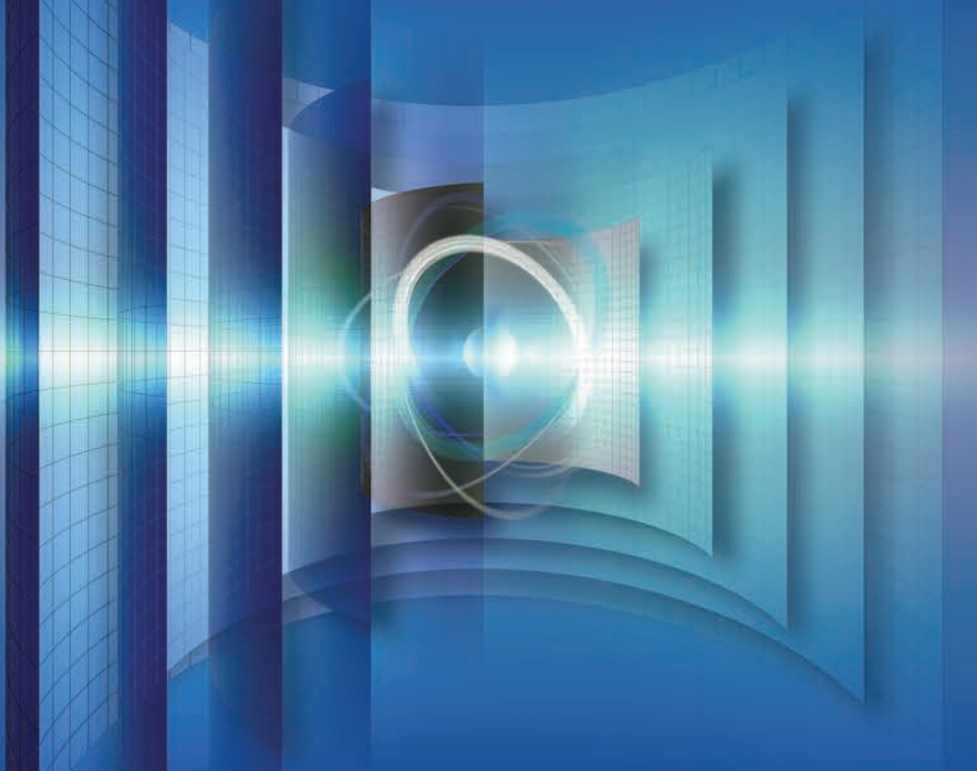
Colección de Seguridad Física Nuclear del OIEA N° 10-G (Rev. 1)

Guía de Aplicación

Evaluación nacional de amenazas para la seguridad física nuclear, amenazas base de diseño y declaraciones de amenazas representativas



IAEA
Organismo Internacional de Energía Atómica

COLECCIÓN DE SEGURIDAD FÍSICA NUCLEAR DEL OIEA

La ***Colección de Seguridad Física Nuclear del OIEA*** trata de cuestiones de seguridad física nuclear relativas a la prevención y detección de actos delictivos o actos intencionales no autorizados que están relacionados con materiales nucleares, otros materiales radiactivos, instalaciones conexas o actividades conexas, o que vayan dirigidos contra ellos, así como a la respuesta a esos actos. Estas publicaciones son coherentes con los instrumentos internacionales de seguridad física nuclear como la Convención sobre la Protección Física de los Materiales Nucleares y su Enmienda, el Convenio Internacional para la Represión de los Actos de Terrorismo Nuclear, las resoluciones 1373 y 1540 del Consejo de Seguridad de las Naciones Unidas, y el Código de Conducta sobre la Seguridad Tecnológica y Física de las Fuentes Radiactivas, y los complementan.

CATEGORÍAS DE LA COLECCIÓN DE SEGURIDAD FÍSICA NUCLEAR DEL OIEA

Las publicaciones de la *Colección de Seguridad Física Nuclear del OIEA* se clasifican en las subcategorías siguientes:

- Las **Nociones Fundamentales de Seguridad Física Nuclear**, que especifican el objetivo del régimen de seguridad física nuclear de un Estado y sus elementos esenciales. Estas Nociones Fundamentales sirven de base para las Recomendaciones de Seguridad Física Nuclear.
- Las **Recomendaciones de Seguridad Física Nuclear**, que establecen las medidas que los Estados deberían adoptar para alcanzar y mantener un régimen nacional de seguridad física nuclear eficaz y conforme a las Nociones Fundamentales de Seguridad Física Nuclear.
- Las **Guías de Aplicación**, que proporcionan orientaciones sobre los medios que los Estados pueden utilizar para aplicar las medidas enunciadas en las Recomendaciones de Seguridad Física Nuclear. Estas guías se centran en cómo cumplir las recomendaciones relativas a esferas generales de la seguridad física nuclear.
- Las **Orientaciones Técnicas**, que ofrecen orientaciones sobre temas técnicos específicos y complementan las que figuran en las Guías de Aplicación. Estas orientaciones se centran en detalles relativos a cómo aplicar las medidas necesarias.

REDACCIÓN Y EXAMEN

En la preparación y examen de las publicaciones de la *Colección de Seguridad Física Nuclear* intervienen la Secretaría del OIEA, expertos de Estados Miembros (que prestan asistencia a la Secretaría en la redacción de las publicaciones) y el Comité de Orientación sobre Seguridad Física Nuclear (NSGC), que examina y aprueba los proyectos de publicación. Cuando procede, también se celebran reuniones técnicas de composición abierta durante la etapa de redacción a fin de que especialistas de los Estados Miembros y organizaciones internacionales pertinentes tengan la posibilidad de estudiar y debatir el proyecto de texto. Además, a fin de garantizar un alto grado de análisis y consenso internacionales, la Secretaría presenta los proyectos de texto a todos los Estados Miembros para su examen oficial durante un período de 120 días.

Para cada publicación, la Secretaría prepara los siguientes documentos, que el NSGC aprueba en etapas sucesivas del proceso de preparación y examen:

- un esquema y plan de trabajo en el que se describe la nueva publicación prevista o la publicación que se va a revisar y su finalidad, alcance y contenidos previstos;
- un proyecto de publicación que se presentará a los Estados Miembros para que estos formulen observaciones durante los 120 días del período de consultas;
- un proyecto de publicación definitivo que tiene en cuenta las observaciones de los Estados Miembros.

En el proceso de redacción y examen de las publicaciones de la *Colección de Seguridad Física Nuclear del OIEA* se tiene en cuenta la confidencialidad y se reconoce que la seguridad física nuclear va indisolublemente unida a preocupaciones sobre la seguridad física nacional de carácter general y específico.

Un elemento subyacente es que en el contenido técnico de las publicaciones se deben tener en cuenta las normas de seguridad y las actividades de salvaguardias del OIEA. En particular, los Comités sobre Normas de Seguridad Nuclear pertinentes y el NSGC analizan las publicaciones de la *Colección de Seguridad Física Nuclear* que se ocupan de ámbitos en los que existen interrelaciones con la seguridad tecnológica, conocidas como documentos de interrelación, en cada una de las etapas antes mencionadas.

EVALUACIÓN NACIONAL DE AMENAZAS PARA LA SEGURIDAD FÍSICA NUCLEAR, AMENAZAS BASE DE DISEÑO Y DECLARACIONES DE AMENAZAS REPRESENTATIVAS

Los siguientes Estados son Miembros del Organismo Internacional de Energía Atómica:

ALBANIA
ALEMANIA
ANGOLA
ANTIGUA Y BARBUDA
ARABIA SAUDITA
ARGELIA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIYÁN
BAHAMAS
BAHREIN
BANGLADESH
BARBADOS
BELARÚS
BÉLGICA
BELICE
BENIN
BOLIVIA, ESTADO PLURINACIONAL DE
BOSNIA Y HERZEGOVINA
BOTSWANA
BRASIL
BRUNEI DARUSSALAM
BULGARIA
BURKINA FASO
BURUNDI
CAMBOYA
CAMERÚN
CANADÁ
COLOMBIA
COMORAS
CONGO
COREA, REPÚBLICA DE
COSTA RICA
CÔTE D'IVOIRE
CROACIA
CUBA
CHAD
CHILE
CHINA
CHIPRE
DINAMARCA
DJIBOUTI
DOMINICA
ECUADOR
EGIPTO
EL SALVADOR
EMIRATOS ÁRABES UNIDOS
ERITREA
ESLOVAQUIA
ESLOVENIA
ESPAÑA
ESTADOS UNIDOS DE AMÉRICA
ESTONIA
ESWATINI
ETIOPÍA
FEDERACIÓN DE RUSIA
FIJI
FILIPINAS
FINLANDIA
FRANCIA
GABÓN
GEORGIA
GHANA
GRANADA
GRECIA
GUATEMALA
GUYANA
HAITÍ
HONDURAS
HUNGRÍA
INDIA
INDONESIA
IRÁN, REPÚBLICA ISLÁMICA DEL
IRAQ
IRLANDA
ISLANDIA
ISLAS MARSHALL
ISRAEL
ITALIA
JAMAICA
JAPÓN
JORDANIA
KAZAJSTÁN
KENYA
KIRGUISTÁN
KUWAIT
LESOTHO
LETONIA
LÍBANO
LIBERIA
LIBIA
LIECHTENSTEIN
LITUANIA
LUXEMBURGO
MACEDONIA DEL NORTE
MADAGASCAR
MALASIA
MALAWI
MALÍ
MALTA
MARRUECOS
MAURICIO
MAURITANIA
MÉXICO
MÓNACO
MONGOLIA
MONTENEGRO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NICARAGUA
NÍGER
NIGERIA
NORUEGA
NUEVA ZELANDIA
OMÁN
PAÍSES BAJOS
PAKISTÁN
PALAU
PANAMÁ
PAPUA NUEVA GUINEA
PARAGUAY
PERÚ
POLONIA
PORTUGAL
QATAR
REINO UNIDO DE GRAN BRETAÑA E IRLANDA DEL NORTE
REPÚBLICA ÁRABE SIRIA
REPÚBLICA CENTROAFRICANA
REPÚBLICA CHECA
REPÚBLICA DE MOLDOVA
REPÚBLICA DEMOCRÁTICA DEL CONGO
REPÚBLICA DEMOCRÁTICA POPULAR LAO
REPÚBLICA DOMINICANA
REPÚBLICA UNIDA DE TANZANÍA
RUMANIA
RWANDA
SAINT KITTS Y NEVIS
SAMOA
SAN MARINO
SAN VICENTE Y LAS GRANADINAS
SANTA LUCÍA
SANTA SEDE
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONA
SINGAPUR
SRI LANKA
SUDÁFRICA
SUDÁN
SUECIA
SUIZA
TAILANDIA
TAYIKISTÁN
TOGO
TONGA
TRINIDAD Y TABAGO
TÚNEZ
TURKMENISTÁN
TÜRKİYE
UCRANIA
UGANDA
URUGUAY
UZBEKISTÁN
VANUATU
VENEZUELA, REPÚBLICA BOLIVARIANA DE
VIET NAM
YEMEN
ZAMBIA
ZIMBABWE

El Estatuto del Organismo fue aprobado el 23 de octubre de 1956 en la Conferencia sobre el Estatuto del OIEA celebrada en la Sede de las Naciones Unidas (Nueva York); entró en vigor el 29 de julio de 1957. El Organismo tiene la Sede en Viena. Su principal objetivo es "acelerar y aumentar la contribución de la energía atómica a la paz, la salud y la prosperidad en el mundo entero".

COLECCIÓN DE SEGURIDAD FÍSICA NUCLEAR DEL OIEA
Nº 10-G (Rev. 1)

EVALUACIÓN NACIONAL DE AMENAZAS PARA LA SEGURIDAD FÍSICA NUCLEAR, AMENAZAS BASE DE DISEÑO Y DECLARACIONES DE AMENAZAS REPRESENTATIVAS

GUÍA DE APLICACIÓN

ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA
VIENA, 2022

DERECHOS DE AUTOR

Dependencia de Mercadotecnia y Venta
Sección Editorial
Organismo Internacional de Energía Atómica
Vienna International Centre
PO Box 100
1400 Viena, Austria
fax: +43 1 26007 22529
tel.: +43 1 2600 22417
correo electrónico: sales.publications@iaea.org
https://www.iaea.org/es/publicaciones

Impreso por el OIEA en Austria
Junio de 2022
STI/PUB/1926

EVALUACIÓN NACIONAL DE AMENAZAS PARA LA SEGURIDAD FÍSICA NUCLEAR, AMENAZAS BASE DE DISEÑO Y DECLARACIONES DE AMENAZAS REPRESENTATIVAS
OIEA, VIENA, 2022
STI/PUB/1926
ISBN 978–92–0–340721–2 (papel) | ISBN 978–92–0–340521–8 (PDF) | ISBN 978–92–0–340621–5 (EPUB)
ISSN 2521–1803

PREFACIO

Rafael Mariano Grossi

Director General

La *Colección de Seguridad Física Nuclear del OIEA* proporciona orientaciones consensuadas a nivel internacional sobre todos los aspectos de la seguridad física nuclear para apoyar a los Estados en su empeño por cumplir sus responsabilidades en esta esfera. El OIEA establece y mantiene actualizadas estas orientaciones como parte de su función central de prestar apoyo y ejercer labores de coordinación en la esfera de la seguridad física nuclear a escala internacional.

