clase social, migración o situación administrativa. También incorpora la accesibilidad universal y la prevención de la victimización secundaria como principios de actuación.

Detección de situaciones de riesgo en entornos digitales

La detección temprana permite actuar antes de que la violencia se intensifique. En muchos casos, la persona afectada puede no identificar la situación como violencia, especialmente cuando las conductas se han normalizado dentro de una relación afectiva, un grupo de amistades, un entorno escolar o una comunidad digital.

Algunos indicadores que pueden requerir atención son los siguientes:

- Cambios bruscos en el uso del teléfono o redes sociales por miedo a recibir mensajes.
- Necesidad de justificar de forma constante la ubicación, los contactos o el tiempo de conexión.
- Aislamiento de amistades y reducción de la participación en actividades.
- Recepción de mensajes insistentes, insultantes o intimidatorios.
- Presión para enviar imágenes íntimas o mantener conversaciones de contenido sexual.
- Amenazas de difundir fotografías, audios, mensajes o información personal.
- Creación de perfiles falsos o publicaciones que suplantan la identidad de una persona.
- Difusión de rumores, contenido manipulado o datos personales.
- Comentarios repetidos sobre el cuerpo, la sexualidad, la maternidad o la apariencia.
- Retirada de una mujer de espacios de debate por ataques o humillaciones.
- Acceso no autorizado a dispositivos, cuentas o redes sociales.
- Instalación sospechosa de aplicaciones de seguimiento o control.

La detección debe realizarse con sensibilidad. Una profesional no debe presionar a una persona para que relate detalles que no desea compartir. Resulta más adecuado ofrecer un espacio de escucha, formular preguntas abiertas, explicar los recursos disponibles y respetar las decisiones de la persona afectada.

Pautas de actuación ante una posible violencia digital

Cuando se detecta una posible situación de violencia digital, la prioridad debe ser proteger a la persona afectada y evitar actuaciones que puedan incrementar el riesgo. La respuesta dependerá de la gravedad, del tipo de contenido, de la edad de la persona, de la existencia de amenazas y de la relación con la persona agresora.

A continuación, se recogen algunas pautas generales para la intervención profesional:

1. **Escuchar sin juzgar.** La persona debe poder explicar lo ocurrido sin recibir reproches sobre sus decisiones, imágenes, contactos o uso de redes sociales.
2. **Valorar la urgencia y el nivel de riesgo.** Debe analizarse si existen amenazas directas, difusión de datos personales, chantaje, control de ubicación, violencia presencial asociada o riesgo para menores.
3. **Evitar la difusión adicional del contenido.** Las personas que reciben una imagen, vídeo o mensaje dañino deben abstenerse de reenviarlo, comentarlo o almacenarlo innecesariamente.
4. **Conservar la información relevante con seguridad.** Puede ser útil registrar capturas, enlaces, fechas, perfiles o mensajes, siempre evitando exponer de nuevo el contenido íntimo o dañino a otras personas.
5. **Activar los protocolos de la entidad.** Centros educativos, empresas, asociaciones y servicios públicos deben contar con procedimientos claros para comunicar, registrar y atender incidencias.
6. **Orientar hacia recursos especializados.** La derivación puede incluir servicios de igualdad, atención psicológica, asesoramiento jurídico, protección de datos, apoyo a víctimas o recursos de emergencia, según el caso.
7. **Proteger la confidencialidad.** La información debe compartirse únicamente con las personas o servicios necesarios para la atención, evitando rumores, comentarios internos o exposición innecesaria.
8. **Revisar la seguridad digital.** Puede ser necesario cambiar contraseñas, revisar accesos, cerrar sesiones abiertas, actualizar configuraciones de privacidad o solicitar apoyo técnico especializado.
9. **Acompañar durante el proceso.** La retirada de contenido, la denuncia o la activación de recursos pueden generar ansiedad. El acompañamiento debe respetar los tiempos y decisiones de la persona afectada.

La AEPD dispone de un **Canal Prioritario** para solicitar la retirada urgente de fotografías, vídeos o audios de contenido sexual o violento difundidos ilícitamente en internet cuando esa difusión supone un grave riesgo para los derechos, libertades o salud física o mental de la persona afectada.



Nota

Las decisiones de seguridad digital deben adoptarse con cautela cuando existe control por parte de una persona agresora. Cambiar una contraseña, bloquear una cuenta o retirar una aplicación puede alertar a quien vigila el dispositivo. La intervención debe valorar cada situación y buscar apoyo especializado cuando exista riesgo.

Prevención en entidades, centros educativos y organizaciones

Las entidades que desarrollan actividades comunitarias, educativas, laborales o sociales deben incorporar medidas de prevención frente a la violencia digital. No basta con reaccionar cuando aparece una incidencia. Es necesario establecer normas de uso, protocolos, formación, canales de comunicación y medidas de protección de datos.

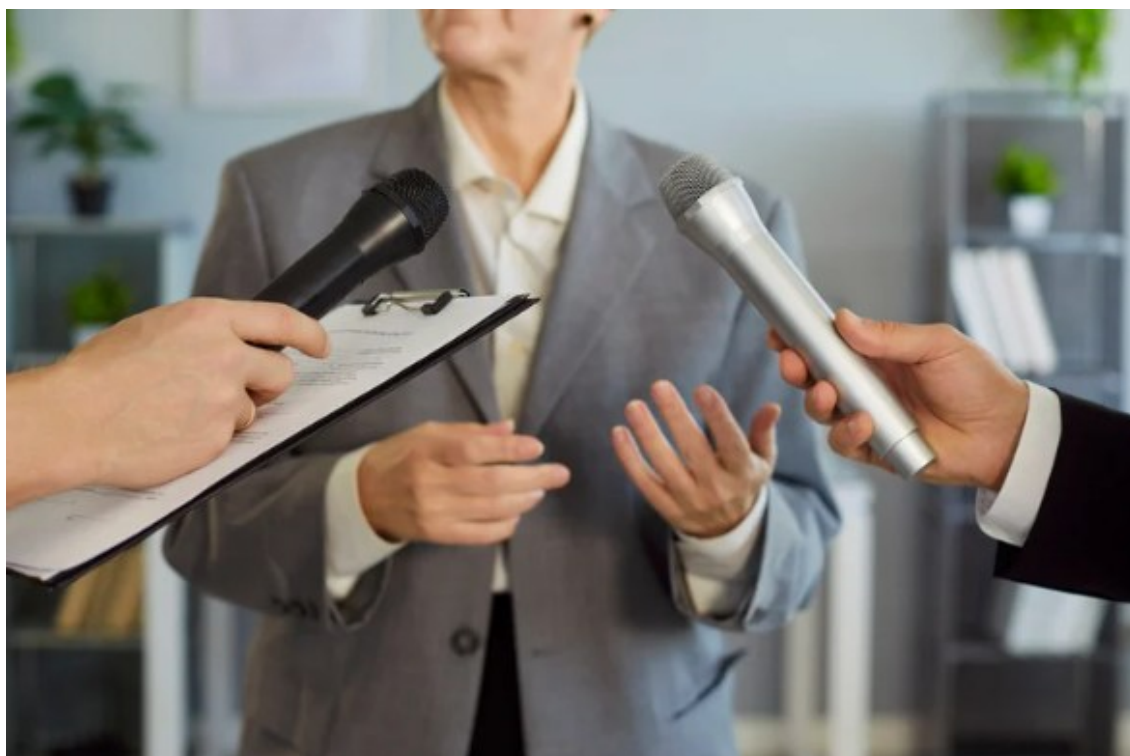
Un plan preventivo puede incluir las siguientes actuaciones:

- Elaborar normas de convivencia digital aplicables a grupos de mensajería, plataformas educativas, redes sociales y actividades en línea.
- Formar al personal en perspectiva de género, violencia digital, privacidad y respuesta ante incidencias.
- Informar a participantes, alumnado, familias o plantilla sobre los canales disponibles para comunicar situaciones de acoso o discriminación.
- Establecer criterios de moderación de comentarios en perfiles institucionales.
- Evitar difundir fotografías, vídeos o datos personales sin la debida valoración de privacidad y consentimiento.
- Incorporar la educación digital y afectivo-sexual en actividades de prevención.
- Analizar la accesibilidad de plataformas, formularios y contenidos.
- Revisar la segmentación de campañas digitales para evitar exclusiones.
- Contar con directorios de recursos especializados para posibles derivaciones.
- Registrar incidencias de forma confidencial para detectar patrones y mejorar las medidas preventivas.

