

Gestión de los riesgos para la seguridad

09 Julio 2025

Puntos clave

- El proceso de gestión de los riesgos para la seguridad (SRM, por sus siglas en inglés) se creó en el marco del sistema de gestión de la seguridad de las Naciones Unidas (SGSNU) para ayudar a los organismos, fondos, programas y organizaciones de las Naciones Unidas a identificar futuros eventos perjudiciales que podrían afectar la consecución de objetivos, a evaluar la probabilidad y nivel de repercusión de dichos eventos y a definir medidas y respuestas adecuadas para la gestión de los riesgos para la seguridad.
- El proceso de SRM asiste a los directivos a analizar los contextos en los que operan las Naciones Unidas, a identificar en qué medida los riesgos pueden afectar al personal, los bienes, los locales y las operaciones de las Naciones Unidas, y a tomar las decisiones apropiadas relativas a la gestión de la seguridad.
- El proceso de SRM les permite a los usuarios aprovechar al máximo las oportunidades programáticas y ejecutar los programas con un nivel de riesgo aceptable, a la vez que se hace una asignación adecuada de los recursos necesarios.
- El proceso de SRM es un mecanismo estructurado que se compone de nueve pasos consecutivos.

1. Líneas generales

La gestión de los riesgos para la seguridad (SRM, por sus siglas en inglés) es un proceso analítico que se creó en el marco del SGSNU para ayudarnos a identificar futuros eventos perjudiciales que podrían afectar la consecución de objetivos, a evaluar la probabilidad y nivel de repercusión de dichos eventos y a definir respuestas adecuadas. Asiste a los directivos a analizar los contextos en los que operan las Naciones Unidas, a identificar en qué medida los riesgos pueden afectar al personal, los bienes, los establecimientos y las operaciones de las Naciones Unidas, y a tomar las decisiones apropiadas relativas a la gestión de la seguridad. Este proceso permite hacer un análisis multifacético de los riesgos que amenazan al personal, incluidos los relativos al

perfil de cada persona. La SRM es importante porque, por medio de una asignación adecuada de los recursos, nos permite aprovechar al máximo las oportunidades de los programas y ejecutarlos con un nivel de riesgo aceptable.

Esta entrada del Manual para Situaciones de Emergencia les proporciona a los directivos y al personal del ACNUR información técnica sobre el proceso de gestión de los riesgos para la seguridad del SGSNU. El capítulo expone los principales conceptos y terminología en torno a la SRM, como "amenaza", "vulnerabilidad", "probabilidad", "impacto" y "riesgo". El objetivo del capítulo es dotar a los directivos y al personal de conocimientos para participar del proceso de gestión de los riesgos para la seguridad del SGSNU con el fin de fomentar la capacidad del ACNUR de continuar con la ejecución de programas, a la vez que se gestionan los riesgos para la seguridad del personal, los locales, las operaciones y los bienes de modo que estén en un nivel aceptable que permita la permanencia y la ejecución de programas. Los directivos siempre deben coordinar todos los pasos de la SRM con el Oficial Superior de Seguridad sobre el Terreno de cada operación.

2. Relevancia para operaciones de emergencia

Dado que el ACNUR da respuesta a emergencias, es posible que sea necesario un proceso específico de gestión de los riesgos para la seguridad para sustentar esta actividad o para determinar los riesgos en una zona donde las Naciones Unidas no hayan operado o lo hayan hecho de manera limitada en el pasado. Es importante que este procedimiento, de ser necesario, se realice por fuera del proceso habitual de SRM.

Nota: En entornos de emergencia, **se recomienda en gran medida que se reduzcan los plazos, ya que los eventos que suponen riesgos y amenazas para el personal y las operaciones evolucionan rápidamente** y, por lo tanto, podrían cambiar en un periodo breve de tiempo, lo que supondría una necesidad de implementar cambios repentinos.

3. Guía principal

Definiciones:

Amenaza: Daños potenciales a causa de acciones deliberadas. En una amenaza se combinan intención, capacidad y un contexto limitante.

Peligro: Daños potenciales a causa de acciones no deliberadas.

Vulnerabilidad: Una desventaja que posibilita que una amenaza o peligro cause daños.

Riesgo: Una combinación de la probabilidad de que ocurra un evento perjudicial y el impacto que tendrá dicho evento si ocurre.

Probabilidad: El grado de potencial evaluado de que un evento perjudicial afecte a la

organización.

Impacto: El grado de potencial daño evaluado que tendría un evento sobre la organización (si ocurriese).

Gestión de los riesgos: La definición y aplicación sistemáticas de medidas eficaces y oportunas para gestionar los efectos de las amenazas sobre la organización.

Prevención: Tomar medidas para reducir la probabilidad.

Mitigación: Tomar medidas para reducir el impacto.