La *Colección de Seguridad Física Nuclear del OIEA* se inició en 2006 y el OIEA la actualiza constantemente en cooperación con expertos de los Estados Miembros. En mi calidad de Director General, me comprometo a garantizar que el OIEA mantenga y mejore este conjunto integrado, exhaustivo y coherente de publicaciones de orientaciones sobre seguridad física de alta calidad, actualizadas, fáciles de usar y adecuadas a su finalidad. La correcta aplicación de estas orientaciones en el uso de la ciencia y la tecnología nucleares debería ofrecer un alto nivel de seguridad física nuclear y brindar la confianza necesaria para posibilitar el uso continuo de la tecnología nuclear en beneficio de todos.

La seguridad física nuclear es una responsabilidad nacional. La *Colección de Seguridad Física Nuclear del OIEA* complementa los instrumentos jurídicos internacionales sobre seguridad física nuclear y sirve de referencia mundial para ayudar a las partes a cumplir sus obligaciones. Si bien las orientaciones sobre seguridad física no son jurídicamente vinculantes para los Estados Miembros, se aplican ampliamente. Se han convertido en un punto de referencia indispensable y en un denominador común para la inmensa mayoría de los Estados Miembros que han adoptado estas orientaciones para utilizarlas en la reglamentación nacional con el objetivo de mejorar la seguridad física nuclear en la generación de energía nucleoeléctrica, los reactores de investigación y las instalaciones del ciclo del combustible, así como en las aplicaciones nucleares en la medicina, la industria, la agricultura y la investigación.

Las orientaciones que figuran en la *Colección de Seguridad Física Nuclear del OIEA* se basan en la experiencia práctica de sus Estados Miembros y se elaboran mediante consenso internacional. La participación de los miembros del Comité de Orientación sobre Seguridad Física Nuclear y de otras personas es especialmente importante, y doy las gracias a todas las personas que aportan sus conocimientos y experiencias a esta labor.

El OIEA también utiliza las orientaciones que figuran en la *Colección de Seguridad Física Nuclear del OIEA* cuando presta asistencia a los Estados Miembros mediante sus misiones de examen y servicios de asesoramiento. Esto ayuda a los Estados Miembros en la aplicación de estas orientaciones y permite el intercambio de experiencias y conocimientos valiosos. Las observaciones recibidas sobre estas misiones y servicios, así como las enseñanzas extraídas de los eventos y la experiencia en el uso y la aplicación de las orientaciones sobre seguridad física, se tienen en cuenta durante su revisión periódica.

Estoy convencido de que las orientaciones que figuran en la *Colección de Seguridad Física Nuclear del OIEA* y su aplicación son una aportación inestimable para garantizar un alto nivel de seguridad física nuclear en el uso de la tecnología nuclear. Animo a todos los Estados Miembros a que promuevan y apliquen estas orientaciones, y a que colaboren con el OIEA para mantener su calidad en el presente y en el futuro.

NOTA EDITORIAL

Las orientaciones publicadas en la Colección de Seguridad Física Nuclear del OIEA *no son vinculantes para los Estados; no obstante, los Estados pueden servirse de ellas como ayuda para cumplir sus obligaciones en virtud de los instrumentos jurídicos internacionales, así como para cumplir sus responsabilidades en materia de seguridad física nuclear en el Estado. Las orientaciones en las que se usan formas verbales condicionales tienen por fin presentar buenas prácticas internacionales e indicar un consenso internacional en el sentido de que es necesario que los Estados adopten las medidas recomendadas o medidas alternativas equivalentes.*

Los términos relacionados con la seguridad física han de entenderse según las definiciones contenidas en la publicación en que aparecen, o en las orientaciones más generales que la publicación concreta complementa. En los demás casos, las palabras se emplean con el significado que se les da habitualmente.

Los apéndices se consideran parte integrante de la publicación. El material que figura en un apéndice tiene la misma jerarquía que el texto principal. Los anexos se usan para dar ejemplos prácticos o facilitar información o explicaciones adicionales. Los anexos no son parte integrante del texto principal.

Aunque se ha puesto gran cuidado en mantener la exactitud de la información contenida en esta publicación, ni el OIEA ni sus Estados Miembros asumen responsabilidad alguna por las consecuencias que puedan derivarse de su uso.

El uso de determinadas denominaciones de países o territorios no implica juicio alguno por parte de la entidad editora, el OIEA, sobre la situación jurídica de esos países o territorios, sus autoridades e instituciones o la delimitación de sus fronteras.

La mención de nombres de empresas o productos específicos (se indiquen o no como registrados) no implica ninguna intención de violar derechos de propiedad ni debe interpretarse como una aprobación o recomendación por parte del OIEA.

ÍNDICE

1. INTRODUCCIÓN

ANTECEDENTES

1.1. En las Nociones Fundamentales de Seguridad Física Nuclear [1] se definen el objetivo de un régimen de seguridad física nuclear y sus elementos esenciales. Las Recomendaciones de Seguridad Física Nuclear indican a qué debería responder un régimen de seguridad física nuclear en relación con los siguientes materiales e instalaciones conexas:

a) los materiales nucleares y las instalaciones nucleares [2];
b) los materiales radiactivos y las instalaciones conexas [3];
c) los materiales nucleares y otros materiales radiactivos no sometidos a control reglamentario [4].

1.2. La determinación y la evaluación de amenazas sientan las bases esenciales para la selección, el diseño y la aplicación de medidas de seguridad física nuclear. En el caso de los materiales nucleares y otros materiales radiactivos sometidos a control reglamentario, así como de las instalaciones y actividades conexas, los resultados de esta determinación y evaluación se expresan como una amenaza base de diseño o una declaración de amenaza representativa en la que se describen las intenciones y capacidades de los posibles adversarios frente a las que se han de proteger los materiales y las instalaciones y actividades conexas.

1.3. La presente publicación es una versión revisada de la publicación Nº 10 de la *Colección de Seguridad Física Nuclear del OIEA*, titulada *Development, Use and Maintenance of the Design Basis Threat*[1], con la que se pretende tener en cuenta los avances en esta esfera y garantizar la coherencia terminológica con las referencias [1 a 4], publicadas después de 2009.

1.4. Asimismo, se ha ampliado el alcance de la presente publicación para aclarar el uso de un enfoque alternativo respecto de la amenaza base de diseño, explicar cómo formular amenazas base de diseño específicas para la aplicación y responder mejor a las amenazas en que se emplean ciberataques [5].

---

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).

OBJETIVO

1.5. El objetivo de la presente publicación es proporcionar una metodología paso a paso para realizar una evaluación nacional de amenazas para la seguridad física nuclear que comprenda aspectos de seguridad física e informática y para formular, usar y mantener amenazas base de diseño y declaraciones de amenazas representativas. Consta de los siguientes pasos:

a) definir las funciones y las responsabilidades del Estado, las autoridades competentes (incluido el órgano regulador[2]) y los explotadores;
b) determinar y evaluar amenazas relacionadas con la seguridad física nuclear;
c) formular declaraciones de amenazas, como amenazas base de diseño y declaraciones de amenazas representativas, utilizando los resultados de la evaluación nacional de amenazas para la seguridad física nuclear;
d) utilizar las amenazas base de diseño y/o las declaraciones de amenazas representativas para desarrollar sistemas y medidas de seguridad física nuclear y requisitos de seguridad física nuclear;
e) mantener la vigencia de la evaluación nacional de amenazas para la seguridad física nuclear y su documentación, y
f) mantener la vigencia de las amenazas base de diseño y las declaraciones de amenazas representativas.

1.6. La presente publicación va dirigida a los Estados, las autoridades competentes (incluido el órgano regulador), las organizaciones de apoyo técnico y científico pertinentes y los explotadores de instalaciones y actividades relacionadas con materiales nucleares y otros materiales radiactivos, incluidos los remitentes y los transportistas.

ALCANCE

1.7. El concepto y la metodología descritos en la presente publicación se aplican a la realización de una evaluación nacional de amenazas para la seguridad física nuclear, incluidos aspectos de seguridad tanto física como informática, y al desarrollo, el uso y el mantenimiento de amenazas base de diseño y declaraciones de amenazas representativas para proteger los materiales nucleares

[2] Algunos Estados tienen diversos órganos reguladores encargados de la seguridad física nuclear de los materiales nucleares y otros materiales radiactivos, así como de las instalaciones y las actividades conexas. En la presente publicación, el término “órgano regulador” se refiere al órgano pertinente (u órganos pertinentes) en un contexto determinado.

y otros materiales radiactivos sometidos a control reglamentario, así como las instalaciones y actividades conexas.

1.8. En la presente publicación no se ofrece orientación sobre la formulación de un enfoque basado en el conocimiento de los riesgos ni sobre la realización de evaluaciones de amenazas y riesgos como base para la seguridad física nuclear de los materiales nucleares y otros materiales radiactivos no sometidos a control reglamentario; puede encontrarse orientación sobre este tema en la publicación Nº 24-G de la *Colección de Seguridad Física Nuclear del OIEA*, titulada *Enfoque basado en el conocimiento de los riesgos en materia de medidas de seguridad física nuclear para los materiales nucleares y otros materiales radiactivos no sometidos a control reglamentario* [6].

ESTRUCTURA

1.9. Tras la introducción, la sección 2 aborda la evaluación nacional de amenazas para la seguridad física nuclear como parte de la aplicación de un enfoque basado en el conocimiento de los riesgos. La sección 3 ofrece una visión panorámica del proceso de realización de una evaluación nacional de amenazas para la seguridad física nuclear y del desarrollo y el uso de dicha evaluación de las amenazas y su documentación y el mantenimiento de su vigencia, así como de las amenazas base de diseño y las declaraciones de amenazas representativas. En la sección 4 se describen las funciones y responsabilidades de las organizaciones que participan en el proceso de evaluación nacional de amenazas para la seguridad física nuclear. En la sección 5 se ofrece orientación más detallada sobre cómo realizar una evaluación nacional de amenazas para la seguridad física nuclear. En la sección 6 se describe la formulación de amenazas base de diseño y declaraciones de amenazas representativas, y en la sección 7 se ofrece orientación con respecto a su uso. La sección 8 proporciona orientación sobre el mantenimiento de la vigencia de la evaluación nacional de amenazas para la seguridad física nuclear y su documentación, así como de las declaraciones de amenazas. En el apéndice de la presente publicación se presenta un modelo de amenaza base de diseño.

2. EVALUACIÓN NACIONAL DE AMENAZAS PARA LA SEGURIDAD FÍSICA NUCLEAR Y USO DE UN ENFOQUE BASADO EN EL CONOCIMIENTO DE LOS RIESGOS

2.1. Las convenciones internacionales y las orientaciones de la *Colección de Seguridad Física Nuclear del OIEA* subrayan la importancia de evaluar las amenazas y usar un enfoque de la seguridad física nuclear basado en el conocimiento de los riesgos. En particular, el Principio Fundamental G (Amenaza) de la Convención sobre la Protección Física de los Materiales Nucleares, en su versión enmendada [7, 8], y la referencia [2] establecen lo siguiente: "La protección física que se aplica en el Estado debe basarse en la evaluación más reciente de la amenaza que haya efectuado el propio Estado".

2.2. En el elemento esencial 9 de la referencia [1] se enuncia lo siguiente:

> "Un *régimen de seguridad física nuclear* aplica enfoques basados en el conocimiento de los riesgos para, entre otras cosas, asignar recursos a los *sistemas de seguridad física nuclear* y las *medidas de seguridad física nuclear* y para realizar actividades relacionadas con la seguridad física nuclear en las que se aplica un *enfoque graduado* y la *defensa en profundidad*, así como los siguientes aspectos:
>
> a) la evaluación vigente realizada por el Estado de las *amenazas para la seguridad física nuclear*, tanto internas como externas;
> b) el atractivo y la vulnerabilidad relativos de los *blancos* de las *amenazas para la seguridad física nuclear* definidos;
> c) las características de los *materiales nucleares*, *otros materiales radiactivos*, las *instalaciones conexas* y las *actividades conexas*;
> d) las posibles consecuencias perjudiciales de los actos delictivos o actos intencionales no autorizados que estén relacionados con *materiales nucleares*, *otros materiales radiactivos*, *instalaciones conexas*, *actividades conexas*, *información de carácter estratégico o recursos de información de carácter estratégico* o que vayan dirigidos contra ellos, y otros actos que el Estado determine que tienen un impacto negativo en la seguridad física nuclear".

2.3. Además, en el párrafo 3.10 de la referencia [2] se señala lo siguiente:

> "El Estado debería definir los requisitos, partiendo de la *evaluación de amenazas* o la *amenaza base de diseño*, relativos a la protección física de los *materiales nucleares* durante su utilización, almacenamiento y *transporte*, y a las *instalaciones nucleares*, en función de las consecuencias conexas de la *retirada no autorizada* o del *sabotaje*".

