

# Evaluación y mitigación de los riesgos de represalias para cooperar con las Naciones Unidas



## UNA HERRAMIENTA PARA LAS PERSONAS DEFENSORAS DE LOS DERECHOS HUMANOS



Para muchas personas defensoras de los derechos humanos en todo el mundo, las Naciones Unidas (ONU) representan una plataforma fundamental para documentar y denunciar abusos, permitir que las víctimas compartan sus testimonios y abogar por una respuesta internacional a las crisis de derechos humanos.



La participación de las personas defensoras de los derechos humanos permite a la ONU tomar decisiones informadas sobre las medidas que deben adoptarse contra los gobiernos o las personas que cometen violaciones de los derechos humanos, y promover las normas de derechos humanos a nivel mundial.



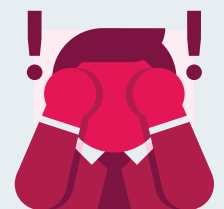
El **derecho a acceder y cooperar con la ONU de forma segura y sin obstáculos**, y a estar **libre de cualquier forma de intimidación o represalia**, es tanto un derecho humano fundamental como un pilar esencial para la labor de la ONU.



Sin embargo, al colaborar o intentar colaborar con las Naciones Unidas, muchas personas defensoras de los derechos humanos y organizaciones de la sociedad civil se enfrentan a actos de intimidación o represalias. Estos pueden ir desde amenazas, difamaciones en Internet y prohibiciones de viajar, hasta desapariciones o detenciones arbitrarias, por parte de gobiernos, empresas u otros.

ISHR ha recopilado todos los casos de represalias documentados por las Naciones Unidas en esta [base de datos](#).

Estos actos pueden tener como objetivo **impedir su participación o infundir miedo**, entre otros. Cualquier persona que coopere con las Naciones Unidas debe ser plenamente consciente de que, por muy importante que sea, hacerlo podría aumentar su exposición a la intimidación o las represalias. Dado que el sistema de las Naciones Unidas puede parecer lejano, las personas defensoras a veces subestiman los riesgos que conlleva colaborar con él.



Esta guía ofrece herramientas y tácticas para que las personas defensoras de los derechos humanos que deseen colaborar con las Naciones Unidas puedan **evaluar y mitigar mejor estos riesgos**. Si defiendes los derechos humanos y deseas colaborar con las Naciones Unidas, lee atentamente esta guía y compártela con personas a tu alrededor.

Estas herramientas buscan prevenir y mitigar las represalias específicamente por cooperar con la ONU. Pero también puede utilizar estas herramientas para evaluar el riesgo en varias otras circunstancias de su trabajo en defensa de los derechos humanos.

Para llevar a cabo una **estrategia eficaz de mitigación de riesgos**, debe:

- Desarrollar una **evaluación de riesgos** exhaustiva, idealmente revisada por pares y actualizada constantemente.
- Decidir el nivel de riesgo que está dispuesto a asumir.
- Desarrollar un **plan de contingencia** con medidas destinadas a reducir sus vulnerabilidades y aumentar sus capacidades.

## EVALUACIÓN DE RIESGOS

**Siempre debe realizar una evaluación de riesgos antes de empezar cualquier forma de cooperación con las Naciones Unidas.** Esto le permitirá reflexionar sobre las posibles consecuencias que podrían surgir según su contexto específico e individual.

Tenga en cuenta que sus **familiares, colegas y organizaciones** también pueden estar en riesgo. Considere a estas personas como posibles objetivos, tanto directos como indirectos, al evaluar el riesgo.

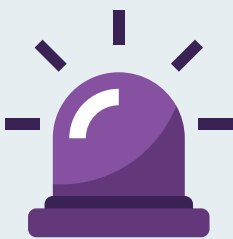
**En primer lugar, ¿qué entendemos por «riesgo»?**

### RIESGO = AMENAZAS X VULNERABILIDADES / CAPACIDADES



**Riesgo** = el impacto y la probabilidad de que una amenaza se materialice (en este caso: por cooperar o intentar cooperar con las Naciones Unidas).

El impacto y la probabilidad del riesgo dependen de factores personales y contextuales que pueden estar o no bajo su control.



**Amenazas** = acontecimientos negativos que podrían materializarse contra usted, sus colegas, socios u organización.

Una amenaza existe independientemente de sus acciones (por ejemplo, un gobierno que suele detener a personas que cooperan con la ONU).



**Vulnerabilidades** = factores negativos que le exponen a amenazas o aumentan su probabilidad o impacto.



**Capacidades** = factores positivos que reducen su exposición a las amenazas o disminuyen su probabilidad o impacto.

## Paso 1: Evaluar las amenazas potenciales

Identifique las amenazas existentes. Evalúe el **impacto** que tendrían si se materializan y la **probabilidad** de que esto ocurra teniendo en cuenta:



- **Tipo de autor:** ¿La amenaza proviene de un actor estatal, un actor no estatal u otra entidad? ¿Tiene ese actor antecedentes de intimidación o represalias contra quienes cooperan con las Naciones Unidas (véase [la base de datos sobre represalias de ISHR](#))?
- **Perfil de la víctima:** ¿Los objetivos son las propias personas defensoras de los derechos humanos, sus familias o sus organizaciones?
- **Naturaleza de la amenaza:** ¿Podría ser la amenaza de naturaleza física, psicológica, digital, informativa, reputacional, política, medioambiental, financiera, relacionada con los recursos humanos, logística o de otra naturaleza?