El proceso de gestión de los riesgos para la seguridad

La SRM del SGSN consiste en un proceso que se adapta al contexto específico donde se identifican eventos que amenazan la seguridad y los niveles de riesgo asociado, y se definen respuestas adecuadas para la gestión de los riesgos para una toma de decisiones estructurada que permita un grado aceptable de riesgos para la seguridad. La SRM ha sido diseñada como herramienta dinámica, receptiva y flexible para poder adaptarse a los cambios repentinos en el contexto o situación de seguridad y en la ejecución de los programas. También fue diseñada para integrar al proceso enfoques centrados en las personas, de modo que las evaluaciones de los riesgos tengan en consideración los perfiles diversos del personal, y que se identifiquen los riesgos y las medidas de mitigación que se deben adoptar en función de cada contexto para que el nivel de riesgo resultante sea aceptable para todos. El enfoque de la SRM centrado en las personas permite que nuestras operaciones tengan un entorno propicio para mantener perfiles heterogéneos dentro del personal y apoyar a las comunidades diversas con las que trabajamos, teniendo en cuenta los matices de cada contexto.

A nivel operacional, el sector de gestión y seguridad sobre el terreno del ACNUR contribuye activamente con el proceso de gestión de los riesgos para la seguridad del SGSNU de las siguientes maneras: a) identifica, establece la magnitud y el alcance, y evalúa las actividades programáticas y la potencial exposición a eventos que amenazan la seguridad y a distintos niveles de riesgo; b) procura que la SRM esté a la altura de las necesidades del ACNUR y que sea adecuadas y viable en términos operativos para su implementación; y c) reduce los riesgos para la seguridad a niveles aceptables para el organismo. El proceso consta de los siguientes nueve pasos:

SECURITY RISK MANAGEMENT PROCESS

STEP 1: Geographical scope and timeframe

 Sets the terms of each SRM process by geography and timeframe. For example, a specific SRM may be completed for upcoming elections in a country, or for a specific area of potential vulnerability to be visited by United Nations staff, such as a large refugee camp.

STEP 2: Situational analysis

 Considers political, economic, social and environmental factors in each area, in relation to possible impacts on the safety and security of UN activities.

STEP 3: Programme assessment

 Formally identifies the goals and specific implementation activities of UNSMS organizations in-country.

STEP 4: Threat assessment

 Assesses actors and actions that may cause harm to the UNSMS in the Designated Area, in the categories of armed conflict, terrorism, crime and civil unrest. The intent and capabilities of the relevant threat actors are identified and assessed.

STEP 5: Security risk assessment

 Assesses the different vulnerabilities of the UNSMS presence and activities in-country against the existing threats to determine the likelihood of harmful threat event occurring, and possible impact on UNSMS personnel, assets and operations.



Paso 1: Alcance geográfico y plazos

El SGSNU establece el alcance geográfico y los plazos del proceso de SRM, es decir, define las ubicaciones geográficas para enmarcar el contexto en que se llevará a cabo el programa y las evaluaciones de vulnerabilidad. En general, las zonas con características similares en cuanto a seguridad deben agruparse dentro del mismo alcance geográfico, al que se denomina "zona de SRM".

Cuando ya se ha definido el alcance geográfico, es importante pautar un periodo de tiempo claro con el fin de precisar mejor los programas, la magnitud, el alcance, los actores amenazantes y, en consecuencia, la probabilidad de amenazas y su impacto sobre las Naciones Unidas. Los periodos de tiempo de la SRM pueden variar considerablemente (desde un par de horas en adelante); no obstante, la duración máxima permitida es de un año.

Tenga en cuenta que cuando una operación de emergencia se considera ya establecida, quizás

sea necesario un nuevo proceso de SRM, ya que la zona geográfica podría quedar fuera de los límites de los procesos ya existentes.

Paso 2: Análisis de la situación

El análisis de situación ofrece información concisa sobre el contexto en la zona de la SRM para que los responsables de la toma de decisiones de seguridad entiendan el entorno operacional desde las diferentes perspectivas: económica, política, ambiental, de la infraestructura, de las fuerzas de seguridad, de los actores o grupos amenazantes y del mandato de las Naciones Unidas, en torno a la protección y seguridad de la organización en la zona geográfica que se evalúa.

Se trata de un resumen práctico de cómo se ve una zona de SRM y qué se puede esperar en cuanto a entorno de trabajo. Esta parte del documento es fundamental para identificar problemas perdurables existentes que podrían generar las condiciones en las que surgen amenazas.

Nota sobre la incorporación de un enfoque centrado en las personas en la gestión de los riesgos para la seguridad

Es esencial que, durante el análisis de la situación del proceso, se lleve a cabo una investigación sobre consideraciones del enfoque centrado en las personas y sobre incidentes previos (tendencias) de la zona de SRM, y que se integren estas consideraciones en su orientación:

1. Violencia de género
2. Percepciones, persecución y violencia contra personas LGBTIQ+
3. Identificación y discriminación de personas con discapacidad
4. Relaciones étnicas, tribales e intercomunitarias, composición de la comunidad, y percepciones de los diversos grupos religiosos de la zona de SRM
5. Otros factores intersectoriales que podrían afectar las operaciones o al personal de las Naciones Unidas

Comprender el contexto y la situación de la zona de SRM y las posibles tendencias centradas en las personas que existen en torno a la violencia de género, la discriminación contra determinados perfiles del personal y las tensiones preexistentes en las comunidades es clave para identificar adecuadamente las amenazas específicas contra el personal del ACNUR, que pueden captarse en la parte relativa a la evaluación de amenazas del proceso y del documento de SRM, y aquellas amenazas contra socios y personas de interés para el ACNUR, en cuyo caso el personal de seguridad involucrará a los actores pertinentes y cooperará con otros sectores para adoptar medidas de mitigación.