Los párrafos 3.17 y 3.18 de la referencia [3] establecen lo siguiente:

> "El Estado tendría que evaluar las *amenazas* nacionales a *materiales radiactivos*, *instalaciones conexas* y *actividades conexas*; debería examinar periódicamente esas *amenazas* y evaluar las consecuencias de cualquier cambio de las mismas para el diseño o la actualización de su *régimen de seguridad física nuclear*. El *órgano regulador* tendría que utilizar los resultados de la *evaluación de las amenazas* como base común tanto para determinar los requisitos relativos a la seguridad física de los *materiales radiactivos* como para evaluar periódicamente su adecuación".

2.4. En las siguientes subsecciones se abordan con más detalle varias cuestiones relacionadas con la evaluación nacional de amenazas para la seguridad física nuclear utilizando un enfoque basado en el conocimiento de los riesgos, los adversarios y sus atributos y características y la seguridad física de la información.

EL ENFOQUE BASADO EN EL CONOCIMIENTO DE LOS RIESGOS Y LAS DECLARACIONES DE AMENAZAS

2.5. Conforme al elemento esencial 9, un régimen de seguridad física nuclear [1] consiste en la aplicación de enfoques basados en el conocimiento de los riesgos para, entre otras cosas, asignar recursos a los sistemas de seguridad física nuclear y las medidas de seguridad física nuclear y para realizar actividades relacionadas con la seguridad física nuclear en las que se aplica un enfoque graduado y la defensa en profundidad. Al adoptarse un enfoque de seguridad física nuclear basado en el conocimiento de los riesgos deberían tenerse en cuenta la amenaza, el atractivo y la vulnerabilidad de los posibles blancos y las consecuencias que podrían derivarse de actos maliciosos.

2.6. En el párrafo 3.41 de la referencia [2] se recomienda lo siguiente: "El Estado debería velar por que el *régimen de protección física* del Estado pueda situar y mantener el riesgo de *retirada no autorizada* y *sabotaje* en niveles

aceptables a través de la gestión del riesgo". La gestión del riesgo debería incluir una revaluación periódica de la amenaza y las posibles consecuencias de los actos dolosos, y debería garantizar que se establecieran sistemas y medidas de seguridad física nuclear adecuados para prevenir o reducir la probabilidad de que se culmine con éxito un acto doloso.

2.7. Una evaluación nacional de amenazas para la seguridad física nuclear es una evaluación de las amenazas que existen en relación con la seguridad física nuclear, incluidas las amenazas para la seguridad física e informática, a fin de determinar los atributos y las características de los posibles adversarios. Este proceso de evaluación nacional de amenazas para la seguridad física nuclear utiliza fuentes de información mundiales, regionales y nacionales.

2.8. Los resultados del proceso de evaluación nacional de amenazas para la seguridad física nuclear quedan registrados en la documentación de la evaluación nacional de amenazas para la seguridad física nuclear y pueden utilizarse para formular declaraciones de amenazas. En una declaración de amenaza se presentan los atributos y las características de posibles adversarios creíbles frente a los cuales se han de proteger las actividades y las instalaciones relacionadas con materiales nucleares y otros materiales radiactivos.

2.9. Una evaluación de la amenaza que existe actualmente en relación con la seguridad física nuclear, recogida en declaraciones de amenazas, como amenazas base de diseño y declaraciones de amenazas representativas, puede servir para facilitar un enfoque de seguridad física nuclear y la gestión de riesgos en instalaciones y actividades individuales que esté basado en el conocimiento de los riesgos. Las declaraciones de amenazas pueden ayudar a diseñar y evaluar sistemas y medidas de seguridad física nuclear que tengan en cuenta las posibles consecuencias de un acto doloso culminado con éxito.

2.10. Los Estados podrían optar por formular declaraciones de amenazas en forma de amenazas base de diseño o declaraciones de amenazas representativas, o utilizar ambas junto con un enfoque normativo adecuado[3] para distintos tipos de instalaciones y actividades. Una declaración de amenaza representativa podría utilizarse para formular requisitos reglamentarios que hagan hincapié en requisitos prescriptivos para un subconjunto concreto de materiales o instalaciones cuyas consecuencias sean menores y que deban protegerse, mientras que podría definirse una amenaza base de diseño para ser utilizada en la aplicación de requisitos

[3] En las referencias [2, 3, 8 y 9] puede encontrarse información más detallada sobre los enfoques normativos prescriptivos y basados en los resultados.

reglamentarios que hagan hincapié en un enfoque basado en los resultados a fin de proteger una determinada instalación o actividad cuyas consecuencias sean mayores. Por ejemplo, una autoridad competente podría servirse de una declaración de amenaza representativa para formular requisitos reglamentarios prescriptivos con fines de protección de las fuentes radiactivas de categoría 1 en uso y almacenamiento; mientras que un explotador podría utilizar una amenaza base de diseño para diseñar y evaluar un sistema de seguridad física nuclear destinado a satisfacer requisitos basados en los resultados a fin de proporcionar una protección eficaz frente a los escenarios de ataque para una fuente radiactiva específica de categoría 1.

2.11. Sobre la base de los resultados de la evaluación nacional de amenazas para la seguridad física nuclear, los Estados podrían optar por definir diferentes declaraciones de amenazas representativas para las distintas categorías de materiales nucleares y otros materiales radiactivos, los distintos tipos de instalaciones y actividades (por ejemplo, fuentes radiactivas de categoría 1, irradiadores, transporte de materiales radiactivos), los diversos objetivos por parte de los adversarios (por ejemplo, robo, sabotaje) y los activos especialmente susceptibles de ser objeto de ciberataques (por ejemplo, información de carácter sensible o sistemas informáticos con fines de seguridad tecnológica nuclear, seguridad física nuclear, contabilidad y control de materiales nucleares o respuesta a emergencias).

2.12. Análogamente, los Estados podrían optar por definir diferentes amenazas base de diseño a partir de la evaluación nacional de amenazas para la seguridad física nuclear que sean aplicables a los materiales de determinadas instalaciones o actividades que entrañan mayores riesgos (por ejemplo, reactores de investigación, transporte de combustible nuclear gastado). Estas amenazas base de diseño tendrían en cuenta las características de las instalaciones o actividades (por ejemplo, el diseño, la ubicación), consideraciones relativas a políticas (por ejemplo, el grado de prudencia necesario para mantener la confianza pública) y las capacidades y los recursos del Estado y del explotador.

2.13. Es probable que algunas amenazas detectadas durante el proceso de evaluación nacional de amenazas para la seguridad física nuclear se excluyan de las amenazas base de diseño o las declaraciones de amenazas representativas, pues se considerará que trascienden la base de diseño. Incluso si el sistema de seguridad física nuclear del explotador brinda cierta protección inherente, es preciso tener en cuenta la protección frente a estas amenazas en el plan de contingencia del Estado coordinando la respuesta estatal con el plan de respuesta a contingencias del explotador. Si bien el Estado debería elaborar medidas para

combatir estas amenazas, el explotador podría seguir desempeñando un papel ayudando al Estado, ya sea a protegerse de estas amenazas para la seguridad física nuclear, ya a mitigar sus consecuencias.

2.14. Las decisiones relativas al riesgo para la seguridad física nuclear se basan en amenazas actuales que son motivo de preocupación para un Estado, la posibilidad de amenazas nuevas y emergentes y decisiones relativas a cómo lograr equilibrio entre el impacto operativo y la prudencia con respecto a los costos. En estas decisiones también se podrían tener en cuenta las amenazas internacionales y regionales, factores políticos y financieros, la percepción del riesgo por el público y las enseñanzas extraídas de anteriores evaluaciones nacionales de amenazas para la seguridad física nuclear.

POSIBLES ADVERSARIOS Y SUS ATRIBUTOS Y CARACTERÍSTICAS

2.15. Entre los posibles adversarios podrían figurar terroristas, otros delincuentes y extremistas que trataran de adquirir y utilizar material nuclear u otro material radiactivo para construir dispositivos nucleares explosivos, dispositivos de dispersión radiactiva o dispositivos de exposición a la radiación. Estos adversarios también podrían intentar sabotear tanto las instalaciones en las que se utiliza o almacena material nuclear o material radiactivo de otro tipo como el transporte de dicho material.

2.16. Un posible adversario se caracteriza por su motivación, su intención y sus capacidades. Por ejemplo, la motivación podría ser financiera, política o ideológica, o ser producto del descontento o la coacción. Las intenciones podrían ser, entre otras, la posesión no autorizada de material nuclear u otro material radiactivo, la adquisición de información sensible o recursos de información sensible, el daño mediante sabotaje o someter a vergüenza pública al explotador de una instalación o actividad o al Estado. Las capacidades de un adversario dependen de características como el número de personas implicadas, el nivel de organización y coordinación y la presencia de agentes internos. Asimismo, abarcan las destrezas de las personas y de la organización, los activos y las competencias pertinentes, como tácticas, armas, explosivos, el transporte, herramientas físicas e informáticas, el conocimiento de la vulnerabilidad de los programas informáticos y el nivel de acceso a una instalación o sus sistemas informáticos.

2.17. Entre los adversarios podrían figurar agentes internos [9]: personas autorizadas para acceder a instalaciones o actividades conexas, a información sensible o a recursos de información sensible, que podrían cometer o facilitar la

comisión de actos delictivos o actos intencionales no autorizados relacionados con materiales nucleares, otros materiales radiactivos, instalaciones conexas o actividades conexas, u otros actos que el Estado determine que tienen un impacto negativo en la seguridad física nuclear. Los adversarios podrían tratar de convertirse en agentes internos obteniendo acceso autorizado a una instalación (por ejemplo, al ser empleados o contratados como contratistas) para aprovecharse más adelante de ese acceso, o quienes ya son miembros del personal podrían convertirse en agentes internos desarrollando o adquiriendo la intención de cometer o facilitar actos dolosos.

2.18. También debería tenerse en cuenta la posibilidad de que agentes internos y adversarios externos actuasen en connivencia. Por ejemplo, un agente interno podría llevar a cabo un acto no autorizado, físicamente o utilizando medios informáticos, para facilitar la comisión de un acto doloso por parte de un adversario externo.

2.19. Los Estados deberían tener en cuenta no solo los posibles actos dolosos consistentes en acceder físicamente a la instalación o actividad, sino también aquellos en que se emplean ciberataques. Dichos ataques podrían ir dirigidos a los sistemas informáticos utilizados con fines de seguridad tecnológica nuclear (incluidos los sistemas de instrumentación y control), contabilidad y control de materiales nucleares, seguridad física nuclear o respuesta a emergencias (incluidos los sistemas de comunicación y alarma). Los adversarios también podrían llevar a cabo un ataque combinado en el que un ataque a un sistema informático vaya acompañado de un ataque físico, como una intrusión armada utilizando credenciales de acceso falsificadas electrónicamente con la intención de sabotear o robar material.

2.20. Debería tenerse en cuenta que tanto agentes internos como adversarios externos podrían llevar a cabo actos que pusieran en peligro la confidencialidad, la integridad y la disponibilidad de información en los sistemas informáticos. Dichos actos podrían ser facilitados por agentes internos o adversarios externos a través de un ciberataque a distancia. También debería tenerse en cuenta la introducción de programas maliciosos en los sistemas informáticos a través de la cadena de suministro.

2.21. Asimismo, debería considerarse la posibilidad de ataques a distancia en los que se podrían utilizar dispositivos manejados a distancia, como drones, misiles o armas de energía dirigida.

CONSIDERACIONES SOBRE LA SEGURIDAD FÍSICA DE LA INFORMACIÓN

2.22. En la formulación y el mantenimiento de las declaraciones de amenazas debería tenerse en cuenta toda información creíble relacionada con amenazas, incluidos los datos nacionales de inteligencia y otra información sensible. Es necesario proteger partes de esa información y muchas de sus fuentes. Una amenaza base de diseño o una declaración de amenaza representativa que se utilice en el diseño y la evaluación de los sistemas de seguridad física nuclear debería protegerse como información sensible, es decir, información, cualquiera que sea su forma, incluidos los programas informáticos, cuya revelación, modificación, alteración, destrucción o denegación de uso no autorizadas podrían comprometer la seguridad física nuclear.

2.23. Puede obtenerse orientación detallada sobre la protección de información sensible sobre seguridad física nuclear en la publicación Nº 23-G de la *Colección de Seguridad Física Nuclear del OIEA*, titulada *Seguridad física de la información nuclear* [10].

3. VISIÓN PANORÁMICA DEL PROCESO DE DESARROLLO, USO Y MANTENIMIENTO DE LA VIGENCIA DE LA EVALUACIÓN NACIONAL DE AMENAZAS PARA LA SEGURIDAD FÍSICA NUCLEAR Y SU DOCUMENTACIÓN, AMENAZAS BASE DE DISEÑO Y DECLARACIONES DE AMENAZAS REPRESENTATIVAS

3.1. En la figura 1 se muestra el proceso de formulación, uso y mantenimiento de la vigencia de la evaluación nacional de amenazas para la seguridad física nuclear y su documentación, así como las amenazas base de diseño y las declaraciones de amenazas representativas, que consta de cinco pasos:

1) definición de funciones y responsabilidades;
2) realización y documentación de la evaluación nacional de amenazas para la seguridad física nuclear;
3) formulación de amenazas base de diseño y/o declaraciones de amenazas representativas;

4) utilización de las amenazas base de diseño y/o las declaraciones de amenazas representativas en el marco regulador, y
5) mantenimiento de la vigencia de la evaluación nacional de amenazas para la seguridad física nuclear, las amenazas base de diseño y/o las declaraciones de amenazas representativas.