Las organizaciones laborales deben prestar especial atención a los canales internos. Los grupos de mensajería, correos electrónicos, plataformas colaborativas y reuniones virtuales pueden convertirse en espacios de acoso, comentarios sexualizados, difusión de contenido ofensivo o exclusión de trabajadoras. La AEPD señala que el acoso digital puede producirse en el ámbito laboral y que las organizaciones tienen responsabilidad en la protección de la seguridad y salud de su plantilla.

Comunicación institucional segura y con perspectiva de género

La comunicación institucional sobre violencia digital debe informar sin generar miedo, culpabilización o exposición innecesaria. Las campañas deben presentar a las mujeres como titulares de derechos y personas con capacidad de decisión. También deben visibilizar recursos, redes de apoyo, vías de atención y responsabilidades colectivas.



La comunicación institucional debe ofrecer información clara, respetuosa y centrada en los derechos de las personas ante situaciones de violencia digital.

Al elaborar mensajes sobre prevención, conviene evitar fórmulas centradas exclusivamente en la autoprotección de las mujeres, como “no compartas imágenes” o “no publiques información personal”. Estas recomendaciones pueden ser útiles dentro de una estrategia de seguridad digital, aunque no deben trasladar la responsabilidad principal a quienes pueden sufrir violencia.

Una comunicación equilibrada puede incorporar mensajes como los siguientes:

- El control del móvil, las contraseñas o la ubicación no es una muestra de afecto.
- Difundir contenido íntimo sin consentimiento es una forma de violencia.
- Reenviar una imagen dañina contribuye a ampliar el daño.
- Las mujeres tienen derecho a participar en espacios digitales sin recibir ataques sexistas.
- Las organizaciones deben moderar y prevenir mensajes discriminatorios.
- La privacidad y el consentimiento deben estar presentes en cualquier interacción digital.
- Pedir ayuda es una decisión legítima y existen recursos de acompañamiento.
- La tecnología debe utilizarse para ampliar la autonomía, la participación y el acceso a derechos.



Ejemplo

Una asociación crea un grupo de mensajería para organizar actividades de participación vecinal. Durante varias semanas, una participante recibe comentarios sobre su apariencia, bromas sexistas y mensajes que cuestionan su presencia en el grupo. Después de plantear una propuesta sobre seguridad en el barrio, varias personas comparten capturas de sus mensajes fuera del grupo y aparece una cuenta falsa que publica comentarios ofensivos utilizando su nombre.

La situación presenta varias manifestaciones de violencia digital: acoso sexista, desvalorización de la participación, difusión de contenido sin autorización, posible suplantación de identidad y ataque a la reputación. El hecho de que se produzca dentro de un grupo comunitario no reduce su gravedad.

La asociación debería activar un procedimiento de actuación. En primer lugar, debe escuchar a la persona afectada y ofrecer un espacio de atención confidencial. Después, puede registrar la incidencia, revisar las pruebas disponibles, limitar la difusión de capturas, comunicar las normas de convivencia digital al grupo, retirar mensajes ofensivos cuando sea posible y bloquear perfiles que incumplan esas normas. También debe valorar la necesidad de derivar a recursos especializados, especialmente si existen amenazas, difusión de datos personales o riesgo de que la violencia se extienda a otros espacios.

La entidad puede utilizar el caso para revisar su funcionamiento interno. Resultaría recomendable establecer normas claras al crear grupos de mensajería, designar personas responsables de moderación, informar de los canales de incidencia y recordar que las capturas, fotografías y mensajes no deben difundirse sin autorización.

Herramienta de diagnóstico de riesgos digitales con perspectiva de género

Antes de poner en marcha una actividad digital, una campaña, una plataforma de participación o un grupo de mensajería, puede aplicarse una revisión preventiva. La siguiente tabla ofrece una propuesta de análisis:

Área de revisión	Preguntas orientadoras
Acceso	¿Las personas destinatarias disponen de canales alternativos si no tienen conexión, dispositivos o competencias digitales suficientes?
Privacidad	¿La actividad requiere datos personales? ¿Son necesarios? ¿Qué medidas protegen esa información?
Seguridad	¿Existe riesgo de que una persona agresora acceda a la información o a los dispositivos utilizados?
Accesibilidad	¿La plataforma puede ser utilizada por personas con distintas capacidades y niveles de alfabetización digital?
Moderación	¿Hay normas claras frente a insultos, acoso, amenazas, sexualización o difusión de datos personales?
Participación	¿Las mujeres pueden intervenir sin temor a burlas, interrupciones o ataques coordinados?
Representación	¿Los contenidos muestran a mujeres diversas como participantes, expertas y referentes?
Segmentación	¿Las campañas digitales pueden excluir a determinados grupos por criterios estereotipados?

EDITORIAL TUTOR FORMACIÓN

Protocolos	¿La entidad sabe qué hacer ante una amenaza, una difusión no consentida o una situación de acoso?
Derivación	¿Existen recursos especializados identificados para apoyar a las personas afectadas?
Seguimiento	¿Se registran las incidencias de forma confidencial para detectar patrones y mejorar las medidas preventivas?

La identificación de desigualdades y violencias de género en entornos digitales exige reconocer que la tecnología puede ampliar la autonomía y la participación, pero también reproducir relaciones de poder, estereotipos y formas de control. La prevención requiere formación, protocolos, accesibilidad, protección de la privacidad, moderación responsable y una intervención centrada en los derechos, la seguridad y la autonomía de las personas afectadas.



Actividad 9

Una organización observa que varias mujeres han dejado de participar en un grupo digital tras recibir comentarios sobre su aspecto físico. Indica dos riesgos presentes en esta situación y propón tres medidas de actuación para mejorar la seguridad del espacio.

5. Procedimientos de detección y registro de incidencias.

La detección de situaciones de discriminación por razón de género, sexismo, acoso o violencia en los procesos de comunicación exige contar con procedimientos claros y conocidos por las personas implicadas. Una incidencia puede surgir en una reunión, una actividad formativa, una campaña, una conversación de atención al público, un grupo de mensajería, una red social, una plataforma educativa o cualquier otro espacio donde se intercambie información. La existencia de un procedimiento facilita una respuesta organizada, evita improvisaciones y ayuda a proteger a las personas afectadas.

Los procedimientos de detección y registro deben adaptarse al tipo de entidad, a la población destinataria, a los canales utilizados y a los recursos disponibles. Una administración pública, un centro educativo, una asociación, una empresa, un servicio social o un proyecto comunitario pueden enfrentarse a situaciones diferentes, aunque todos comparten la necesidad de establecer pautas para identificar conductas discriminatorias, registrar la información relevante, valorar el riesgo y activar las medidas de apoyo o derivación que correspondan.

El registro de una incidencia no implica automáticamente presentar una denuncia formal ni iniciar un procedimiento disciplinario. Su función principal es dejar constancia de una situación que puede requerir atención, seguimiento o medidas preventivas. También permite identificar patrones: por ejemplo, comentarios sexistas reiterados en reuniones, exclusión de mujeres de espacios de decisión, ataques a participantes en redes sociales o dificultades persistentes para acceder a información relevante.