Algunos ejemplos de amenazas son, entre otros:

- Amenazas e intimidaciones (en línea y fuera de línea)
- Vigilancia (en línea y fuera de línea)
- Difamación, incluida la difamación en línea
- Restricciones de viaje
- Expulsión o denegación de visado
- Agresiones físicas
- Detención y encarcelamiento
- Desaparición forzada, secuestro
- Investigación y enjuiciamiento penal
- Daños a la propiedad, redadas, registros por la policía y confiscación de bienes
- Represalias relacionadas con su profesión
- Persecución de familiares, colegas de trabajo o amigas y amigos
- Represalias administrativas
- Bloqueo del acceso a una persona experta o mecanismo de las Naciones Unidas
- Denegación de acceso a las instalaciones de la ONU
- Deterioro de las condiciones de detención

## Paso 2: Evaluar sus vulnerabilidades y capacidades



Sus vulnerabilidades y capacidades actuales pueden ser de naturaleza digital, informativa, física, organizativa, jurídica, política, social, psicológica, logística o financiera. Muy a menudo, una es lo opuesto de la otra (por ejemplo, una vulnerabilidad podría ser «no tengo acceso a un equipo jurídico», frente a una capacidad que podría ser «tengo acceso a un equipo jurídico»).

Utilice la tabla siguiente para trazar un mapa de sus amenazas:

**Probabilidad**

	Baja	Media	Alta	Muy alta
Bajo				
Medio				
Alto				
Muy alto				

Utilice la tabla siguiente para evaluar sus vulnerabilidades y capacidades:

	Vulnerabilidades	Capacidades
Digital	<p>Por ejemplo, dispositivos inseguros; falta de acceso a Internet o a las telecomunicaciones; aplicación desigual de prácticas de ciberseguridad; falta de conocimientos sobre seguridad informática y digital.</p>	<p>Por ejemplo, dispositivos informáticos actualizados; conocimientos sobre seguridad digital; acceso a cursos de formación.</p>
Informativa	<p>Por ejemplo, posesión de información altamente confidencial.</p>	<p>Por ejemplo, formas y medios para proteger información altamente sensible, tanto en línea como fuera de línea.</p>
Física	<p>Por ejemplo, afecciones médicas; contexto geográfico; falta de seguridad social y asistencia sanitaria.</p>	<p>Por ejemplo, estar en buena salud; tener acceso a una atención médica adecuada.</p>
Organizativa	<p>Por ejemplo, falta de políticas organizativas; falta de estatus legal; entorno de trabajo insalubre; falta de planes de contingencia; falta de medidas de seguridad en la oficina (cámaras, cerraduras, etc.).</p>	<p>Por ejemplo, seguridad de la ubicación; contactos de emergencia, incluidos locales y diplomáticos; plan de seguridad existente.</p>
Legal	<p>Por ejemplo, falta de conocimientos jurídicos; falta de acceso a una persona abogada; situación migratoria irregular; falta de documentos de viaje.</p>	<p>Por ejemplo, acceso a un equipo jurídico; conocimiento del contexto jurídico, incluidos sus derechos a nivel nacional y el marco de protección internacional para las personas defensoras de los derechos humanos.</p>
Política	<p>Por ejemplo, sensibilidad del tema; nacionalidad; contexto político y jurídico (incluidas las leyes restrictivas); falta de apoyo diplomático o internacional; falta de visibilidad pública o, por el contrario, exceso de visibilidad.</p>	<p>Por ejemplo: acceso a apoyo diplomático u otro tipo de apoyo internacional; la visibilidad pública también puede ser una capacidad en la medida en que puede ser protectora (depende del contexto).</p>
Social	<p>Por ejemplo, género, SOGIESC (orientación sexual, identidad de género, expresión de género y características sexuales), raza, etnia, religión, situación económica u otros motivos de discriminación en la sociedad o comunidad en la que vive; barreras lingüísticas; falta de redes de apoyo; familia aún en el país si se encuentra en el exilio; desconfianza dentro de la familia o las comunidades.</p>	<p>Por ejemplo, acceso a una red de apoyo sobre el terreno o en línea; conocimiento del idioma; apoyo de familiares y personas de confianza.</p>
Psicológica	<p>Por ejemplo, ansiedad; incapacidad para gestionar el estrés o el miedo; trastorno por estrés posttraumático (TEPT) y otras afecciones psiquiátricas/psicológicas; falta de apoyo psicosocial adecuado y de acceso a terapia; estado emocional inestable; factores disruptivos en la vida (familia, relaciones, etc.); marcadores de identidad en contextos específicos (por ejemplo, LGBTQI+).</p>	<p>Por ejemplo: capacidad para gestionar el estrés y el miedo; acceso a apoyo psicosocial adecuado de forma periódica o regular; prácticas de bienestar; grupos de apoyo; permitirse desconectar.</p>
Logística	<p>Por ejemplo: falta de seguro de viaje (vuelo y alojamiento); incertidumbre sobre el visado.</p>	<p>Por ejemplo, apoyo con los preparativos del viaje.</p>
Financieras	<p>Por ejemplo, falta de una fuente de ingresos sostenible; falta de fondos para imprevistos; dependencia de donantes.</p>	<p>Por ejemplo, recursos financieros suficientes; incluidos los necesarios para hacer frente a imprevistos; conocimiento de las subvenciones urgentes disponibles para personas defensoras de los derechos humanos.</p>