3.2. Durante el paso 1, el Estado debería definir las funciones y responsabilidades que corresponden en este proceso al órgano regulador y otras autoridades competentes, así como a los explotadores, de acuerdo con el marco jurídico y regulador del Estado.

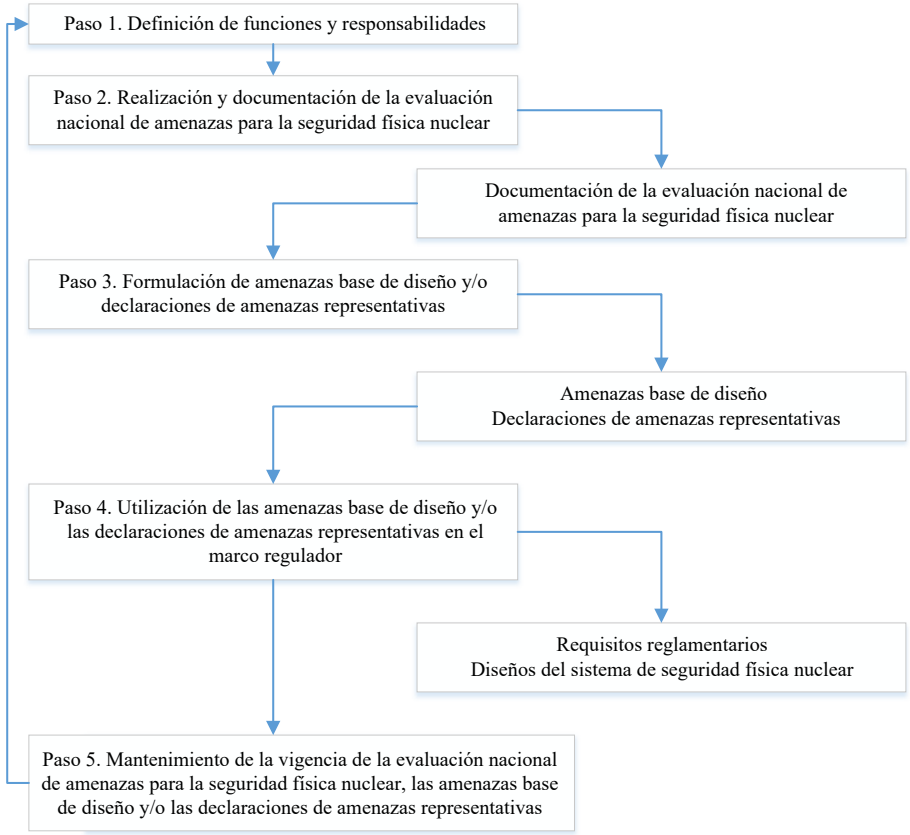


Fig. 1. Proceso de desarrollo, uso y mantenimiento de la vigencia de la evaluación nacional de amenazas para la seguridad física nuclear y su documentación, así como de las amenazas base de diseño y las declaraciones de amenazas representativas.

3.3. Durante el paso 2 —realización de la evaluación nacional de amenazas para la seguridad física nuclear—, la autoridad competente encargada de realizar dicha evaluación, junto con otras autoridades competentes pertinentes, debería recopilar datos de inteligencia y otra información sobre las amenazas, como información procedente de fuentes abiertas, anteriores sucesos relacionados con la seguridad física nuclear y sucesos relacionados con la seguridad física de actividades ajenas al ámbito nuclear. Las autoridades competentes deberían analizar la información recopilada y evaluar su posible pertinencia para la seguridad física nuclear. Asimismo, deberían evaluar la credibilidad de la información sobre las amenazas y descartar la información que no sea creíble. Sobre la base de la información restante, las autoridades competentes deberían identificar posibles adversarios y caracterizar la probabilidad de que estos actúen, así como sus atributos y características. Por último, las autoridades competentes deberían evaluar si determinadas capacidades del adversario son pertinentes para los posibles blancos. Los resultados de este proceso deberían registrarse en la documentación de la evaluación nacional de amenazas para la seguridad física nuclear.

3.4. En el paso 3, utilizando los resultados de la evaluación nacional de amenazas para la seguridad física nuclear, la autoridad competente encargada de elaborar las declaraciones de amenazas, en acuerdo con otras autoridades competentes, según proceda, debería elaborar amenazas base de diseño referidas específicamente a materiales, instalaciones o actividades y/o elaborar declaraciones de amenazas representativas aplicables a distintos tipos y categorías de material nuclear, otros materiales radiactivos e instalaciones y actividades conexas.

3.5. En el paso 4, las medidas del órgano regulador dependerán del enfoque normativo seguido:

a) En el caso de un enfoque basado en los resultados, el órgano regulador debería divulgar las amenazas base de diseño entre los explotadores pertinentes, que a continuación deberían desarrollar escenarios de ataque específicos en función de las instalaciones y utilizar estos escenarios para diseñar sistemas de seguridad física nuclear que contrarresten las amenazas base de diseño y cumplan los objetivos de seguridad física nuclear establecidos en el marco jurídico del Estado.
b) En el caso de un enfoque prescriptivo, el órgano regulador debe elaborar requisitos reglamentarios basados en las declaraciones de amenazas representativas y en los objetivos de seguridad física nuclear establecidos en el marco jurídico del Estado, así como garantizar que los explotadores apliquen sistemas y medidas de seguridad física nuclear de conformidad con esos requisitos.

c) En el caso de un enfoque combinado, el órgano regulador debería incorporar elementos extraídos tanto del enfoque basado en los resultados como del enfoque prescriptivo.

3.6. En el paso 5, las autoridades competentes deberían examinar y, si procede, enmendar la evaluación nacional de amenazas para la seguridad física nuclear y su documentación, las amenazas base de diseño y/o las declaraciones de amenazas representativas. La decisión de revisar estos documentos podría tomarse con arreglo a un ciclo de examen definido, en caso de cambio en el entorno de la amenaza y/o para incorporar las enseñanzas extraídas a raíz de un suceso relacionado con la seguridad física nuclear. En el caso de amenazas nuevas o emergentes que sea preciso considerar de manera inmediata, las autoridades competentes, junto con los explotadores, deberían adoptar las medidas necesarias para manejarlas, si es necesario al margen de las amenazas base de diseño o las declaraciones de amenazas representativas existentes, a la espera de su enmienda. Este proceso debería integrarse en el régimen de seguridad física nuclear del Estado.

3.7. En las secciones 4 a 8 se aborda cada uno de estos pasos con más detalle, y se orienta de manera más específica a los Estados, las autoridades competentes y los explotadores en lo que respecta a su puesta en práctica.

4. FUNCIONES Y RESPONSABILIDADES

4.1. El Estado, las autoridades competentes pertinentes (incluido el órgano regulador) y los explotadores tienen funciones y responsabilidades relacionadas con la evaluación nacional de amenazas para la seguridad física nuclear y la formulación de amenazas base de diseño y/o declaraciones de amenazas representativas. Estas funciones y responsabilidades deberían estar definidas claramente antes de que comiencen las labores de evaluación nacional de amenazas para la seguridad física nuclear.

EL ESTADO

4.2. El Estado se encarga de asignar, coordinar y supervisar a las autoridades competentes que dirigen las siguientes actividades y participan en ellas:

a) realización de una evaluación nacional de amenazas para la seguridad física nuclear y mantenimiento de la vigencia de la evaluación y su documentación;
b) formulación de amenazas base de diseño y/o declaraciones de amenazas representativas y mantenimiento de su vigencia, y
c) uso de las amenazas base de diseño y/o las declaraciones de amenazas representativas[4].

4.3. Un suceso relacionado con la seguridad física nuclear podría dar lugar a una emergencia nuclear o radiológica. El párrafo 4.22 de la publicación Nº GSR Part 7 de la *Colección de Normas de Seguridad del OIEA*, titulada *Preparación y respuesta para casos de emergencia nuclear o radiológica* [11], establece lo siguiente: "El Gobierno se asegurará de que en la evaluación de los peligros se tomen en consideración los resultados de las evaluaciones de amenazas que se hayan realizado con fines de seguridad física nuclear".

LAS AUTORIDADES COMPETENTES

4.4. Todas las autoridades competentes pertinentes deberían participar en el proceso de evaluación nacional de amenazas para la seguridad física nuclear con objeto de que se pueda determinar la gama más completa posible de amenazas creíbles y se pueda tenerla en cuenta en la evaluación.

4.5. Podría disponerse de los conocimientos técnicos pertinentes para detectar y evaluar amenazas creíbles en varias organizaciones de un Estado, como en organizaciones de inteligencia (incluidos los organismos de seguridad física), ministerios del interior y de relaciones exteriores, centros de seguridad informática, fuerzas del orden, servicios militares, el órgano regulador en materia de seguridad física nuclear y otras organizaciones pertinentes. Dichas organizaciones contarán con personal familiarizado con los procesos de recopilación y análisis de la información y capacitado para emitir los juicios necesarios. Además, esas

[4] El Estado podría asignar a diferentes autoridades competentes la dirección de los distintos procesos; sin embargo, las funciones y responsabilidades deben estar definidas claramente y el mecanismo de coordinación entre las autoridades competentes debe estar bien establecido y ponerse en práctica.

organizaciones podrían tener acceso a determinadas fuentes de información, como información procedente de contactos con otros Estados u organizaciones regionales o internacionales.

4.6. Las autoridades competentes podrían encargarse, entre otras cosas, de:

a) recopilar y compilar información sobre posibles amenazas;
b) analizar la información sobre amenazas disponible para garantizar su credibilidad;
c) intercambiar con otras autoridades competentes información pertinente sobre amenazas;
d) coordinarse con otras autoridades competentes para determinar el subconjunto de amenazas creíbles que resultan pertinentes en materia de seguridad física nuclear;
e) cooperar en el proceso de evaluación de las amenazas identificando posibles adversarios y documentando la evaluación nacional de amenazas para la seguridad física nuclear;
f) formular amenazas base de diseño y/o declaraciones de amenazas representativas a partir de los resultados de la evaluación nacional de amenazas para la seguridad física nuclear;
g) mantener la vigencia de la evaluación nacional de amenazas para la seguridad física nuclear y su documentación, así como de las amenazas base de diseño y las declaraciones de amenazas representativas;
h) compartir, según proceda, la documentación de la evaluación nacional de amenazas para la seguridad física nuclear con organizaciones pertinentes de respuesta a emergencias[5];
i) tener en cuenta la evaluación nacional de amenazas para la seguridad física nuclear al llevar a cabo la evaluación de los peligros [12], y
j) aplicar consideraciones en materia de seguridad física de la información.

4.7. Algunas autoridades competentes (como las autoridades policiales nacionales y locales, las fuerzas armadas, las autoridades de control fronterizo y las autoridades aduaneras) tienen esferas de responsabilidad mucho más amplias dentro de un Estado en el marco de las cuales podrían contribuir a la protección frente a las amenazas relacionadas con la seguridad física nuclear, ya

[5] Puesto que en el ámbito de la seguridad física nuclear la respuesta se refiere a la respuesta a un suceso relacionado con la seguridad física nuclear, en la presente publicación se recurre al término “organización de respuesta a emergencias” para evitar interpretaciones erróneas. Dicho término se emplea de acuerdo con la definición establecida de “organización de respuesta” que aparece en la publicación GSR Part 7 [11].

sea por cuenta propia o en cooperación con otras instancias. Algunas autoridades competentes podrían encargarse también de prestar apoyo al explotador durante un suceso relacionado con la seguridad física nuclear. Dichas autoridades competentes deberían participar o ser consultadas en el proceso de elaboración de amenazas base de diseño y/o declaraciones de amenazas representativas, así como de los requisitos reglamentarios.

4.8. Corresponden al órgano regulador en materia de seguridad física nuclear, en coordinación con otras autoridades competentes, según corresponda, las siguientes tareas:

a) formular requisitos prescriptivos para los explotadores sobre la base de declaraciones de amenazas representativas y/o proporcionar a los explotadores las amenazas base de diseño y los requisitos basados en los resultados que se utilizarán para elaborar escenarios de ataque y diseñar sistemas y medidas de seguridad física nuclear, y
b) garantizar que los explotadores examinen adecuadamente las disposiciones en materia de seguridad física y emergencia y, si es necesario, las revisen teniendo en cuenta los escenarios de ataque elaborados y los resultados de las evaluaciones de las amenazas.

LOS EXPLOTADORES

4.9. Los explotadores deberían aplicar sistemas y medidas de seguridad física nuclear que logren al menos uno de los dos objetivos siguientes:

a) cumplir los requisitos reglamentarios, incluidos los requisitos prescriptivos pertinentes elaborados sobre la base de la declaración de amenaza representativa;
b) proteger frente a una serie de escenarios de ataque referidos específicamente a la instalación o la actividad, elaborados a partir de la amenaza base de diseño.