Un procedimiento adecuado debe equilibrar varios objetivos: proteger a la persona afectada, garantizar la confidencialidad, evitar la revictimización, recoger datos útiles y permitir que la entidad adopte decisiones proporcionadas. La información debe registrarse con rigor, aunque sin exigir a las personas afectadas que relaten una experiencia más veces de las necesarias ni que aporten pruebas que no estén en condiciones de facilitar.

Finalidad de los procedimientos de detección y registro
--

Los procedimientos de detección permiten reconocer situaciones que pueden pasar inadvertidas o normalizarse dentro de una organización, un grupo o una comunidad. Algunas conductas discriminatorias se presentan mediante bromas, comentarios aparentemente informales, exclusión de determinados canales de información, interrupciones reiteradas o uso de imágenes estereotipadas. Cuando estas prácticas no se registran ni se analizan, pueden repetirse y consolidarse como formas habituales de relación.

El registro de incidencias cumple varias funciones. Entre las más relevantes se encuentran las siguientes:

- **Dar respuesta a una situación concreta** comunicada por una persona afectada, testigo o profesional.
- **Proteger a las personas implicadas**, especialmente cuando existe riesgo de acoso, violencia, exposición pública o represalias.
- **Documentar los hechos** de manera ordenada, evitando pérdidas de información relevante.
- **Facilitar la activación de protocolos internos** de igualdad, convivencia, prevención del acoso, protección de datos o atención a víctimas.

- **Orientar la derivación** hacia recursos especializados cuando la situación supera las competencias de la entidad.
- **Identificar patrones de desigualdad**, como comentarios sexistas frecuentes, exclusión de mujeres de espacios de participación o ataques digitales reiterados.
- **Mejorar los procesos comunicativos**, revisando canales, normas de convivencia, materiales, horarios, accesibilidad y mecanismos de moderación.
- **Evaluar la eficacia de las medidas adoptadas**, comprobando si las incidencias disminuyen o si aparecen nuevas formas de discriminación.

El objetivo del registro no es acumular información sobre las personas, sino disponer de datos suficientes para actuar de forma responsable. Por esta razón, deben recogerse únicamente los datos necesarios para comprender la situación, proteger a las personas afectadas y orientar una respuesta adecuada.



Nota

Registrar una incidencia no equivale a cuestionar el relato de la persona afectada. El procedimiento debe partir de la escucha, el respeto y la valoración de las necesidades de protección, sin exigir pruebas imposibles ni trasladar a la víctima la responsabilidad de resolver la situación.

Qué se considera una incidencia comunicativa

Una **incidencia comunicativa con perspectiva de género** es cualquier hecho, mensaje, conducta, omisión o dinámica que pueda generar discriminación, exclusión, acoso, violencia, inseguridad o desigualdad en el acceso a la información y a la participación.

Las incidencias pueden ser puntuales o repetidas. También pueden tener distinta gravedad. Un comentario sexista aislado, una campaña con imágenes estereotipadas, una exclusión reiterada de mujeres en reuniones, una amenaza en redes sociales o la difusión no consentida de información íntima requieren respuestas diferentes. Sin embargo, todas deben poder ser detectadas y valoradas mediante criterios claros.

La siguiente tabla recoge algunos ejemplos de incidencias que pueden aparecer en procesos de comunicación e información:

Tipo de incidencia	Ejemplo	Posible respuesta inicial
Lenguaje sexista	Uso de expresiones ofensivas, paternalistas o que invisibilizan a las mujeres.	Revisar el contenido, corregirlo y registrar la incidencia si existe reiteración o afectación a personas concretas.
Representación estereotipada	Campaña que muestra a mujeres únicamente como cuidadoras y a hombres como responsables técnicos.	Revisar el material, sustituir imágenes y establecer criterios de diseño inclusivo.
Exclusión de la participación	Mujeres que no reciben información sobre reuniones o	Analizar canales, horarios, responsables de difusión y mecanismos de convocatoria.

EDITORIAL TUTOR FORMACIÓN

	quedan fuera de decisiones relevantes.	
Interrupciones y desvalorización	Una participante es interrumpida de forma reiterada o sus propuestas no se recogen.	Registrar la dinámica, intervenir en la reunión y revisar normas de participación.
Acoso por razón de sexo	Comentarios humillantes sobre embarazo, maternidad, apariencia o presencia de una mujer en un puesto.	Activar el protocolo interno correspondiente y proteger a la persona afectada.
Acoso sexual	Mensajes, bromas o contenidos de carácter sexual no deseados.	Valorar urgencia, activar medidas de protección y derivar si procede.
Violencia digital	Amenazas, control del teléfono, difusión de imágenes, suplantación de identidad o ataques coordinados.	Preservar información relevante, valorar riesgo y activar recursos especializados.
Falta de accesibilidad	Información relevante difundida solo mediante una plataforma difícil de utilizar.	Incorporar canales alternativos y revisar barreras de acceso.
Difusión inadecuada de datos	Publicación de fotos, nombres o información personal sin valorar su impacto.	Retirar o limitar el contenido, revisar consentimiento y reforzar medidas de privacidad.
Revictimización	Preguntas culpabilizadoras o difusión de detalles innecesarios sobre una situación de violencia.	Corregir el tratamiento, proteger la confidencialidad y revisar el procedimiento de atención.

La clasificación ayuda a organizar la respuesta, aunque las situaciones reales pueden combinar varias manifestaciones. Una campaña digital, por ejemplo, puede incluir imágenes estereotipadas, excluir a determinados grupos mediante su segmentación y recibir comentarios sexistas que no son moderados. El análisis debe atender al conjunto de elementos presentes.

Principios que deben orientar la detección y el registro

Los procedimientos deben diseñarse antes de que aparezca una incidencia. Cuando una entidad dispone de pautas claras, las personas responsables pueden actuar con mayor seguridad y evitar respuestas que agraven la situación.

Los siguientes principios deben estar presentes en todo el proceso:

Principio	Aplicación práctica
Respeto y dignidad	Escuchar sin ridiculizar, minimizar ni cuestionar de forma innecesaria la experiencia comunicada.
Confidencialidad	Limitar el acceso a la información a las personas responsables de gestionar la incidencia.
Protección frente a represalias	Evitar que la persona afectada sufra consecuencias negativas por comunicar una situación.
No revictimización	Evitar que la persona tenga que repetir su relato ante múltiples profesionales o grupos.

Perspectiva de género	Analizar cómo influyen los roles, estereotipos, relaciones de poder y desigualdades estructurales.
Enfoque interseccional	Considerar factores como edad, discapacidad, origen, situación económica, identidad de género, orientación sexual o lugar de residencia.
Proporcionalidad	Ajustar la respuesta a la gravedad, continuidad y efectos de la incidencia.
Accesibilidad	Ofrecer canales de comunicación comprensibles, seguros y adaptados a diferentes necesidades.
Objetividad en el registro	Diferenciar entre hechos observados, información aportada, interpretaciones y medidas adoptadas.
Seguimiento	Comprobar si la situación se resuelve, si se repite o si requiere nuevas medidas.

La aplicación de estos principios es especialmente importante cuando una persona comunica una situación de acoso, violencia sexual, control digital o discriminación continuada. En estos casos, el primer contacto puede influir en que la persona se sienta acompañada y pueda acceder a recursos de protección.

Canales para detectar incidencias

Las incidencias pueden detectarse de forma directa o indirecta. Algunas personas comunican lo ocurrido de manera expresa; otras pueden mostrar señales de malestar, evitar determinados espacios, reducir su participación o pedir ayuda sin utilizar términos como “acoso” o “violencia”.