Paso 3: Evaluación de programas

La evaluación de programas les permite a los profesionales de seguridad entender formalmente los requisitos de los programas de las organizaciones del SGSNU. Además, destaca los programas que están expuestos a amenazas específicas. Las evaluaciones de programas ofrecen información general y específica acerca de las actividades que cada organismo lleva adelante en la zona de SRM.

Para que el SGSNU comprenda el alcance y la magnitud de los programas y las operaciones del ACNUR, así como los potenciales riesgos y amenazas para el personal, los bienes, las operaciones y los locales del ACNUR, es de vital importancia que la operación del ACNUR en el país ofrezca información relevante y actualizada al Departamento de Seguridad con el fin de que este lleve a cabo una evaluación minuciosa de los programas. Asimismo, algunos programas en particular podrían estar sujetos a mayores riesgos que otros.

Por ejemplo:

- Las actividades de vigilancia de las labores de protección del ACNUR pueden enfrentarse a amenazas específicas debido al manejo de información sensible sobre las poblaciones vulnerables y las acciones de actores amenazantes, autoridades estatales o de facto, o grupos armados no estatales.
- Debido a la modalidad operacional única del ACNUR, donde las personas que se ven en la obligación de huir se reúnen con equipos de protección en las oficinas o establecimientos del ACNUR, el organismo se enfrenta a una mayor probabilidad de enfrentarse a episodios violentos o no violentos de desorden público, ingreso de intrusos en las oficinas, ocupación de establecimientos, etc.

Nota sobre la incorporación de un enfoque centrado en las personas en la gestión de los riesgos para la seguridad

La parte de evaluación de programas de la SRM también debería hacer mención de las actividades que emprenden el ACNUR y otras organizaciones del SGSNU que podrían considerarse como más expuestas a un riesgo específico o mayor probabilidad de estar en la mira, como, por ejemplo, actividades del ámbito de la protección, el trabajo con personas LGBTIQ+, las campañas de vacunación, el empoderamiento femenino (en sociedades patriarcales), o cuando la identidad del personal que ejecuta el programa podría agravar el riesgo (por su edad, religión, origen étnico o en un entorno tribal).

Identificar dificultades que podrían surgir de las actividades programáticas es clave para poder perfeccionar la detección de amenazas específicas más adelante en el proceso de SRM.

Paso 4: Evaluación de amenazas

La evaluación de amenazas identifica y examina a los actores y las acciones de una zona geográfica dada que podrían perjudicar el sistema de las Naciones Unidas. Estas evaluaciones se dividen en función de si son de carácter específico o general.

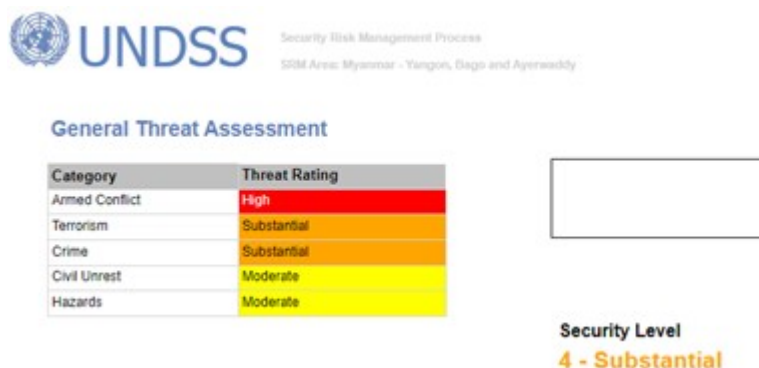
La evaluación de amenazas en el marco de la SRM tiene dos componentes.

Una evaluación general de amenazas valora y describe de forma objetiva las amenazas y peligros para la seguridad del entorno en una zona de SRM (en el SGSNU, el concepto de "seguridad" abarca la noción de amenazas y el de "protección", la noción de peligros. No obstante, la esfera de protección del SGSNU no incluye todos los eventos que suponen un peligro no deliberado. El SGSNU tiene competencia únicamente en tres ámbitos de la protección: seguridad vial, prevención de incendios y seguridad aérea).

Se evalúa cada evento en una escala del 1 al 5 teniendo en cuenta tres variables:

- Intención: la motivación o predisposición de un actor amenazante para provocar el evento que supone una amenaza.
- Capacidad: la habilidad o aptitud de un actor amenazante para provocar el evento que supone una amenaza.
- Contexto limitante: factores ajenos a las Naciones Unidas de la zona geográfica que limitan la intención o la capacidad.

El resultado de una evaluación general de amenazas es una calificación de cada tipo de amenaza o peligro, junto con un nivel de seguridad que tiene en cuenta dicha calificación.



Evaluación específica de amenazas

Estas evaluaciones identifican amenazas en particular que afectan a los fondos, programas, organizaciones y organismos de las Naciones Unidas en una determinada zona de SRM. A diferencia de las evaluaciones generales, que son genéricas, estas identifican amenazas concretas que afectan a las Naciones Unidas en general o a un organismo en particular en la zona en cuestión.

Para llevar a cabo una evaluación específica de amenazas, es necesario contar con descripciones exhaustivas de los eventos asociados a la categoría general de cada amenaza.