4.10. En algunos casos, el conocimiento por los explotadores de las repercusiones financieras, operativas y de seguridad tecnológica de determinadas medidas de seguridad física nuclear podría influir en el reparto de responsabilidades entre los explotadores y las autoridades competentes en lo que respecta a las medidas de seguridad física nuclear. Las aportaciones de los explotadores, ya sean oficiales u oficiosas, deberían tenerse en cuenta al elaborar amenazas base de diseño,

declaraciones de amenazas representativas y requisitos reglamentarios. Los explotadores deberían proporcionar concretamente lo siguiente:

a) aportaciones sobre amenazas relacionadas con la seguridad física nuclear referidas a instalaciones y actividades específicas cuya inclusión en las amenazas base de diseño y/o las declaraciones de amenazas representativas debería examinarse;
b) comentarios para el órgano regulador, si se consideran necesarios y se solicitan dentro del marco jurídico y regulador, en relación con el impacto financiero, operacional y en materia de seguridad física y de seguridad tecnológica que tendrían las posibles decisiones relativas a las amenazas base de diseño, las declaraciones de amenazas representativas y/o los requisitos reglamentarios, e
c) información complementaria, si se considera necesaria y se solicita dentro del marco jurídico y regulador, en relación con los escenarios de ataque y los atributos y características de los adversarios, procedente de ataques físicos, ciberataques y ataques combinados que se hayan producido.

5. REALIZACIÓN DE UNA EVALUACIÓN NACIONAL DE AMENAZAS PARA LA SEGURIDAD FÍSICA NUCLEAR

5.1. El objetivo de la evaluación nacional de amenazas para la seguridad física nuclear es proporcionar una evaluación de las amenazas creíbles describiendo las motivaciones, las intenciones y las capacidades de los posibles adversarios. No tiene por objeto describir escenarios de ataque concretos.

5.2. Una descripción suficientemente detallada y específica de las posibles amenazas puede servir para determinar el nivel de protección adecuado y suficiente para los materiales nucleares y otros materiales radiactivos, así como para las instalaciones y actividades conexas, y ofrece una base sobre la que poder diseñar eficazmente un sistema de seguridad física nuclear.

5.3. Durante el proceso de evaluación nacional de amenazas para la seguridad física nuclear, se recopila y analiza información sobre las amenazas existentes y las posibles amenazas creíbles, y se recopila y agrupa información sobre los atributos y las características de los posibles adversarios. El resultado de la evaluación

nacional de amenazas para la seguridad física nuclear es una descripción detallada de las amenazas relacionadas con la seguridad física nuclear y se conoce como documentación de la evaluación nacional de amenazas para la seguridad física nuclear. Todas las organizaciones pertinentes con distintas esferas de especialidad y responsabilidad deberían colaborar estrechamente en la recopilación y el análisis de esta información. A fin de que la evaluación nacional de amenazas para la seguridad física nuclear sea eficaz, es necesario que todas las organizaciones pertinentes colaboren estrechamente. Deberían mantenerse registros de las evaluaciones nacionales de amenazas para la seguridad física nuclear realizadas con el objeto de apoyar el proceso de examen y revisión periódicos para mantener la vigencia de la evaluación.

5.4. En la sección 4 se describen las funciones y responsabilidades para llevar a cabo las acciones descritas con detalle en las siguientes subsecciones o garantizar su conclusión.

APORTACIÓN: RECOPILACIÓN DE INFORMACIÓN PERTINENTE SOBRE AMENAZAS

5.5. La primera tarea en el proceso de evaluación nacional de amenazas para la seguridad física nuclear es recopilar y compilar información exhaustiva sobre todos los posibles adversarios, así como sus motivaciones, intenciones y capacidades. Esta información podría constar de datos tanto sensibles como de carácter no sensible y debería referirse a las capacidades físicas e informáticas y a los posibles adversarios, tanto internos como externos.

5.6. Deberían determinarse posibles fuentes de información y debería recopilarse la información pertinente. Debería tenerse en cuenta la sensibilidad de la información a fin de garantizar la aplicación de un nivel adecuado de seguridad física tanto a la información como a sus fuentes. Si todavía no se ha hecho, debería establecerse un mecanismo para que todas las organizaciones pertinentes intercambien información sobre las amenazas durante el proceso de evaluación de las amenazas; ese mecanismo debería prever la seguridad física de la información sensible. Podrían necesitarse acuerdos por escrito para establecer disposiciones relativas al intercambio de información sobre amenazas.

5.7. Los servicios de inteligencia y otras fuentes de información relacionadas con las amenazas podrían proporcionar información suficiente para diseñar un sistema de seguridad física nuclear. Sin embargo, debido a las limitaciones de los servicios de inteligencia y a la naturaleza dinámica de las amenazas, puede que

los sistemas de seguridad física nuclear diseñados únicamente para las amenazas conocidas hasta la fecha no sean eficaces contra las futuras amenazas.

5.8. La evaluación nacional de amenazas para la seguridad física nuclear no debería basarse en una sola fuente. El uso de información de inteligencia y sobre amenazas procedente de múltiples fuentes fusionadas en una única evaluación coherente constituirá la evaluación nacional más completa, fiable y sólida de las amenazas para la seguridad física nuclear. Al recopilarse los datos deberían tenerse en cuenta todas las fuentes nacionales e internacionales creíbles y pertinentes de información de inteligencia y sobre amenazas.

5.9. Las fuentes de información e inteligencia deberían incluir, según proceda, organizaciones de inteligencia (comprendidos organismos de seguridad física), organizaciones de seguridad física de los sistemas informáticos y de la información, fuerzas del orden, la Organización Internacional de Policía Criminal, el órgano regulador en materia de seguridad física nuclear y otras autoridades competentes, organismos de aduanas y control de fronteras, servicios militares, remitentes y transportistas, informes oficiales de los poderes públicos, informes sobre incidentes presentados por los explotadores, bases de datos mantenidas por organizaciones internacionales y otras fuentes de libre acceso.

5.10. Podrían utilizarse organizaciones de apoyo técnico y científico, entidades comerciales y bases de datos de libre acceso como fuentes de información adicional sobre posibles amenazas, especialmente las que afectan a la seguridad informática. Los explotadores también podrían tener información sobre esas amenazas y sus atributos y características.

5.11. Debería tenerse en cuenta información pertinente sobre los atributos y las características de las posibles amenazas para otros tipos de infraestructura crítica, dada su posible analogía con las amenazas para la seguridad física nuclear.

5.12. Si procede, debería recopilarse información sobre sucesos recientes e históricos relacionados con la seguridad física nuclear (incluidos los relacionados con la seguridad informática).

5.13. La tarea de recopilar información debería tener por objeto señalar todos los tipos de amenazas pertinentes, incluidas las siguientes:

a) amenazas mundiales, nacionales y locales;
b) ataques físicos, ciberataques y ataques combinados, y

c) amenazas internas, adversarios externos y amenazas resultantes de la connivencia de adversarios internos y externos.

5.14. Asimismo, deberían tenerse en cuenta las capacidades creíbles del adversario, aunque no se hayan demostrado. También deberían tenerse en cuenta los posibles adversarios persistentes que planifican ataques en varias etapas durante períodos extensos, los posibles avances tecnológicos, la posible frecuencia de los ataques y la posibilidad de ataques a la cadena de suministro (por ejemplo, poniendo en peligro el equipo informático y/o los programas informáticos modificados antes de la entrega).

ANÁLISIS DE LA INFORMACIÓN PERTINENTE SOBRE LA AMENAZA

5.15. Una vez recopilada información pertinente sobre las amenazas, debería procederse a su compilación utilizando herramientas de gestión de la información a fin de indexarla y clasificarla antes de comenzar el análisis. La organización eficaz de todos los datos de inteligencia y otra información disponible garantizará la disponibilidad de toda la información necesaria con fines de análisis. A continuación, la información organizada debería analizarse para determinar y documentar las motivaciones, intenciones y capacidades creíbles de los posibles adversarios en relación con la seguridad física nuclear.

5.16. La exhaustividad de la información recopilada y la precisión del análisis repercutirán en la confianza que pueda depositarse en las amenazas base de diseño y/o las declaraciones de amenazas representativas resultantes del proceso.

5.17. Es probable que la recopilación y el análisis de la información sean iterativos. El análisis demostrará a menudo la necesidad de más información o detectará amenazas previamente desconocidas o emergentes sobre las cuales se precisa información. El análisis de la información sobre amenazas consiste en evaluar lo que se conoce a partir de esa información y emitir un juicio sobre la posible evolución futura de los atributos y las características de los adversarios.

5.18. Durante el proceso de análisis, debería evaluarse la credibilidad de la información utilizada en la evaluación nacional de amenazas para la seguridad física nuclear. En general, al evaluar la credibilidad de la información sobre amenazas es importante tener en cuenta tanto la fiabilidad como los conocimientos técnicos especializados de la fuente de la información. Las fuerzas del orden y los organismos de inteligencia, incluidos los organismos de seguridad física, deberían

indicar el grado de confianza que, a su juicio, puede otorgarse a la información que aportan. La información de libre acceso (por ejemplo, de medios de comunicación públicos o de redes sociales) que puede consultarse fácilmente podría ser útil, pero debería examinarse cuidadosamente su exactitud. Al decidirse cómo habrá de utilizarse posteriormente cualquier información, debería tenerse en cuenta el grado de confianza que cabe depositar en ella. Al evaluar la credibilidad de la información, podría excluirse también alguna información por no ser pertinente para el análisis, y podrían detectarse nuevas lagunas de información (por ejemplo, si se determina que la información que parecía colmar una laguna no es suficientemente creíble).

5.19. En el proceso de evaluación nacional de amenazas para la seguridad física nuclear deberían tenerse en cuenta, como mínimo, los siguientes atributos y características de los adversarios respecto de cada amenaza detectada (aunque podría no disponerse de datos relativos a todos los atributos y características enumerados en relación con todas las amenazas):

a) las motivaciones del adversario, que podrían ser, por ejemplo, políticas, financieras, ideológicas y/o personales (por ejemplo, como resultado del descontento o la coacción);
b) la persistencia del adversario;
c) el empeño del adversario, incluido el nivel de aversión al riesgo y la voluntad de poner en peligro su propia vida;
d) las capacidades demostradas del adversario, incluida la caracterización de sucesos relacionados con la seguridad física nuclear ocurridos en el pasado;
e) las intenciones del adversario, como el sabotaje de material o de una instalación, la retirada no autorizada de material nuclear u otro material radiactivo o el robo de información sensible;
f) el número de adversarios en un grupo, con inclusión de la fuerza de ataque, el personal de coordinación y el personal de apoyo;
g) los tipos y el número de armas de que dispone el adversario;
h) los tipos y las cantidades de los explosivos de que dispone el adversario, ya se hayan adquirido en forma de artefactos o se hayan improvisado, y la sofisticación de los mecanismos de activación;
i) las herramientas de las que dispone el adversario, como equipos mecánicos, térmicos o electromagnéticos, manuales o electrónicos o de comunicaciones;
j) el transporte de que dispone el adversario, incluido el tipo (público, privado), el modo (terrestre, marítimo, aéreo) y los tipos y el número de vehículos;
k) los modos probables de acceso a los blancos, tanto físicos como informáticos;
l) la influencia sobre las operaciones y/o el personal;

m) las posibles tácticas del adversario, como la ocultación, el engaño, la fuerza, las actividades de reconocimiento o la ingeniería social;
n) las aptitudes de planificación del adversario, como la capacidad de planificar una desviación o de coordinar ataques simultáneos de grupos más pequeños;
o) las aptitudes prácticas, los conocimientos y la experiencia de que dispone el adversario, incluidas aptitudes en materia de ingeniería, uso de explosivos, productos químicos y comunicaciones, y experiencia militar o paramilitar;
p) el acceso a conocimientos informáticos y de seguridad informática, como el conocimiento de los sistemas de control, las medidas de seguridad informática, la ingeniería inversa y la evaluación de la vulnerabilidad, la ingeniería de protocolos de comunicación, la ingeniería social, la ofuscación de fuentes, la redirección de atribuciones, la vigilancia de redes y la manipulación del tráfico;
q) el conocimiento de información sobre los blancos o el acceso a esa información, lo cual incluye las características de estos, la distribución de las instalaciones, los planos y procedimientos del emplazamiento, los planes en materia de seguridad física, las medidas de seguridad física, las medidas de seguridad tecnológica y protección radiológica, las operaciones de las instalaciones y de transporte, los posibles puntos de entrada de los ciberataques, los procedimientos y planes de apoyo a los proveedores y los procedimientos de la cadena de suministro y de adquisición;
r) las fuentes y las cantidades de financiación, y cómo se accede a ellas;
s) el potencial de aprovechar agentes internos (por ejemplo, mediante connivencia, coacción o engaño), el posible número de agentes internos y si son pasivos o activos, violentos o no violentos, y
t) las estructuras de apoyo de los adversarios, como la presencia o ausencia de simpatizantes locales, organizaciones de apoyo o apoyo logístico.