La atención individualizada y la escucha activa facilitan la detección de incidencias y la identificación de necesidades de apoyo.

EDITORIAL TUTOR FORMACIÓN

La detección puede producirse a través de varios canales. Entre ellos se encuentran los siguientes:

- Comunicación directa de la persona afectada.
- Comunicación realizada por una persona testigo.
- Observación profesional durante una reunión, actividad o atención individual.
- Revisión de materiales, campañas o publicaciones antes o después de su difusión.
- Mensajes recibidos mediante formularios, buzones de sugerencias o canales de quejas.
- Incidencias detectadas en redes sociales, grupos de mensajería o plataformas digitales.
- Datos de participación que muestran desigualdades persistentes.
- Encuestas de satisfacción, cuestionarios de clima o evaluaciones de actividades.
- Informes de moderación de contenidos digitales.
- Comentarios recogidos en grupos de discusión o entrevistas.
- Revisión de indicadores desagregados por sexo y otras variables relevantes.

La existencia de diferentes canales facilita que las personas puedan elegir la vía que les resulte más segura. Algunas personas preferirán hablar directamente con una profesional de referencia; otras pueden necesitar utilizar un formulario confidencial, un correo electrónico o un canal externo al grupo donde se ha producido la incidencia.

La entidad debe informar con claridad sobre estos mecanismos. Las personas participantes, trabajadoras, usuarias o integrantes de una comunidad deben conocer dónde pueden acudir, qué tipo de situaciones pueden comunicar y qué ocurrirá después de presentar una incidencia.



Nota

Un canal de comunicación solo resulta útil cuando es accesible, conocido y percibido como seguro. Si las personas temen ser cuestionadas, identificadas públicamente o sufrir represalias, es probable que muchas incidencias no lleguen a registrarse.

Detección temprana: señales que requieren atención

La detección temprana no consiste en interpretar cualquier desacuerdo como una situación de discriminación. Los espacios comunitarios, educativos y laborales pueden incluir diferencias de opinión, conflictos puntuales o problemas de comunicación que requieren mediación. La perspectiva de género permite analizar si estas situaciones se relacionan con estereotipos, desigualdades de poder, exclusión, sexualización, control o desvalorización de las mujeres.

Algunas señales que pueden requerir una observación más detenida son las siguientes:

- Una mujer deja de participar en reuniones en las que antes intervenía con frecuencia.
- Una participante evita hablar después de recibir comentarios burlones o descalificadores.
- Se repiten bromas, mensajes o imágenes sexistas en un grupo de trabajo o mensajería.
- Las mujeres reciben preguntas sobre su vida personal, maternidad o disponibilidad que no se dirigen a los hombres.

- Las propuestas realizadas por mujeres se ignoran o solo se reconocen cuando las repite un hombre.
- Determinadas mujeres no reciben información relevante sobre actividades, convocatorias o procesos de decisión.
- Las imágenes y mensajes de una entidad muestran de forma constante roles de género estereotipados.
- Las mujeres aparecen de forma minoritaria como fuentes expertas, portavoces o responsables de proyectos.
- Una participante recibe ataques en redes sociales después de expresar una opinión.
- Una persona manifiesta miedo a utilizar el teléfono, revisar mensajes o participar en espacios digitales.
- Se detectan perfiles falsos, difusión de capturas, amenazas o publicaciones que revelan información personal.
- Una mujer abandona una actividad, una formación o una red comunitaria después de una situación de humillación o acoso.

Estas señales no deben interpretarse de forma automática. Pueden requerir una conversación cuidadosa, una observación adicional o la revisión de los canales de participación. La actuación debe respetar la voluntad de la persona afectada y evitar que la detección se convierta en una nueva fuente de presión.

Fases de un procedimiento de detección y registro

Un procedimiento puede organizarse en fases para facilitar que todas las personas responsables actúen de manera coordinada. La extensión de cada fase dependerá de la gravedad de la situación y del contexto de la entidad.

1. Recepción de la incidencia:

La primera fase consiste en recibir la comunicación, observación o aviso relacionado con una posible situación de discriminación. La persona que atiende debe ofrecer una escucha respetuosa y explicar, de forma comprensible, qué pasos pueden seguirse.

En esta fase conviene:

- Facilitar un espacio privado y seguro para la conversación.
- Escuchar sin interrumpir ni presionar a la persona para que aporte más información de la que desea compartir.
- Evitar preguntas culpabilizadoras o centradas en decisiones personales de la persona afectada.
- Explicar los límites de confidencialidad, especialmente si existe riesgo grave para la persona o para terceras personas.
- Informar sobre las opciones disponibles dentro de la entidad.
- Valorar si se requiere una medida inmediata de protección.
- Preguntar qué necesita la persona en ese momento.

La escucha inicial debe diferenciar entre la información que la persona desea comunicar y las interpretaciones que pueda hacer la profesional. El registro debe recoger los hechos de forma clara, sin añadir juicios de valor ni conclusiones anticipadas.

2. Valoración inicial de urgencia y riesgo:

Después de recibir la incidencia, debe realizarse una valoración inicial para determinar si existe una situación que requiere actuación inmediata. Esta valoración no sustituye una evaluación especializada de riesgo, aunque permite decidir si es necesario activar recursos urgentes.

Algunos elementos que pueden indicar mayor gravedad son los siguientes:

- Amenazas directas contra la integridad física o psicológica de una persona.
- Difusión o amenaza de difusión de contenido íntimo.
- Control de dispositivos, ubicación o comunicaciones.
- Acoso sexual persistente o mensajes de carácter sexual no deseados.
- Exposición de datos personales, domicilio, teléfono o lugar de trabajo.
- Ataques coordinados en redes sociales.
- Existencia de violencia presencial asociada.
- Participación de niñas, niños o adolescentes.
- Riesgo de represalias dentro de una organización o comunidad.
- Aislamiento de la persona afectada o falta de red de apoyo.
- Necesidad de retirar de forma urgente un contenido perjudicial.

Cuando se detecte un riesgo elevado, la prioridad debe ser la protección. La entidad debe activar los recursos especializados, servicios de emergencia o mecanismos internos previstos en sus protocolos, según la naturaleza de la situación.

3. Clasificación inicial de la incidencia:

La clasificación permite organizar la información y orientar la respuesta. No tiene como finalidad realizar una calificación jurídica definitiva. Una entidad puede registrar una situación como posible lenguaje sexista, exclusión de participación, acoso por razón de sexo, acoso sexual, violencia digital, falta de accesibilidad o difusión indebida de información, entre otras categorías.

Una clasificación inicial puede incluir los siguientes aspectos:

Aspecto	Preguntas orientadoras
Tipo de incidencia	¿Se trata de lenguaje sexista, exclusión, acoso, violencia digital, falta de accesibilidad u otra situación?
Canal o espacio	¿Ha ocurrido en una reunión, red social, grupo de mensajería, actividad presencial, campaña o atención individual?
Personas implicadas	¿Quién comunica la situación? ¿Existen personas afectadas, testigos o responsables de la conducta?
Frecuencia	¿Se trata de un hecho aislado o de una conducta repetida?

EDITORIAL TUTOR FORMACIÓN

Impacto	¿Ha afectado a la participación, la seguridad, el bienestar, la imagen pública o el acceso a derechos?
Riesgo	¿Existen amenazas, control, exposición de datos, violencia sexual o posibles represalias?
Medidas previas	¿La situación ya había sido comunicada o se habían adoptado medidas anteriormente?

La clasificación debe revisarse si aparece nueva información. Una incidencia registrada inicialmente como conflicto comunicativo puede revelar posteriormente una situación de acoso o violencia digital. El procedimiento debe permitir actualizar los datos sin borrar la información inicial.