La descripción de un evento es una explicación clara de un episodio perjudicial que se estudiará en detalle en la evaluación de los riesgos para la seguridad para luego establecer el nivel de riesgo. Debe tener en cuenta los efectos negativos del evento sobre la organización, así como aplicar una metodología que aborde las preguntas "quién", "qué", "cuándo", "dónde" y "cómo".

Nota: Las descripciones de los eventos deben ofrecer información suficiente para delimitar los parámetros, de modo que les permita a los responsables de la toma de decisiones evaluar los eventos con una mayor precisión que si tuvieran como base la evaluación general de amenazas.

- No todos los eventos están dirigidos a las Naciones Unidas. Por lo tanto, las descripciones de cada evento deben aclarar si la amenaza es "directa" o "indirecta".
- **Las amenazas directas apuntan específicamente a las Naciones Unidas.** Si un grupo en particular declara que tiene la intención de hacer daño a la organización, por

ejemplo, o hay antecedentes recientes que indican que es objeto de amenazas, la amenaza se considerará "directa".

"Secuestro de un miembro del personal internacional de las Naciones Unidas para pedir rescate por parte de actores no estatales en X ubicación".

[Qué] [Dirigido directamente a las Naciones Unidas] [Qué] [Quién] [Dónde]

- **Las amenazas indirectas son aquellas que podrían perjudicar a las Naciones Unidas, aunque la organización no sea necesariamente su objetivo principal.** Podría verse perjudicada si su personal o sus bienes están en el lugar y en el momento incorrectos, si sufren daños colaterales, si están asociados al objetivo de la amenaza o si obstaculizan su camino, por ejemplo.

"Un vehículo de las Naciones Unidas fue dañado por un artefacto explosivo improvisado en la carretera X camino a la oficina sobre el terreno Y"

[Dirigido indirectamente a las Naciones Unidas] [Qué/Cómo] [Dónde]

Tanto las amenazas directas como las indirectas pueden subdividirse en "conocidas" y "evaluadas":

- Amenazas conocidas: Se hizo una declaración de intención de hacer daño a las Naciones Unidas o se ha infligido daño a la organización anteriormente.
- Amenazas evaluadas: No se ha expresado una intención de hacer daño, pero los análisis o evaluaciones indican que existe esta amenaza.

Una vez que se han identificado amenazas específicas y que se han consensuado las descripciones de los eventos, se prepara una evaluación de amenazas de cada evento, a partir de la observación de tres variables: la intención del actor amenazante o la parte responsable, su capacidad y el contexto limitante del entorno en el que ocurre la amenaza (como la capacidad de las fuerzas de seguridad o el rechazo de dichos actos por parte de la población). Las evaluaciones de amenazas se valoran y se clasifican de la misma manera que las generales (véase más arriba).

Nota: No base sus evaluaciones y decisiones en la amenaza sino en el riesgo que esta supone. En cada zona de riesgos para la seguridad se podría identificar una amenaza grave (por naturaleza) que, no obstante, supone un riesgo relativamente bajo para las Naciones Unidas (véase más abajo el apartado sobre **riesgo**).

Nota sobre la incorporación de un enfoque centrado en las personas en la gestión de los riesgos para la seguridad

Es fundamental que el personal de seguridad del ACNUR participe en el proceso colectivo y se asegure de que las amenazas contra ciertos perfiles se tengan en cuenta adecuadamente en el proceso de gestión de los riesgos para la seguridad. Por ejemplo:

1. En el proceso de gestión de los riesgos para la seguridad, ¿se identificó una zona con conflicto armado, una vulneración de la ley y el orden, tasas altas de delincuencia o una prevalencia de violencia de género?
2. Al identificar amenazas, ¿se han tenido en cuenta indicadores o desencadenantes del contexto específico relacionados con determinados perfiles del personal?

Por otro lado, el personal de seguridad del ACNUR procurará que las descripciones de los eventos se basen en información relacionada con las amenazas que se hayan recopilado y reflejado en las secciones anteriores del proceso de SRM (el análisis de la situación). A su vez, se asegurará de que las descripciones identifiquen las amenazas contra las actividades detalladas en la evaluación de programas, que estas descripciones estén redactadas de manera adecuada y rigurosa, de modo que reflejen la categoría de personal que se verá afectado, sus perfiles personales y los actores amenazantes (a quién, qué y por parte de quién), y que incluyan el lugar y periodo de tiempo específicos en que podrían ocurrir los episodios que suponen una amenaza para que se diseñen las medidas correspondientes en el marco de la SRM (posteriormente en el proceso) con el fin de mitigar la probabilidad y el impacto.

Paso 5: Evaluación de los riesgos para la seguridad

Una evaluación de riesgos para la seguridad define y pretende cuantificar la probabilidad y el impacto de los eventos que suponen amenazas, teniendo en cuenta la vulnerabilidad de las Naciones Unidas.

Probabilidad

En el modelo de SRM, la probabilidad se define como “el grado de potencial evaluado de que un evento perjudicial afecte a la organización”. Evalúa la probabilidad de que se produzca un evento determinado intencional que cause daño. El descriptor de probabilidad es un producto de la vulnerabilidad a la amenaza y de prevención.

Las medidas de prevención se adoptan para reducir la probabilidad de que ocurra determinado evento dañino. Pueden implicar tomar vías alternativas, controles de acceso, medidas de disuasión, comunicación, toques de queda, entre otras. Para que sean eficaces, las medidas de prevención deben ponerse en marcha antes de que se produzca el evento en cuestión.