RESULTADO: DOCUMENTACIÓN DE LA EVALUACIÓN NACIONAL DE AMENAZAS PARA LA SEGURIDAD FÍSICA NUCLEAR

5.20. El resultado del proceso de evaluación nacional de amenazas para la seguridad física nuclear se registra en la documentación de la evaluación nacional de amenazas para la seguridad física nuclear, en la que se describen el entorno general de las amenazas para la seguridad física nuclear y todas las amenazas creíbles conocidas que deberían tenerse en cuenta. La descripción analítica complementaria debería proporcionar tantos detalles como sea posible sobre estas amenazas y la credibilidad de la información.

5.21. Tanto la documentación de la evaluación nacional de amenazas para la seguridad física nuclear como los detalles de las fuentes de inteligencia suelen estar protegidos como información sensible.

6. FORMULACIÓN DE AMENAZAS BASE DE DISEÑO Y DECLARACIONES DE AMENAZAS REPRESENTATIVAS

6.1. Como se describe en la sección 5, el proceso de evaluación nacional de amenazas para la seguridad física nuclear culmina con la preparación de la documentación de la evaluación nacional de amenazas para la seguridad física nuclear. Utilizar como base la evaluación nacional de amenazas para la seguridad física nuclear permite formular declaraciones de amenazas en forma de amenazas base de diseño y/o declaraciones de amenazas representativas. En estas declaraciones se describen los adversarios creíbles contra los que hay que proteger las instalaciones y actividades que utilizan o almacenan material nuclear u otro material radiactivo, así como los atributos y características de estos adversarios.

ENFOQUES NORMATIVOS Y DECLARACIONES DE AMENAZAS

6.2. A la hora de regular la explotación de una instalación o la realización de una actividad es posible utilizar tres enfoques normativos: el enfoque basado en los resultados, el enfoque prescriptivo y el enfoque combinado. En el enfoque basado en los resultados, el explotador debe diseñar e implantar un sistema de seguridad física nuclear para cumplir los objetivos de seguridad física nuclear establecidos por el Estado teniendo en cuenta la amenaza base de diseño difundida por el órgano regulador, el nivel de eficacia especificado para la protección contra actos dolosos y la provisión de respuestas de contingencia. En el enfoque prescriptivo, el órgano regulador, sin compartir la información sobre amenazas con los explotadores, establece medidas de seguridad física nuclear específicas que ha considerado necesarias para cumplir los objetivos de seguridad física nuclear definidos para cada categoría de material nuclear u otro material radiactivo y cada nivel de posibles consecuencias radiológicas. Se determina así un conjunto de medidas "de referencia" que el explotador tiene que aplicar. El enfoque combinado incluye elementos del enfoque prescriptivo y del enfoque basado en los resultados. Se

puede encontrar información más detallada sobre cada uno de estos enfoques normativos en las referencias [13, 14].

6.3. Como se indicaba en el párrafo 2.10, las declaraciones de amenazas representativas se utilizan a menudo para formular requisitos normativos prescriptivos para un subconjunto específico de materiales, actividades y/o instalaciones que deben protegerse, mientras que las amenazas base de diseño suelen formularse para instalaciones o actividades específicas. El órgano regulador debería adoptar el enfoque normativo y elegir las correspondientes declaraciones de amenazas representativas y/o amenazas de base de diseño que mejor se adapten a las necesidades del Estado, en consonancia con su marco jurídico y regulador. El enfoque elegido por el órgano regulador debería ser aprobado por el Estado, ya que la elección probablemente tendrá implicaciones financieras para el órgano regulador y los explotadores.

6.4. El uso de una amenaza base de diseño en un enfoque normativo basado en los resultados como base para diseñar sistemas y medidas de seguridad física nuclear puede redundar en una asignación eficiente de los recursos, al permitir que se elaboren requisitos de protección y sistemas y medidas de seguridad física nuclear contra amenazas específicas pertinentes, y no contra amenazas genéricas. El uso de un enfoque basado en los resultados y una amenaza base de diseño permite personalizar el diseño del sistema de seguridad física nuclear en función de las características únicas del material, las actividades o las instalaciones (incluidos sus sistemas de instrumentación y control), pero también establece unos valores de referencia para evaluar los sistemas y las medidas de seguridad física nuclear (y realizar modificaciones si es necesario) y proporciona una base clara para definir las responsabilidades del explotador en materia de seguridad física nuclear. El uso de una amenaza de base de diseño también proporciona una base técnica más detallada y precisa para los criterios de diseño y evaluación y puede ofrecer mayor garantía de que la protección es suficiente.

6.5. El uso de una amenaza base de diseño en un enfoque basado en los resultados implica una mayor necesidad de recursos y de competencia por parte del órgano regulador y del explotador. Por ese motivo, la decisión de aplicar una amenaza base de diseño podría verse influida por el hecho de que el órgano regulador y el explotador dispongan de los recursos y la competencia necesarios, para definir una amenaza base de diseño en el caso del órgano regulador y para utilizar eficazmente la amenaza base de diseño a fin de diseñar sistemas y medidas de seguridad nuclear, en el caso del explotador. Sin embargo, si el Estado determina que es necesario el nivel de garantía correspondiente a una amenaza base de diseño, debería facilitar los recursos y la competencia requeridos.

6.6. Los Estados deberían considerar la posibilidad de basar sus requisitos de protección física para los materiales y las instalaciones nucleares en una amenaza base de diseño, específicamente en el caso de la retirada no autorizada de materiales nucleares de la categoría 1 y el sabotaje de materiales e instalaciones nucleares que podrían tener graves consecuencias radiológicas si el Estado está en posesión de dichos materiales o instalaciones [2]. Los Estados también deberían considerar la opción de formular una amenaza base de diseño para otros casos en los que determinen que las consecuencias de un acto doloso podrían ser graves.

6.7. Debería considerarse la posibilidad de formular una amenaza base de diseño para proteger los materiales nucleares u otros materiales radiactivos, una actividad conexa o una instalación conexa que podrían tener consecuencias menores en cualquiera de los siguientes casos:

a) la evaluación nacional de amenazas para la seguridad física nuclear indica la existencia de una amenaza con intención conocida de cometer un acto doloso;
b) la evaluación nacional de amenazas para la seguridad física nuclear señala una amenaza de gran capacidad cuya intención se desconoce;
c) en la evaluación nacional de amenazas para la seguridad física nuclear se tiene en cuenta un nivel demasiado alto de incertidumbre debido a la insuficiencia de los datos o de la confianza en las fuentes de los datos.

6.8. En el caso de las nuevas instalaciones, un Estado puede tener en cuenta las posibles ventajas a largo plazo de diseñar medidas de protección contra atributos y características de las amenazas más prudentes que los indicados en la evaluación nacional de amenazas para la seguridad física nuclear vigente a fin de reducir los posibles costos que comportaría añadir mejoras una vez puesta en servicio la instalación.

FORMULACIÓN DE UNA AMENAZA BASE DE DISEÑO

6.9. Una amenaza base de diseño debería formularse a partir de la evaluación nacional de amenazas para la seguridad física nuclear realizando las cinco tareas siguientes:

1) examen de la documentación de la evaluación nacional de amenazas para la seguridad física nuclear para determinar las amenazas pertinentes que obedezcan a la motivación, la intención y/o la capacidad de cometer un acto doloso;

2) compilación de los atributos y características de los adversarios;
3) ajuste de los atributos y características de los adversarios compilados para tener en cuenta factores de políticas;
4) adaptación de los atributos y características de los adversarios a instalaciones y actividades específicas, y
5) finalización y establecimiento de la amenaza base de diseño.

Examen de la documentación de la evaluación nacional de amenazas para la seguridad física nuclear

6.10. Deberían determinarse los blancos respecto de los cuales un acto doloso podría tener consecuencias radiológicas inaceptables, según la definición del Estado. A continuación, estos blancos deberían tenerse en cuenta en combinación con los atributos y características de los posibles adversarios descritos en la documentación de la evaluación nacional de amenazas para la seguridad física nuclear, con el fin de determinar las amenazas que son pertinentes para estos blancos y que, por lo tanto, podrían tener consecuencias radiológicas inaceptables. Para ello, deberían examinarse las motivaciones, intenciones y capacidades de los adversarios con respecto a estos blancos.

6.11. Deberían examinarse las descripciones de los adversarios que figuran en la documentación de la evaluación nacional de amenazas para la seguridad física nuclear a fin de determinar cuáles de ellos poseen las capacidades necesarias para cometer un acto doloso que pueda tener consecuencias radiológicas inaceptables. Si un determinado adversario no tiene capacidad suficiente para cometer un acto de ese tipo, puede excluirse del examen ulterior. Sin embargo, debería procederse con cautela al tomar esa decisión; en particular, no debería excluirse del examen ulterior una amenaza sobre la base de que el sistema de seguridad física nuclear del que dispone para proteger una instalación o actividad es suficiente para derrotar al adversario. Las medidas de seguridad física nuclear existentes no deberían tenerse en cuenta al valorar las capacidades de los adversarios durante la formulación de una amenaza base de diseño[6].

6.12. A continuación debería examinarse cada adversario cuya capacidad se considere suficiente para cometer un acto doloso que pueda tener consecuencias radiológicas inaceptables a fin de determinar si ese adversario también tiene

[6] Este es un supuesto deliberadamente prudente. Por ejemplo, un explotador podría eliminar *a posteriori* estas medidas de seguridad física nuclear si la amenaza base de diseño no incluye atributos y características de un adversario contra los cuales las medidas serían necesarias y eficaces.

suficiente motivación o intención para cometer dicho acto. Si se determina que no hay suficiente motivación ni intención, el adversario puede excluirse del examen ulterior. Sin embargo, debería procederse con cautela al plantear la exclusión de un adversario altamente capacitado únicamente porque se considere que carece de motivación o intención. Para decidir si excluirlo o no, debería determinarse si su motivación percibida es coherente con las posibles consecuencias de dicho acto doloso y si es suficiente el grado de confianza en los datos utilizados para evaluar su motivación e intención.

6.13. Deberían quedar bien documentadas las razones que llevaron a excluir del ulterior examen de la amenaza base de diseño a cualquier adversario descrito en la documentación de la evaluación nacional de amenazas para la seguridad física nuclear. Todo adversario excluido del examen debería volver a tenerse en cuenta si posteriormente se adquiere nueva información que afecte a las razones que llevaron a su exclusión.

6.14. Al final del proceso de examen, debería elaborarse una lista de todos los adversarios creíbles que tienen capacidad y podrían tener la motivación y la intención de cometer un acto doloso con posibles consecuencias radiológicas inaceptables.

Compilación de los atributos y características de los adversarios

6.15. Cada uno de los adversarios pertinentes identificados a partir de la documentación de la evaluación nacional de amenazas para la seguridad física nuclear debería asignarse a un tipo de adversario apropiado, y deberían formularse descripciones creíbles de cada tipo. Si bien es posible asignar a cada tipo de adversario una etiqueta ilustrativa que facilite la consulta (por ejemplo, “terroristas”, “delincuentes”, “extremistas”), los tipos de adversarios deberían definirse en función de sus atributos y características específicos. La amenaza que supone un tipo de adversario debería reflejar la gama completa de atributos y características de los distintos adversarios agrupados bajo el mismo tipo de adversario.

6.16. Deberían compilarse los atributos y características pertinentes asociados a un determinado tipo de adversario. Esta compilación no debería consistir sin más en una combinación de los atributos y características más extremos de los diferentes adversarios, sino en una combinación creíble que sería realista observar en un adversario.

Ajuste de los atributos y características compilados de los adversarios para tener en cuenta factores de políticas

6.17. Los atributos y características compilados de los adversarios deberían evaluarse teniendo en cuenta todos los factores de políticas pertinentes que se determinen. Ello podría llevar a realizar ajustes en los atributos y características compilados de los tipos de adversarios para permitir un nivel de seguridad física sostenible, y podría conllevar cambios en el nivel de las capacidades de los adversarios previstas.

6.18. Por ejemplo, pueden realizarse ajustes en los atributos y características compilados de los adversarios para incorporar el grado de prudencia deseado en la evaluación nacional de amenazas para la seguridad física nuclear. Estos ajustes pueden tener como objetivo compensar la incertidumbre y las diferentes interpretaciones de los datos utilizados en la evaluación nacional de amenazas para la seguridad física nuclear; garantizar la eficacia constante de los sistemas y medidas de seguridad física nuclear de los explotadores a medida que la amenaza evoluciona con el paso del tiempo, o incluir atributos y características de las amenazas sobre los que actualmente se tiene poca o ninguna información de los servicios de inteligencia, como enfoque prudente.

6.19. Asimismo, las consideraciones costo-beneficio también pueden dar lugar a ajustes en los atributos y características compilados de los adversarios, por ejemplo buscando el equilibrio entre el beneficio para la sociedad en relación con los blancos potenciales, las consecuencias para la sociedad de los actos dolosos contra esos blancos que prosperan y los costos para la sociedad de la reducción de los riesgos de esos actos mediante la aplicación de medidas de seguridad física nuclear adecuadas y los costos derivados de proteger otros activos que podrían tener consecuencias de gravedad similar (por ejemplo, explosivos, productos químicos, agentes biológicos) u otras infraestructuras críticas.