4. Registro de la incidencia:

El registro debe realizarse lo antes posible, utilizando un formato claro y seguro. Conviene diferenciar entre información objetiva, relato de la persona afectada, observaciones de la profesional y medidas adoptadas.

La ficha de registro debe recoger únicamente los datos necesarios. No es recomendable incluir detalles íntimos, información irrelevante o interpretaciones que puedan perjudicar a la persona afectada.

A continuación, se presenta un modelo orientativo de ficha.

Apartado	Información que puede recogerse
Código de incidencia	Número o referencia interna que permita identificar el caso sin utilizar datos visibles para terceras personas.
Fecha y hora de recepción	Momento en que se comunica o detecta la situación.
Canal de detección	Comunicación directa, observación, formulario, red social, correo electrónico, testimonio de tercera persona u otro medio.
Espacio donde ocurrió	Reunión, actividad, grupo de mensajería, red social, plataforma digital, atención presencial o material comunicativo.
Descripción objetiva de los hechos	Relato breve, claro y ordenado de lo ocurrido, evitando valoraciones personales.
Tipo de incidencia	Lenguaje sexista, exclusión, acoso, violencia digital, representación estereotipada, falta de accesibilidad u otra categoría.
Personas afectadas	Datos mínimos necesarios, utilizando códigos o mecanismos que preserven la confidencialidad cuando sea posible.
Personas testigos	Información relevante sobre quienes pudieron observar o conocer los hechos.
Evidencias disponibles	Capturas, enlaces, fotografías, correos, mensajes, documentos o registros de observación.

EDITORIAL TUTOR FORMACIÓN

Valoración inicial de riesgo	Bajo, medio, alto o urgente, según los criterios internos establecidos.
Medidas adoptadas	Escucha inicial, retirada de contenido, moderación, derivación, activación de protocolo, adaptación de canal u otras acciones.
Persona responsable del seguimiento	Profesional o equipo designado para mantener la atención y actualizar el registro.
Fecha de revisión	Momento previsto para comprobar la evolución de la incidencia.
Cierre o continuidad	Información sobre la resolución, seguimiento pendiente o necesidad de nuevas medidas.

La ficha debe diseñarse de forma accesible. Las personas responsables deben recibir formación para completarla con lenguaje respetuoso y preciso. Expresiones como “la persona exagera”, “parece un malentendido” o “posible problema personal” no son adecuadas si no están respaldadas por información objetiva y pueden invalidar el relato de quien comunica una situación.

5. Adopción de medidas iniciales:

Una vez registrada la incidencia, deben adoptarse medidas ajustadas a la situación. Algunas actuaciones pueden realizarse de forma inmediata, mientras que otras requerirán análisis, coordinación o derivación.

Las medidas iniciales pueden incluir:

- Retirar o corregir un contenido sexista o discriminatorio.
- Moderar comentarios ofensivos en una red social o grupo de mensajería.
- Suspender la difusión de imágenes o datos personales.
- Revisar una convocatoria, un horario o un canal que esté generando exclusión.
- Facilitar acompañamiento a la persona afectada.
- Activar normas de convivencia en una reunión o actividad.
- Limitar el contacto entre personas cuando exista riesgo de acoso o represalias.
- Informar sobre recursos especializados.
- Recoger y conservar información relevante de forma segura.
- Comunicar la situación a la persona o unidad responsable dentro de la entidad.
- Revisar medidas de accesibilidad y participación.

La actuación debe ser proporcional. Una campaña con lenguaje excluyente puede requerir revisión y corrección; un caso de amenazas, difusión de contenido íntimo o acoso sexual puede necesitar una respuesta urgente y coordinada con recursos especializados.

6. Seguimiento y cierre:

El seguimiento permite comprobar si las medidas adoptadas han sido eficaces y si la persona afectada continúa necesitando apoyo. Una incidencia no debe considerarse resuelta únicamente

porque se haya retirado una publicación o porque la persona agresora haya dejado de participar temporalmente.

Durante el seguimiento conviene valorar:

- Si la conducta se ha repetido.
- Si la persona afectada se siente segura.
- Si existen nuevas amenazas, comentarios o formas de represalia.
- Si los contenidos ofensivos siguen circulando en otros canales.
- Si los cambios realizados han mejorado el acceso a la información o la participación.
- Si se han producido efectos negativos no previstos.
- Si es necesario ampliar la derivación o activar nuevos recursos.
- Si la entidad debe modificar sus normas, protocolos o canales de comunicación.

El cierre debe registrarse de forma clara, indicando las medidas adoptadas, los resultados observados y las acciones pendientes. Cuando la situación requiera seguimiento prolongado, el expediente debe mantenerse activo según los criterios de la entidad y respetando la normativa aplicable de protección de datos.

Registro de incidencias digitales

Las incidencias digitales requieren precauciones específicas porque los contenidos pueden difundirse rápidamente, desaparecer de una plataforma o replicarse en otros espacios. El registro debe recoger información que permita comprender qué ocurrió, cuándo, en qué canal y qué alcance tuvo.

Cuando sea seguro hacerlo, conviene registrar:

- Nombre de la plataforma, red social, aplicación o servicio utilizado.
- Enlace o dirección concreta del contenido.
- Fecha y hora aproximada de publicación o recepción.
- Nombre de usuario, perfil o identificador visible.
- Capturas de pantalla que muestren el contenido, el perfil y la fecha.
- Tipo de interacción: comentario, mensaje directo, publicación, vídeo, imagen, perfil falso, difusión de datos u otro formato.
- Número aproximado de personas alcanzadas o participantes, cuando sea relevante.
- Posibles reenvíos, menciones o publicaciones relacionadas.
- Acciones realizadas por la plataforma: retirada, bloqueo, denuncia, restricción o respuesta recibida.
- Riesgos asociados: amenazas, exposición de datos, contenido íntimo, chantaje, control de ubicación o ataques coordinados.

La recogida de evidencias debe realizarse evitando ampliar la difusión del daño. No es adecuado reenviar contenido íntimo, almacenarlo en dispositivos personales o compartirlo con personas ajenas al procedimiento. La entidad debe contar con pautas de custodia, acceso restringido y eliminación segura de la información cuando ya no sea necesaria.



Nota

En casos de difusión no consentida de contenido íntimo, la prioridad es reducir la exposición y proteger a la persona afectada. La recopilación de información debe limitarse a lo estrictamente necesario para activar los recursos de apoyo, retirada o protección.

Confidencialidad, privacidad y protección de datos

El tratamiento de incidencias relacionadas con discriminación, acoso o violencia implica manejar información especialmente sensible. Los registros pueden contener datos sobre salud, vida personal, relaciones, orientación sexual, identidad de género, situación familiar, violencia sufrida, comunicaciones privadas o circunstancias laborales. Por este motivo, la confidencialidad debe estar presente en todas las fases.



La protección de los datos y el acceso restringido a los registros son esenciales para garantizar la confidencialidad de las personas afectadas.

La entidad debe definir quién puede acceder a los registros, dónde se almacenan, durante cuánto tiempo se conservan y qué medidas de seguridad se aplican. También debe evitar que la información circule mediante canales informales, grupos de mensajería no seguros o correos compartidos sin control.

Para proteger la privacidad, conviene aplicar las siguientes medidas:

- Utilizar códigos internos en lugar de nombres completos cuando sea posible.
- Limitar el acceso a los registros a las personas responsables de gestionar la incidencia.
- Evitar incluir datos personales que no sean necesarios.
- Guardar documentos y evidencias en espacios protegidos.