La vulnerabilidad de prevención se define como "la ausencia de medidas de prevención dirigidas a reducir la probabilidad de que ocurra el evento tal como se describió". Dado que las amenazas son externas a las Naciones Unidas, la organización no puede controlarlas fácilmente. Podemos esforzarnos al máximo para protegernos reduciendo nuestra vulnerabilidad de prevención y, en consecuencia, minimizar la probabilidad de que se produzcan las amenazas.

La vulnerabilidad de prevención se analiza en una escala del 1 al 5, en función de los siguientes descriptores:

1. Se han adoptado a cabalidad y se aplican de forma sistemática procedimientos y contramedidas de prevención eficaces para la gestión de riesgos.
2. Se han adoptado a cabalidad procedimientos y medidas de prevención eficaces, pero tienen defectos que podrían ser explotados.
3. No se han adoptado a cabalidad O no se aplican de forma sistemática procedimientos y

medidas de prevención.

4. No se han adoptado a cabalidad Y no se aplican de forma sistemática procedimientos y medidas de prevención.

5. No se han adoptado procedimientos y medidas de prevención eficaces.

Luego, la herramienta de SRM genera una clasificación de la probabilidad multiplicando la vulnerabilidad a la amenaza y de prevención:

- 1 - Muy improbable.
- 2 - Improbable.
- 3 - Moderadamente probable.
- 4 - Probable.
- 5 - Muy probable.

Impacto

El impacto se define como "el grado de potencial daño evaluado que tendría un evento sobre la organización (si ocurriese)". Engloba al personal y las operaciones. También comprende nuestra capacidad de controlar o reducir las consecuencias por medio de la vulnerabilidad de mitigación.

El impacto es un producto de tres componentes:

- Efectos sobre el personal
- Efectos sobre las operaciones
- Vulnerabilidad a la mitigación

Se utiliza una escala del 1 al 5 con descriptores asociados para medir los efectos sobre el personal y las operaciones.

Efectos sobre el personal

1. Ningún efecto
2. Efectos ligeramente perjudiciales
3. Efectos moderadamente perjudiciales o traumáticos a nivel psicológico
4. Efectos perjudiciales graves, muy traumáticos a nivel psicológico o mortales (una persona o pocas víctimas)
5. Efectos mortales a nivel catastrófico (múltiples víctimas)

Efectos sobre las operaciones

1. Ningún efecto
2. Efectos ligeramente disruptivos sobre los programas o daños menores a los bienes
3. Efectos disruptivos graves sobre los programas o daños significativos a los bienes
4. Suspensión de programas a corto o mediano plazo
5. Suspensión de programas a largo plazo o cancelación

Vulnerabilidad de mitigación

La vulnerabilidad de mitigación se refiere a la "ausencia de procedimientos y contramedidas de

seguridad diseñados para reducir el impacto de un evento (si ocurriera el evento)". Las medidas de mitigación se toman para reducir el impacto. Entre ellas, se encuentra la evacuación de bajas (CASEVA) y la [evacuación médica](#) (MEDEVAC), los botiquines de socorrismo y los botiquines individuales de primeros auxilios, la gestión de incidentes de toma de rehenes, la preparación por medio de coordinación con el gobierno de acogida, la planificación ante incidentes con múltiples víctimas, los simulacros, la recuperación en casos de desastre, [la planificación de la continuidad de las operaciones](#), etc. Aunque las medidas de mitigación apuntan a reducir el impacto de los eventos cuando ocurren y con posterioridad, deben planificarse e implementarse antes de que sucedan para que den resultado.

Para establecer el nivel de impacto, es esencial evaluar en qué grado se han implementado las medidas de mitigación. En este sentido, el modelo de gestión de los riesgos para la seguridad emplea una escala del 1 al 5 en función de los siguientes descriptores:

1. Se han adoptado a cabalidad y se aplican de forma sistemática procedimientos y contramedidas de mitigación para la gestión de riesgos
2. Se han adoptado procedimientos y medidas de mitigación, pero no se aplican de forma sistemática o tienen defectos
3. No se han adoptado a cabalidad O no se aplican de forma sistemática procedimientos y medidas de mitigación
4. No se han adaptado a cabalidad Y no se aplican de forma sistemática procedimientos y medidas de mitigación
5. No se han adoptado procedimientos y medidas de mitigación

El modelo de SRM suma los efectos sobre el personal y las operaciones y la vulnerabilidad de mitigación para definir el impacto (efectos sobre el personal + efectos sobre las operaciones + vulnerabilidad de mitigación).

La herramienta de SRM hace automáticamente una [clasificación del impacto](#) con una escala del 1 al 5, como se describe a continuación:

- 1 - Insignificante
- 2 - Leve
- 3 - Moderado
- 4 - Grave
- 5 - Crítico

Niveles de riesgo

Una evaluación del riesgo estudia una combinación de los potenciales eventos que podrían ocurrir en el futuro y la medida en que dichos eventos perjudicarían a la organización.