6.20. Puede también que sea necesario tener en cuenta otros factores de políticas, como el reparto de las responsabilidades en materia de seguridad física nuclear entre el Estado y los explotadores, la repercusión en la confianza del público de las decisiones relativas a la aceptación del riesgo, la contribución al bienestar público de los blancos potenciales (por ejemplo, las aplicaciones para las que se utiliza el material nuclear o el material radiactivo), la confianza de los Estados vecinos en la seguridad física nuclear de un Estado y las amenazas en los Estados vecinos.

6.21. Es probable que la prudencia y los demás factores de políticas aquí señalados den lugar a un aumento de los presuntos niveles de capacidad de los atributos

y características compilados de los adversarios en la amenaza base de diseño, mientras que las consideraciones costo-beneficio podrían disminuirlos.

Adaptación de los atributos y características de los adversarios a instalaciones y actividades específicas

6.22. Los atributos y características de los adversarios ampliamente representativos, ajustados en función de los factores de políticas, deberían adaptarse para tener en cuenta las características de instalaciones y actividades específicas. En el caso de las instalaciones, estas consideraciones pueden incluir la ubicación y la accesibilidad del emplazamiento, las características de diseño específicas de la instalación, las prácticas de funcionamiento de la instalación y todas las amenazas locales específicas. En el caso de las actividades, pueden incluir los procedimientos operativos, los modos y rutas de transporte y todas las amenazas específicas para determinados lugares o rutas.

Finalización y establecimiento de la amenaza base de diseño

6.23. Antes de utilizar una amenaza base de diseño en el marco regulador, deberían tenerse en cuenta las observaciones de otras autoridades competentes y de las partes afectadas. La decisión final sobre el contenido de una amenaza base de diseño y la responsabilidad general de este contenido deberían recaer en la autoridad competente designada por el Estado para dirigir el proceso de formulación.

6.24. En el apéndice figura una amenaza base de diseño modelo.

FORMULACIÓN DE UNA DECLARACIÓN DE AMENAZA REPRESENTATIVA

6.25. Como ocurre con una amenaza base de diseño, una declaración de amenaza representativa debería elaborarse a partir de la evaluación nacional de amenazas para la seguridad física nuclear. El proceso de formulación de una declaración de amenaza representativa sigue el método descrito en los párrafos 6.9 a 6.24 para una amenaza base de diseño, pero suele ser menos riguroso en cada paso, y es posible que en él participen menos organizaciones. Además, los atributos y características de los adversarios no están adaptados a una instalación o actividad específica.

6.26. El proceso de formulación de una declaración de amenaza representativa debería incluir las cuatro tareas siguientes:

1) examen de la documentación de la evaluación nacional de amenazas para la seguridad física nuclear para determinar las amenazas pertinentes que obedezcan a la motivación, la intención y/o la capacidad de cometer un acto doloso;
2) compilación de los atributos y características de los adversarios en grupos representativos del conjunto de atributos y características;
3) adaptación de los atributos y características representativos de los adversarios sobre la base de las consideraciones de política pertinentes, y
4) finalización y establecimiento de la declaración de amenaza representativa.

AMENAZAS DENTRO DE LA AMENAZA BASE DE DISEÑO Y AL MARGEN DE ESTA

6.27. Es probable que durante el proceso de evaluación nacional de amenazas para la seguridad física nuclear se detecte una gran variedad de capacidades de adversarios. Teniendo en cuenta las amenazas conocidas, reales y predominantes, el Estado deberá determinar un nivel de amenaza o de capacidad de los adversarios por encima del cual la responsabilidad de la respuesta recaiga en el Estado y no en el explotador, cuyas capacidades y/o recursos de protección y respuesta tal vez sean insuficientes para un nivel tan alto de capacidades y posibles consecuencias. Aun así, puede que el explotador contribuya a ayudar al Estado en la protección contra estas amenazas para la seguridad física nuclear o en la mitigación de sus consecuencias.

6.28. Por lo tanto, las amenazas base de diseño deberían basarse en adversarios que tengan capacidades inferiores a este umbral, lo que implica que no corresponde al explotador la responsabilidad principal de protección contra adversarios con capacidades superiores ni de respuesta a ellos. La responsabilidad de contrarrestar a los adversarios con capacidades superiores a este umbral recaerá principalmente en el Estado. Al determinar este umbral, el Estado deberá sopesar el costo, el impacto operacional y otras consideraciones.

7. USO DE LAS AMENAZAS BASE DE DISEÑO Y LAS DECLARACIONES DE AMENAZAS REPRESENTATIVAS

7.1. Como se describe en los párrafos 6.2 a 6.8, un Estado puede optar por utilizar un enfoque normativo basado en los resultados, un enfoque normativo prescriptivo o un enfoque combinado. En esta sección se analiza el uso de amenazas base de diseño y declaraciones de amenazas representativas en cada uno de estos enfoques normativos.

ENFOQUE NORMATIVO BASADO EN LOS RESULTADOS

7.2. En un enfoque normativo basado en los resultados, las amenazas base de diseño y los objetivos de seguridad física nuclear del Estado proporcionan la base para diseñar, aplicar y evaluar sistemas y medidas de seguridad física nuclear.

7.3. El proceso para utilizar las amenazas base de diseño en un enfoque normativo basado en los resultados incluye las siguientes tareas:

a) el órgano regulador debería difundir entre los explotadores las amenazas base de diseño;
b) cada explotador, en cooperación con el órgano regulador, debería definir escenarios de ataque creíbles a partir de las amenazas base de diseño proporcionadas;
c) cada explotador debería diseñar sistemas y medidas de seguridad física nuclear que sean eficaces contra los escenarios de ataque definidos para su instalación o actividad;
d) cada explotador debería describir su diseño del sistema de seguridad física nuclear en su plan de seguridad física y presentar este plan al órgano regulador para su aprobación, si fuera necesario;
e) el órgano regulador debería evaluar la eficacia del diseño del sistema de seguridad física nuclear de cada explotador sobre la base del plan de seguridad física presentado, y
f) una vez aprobado el plan de seguridad física, el explotador puede explotar su instalación o realizar su actividad.

7.4. Las organizaciones pertinentes de respuesta a emergencias, incluidos el órgano regulador y el explotador, deberían utilizar los resultados de la evaluación nacional de amenazas para la seguridad física nuclear en la evaluación del peligro para establecer disposiciones de emergencia adecuadas en materia de preparación y respuesta para casos de emergencia nuclear o radiológica desencadenada por un suceso relacionado con la seguridad física nuclear, así como para una respuesta a contingencias coordinada e integrada.

ENFOQUE NORMATIVO PRESCRIPTIVO

7.5. En un enfoque normativo prescriptivo, el órgano regulador debería utilizar las declaraciones de amenaza representativa apropiadas para cada categoría de materiales y cada tipo de instalación o actividad para elaborar requisitos normativos prescriptivos teniendo en cuenta los objetivos de seguridad física nuclear definidos por el Estado. Los requisitos normativos prescriptivos deberían especificar los sistemas y medidas de seguridad física nuclear que deben aplicarse para garantizar una protección suficiente para cumplir los objetivos del régimen de seguridad física nuclear del Estado. En las referencias [13 a 16] figuran orientaciones que podrían ayudar a los Estados a formular estos requisitos normativos prescriptivos.

7.6. El proceso para utilizar declaraciones de amenazas representativas como parte de un enfoque normativo prescriptivo incluye las siguientes tareas:

a) el órgano regulador debería definir escenarios de ataque creíbles basados en cada declaración de amenaza representativa y diseñar medidas de seguridad física nuclear para diferentes categorías de materiales y tipos de instalaciones y actividades;
b) el órgano regulador debería tener en cuenta las medidas recomendadas o sugeridas en las publicaciones del OIEA pertinentes, como las referencias [2, 3, 9, 13 a 16], según corresponda, y determinar si estas medidas son suficientes para cumplir los objetivos de seguridad física nuclear o si son necesarias medidas adicionales para proporcionar el nivel de protección requerido para la declaración de amenaza representativa pertinente;
c) el órgano regulador debería elaborar requisitos normativos prescriptivos para aplicar las medidas de seguridad física nuclear diseñadas,
d) los explotadores deberían aplicar las medidas de seguridad física nuclear prescritas por los requisitos normativos pertinentes.

ENFOQUE COMBINADO

7.7. Como se indicó en el párrafo 6.2 y en las referencias [13, 14], en un enfoque normativo combinado se utilizan elementos del enfoque prescriptivo y del enfoque basado en los resultados.

7.8. El Estado puede aplicar un enfoque basado en los resultados para las instalaciones y actividades en las que el beneficio supera el costo, por ejemplo, cuando es conveniente una mayor garantía debido a las posibles consecuencias que podrían derivarse de un suceso relacionado con la seguridad física nuclear. Podría aplicarse un enfoque prescriptivo a los materiales, las instalaciones conexas y las actividades conexas en los que un suceso relacionado con la seguridad física nuclear tendría posibles consecuencias de menor gravedad. El Estado también puede optar por abordar algunas amenazas con un enfoque basado en los resultados y otras con un enfoque prescriptivo.

ELABORACIÓN DE ESCENARIOS DE ATAQUE

7.9. Para elaborar escenarios de ataque es necesario comprender cómo los atributos y características de los adversarios podrían ser utilizados para llevar a cabo un acto doloso, así como si los diferentes adversarios podrían cooperar en la ejecución de dicho acto y cómo lo harían.

7.10. Un escenario de ataque es un conjunto postulado o supuesto de condiciones y sucesos, utilizado habitualmente con fines de análisis o evaluación para representar y luego modelizar posibles condiciones y sucesos futuros, como un posible suceso relacionado con la seguridad física nuclear. Un escenario de ataque puede representar o bien las condiciones en un determinado momento o durante un único suceso o bien un historial de condiciones o sucesos (incluidos procesos) a lo largo del tiempo que desencadenan un suceso relacionado con la seguridad física nuclear, o que se derivan de este, incluidos posibles efectos diferidos.

7.11. Los escenarios de ataque deberían definirse de tal forma que incluyan todas las combinaciones creíbles de atributos y características de los adversarios determinadas en una declaración de amenaza representativa o una amenaza base de diseño, incluida la connivencia entre adversarios internos y externos y combinaciones de ataques físicos y ciberataques. Los escenarios deberían definir a) las vías probables del adversario, b) los tiempos de penetración basados en las tácticas de ataque supuestas y los tiempos de dilación de las medidas de seguridad física e informática, y c) las probabilidades de detección basadas en

sensores y las medidas de vigilancia y las tácticas supuestas para sortear o frustrar dichas medidas.

7.12. En particular, deberían tenerse en cuenta los escenarios de ataque en que se emplean ciberataques. Aunque es muy poco probable que un ciberataque baste por sí solo para la retirada no autorizada de material, podría poner en peligro las medidas de seguridad física nuclear encaminadas a la disuasión, detección, dilación o respuesta frente a un intento de retirada no autorizada o de sabotaje. Un ciberataque también podría dar lugar a la degradación de la seguridad tecnológica, la seguridad física, la contabilidad y el control de los materiales nucleares o la preparación y respuesta para casos de emergencia en apoyo de dicho ataque.

7.13. Los factores que afectan a la viabilidad de un ataque pueden incluir su complejidad; la cantidad y sofisticación de los instrumentos y otros recursos necesarios; las aptitudes y capacidades de los adversarios; sus conocimientos de la instalación y de los puntos de acceso (incluidos conocimientos sobre los escondites para los adversarios o los instrumentos y conocimientos de las vulnerabilidades de los sistemas que pueden explotarse); el número total de adversarios externos; las capacidades de las fuerzas de respuesta; el número y la naturaleza de los agentes internos involucrados y su grado de connivencia, y la eficacia de las barreras físicas, las medidas de seguridad informática y la tecnología de detección y monitorización.

8. MANTENIMIENTO DE LA VIGENCIA Y EXAMEN DE LA EVALUACIÓN NACIONAL DE AMENAZAS PARA LA SEGURIDAD FÍSICA NUCLEAR Y SU DOCUMENTACIÓN Y DE LAS DECLARACIONES DE AMENAZAS

8.1. La documentación de la evaluación nacional de amenazas para la seguridad física nuclear debería examinarse periódicamente para valorar si la evaluación sigue ofreciendo una visión completa y equilibrada de las amenazas creíbles para la seguridad física nuclear en el Estado, y, si fuera necesario, esa evaluación debería revisarse.

8.2. Es posible que las amenazas base de diseño y las declaraciones de amenazas representativas tengan que examinarse (y, de ser preciso, revisarse), si se revisa

la documentación de la evaluación nacional de amenazas para la seguridad física nuclear o para reflejar cambios en los factores de políticas o tomar en consideración la experiencia adquirida en el diseño y evaluación de sistemas y medidas de seguridad física nuclear o en un suceso relacionado con la seguridad física nuclear.

8.3. El examen periódico de la evaluación nacional de amenazas para la seguridad física nuclear, las amenazas base de diseño y las declaraciones de amenazas representativas podría iniciarse, por ejemplo, cada 12 a 18 meses. El examen periódico debería seguir el mismo proceso utilizado para realizar la evaluación nacional de amenazas para la seguridad física nuclear.