EDITORIAL TUTOR FORMACIÓN

- No compartir capturas, mensajes o fotografías en grupos de trabajo informales.
- Informar a la persona afectada sobre el uso que se hará de sus datos.
- Evitar divulgar detalles de una situación durante reuniones o actividades generales.
- Establecer plazos de conservación ajustados a la finalidad del registro.
- Eliminar de forma segura la información que ya no sea necesaria.
- Formar al personal sobre confidencialidad, privacidad y tratamiento respetuoso de la información.

La confidencialidad no significa aislamiento. Puede ser necesario compartir información con recursos especializados, responsables de protocolo o servicios competentes. Esta comunicación debe realizarse de forma justificada, limitada y orientada a la protección de la persona afectada.

Evitar la revictimización durante el procedimiento

La **revictimización** puede producirse cuando una persona que comunica una situación de discriminación o violencia recibe un trato que aumenta su malestar, cuestiona su relato o la obliga a revivir los hechos de manera innecesaria. Puede aparecer mediante preguntas culpabilizadoras, comentarios minimizadores, exposición pública, exigencia de pruebas imposibles o repetición constante de entrevistas.

Para evitarla, resulta recomendable:

- Escuchar con atención y recoger la información de forma ordenada desde el primer contacto.
- Evitar frases como “seguro que no fue para tanto”, “quizá lo entendiste mal” o “deberías haberlo evitado”.
- No cuestionar por qué la persona compartió una imagen, aceptó una conversación, asistió a una actividad o utilizó un determinado canal.
- No pedir detalles íntimos que no sean necesarios para la intervención.
- No obligar a la persona a enfrentarse a quien ha realizado la conducta.
- Evitar que tenga que repetir su relato ante diferentes profesionales sin necesidad.
- Explicar cada paso del procedimiento y solicitar su participación en las decisiones que le afecten.
- Respetar sus tiempos, necesidades y límites.
- Mantener una comunicación clara sobre las medidas adoptadas.
- Facilitar apoyo especializado cuando la situación lo requiera.

La persona afectada debe conservar la mayor capacidad posible de decisión sobre el proceso. La entidad puede informar, orientar y activar medidas de protección, pero debe evitar sustituir la voluntad de la persona salvo en situaciones de riesgo grave o cuando existan obligaciones específicas de actuación.

Roles y responsabilidades dentro de la entidad

Un procedimiento eficaz requiere que las funciones estén definidas con antelación. Cuando no existe claridad sobre quién recibe una incidencia, quién registra los hechos, quién adopta medidas o quién realiza el seguimiento, pueden producirse retrasos, duplicidades o respuestas contradictorias.

La siguiente tabla presenta una distribución orientativa de responsabilidades:

Rol o figura	Responsabilidades principales
Persona de referencia	Recibir la comunicación inicial, escuchar, informar y orientar sobre los pasos disponibles.
Equipo responsable de igualdad o convivencia	Valorar la incidencia, proponer medidas y coordinar actuaciones internas.
Responsable de comunicación	Revisar y corregir contenidos, moderar canales y aplicar criterios de comunicación no sexista.
Dirección o coordinación de la entidad	Garantizar recursos, aprobar medidas organizativas y asegurar el cumplimiento del procedimiento.
Profesionales de atención directa	Detectar señales, registrar observaciones relevantes y facilitar derivaciones.
Moderación digital	Vigilar comentarios, retirar contenido ofensivo, bloquear perfiles cuando proceda y registrar incidencias.
Personas participantes o plantilla	Conocer las normas, comunicar situaciones de riesgo y evitar difundir contenido dañino.
Recursos especializados externos	Ofrecer atención jurídica, psicológica, social, técnica o de protección cuando la situación lo requiera.

En entidades pequeñas, una misma persona puede asumir varias funciones. En estos casos, resulta esencial establecer apoyos externos y evitar que una única profesional gestione situaciones complejas sin supervisión ni recursos suficientes.

Procedimientos específicos según el contexto

Los procedimientos deben adaptarse al espacio donde se producen las incidencias. No requiere la misma respuesta una campaña institucional, una reunión vecinal, un grupo de mensajería de familias, una red social corporativa o una actividad educativa con adolescentes.

○ **En actividades comunitarias:**

En actividades comunitarias, resulta importante establecer normas de participación desde el inicio. Estas normas pueden incluir respeto a los turnos de palabra, prohibición de comentarios sexistas, rechazo de burlas y mecanismos para comunicar incidencias.

También conviene prever horarios inclusivos, canales de propuesta alternativos y medidas que faciliten la participación de mujeres con responsabilidades de cuidado, dificultades de movilidad o menor acceso digital.

○ **En organizaciones laborales:**

En el ámbito laboral, las incidencias pueden aparecer en correos electrónicos, grupos de mensajería, reuniones, plataformas colaborativas, procesos de selección, comunicaciones internas o actividades

de representación. Las empresas y organizaciones deben coordinar los registros de incidencias con sus protocolos de igualdad, prevención del acoso y protección de datos.

La comunicación sobre estos procedimientos debe llegar a toda la plantilla, incluidas las personas con trabajo a distancia, turnos variables, contratos temporales o menor acceso a canales corporativos.

○ **En centros educativos:**

En centros educativos, la detección debe incorporar la observación de relaciones entre iguales, grupos de mensajería, redes sociales, actividades formativas y materiales utilizados en el aula. Las situaciones que afectan a menores requieren una actuación especialmente cuidadosa, coordinada con los protocolos de convivencia y protección existentes.

La prevención debe incluir educación afectivo-sexual, alfabetización digital, respeto a la privacidad, análisis crítico de estereotipos y formación para profesorado, alumnado y familias.

○ **En redes sociales y espacios digitales:**

Las entidades que gestionan perfiles digitales deben establecer normas de moderación visibles. Estas normas pueden indicar que no se permitirán insultos, amenazas, comentarios sexistas, difusión de datos personales, contenido sexual no solicitado o ataques dirigidos contra participantes.

La moderación debe combinar rapidez y registro. Retirar un comentario ofensivo puede ser necesario para proteger a la persona afectada, aunque también conviene conservar de manera segura la información necesaria para valorar la incidencia y realizar un seguimiento.

Errores frecuentes en la gestión de incidencias

La detección y el registro pueden perder eficacia cuando se cometen determinados errores. Identificarlos ayuda a mejorar los procedimientos internos.

Error frecuente	Riesgo que genera	Alternativa adecuada
Restar importancia a la situación	La persona afectada puede dejar de pedir ayuda.	Escuchar, registrar y valorar con seriedad.
Pedir pruebas inmediatas como condición para actuar	Puede impedir la protección ante situaciones de riesgo.	Recoger la información disponible y valorar medidas preventivas.
Tratar el hecho como un conflicto entre iguales sin analizar el género	Puede ocultar relaciones de poder y discriminación.	Aplicar perspectiva de género e interseccional.
Compartir la información con demasiadas personas	Aumenta la exposición y el riesgo de represalias.	Limitar el acceso a quienes deban intervenir.
Usar grupos de mensajería para gestionar casos sensibles	Puede vulnerar la privacidad y difundir datos.	Utilizar canales internos seguros y restringidos.
Obligar a la persona afectada a enfrentarse a quien ha ejercido la conducta	Puede aumentar el malestar y el riesgo.	Respetar su voluntad y valorar alternativas de intervención.

EDITORIAL TUTOR FORMACIÓN

Corregir solo el contenido sin revisar la causa	La incidencia puede repetirse.	Analizar normas, canales, formación y dinámicas organizativas.
Cerrar el caso demasiado pronto	Puede invisibilizar represalias o repetición de conductas.	Establecer seguimiento y fechas de revisión.
Centrar la prevención solo en la autoprotección de las mujeres	Traslada la responsabilidad a quien puede sufrir la violencia.	Trabajar sobre normas, cultura organizativa, moderación y corresponsabilidad colectiva.