Riesgo = probabilidad x impacto

Risk Matrix		Impact				
		Negligible	Minor	Moderate	Severe	Critical
Likelihood	Very likely	Low	Medium	High	Very High	Unacceptable
	Likely	Low	Medium	High	High	Very High
	Moderately Likely	Low	Low	Medium	High	High
	Unlikely	Low	Low	Low	Medium	Medium
	Very Unlikely	Low	Low	Low	Low	Low

Dicho de otra manera:

Risk Score Range	Risk Level
1 to 6	Low
>6 to 10	Medium
>10 to 16	High
>16 to 20	Very High
>20 to 25	Unacceptable

Los niveles de riesgo, que son el producto de la evaluación de los riesgos para la seguridad, conforman la base para tomar decisiones durante el proceso de SRM. Les permiten a los responsables de la toma de decisiones formular estrategias adecuadas para la gestión del riesgo y establecer prioridades que sean proporcionales a los niveles de riesgo y a los descriptores de eventos asociados.

Nota: Con el fin de tomar decisiones en torno al **riesgo aceptable**, se aplica el nivel más alto de riesgo asociado con cualquiera de los eventos a la zona de SRM o a la actividad del programa en cuestión.

Paso 6: Medidas de SRM

Gestionamos el riesgo definiendo y aplicando medidas de SRM que minimizan la probabilidad o el impacto al reducir las vulnerabilidades.

Solo se pueden identificar medidas de SRM después de evaluar:

- Las debilidades y fortalezas de las medidas de prevención y de mitigación existentes (en relación con las amenazas en cuestión)
- Los niveles de riesgo asociados a las amenazas, según su probabilidad e impacto

En el marco de las estrategias mencionadas, las medidas de SRM pueden usarse con los eventos que supongan amenazas que se hayan identificado. Después de evaluar las vulnerabilidades de prevención y de mitigación (según se describió en el paso anterior), los profesionales de seguridad pueden determinar qué medidas adicionales (que no estén en curso en ese momento)

se necesitan, como, por ejemplo, medidas y procedimientos para reducir la probabilidad o el impacto, o ambos. Por lo general, estas decisiones implican elegir la mejor opción entre diversas alternativas.

El proceso de gestión de los riesgos para la seguridad procura lograr un equilibrio entre el impacto de los riesgos y el costo de las soluciones de seguridad diseñadas para afrontarlos. El potencial de una medida de seguridad para salvar vidas y la importancia de los programas y mandatos en cuestión son factores mucho más importantes que el costo a la hora de tomar decisiones.

Nota para los directivos: No base sus decisiones en el nivel de amenaza. Decida cómo actuar una vez definida la vulnerabilidad de su organización frente a las amenazas. La gestión de riesgos implica costos y beneficios: tenga en cuenta ambos. Es igualmente importante considerar los costos de no gestionar los riesgos: pueden llegar a ser excesivamente altos porque los eventos indeseables tienen una consecuencia principal, pero siempre acarrear costos secundarios y terciarios para la organización perjudicada.

Recuerde que la gestión de riesgos también ayuda a ahorrar dinero, ya que reduce las pérdidas. Al seleccionar posibles medidas de SRM, es importante tener en cuenta:

- Que la medida elegida efectivamente reduzca el riesgo que supone la amenaza.
- Los efectos adversos. Al intentar gestionar un riesgo se podría generar o acentuar otro de manera involuntaria. Por ejemplo, los controles de acceso muy prolongados que demoran el ingreso a los locales pueden exponer al personal a una amenaza que se supone que deberían mitigar.
- Los costos. Reparar el daño ocasionado por las amenazas puede ser costoso, pero mejorar la seguridad también puede serlo.
- Los recursos adicionales. Considere el costo de la capacitación, el apoyo, el mantenimiento y otros factores necesarios para garantizar que las medidas de SRM se mantengan operativas.
- El tiempo necesario para la implementación. Cuando existen restricciones temporales, se deben tener en cuenta una variedad de opciones. Aunque se estén aplicando medidas nuevas, podrían necesitarse medidas provisionales para cubrir las lagunas.

Un enfoque integral para la seguridad que combine aspectos físicos, procedimentales, técnicos y humanos podría multiplicar los beneficios de las medidas de SRM. De conformidad con los principios de disuasión, detección, demora y negación, dicho enfoque por lo general se denomina “seguridad concéntrica en niveles” o “defensa en profundidad”. Cuando los componentes de un sistema de seguridad se ordenan en niveles, es más difícil transgredirlo.

El proceso de SRM es lo suficientemente flexible como para garantizar que las medidas se adapten a una zona específica de SRM (si no coincide con el área designada). De este modo, se elimina la necesidad de adoptar las mismas medidas mínimas en todo el país. Dicho esto, deben cumplirse los requisitos que son obligatorios para todos los lugares de destino, como impartir la capacitación sobre seguridad BSAFE y contar con kits de profilaxis posterior a la exposición. Tenga en cuenta la incorporación de un enfoque centrado en las personas en la gestión de los riesgos para la seguridad.