# MITIGACIÓN DEL RIESGO

Una vez realizada la evaluación de riesgos, puede planificar su **estrategia de mitigación de riesgos**, que incluya medidas para **reducir sus vulnerabilidades, aumentar sus capacidades** y un plan para **hacer frente a los riesgos que ha identificado**.

Su estrategia de mitigación de riesgos debe incluir, como mínimo, medidas para hacer frente a *todos los riesgos de alto impacto y/o alta probabilidad*.

Si dispone de tiempo y recursos adicionales, considere la posibilidad de tomar todas las medidas contra otras amenazas con probabilidad y/o impacto medio/bajo.

En primer lugar, revise su evaluación de riesgos, identifique las amenazas que desea abordar con prioridad, identifique las vulnerabilidades relacionadas con esa amenaza que desea y pueda reducir, y las capacidades que desea y pueda desarrollar o aumentar.

Las medidas para **prevenir** que se produzcan amenazas incluyen:

- **Informar y planificar:** decida a quién informará sobre sus actividades y con quién deben ponerse en contacto si algo sale mal.
- **Discutir los riesgos:** hable con sus familiares y personas asociadas sobre qué hacer y a quién contactar si usted no puede hacerlo.
- **Proteger a las personas vulnerables:** asegúrese de que sus familiares o personas asociadas en situación de riesgo se encuentran en un lugar seguro.
- **Utilizar herramientas de seguridad físicas y en línea:** considere opciones de VPN, gestores de contraseñas (*password managers*) y otras herramientas de seguridad digital, cámaras y otros equipos físicos.
- **Conozca sus derechos:** comprenda qué puede esperar si lo detienen o arrestan.
- **Ten preparado apoyo legal:** identifica con antelación a una persona abogada o contacto legal.
- **Cree redes de apoyo:** póngase en contacto con ONG internacionales, mecanismos de la ONU u otras organizaciones.

A continuación, elabore un **plan de contingencia** por si, a pesar de sus esfuerzos por reducir el riesgo, estas amenazas se materializan.

**Importante:** Recuerde que no existe un enfoque de «riesgo cero»: en su lugar, utilice estas herramientas para identificar el grado de riesgo que está dispuesto a asumir en su cooperación con las Naciones Unidas y las tácticas para mitigar esos riesgos.

Las medidas que se deben tomar para **protegerse** cuando se producen amenazas incluyen las siguientes (considere si será más eficaz una acción privada o pública):

- **Denunciar las amenazas:** presente denuncias ante la policía local, las autoridades nacionales, si es seguro hacerlo, o el personal de seguridad de las Naciones Unidas.
- **Denunciar las amenazas en línea:** denunciar el acoso a las empresas de redes sociales.
- **Alertar a los contactos clave:** mantenga una lista de embajadas, medios de comunicación, líderes comunitarios, ONG, periodistas y otras personas que puedan ayudar (incluso a través de [directrices diplomáticas para la protección de activistas](#)).
- **Buscar apoyo local:** ponerse en contacto con los organismos nacionales de derechos humanos, las oficinas del defensor del pueblo y los mecanismos de protección para obtener apoyo.
- **Informa a su red:** informe a las organizaciones o redes de derechos humanos de las que forma parte y acuerde cómo pueden ayudarle.
- **Asistencia de emergencia:** recopile los datos de contacto de los grupos que ayudan a las personas en situación de riesgo y averigüe qué necesitan para ayudarle.

**Importante:** si sufre intimidación o represalias por colaborar con las Naciones Unidas, existen muchos mecanismos de la ONU que pueden recibir y reportar estos casos, tanto de forma pública como privada. Haga clic [aquí](#) para obtener más información y no dude en ponerse en contacto con ISHR para solicitar ayuda.

**Ahora es su turno: ¡prepare su propio plan de contingencia!**

Amenazas	Medidas para aumentar las capacidades y reducir las vulnerabilidades	Medidas de contingencia que se deben adoptar si la amenaza se materializa

**Importante:** le animamos a que comente y revise su evaluación de riesgos y su plan de contingencia con familiares o colegas de confianza. Pero recuerde que se tratan de medidas individualizadas y contextualizadas: cada persona u organización tiene un perfil de riesgo diferente.