Ejemplo aplicado: incidencia en una actividad formativa

Durante una formación comunitaria sobre empleo y competencias digitales, una participante interviene para plantear dudas sobre las dificultades de acceso a plataformas de búsqueda de empleo. Dos asistentes realizan comentarios despectivos sobre su edad y afirman que “la tecnología no es para todo el mundo”. Más tarde, uno de ellos comparte en un grupo de mensajería una fotografía tomada durante la sesión, acompañada de un comentario burlón sobre la participante.

La profesional responsable detecta dos tipos de incidencia: una desvalorización por razón de edad y género durante la actividad, y una difusión no autorizada de una imagen en un canal digital. La actuación puede desarrollarse de la siguiente manera:

1. La profesional informa a la participante de que puede comunicar formalmente la situación y le ofrece un espacio de conversación confidencial.
2. Se registra la incidencia, incluyendo fecha, lugar, tipo de comentarios, personas presentes y publicación realizada en el grupo de mensajería.
3. Se valora si la imagen debe retirarse de forma inmediata y se solicita a la persona responsable que elimine el contenido.
4. Se recuerda al grupo la prohibición de difundir imágenes o comentarios sobre participantes sin autorización.
5. Se revisan las normas de convivencia de la actividad y se incorporan pautas específicas sobre respeto, privacidad y participación igualitaria.
6. La profesional realiza seguimiento con la participante para comprobar si la situación se ha repetido o si necesita apoyo adicional.
7. La entidad analiza si debe incorporar medidas preventivas en futuras actividades, como avisos previos sobre uso de imágenes, normas de moderación y formación para las personas responsables.

Este ejemplo muestra que una incidencia puede afectar tanto al espacio presencial como al digital. La respuesta debe atender a ambas dimensiones y evitar limitarse a una corrección superficial del mensaje.

Instrumento de revisión del procedimiento de detección y registro

Antes de implantar o actualizar un protocolo interno, puede utilizarse una lista de comprobación que permita valorar si el procedimiento incluye los elementos esenciales.

Área de revisión	Preguntas de comprobación
Canales de comunicación	¿Existen vías claras, accesibles y confidenciales para comunicar incidencias?
Información a participantes	¿Las personas conocen sus derechos, las normas de convivencia y los procedimientos disponibles?
Formación del personal	¿Las personas responsables saben detectar situaciones de discriminación, acoso o violencia digital?
Registro	¿Existe una ficha clara, segura y adaptada a distintos tipos de incidencia?
Confidencialidad	¿Se ha definido quién accede a los datos y cómo se protege la información?
Valoración de riesgo	¿El procedimiento incluye criterios para identificar situaciones urgentes o de mayor gravedad?
Medidas inmediatas	¿La entidad puede retirar contenidos, moderar espacios, proteger a participantes o adaptar canales?
Derivación	¿Se conocen los recursos especializados a los que puede orientarse a las personas afectadas?
Seguimiento	¿Se establecen fechas de revisión y responsables de comprobar la evolución del caso?
Prevención	¿Las incidencias registradas se utilizan para mejorar campañas, normas, horarios, canales y formación?
Accesibilidad	¿El procedimiento puede ser utilizado por personas con distintas capacidades, idiomas y niveles de alfabetización digital?
Perspectiva interseccional	¿Se consideran las barreras específicas que pueden afectar a mujeres con perfiles diversos?

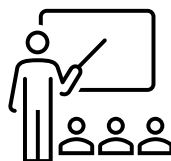
Los procedimientos de detección y registro de incidencias permiten convertir la perspectiva de género en una práctica concreta dentro de los procesos comunicativos. Su utilidad depende de que estén bien definidos, se apliquen con sensibilidad y se revisen de forma periódica. Registrar, analizar y aprender de las situaciones detectadas contribuye a construir espacios de información y participación más seguros, accesibles e igualitarios.



Actividad 10

Una participante informa de que ha recibido mensajes sexistas en el grupo de mensajería de una actividad. Enumera los datos básicos que deberían recogerse en el registro de la incidencia y señala dos actuaciones iniciales que debería realizar la entidad.

6. Resumen.



Las situaciones de discriminación por razón de género pueden aparecer de forma directa, mediante expresiones ofensivas, exclusiones manifiestas o un trato desigual, pero también de forma indirecta y menos visible. Una práctica aparentemente neutra puede perjudicar especialmente a determinadas mujeres si no tiene en cuenta sus responsabilidades de cuidado, sus condiciones de acceso a la información, su nivel de alfabetización digital o la existencia de barreras de idioma, movilidad o seguridad. La detección de estas situaciones requiere observar tanto los mensajes como las condiciones en las que se producen, difunden y reciben.

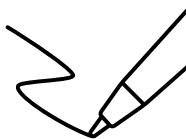
El sexismo en el lenguaje constituye una de las manifestaciones más frecuentes de desigualdad comunicativa. Puede expresarse mediante el uso sistemático del masculino como referencia universal, denominaciones profesionales que invisibilizan a las mujeres, comentarios que cuestionan sus capacidades o expresiones que las reducen a su apariencia, vida familiar o relaciones personales. La comunicación no sexista busca nombrar con precisión a las personas, evitar asociaciones estereotipadas y emplear fórmulas claras que no reproduzcan una visión androcéntrica de la realidad.

Las imágenes, la publicidad y los contenidos audiovisuales también pueden transmitir discriminación. La repetición de modelos que presentan a las mujeres como responsables principales de las tareas domésticas, como objetos de consumo o como figuras secundarias frente a hombres protagonistas contribuye a normalizar una distribución desigual de roles. Del mismo modo, la ausencia de mujeres en ámbitos científicos, técnicos, políticos, deportivos o empresariales limita la diversidad de referentes disponibles. La revisión de los materiales debe valorar quién aparece, qué papel desempeña, qué grado de autonomía posee y si existe una representación equilibrada y plural.

Los entornos digitales amplían las oportunidades de participación y acceso a la información, aunque también generan riesgos específicos. La brecha digital de género, los sesgos algorítmicos, la publicidad segmentada, el ciberacoso, los discursos de odio, la difusión no consentida de contenidos íntimos y el control tecnológico pueden dificultar la participación segura de mujeres y personas con identidades diversas. Las organizaciones deben incorporar medidas de prevención, moderación, protección de datos, respuesta ante conductas discriminatorias y adaptación de los contenidos a distintos niveles de competencia digital.

La detección de discriminaciones debe acompañarse de procedimientos claros de actuación. Resulta necesario disponer de canales accesibles y confidenciales para comunicar incidencias, registrar la información de manera segura, valorar el nivel de riesgo y adoptar medidas proporcionadas. Estos procedimientos deben prever la retirada o corrección de contenidos, la moderación de espacios, la atención a las personas afectadas, la derivación a recursos especializados y el seguimiento posterior. El registro de incidencias permite identificar problemas recurrentes y utilizar lo aprendido para mejorar campañas, materiales, canales de participación y normas de convivencia.

7. Prueba de autoevaluación.



1. Una entidad rechaza la inscripción de una mujer en una actividad técnica porque considera que el grupo “es más adecuado para hombres”. Esta situación constituye:

- a) Una medida de acción positiva.
- b) Una discriminación directa por razón de género.
- c) Una adaptación razonable del servicio.
- d) Una medida de comunicación inclusiva.

2. Una convocatoria se publica únicamente en formato digital, sin vías alternativas, en una zona donde muchas mujeres mayores tienen baja competencia tecnológica. ¿Qué tipo de discriminación puede producirse?

- a) Discriminación directa, porque el contenido nombra expresamente a las mujeres.
- b) Representación equilibrada, porque la convocatoria se dirige a toda la población.
- c) Discriminación múltiple exclusivamente por edad.
- d) Discriminación indirecta, al generar una desventaja mediante una medida aparentemente neutra.