Es obligatorio que las medidas de SRM estén centradas en las personas. Se espera que el personal de seguridad trabaje con la célula de seguridad para identificar medidas adecuadas, idóneas y receptivas que ayuden a todo el personal a reducir el riesgo a niveles aceptables. El manual sobre género y las directrices de consideraciones en torno a la discapacidad en la gestión de la seguridad describen en detalle qué factores deben tenerse en cuenta al definir una medida para garantizar que se tenga un enfoque centrado en las personas. Algunas de estas consideraciones incluyen, entre otras:

1. Que las medidas den respuesta específicamente a los descriptores de eventos identificados y que reduzcan la probabilidad o el impacto de dichos eventos.
2. Que las medidas sean sensibles a categorías específicas de personal con perfiles diversos. P. ej., personal del SGSNU de una zona o tribu diferente, con religiones minoritarias, mujeres, LGBTQ+, con discapacidad, embarazadas, etc.
3. Que las medidas propuestas no impongan límites discriminatorios sobre el personal en función de su género, orientación sexual, identidad, expresiones o características sexuales.

El ACNUR tiene el deber de garantizar el cumplimiento de la página 22 del manual sobre género en la gestión de seguridad y las páginas 6 a 10 de los lineamientos de consideraciones en torno a la discapacidad en la gestión de los riesgos para la seguridad, que constituye un capítulo independiente.

Paso 7: Aplicación de la SRM

Una vez que se hayan decidido y consensuado las medidas de seguridad, debe asumirse un sólido compromiso de aplicarlas cuanto antes. Cuando los procesos y las medidas de gestión de riesgos se aprueban en el nivel adecuado, se convierten en requisitos. Se debe formular un plan de ejecución para garantizar que las medidas se adopten y se apliquen de manera oportuna y eficaz. Sin esta etapa, todo el proceso de SRM podría ser infructuoso.

Por lo tanto, los directivos deben asegurarse de que los actores de seguridad y otras partes interesadas relevantes (como ingenieros, especialistas en tecnologías de la información y las comunicaciones, personal de las áreas de administración y suministros, etc.) adopten un enfoque integral en la gestión de proyectos al momento de documentar los recursos para la gestión, organización y planificación que se necesitan para implementar las medidas de SRM de manera eficaz.

Deben tenerse en cuenta los siguientes aspectos:

- Las medidas de mitigación y prevención. Preparar una lista concreta y detallada de las medidas propuestas.
- El objetivo de la mitigación y la prevención. Explicar cómo las medidas en cuestión darán respuesta a los riesgos identificados. ¿Lo harán reduciendo la probabilidad, el impacto o ambos aspectos?
- Los recursos y los costos. Especificar qué recursos se necesitan, incluidos los costos de la financiación y la cooperación. Tener en cuenta los costos únicos y los recurrentes (de mantenimiento, capacitaciones, etc.).
- El actor responsable. Decidir qué directivo, persona o entidad es responsable de poner en marcha cada medida.

- El plazo. Definir un cronograma realista para llevar a cabo cada acción y una fecha límite para completar el proyecto. Puede que sea necesario aplicar medidas temporales o alternativas para cubrir las lagunas hasta que la implementación se haya completado.
- La actualización de avances. Informar periódicamente acerca de los avances en el proceso de implementación. Enumerar las acciones pendientes y las completadas, así como los pasos que será necesario emprender a continuación. Incorporar mecanismos para la evaluación, la provisión de pruebas y la validación.
- El presupuesto. Definir si las medidas de SRM son comunes a todas las Naciones Unidas o de un organismo en particular, con el fin de identificar al responsable del presupuesto pertinente y de obtener la autorización presupuestaria para las medidas planificadas.

Paso 8: Determinación del riesgo aceptable

Aunque el proceso de SRM reduce el riesgo por medio de la mitigación y la prevención (tal como se describe en las secciones anteriores), no todos los riesgos se pueden erradicar del todo. Los principios que se expresan a continuación orientan al SGSNU en relación con el riesgo aceptable.

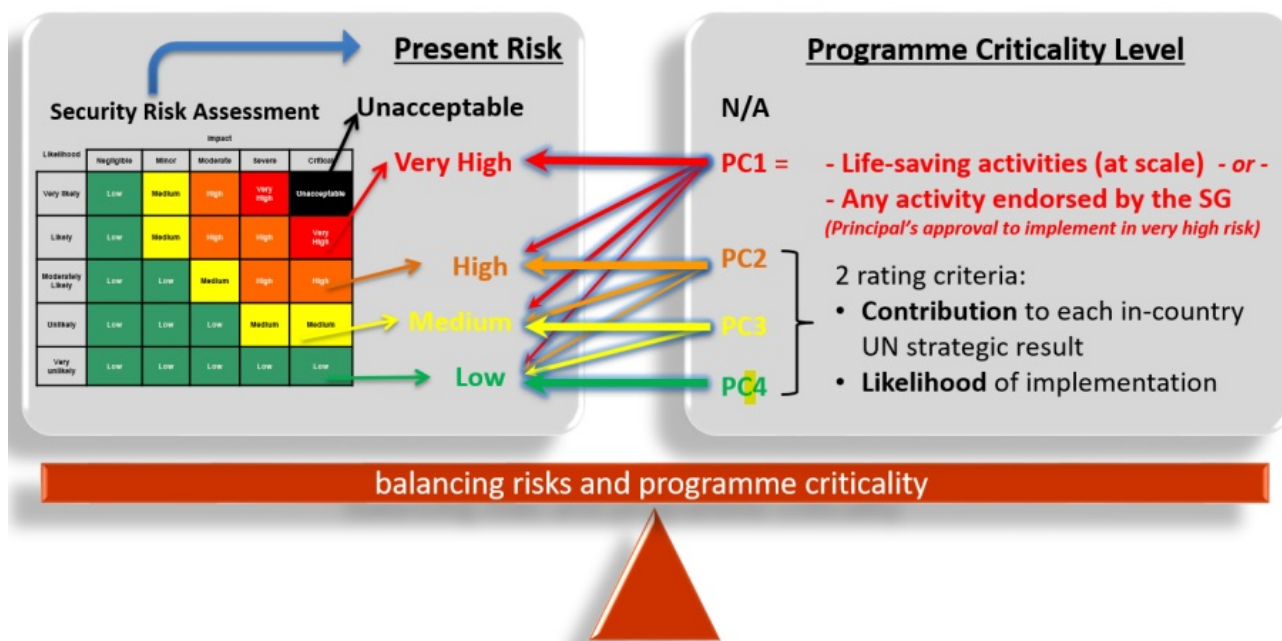
- No se deben aceptar riesgos innecesarios. No hay ninguna ventaja en aceptar un riesgo si no ayuda a las Naciones Unidas a lograr sus objetivos.
- Se deben aceptar riesgos cuando los beneficios superen las desventajas. Aunque no todos los riesgos se pueden eliminar, evitar todos los riesgos tampoco ayuda a las Naciones Unidas a cumplir sus objetivos.
- Se deben tomar decisiones de gestión de riesgos en el nivel adecuado. Las organizaciones deben cerciorarse de que las decisiones en torno al riesgo se tomen en el nivel de autoridad adecuado. Los directivos y el personal no deben asumir un riesgo que no se haya autorizado debidamente.
- Se debe hacer todo lo que sea razonable para reducir el riesgo. Siempre debemos intentar minimizar el riesgo cuando sea viable, incluso aunque se acepte cierto nivel de riesgo.

Modelo de riesgo aceptable

El modelo de riesgo aceptable del SGSNU establece un equilibrio entre los riesgos para la seguridad y los beneficios del programa (esto se denomina "[esencialidad de los programas](#)"). Para evaluar el riesgo aceptable, se comparan cuatro niveles de [esencialidad de los programas](#) con los niveles de riesgo que se identifican en el paso 5 (la evaluación de los riesgos para la seguridad). El modelo de riesgo aceptable distingue entre las actividades que lleva a cabo el personal de las Naciones Unidas y las actividades que llevan a cabo los socios en la ejecución, y únicamente aborda las primeras. Establece el nivel máximo de riesgo para la seguridad que es aceptable para cada nivel de [esencialidad de los programas](#). Se emplea una herramienta independiente de [esencialidad de los programas](#) para establecer los niveles de las actividades en las que participa personal de las Naciones Unidas.

Hay un nivel de riesgo (el nivel máximo de probabilidad y el nivel máximo de impacto) que es inaceptable, independientemente de la importancia de la actividad que desee emprender el personal de las Naciones Unidas. El cuadro que aparece a continuación indica la relación entre riesgo aceptable y esencialidad de los programas, y la responsabilidad de tomar decisiones (se basa en la premisa de que la organización ha hecho todo lo posible por reducir los riesgos de

seguridad).



Nivel 1 actividades solo en entornos de riesgo actual muy alto;

Nivel 1 y 2 en entornos de riesgo actual alto;

Nivel 1, 2 y 3 en entornos de riesgo actual medio;

Nivel 1, 2, 3 y 4 en entornos de riesgo actual bajo.

Paso 9: Monitoreo y revisión

El objetivo del monitoreo y la revisión es mejorar la eficacia de las medidas de gestión de los riesgos para la seguridad y permitir que, cada vez más, los programas se implementen con un nivel de riesgo aceptable. El monitoreo ofrece indicios de progreso, o de la falta de progreso, al aplicar medidas de SRM. Por lo general, a esto se le denomina "cumplimiento". La revisión es clave para garantizar que la SRM se adecúa a su finalidad.

Lista de Verificación

- Comprender la estructura de seguridad en las Naciones Unidas y los actores fundamentales (el Oficial Designado, los Coordinadores de Seguridad de Zona, el equipo de gestión de la seguridad, el equipo de gestión de la seguridad de la zona, etc.), así como el personal de seguridad del ACNUR de la operación, teniendo en cuenta que todos desempeñan un papel clave en el proceso de SRM.

- Ayudar activamente en la ejecución de la SRM. Procurar la implementación e incorporación del enfoque centrado en las personas en los procesos de gestión de los riesgos para la seguridad para garantizar que el riesgo asumido por el ACNUR sea aceptable para todos.
- Completar el examen de la esencialidad de los programas conjuntamente con otras organizaciones de las Naciones Unidas y usar la información como base para la planificación operacional.
- Asegurarse de que los riesgos identificados en la SRM también se reflejen en el registro de riesgos interno de la operación, y de que el tratamiento de los riesgos esté en consonancia con las medidas de SRM.

4. Políticas y directrices

5. Enlaces

[Manual de políticas de seguridad del sistema de gestión de la seguridad de las ... Gestión de riesgos: deber de diligencia, salud y seguridad ocupacionales](#)

6. Contactos principales

Servicio de Seguridad sobre el Terreno y División de Emergencia, Seguridad y Suministros (DESS) del ACNUR. Escribir a: FS00@unhcr.org