3. ¿Qué expresa el concepto de androcentrismo?

- a) La visión que toma la experiencia masculina como referencia universal.
- b) La presencia equilibrada de mujeres y hombres en los medios de comunicación.
- c) La adaptación de contenidos a distintos niveles de alfabetización digital.
- d) La participación de hombres en las tareas de cuidado.

4. ¿Cuál de las siguientes situaciones puede considerarse un micromachismo?

- a) Solicitar una revisión de accesibilidad de un formulario digital.
- b) Organizar una mesa redonda con profesionales de distintos perfiles.
- c) Interrumpir de forma reiterada a una compañera y atribuir después su idea a otro participante.
- d) Facilitar información sobre un recurso de conciliación a toda la plantilla.

5. ¿Qué práctica se ajusta mejor a un uso no sexista del lenguaje?

- a) Utilizar siempre el masculino genérico para evitar textos más largos.
- b) Emplear términos colectivos o reformular las frases para nombrar a las personas con precisión.
- c) Sustituir todas las referencias a personas por símbolos o abreviaturas.
- d) Utilizar únicamente el femenino en cualquier documento dirigido a la población.

- 6.** ¿Qué efecto puede producir la sexualización de las mujeres en contenidos comunicativos?
- a) Mejora automáticamente la comprensión del mensaje.
 - b) Incrementa la presencia de mujeres como referentes profesionales.
 - c) Facilita una representación más diversa de sus trayectorias.
 - d) Desplaza la atención de sus capacidades y aportaciones hacia su apariencia física.
- 7.** ¿Cuál de las siguientes situaciones constituye una forma de violencia digital de género?
- a) Difundir contenido íntimo de una persona sin su consentimiento.
 - b) Publicar una guía sobre seguridad y privacidad en redes sociales.
 - c) Ofrecer un canal de consulta confidencial mediante correo electrónico.
 - d) Adaptar un formulario para facilitar su uso desde dispositivos móviles.
- 8.** Ante un comentario sexista en una red social institucional, la actuación inicial más adecuada es:
- a) Mantener el comentario visible para fomentar un debate abierto sin límites.
 - b) Responder públicamente con información personal de quien lo ha publicado.
 - c) Aplicar las normas de moderación, registrar la incidencia y valorar las medidas necesarias.
 - d) Cerrar de manera permanente todos los perfiles digitales de la entidad.
- 9.** ¿Qué criterio es esencial en un procedimiento de registro de incidencias?
- a) Difundir los datos recogidos a toda la organización para garantizar transparencia.
 - b) Limitar el acceso a la información sensible y proteger la confidencialidad.
 - c) Registrar únicamente las incidencias que aparezcan en redes sociales.
 - d) Eliminar los registros al finalizar cada actividad, aunque existan riesgos pendientes.
- 10.** ¿Para qué sirve analizar las incidencias comunicativas registradas a lo largo del tiempo?
- a) Para reducir el número de personas responsables de la comunicación.
 - b) Para sustituir los protocolos por decisiones improvisadas.
 - c) Para evitar que las personas afectadas aporten información sobre lo ocurrido.
 - d) Para identificar problemas recurrentes y mejorar materiales, canales y procedimientos.

Capítulo 3



Diseño de actuaciones de comunicación e información desde la perspectiva de género. SSC_A_1401_03.

El diseño de una actuación de comunicación con perspectiva de género parte de una necesidad concreta y de un conocimiento suficiente del contexto en el que se va a intervenir. Antes de elaborar materiales o seleccionar canales, es necesario definir qué desigualdad se pretende abordar, qué personas pueden verse afectadas, qué barreras existen y qué cambios se esperan alcanzar. Esta fase permite formular objetivos coherentes, elegir contenidos pertinentes y prever recursos ajustados a las características de la población destinataria. Una planificación rigurosa reduce el riesgo de desarrollar acciones genéricas que no respondan a las necesidades reales del entorno.

Los mensajes, formatos y canales deben facilitar una representación equilibrada de mujeres y hombres y evitar asociaciones simplificadas entre género, capacidades, tareas o espacios sociales. El diseño debe incorporar criterios de accesibilidad, claridad y adecuación cultural, de manera que la información pueda ser comprendida y utilizada por personas con perfiles diversos. También resulta relevante incluir mecanismos de participación que permitan contrastar las propuestas con las personas destinatarias, entidades comunitarias y profesionales implicadas. Esta participación mejora la calidad de la intervención y ayuda a detectar aspectos que podrían quedar fuera de la planificación inicial.

1. Diagnóstico, justificación y formulación de objetivos.

El diseño de una actuación de comunicación e información con perspectiva de género debe partir de un conocimiento suficiente de la realidad en la que se pretende intervenir. Antes de elaborar una campaña, seleccionar canales, crear materiales o programar actividades, es necesario identificar qué situación se quiere mejorar, a qué personas afecta, qué barreras existen y qué recursos están disponibles. Este análisis previo permite evitar actuaciones genéricas, poco accesibles o desconectadas de las necesidades de la población destinataria.

El **diagnóstico** constituye la base de la planificación. Aporta información sobre los problemas detectados, los factores que los explican, las desigualdades presentes en el acceso a la información y las condiciones que pueden facilitar o dificultar la participación. Desde la perspectiva de género, debe examinarse cómo influyen los roles tradicionales, las responsabilidades de cuidado, la brecha digital, la distribución desigual de la palabra, la falta de referentes femeninos, la accesibilidad de los canales y la presencia de discriminaciones directas o indirectas.

La **justificación** explica por qué resulta necesaria una actuación concreta y qué necesidad pretende atender. Debe relacionar los resultados del diagnóstico con la propuesta de intervención, mostrando de forma clara qué problema se ha identificado, qué consecuencias genera y por qué la comunicación puede contribuir a su mejora. Una justificación sólida evita que las acciones se diseñen únicamente por intuición, repetición de actividades anteriores o respuesta a una demanda aislada.

Los **objetivos** orientan el conjunto de la actuación. Definen los cambios, aprendizajes, mejoras o resultados que se pretenden alcanzar. Deben formularse de manera clara, viable y coherente con el diagnóstico. También permiten seleccionar actividades adecuadas, asignar recursos, establecer indicadores y evaluar posteriormente si la intervención ha producido los efectos esperados.

El diagnóstico como punto de partida de la intervención

Un diagnóstico comunicativo con perspectiva de género permite conocer cómo se produce, distribuye y recibe la información en un contexto determinado. Puede centrarse en una entidad, un barrio, un centro educativo, una organización laboral, un servicio público, una campaña concreta o un grupo de población.

La información obtenida debe responder a preguntas relacionadas con el acceso, la comprensión, la participación y la representación. Por ejemplo, puede resultar necesario conocer si las mujeres reciben información sobre los recursos existentes, si los horarios de las actividades facilitan su asistencia, si los mensajes están redactados de forma accesible, si las campañas muestran referentes diversos o si determinadas participantes sufren interrupciones, desvalorización o ataques en espacios digitales.

El diagnóstico debe prestar atención a las desigualdades visibles, aunque también a aquellas que permanecen ocultas por falta de datos o por la normalización de determinadas prácticas. Una actividad comunitaria puede registrar una alta asistencia general y, al analizarla con mayor detalle, comprobar que las mujeres participan menos en los espacios de decisión. Una campaña puede alcanzar muchas visualizaciones en redes sociales, pero no llegar a mujeres mayores, personas con baja alfabetización digital o mujeres que necesitan canales seguros y confidenciales para informarse.

Para desarrollar un diagnóstico útil, conviene analizar varios ámbitos de manera relacionada.