8.4. Al examinar la evaluación nacional de amenazas para la seguridad física nuclear podrían tenerse en cuenta las amenazas y capacidades nuevas y cambiantes cuya relación directa con la seguridad física nuclear se desconozca, a fin de detectar su posible pertinencia para el material nuclear, otros materiales radiactivos y las instalaciones y actividades conexas.

8.5. Podrían darse otras situaciones diversas que obligaran a examinar la evaluación nacional de amenazas para la seguridad física nuclear, las amenazas base de diseño y las declaraciones de amenazas representativas al margen del proceso de examen periódico. Algunas de las condiciones o sucesos que podrían propiciar dicho examen son los siguientes:

a) Cualquier suceso o acto, dentro o fuera del Estado, esté o no directamente relacionado con materiales nucleares, otros materiales radiactivos o instalaciones o actividades conexas, que cambie significativamente la percepción o el nivel real de la amenaza para la seguridad física nuclear.
b) Cambios significativos en la política gubernamental, la legislación o los arreglos internacionales que afecten a la responsabilidad de las autoridades competentes o del explotador, como cambios en las disposiciones de respuesta o en las responsabilidades institucionales.
c) Cambios en las instalaciones o actividades relacionadas con material nuclear y otros materiales radiactivos que podrían comportar cambios o posibles consecuencias nuevas. Serían cambios de ese tipo la construcción de un tipo distinto de instalación, el uso de material más enriquecido, el uso de material en una nueva práctica, la repatriación de uranio muy enriquecido, cambios en la explotación para utilizar material de categoría inferior o mejoras en la seguridad tecnológica nuclear.
d) Una propuesta sometida al examen de una autoridad competente, una organización de apoyo técnico o científico o un explotador.

8.6. Un examen no hará necesariamente que se revisen la evaluación nacional de amenazas para la seguridad física nuclear, las amenazas base de diseño o las declaraciones de amenazas representativas. Sin embargo, si el examen muestra que la evaluación nacional de amenazas para la seguridad física nuclear no aborda adecuadamente todas las amenazas creíbles, incluidas las nuevas y emergentes, deberían revisarse tanto la evaluación nacional de amenazas para la seguridad física nuclear como su documentación, con la participación de todas las organizaciones pertinentes. Si se producen cambios sustanciales y fundamentales en la evaluación nacional de amenazas para la seguridad física nuclear, también deberían revisarse las amenazas base de diseño y las declaraciones de amenazas representativas.

RESPUESTA A AMENAZAS NUEVAS Y EMERGENTES

8.7. Fuera del proceso de examen periódico podrían surgir situaciones en las que se demuestre o sospeche que los adversarios poseen capacidades físicas o informáticas nuevas o inesperadas lo suficientemente amenazantes como para exigir al Estado una acción inmediata. En canales oficiales y oficiosos podrían aparecer datos de inteligencia y sobre amenazas relativos a estos temas.

8.8. Además del proceso de formulación de amenazas base de diseño y declaraciones de amenazas representativas y de mantener su vigencia, el órgano regulador y otras autoridades competentes deberían establecer un proceso para que las autoridades competentes y los explotadores pertinentes intercambiaran información sobre las amenazas. Ello es especialmente necesario cuando el nivel de amenaza cambia rápidamente y no hay tiempo suficiente para revisar por completo la evaluación nacional de amenazas para la seguridad física nuclear.

8.9. Si un explotador recibe por canales oficiosos información sobre un cambio de este tipo en la amenaza, debería informar al órgano regulador y a otras autoridades competentes, según corresponda, para que puedan evaluar la credibilidad, la pertinencia y la gravedad del posible impacto de este cambio en la amenaza y determinar cómo, y con qué urgencia, deben responder el Estado y/o el explotador.

8.10. El establecimiento de un sistema de niveles de amenaza elevada predeterminados y los correspondientes conjuntos predeterminados de medidas de seguridad física nuclear adicionales que habrán de aplicar los explotadores en cada nivel de amenaza elevada puede proporcionar protección adicional en tales situaciones.

Apéndice

MODELO DE AMENAZA BASE DE DISEÑO

A.1. El cuadro 1 ofrece un ejemplo de cómo podrían reflejarse los atributos y características del adversario en una amenaza base de diseño.

A.2. Para las declaraciones de amenazas representativas, por lo general menos detallado, se podría utilizar un formato similar o un formato menos formal.

CUADRO 1. EJEMPLO DE LISTA DE ATRIBUTOS Y CARACTERÍSTICAS DEL ADVERSARIO PARA UNA AMENAZA BASE DE DISEÑO

	Armado	Desarmado
Acción		
Robo[a]	Insertar *sí* o *no*	Insertar *sí* o *no*
Sabotaje[b]	Insertar *sí* o *no*	Insertar *sí* o *no*
Atributos y características comunes		
Número	Insertar un número	Insertar un número
Nivel de financiación	Insertar *bajo* o *alto*	Insertar *bajo* o *alto*
Apoyo de agentes internos	Insertar *activo* o *pasivo* y *violento* o *no violento*	Insertar *activo* o *pasivo* y *violento* o *no violento*
Tácticas	Insertar *ocultación* y/o *fuerza*	Insertar *ocultación* y/o *fuerza*
Aptitudes de planificación	Insertar *capacidad de planificar una desviación*, y/o *adversarios que atacan simultáneamente en grupos más pequeños*, y/o *conocimiento de la distribución de las instalaciones* y/o *capacidad de planificar un ataque combinado*	Insertar *capacidad de planificar una desviación*, y/o *adversarios que atacan simultáneamente en grupos más pequeños*, y/o *conocimiento de la distribución de las instalaciones* y/o *capacidad de planificar un ataque combinado*
Atributos y características físicas		
Disposición a matar	Insertar *sí* o *no*	Insertar *sí* o *no*
Disposición a morir	Insertar *sí* o *no*	Insertar *sí* o *no*
Vía	Insertar *aérea*, *por carretera*, *por ferrocarril*, *acuática* y/o *subterránea*	Insertar *aérea*, *por carretera*, *por ferrocarril*, *acuática* y/o *subterránea*

CUADRO 1. EJEMPLO DE LISTA DE ATRIBUTOS Y CARACTERÍSTICAS DEL ADVERSARIO PARA UNA AMENAZA BASE DE DISEÑO (cont.)

	Armado	Desarmado
Tipo de armas	Insertar *armas automáticas*, *armas semiautomáticas*, *armas cortas* y/o *cuchillos*	No se aplica
Explosivos	Insertar el tipo y la cantidad de explosivos	No se aplica
Herramientas	Insertar *herramientas eléctricas*, *herramientas manuales* y/o *herramientas disponibles en el lugar*	Insertar *herramientas eléctricas*, *herramientas manuales* y/o *herramientas disponibles en el lugar*
Aptitudes técnicas	Insertar *apertura de brechas con explosivos sofisticados*, *inutilización de las líneas de comunicación* y/o *manejo de equipo presente en las instalaciones*	Insertar *apertura de brechas con explosivos sofisticados*, *inutilización de las líneas de comunicación* y/o *manejo de equipo presente en las instalaciones*
Ayuda de agentes internos	Insertar *autorización de acceso*, *guardia de seguridad*, *mantenimiento técnico de equipos* y/o *manipulador de materiales*	Insertar *autorización de acceso*, *guardia de seguridad*, *mantenimiento técnico de equipos* y/o *manipulador de materiales*
Atributos y características cibernéticos		
Herramientas informáticas	Insertar *programas informáticos estándar*, *programas maliciosos* y/o *programas de desarrollo propio*	Insertar *programas informáticos estándar*, *programas maliciosos* y/o *programas de desarrollo propio*

CUADRO 1. EJEMPLO DE LISTA DE ATRIBUTOS Y CARACTERÍSTICAS DEL ADVERSARIO PARA UNA AMENAZA BASE DE DISEÑO (cont.)

	Armado	Desarmado
Conocimientos especializados	Insertar *ingeniería social*, *uso de herramientas comerciales*, *desarrollo de nuevas herramientas informáticas, dominio de oficina*, *dominio sobre el control de procesos* y/o *conocimientos sobre el sistema de TI aplicado*	Insertar *ingeniería social*, *uso de herramientas comerciales*, *desarrollo de nuevas herramientas informáticas, dominio de oficina*, *dominio sobre el control de procesos* y/o *conocimientos sobre el sistema de TI aplicado*
Herramientas de equipo informático	Insertar *ordenador*, *teléfono móvil*, cableado y/o *enrutadores*	Insertar *ordenador*, *teléfono móvil*, cableado y/o *enrutadores*
Capacidad de influir en la cadena de suministro	Insertar *sí* o *no*	Insertar *sí* o *no*
Persistencia del adversario	Insertar *capacidad de ataque a largo plazo* y/o *repetido*	Insertar *capacidad de ataque a largo plazo* y/o *repetido*
Ayuda de agentes internos	Insertar *autorización de acceso*, *control de los procesos por un usuario normal*, *el administrador y/o el proveedor de terceros en los sistemas de I y C*	Insertar *autorización de acceso*, *control de los procesos por un usuario normal*, *el administrador y/o el proveedor de terceros en los sistemas de I y C*

Nota: I y C: instrumentación y control; TI: tecnología de la información.

[a] Podrían añadirse criterios sobre la cantidad de material retirado y/o el robo puntual o prolongado.

[b] Podrían añadirse criterios sobre las consecuencias radiológicas.

REFERENCIAS

[1] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Objetivo y elementos esenciales del régimen de seguridad física nuclear de un Estado*, *Colección de Seguridad Física Nuclear del OIEA* Nº 20, OIEA, Viena, 2014.

[2] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Recomendaciones de seguridad física nuclear sobre la protección física de los materiales y las instalaciones nucleares* (INFCIRC/225/Revision 5), *Colección de Seguridad Física Nuclear del OIEA* Nº 13, OIEA, Viena, 2012.

[3] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Recomendaciones de seguridad física nuclear sobre materiales radiactivos e instalaciones conexas*, *Colección de Seguridad Física Nuclear del OIEA* Nº 14, OIEA, Viena, 2012.

[4] INSTITUTO INTERREGIONAL DE LAS NACIONES UNIDAS PARA INVESTIGACIONES SOBRE LA DELINCUENCIA Y LA JUSTICIA, OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO, OFICINA EUROPEA DE POLICÍA, ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL, ORGANIZACIÓN INTERNACIONAL DE POLICÍA CRIMINAL-INTERPOL, ORGANIZACIÓN MUNDIAL DE ADUANAS, *Recomendaciones de seguridad física nuclear sobre materiales nucleares y otros materiales radiactivos no sometidos a control reglamentario*, *Colección de Seguridad Física Nuclear del OIEA* Nº 15, OIEA, Viena, 2012.

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security for Nuclear Security, IAEA Nuclear Security Series No. 42-G, IAEA, Vienna (2021).

[6] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA Y LA ORGANIZACIÓN INTERNACIONAL DE POLICÍA CRIMINAL-INTERPOL, *Enfoque basado en el conocimiento de los riesgos en materia de medidas de seguridad física nuclear para los materiales nucleares y otros materiales radiactivos no sometidos a control reglamentario*, *Colección de Seguridad Física Nuclear del OIEA* Nº 24-G, OIEA, Viena, 2022.

[7] *Convención sobre la Protección Física de los Materiales Nucleares*, INFCIRC/274/Rev.1, OIEA, Viena, 1980.

[8] *Enmienda de la Convención sobre la Protección Física de los Materiales Nucleares*, INFCIRC/274/Rev.1/Mod.1, OIEA, Viena, 2016.

[9] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Medidas de prevención y de protección contra las amenazas de agentes internos*, *Colección de Seguridad Física Nuclear del OIEA* Nº 8-G (Rev. 1), OIEA, Viena, 2022.

[10] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Seguridad física de la información nuclear*, *Colección de Seguridad Física Nuclear del OIEA* Nº 23-G, OIEA, Viena, 2018.

[11] AGENCIA PARA LA ENERGÍA NUCLEAR DE LA OCDE, COMISIÓN PREPARATORIA DE LA ORGANIZACIÓN DEL TRATADO DE PROHIBICIÓN COMPLETA DE LOS ENSAYOS NUCLEARES, OFICINA DE COORDINACIÓN DE ASUNTOS HUMANITARIOS DE LAS NACIONES UNIDAS, ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL, ORGANIZACIÓN DE LAS NACIONES UNIDAS PARA LA ALIMENTACIÓN Y LA AGRICULTURA, ORGANIZACIÓN INTERNACIONAL DE POLICÍA CRIMINAL (INTERPOL), ORGANIZACIÓN INTERNACIONAL DEL TRABAJO, ORGANIZACIÓN MARÍTIMA INTERNACIONAL, ORGANIZACIÓN METEOROLÓGICA MUNDIAL, ORGANIZACIÓN MUNDIAL DE LA SALUD, ORGANIZACIÓN PANAMERICANA DE LA SALUD, PROGRAMA DE LAS NACIONES UNIDAS PARA EL MEDIO AMBIENTE, *Preparación y respuesta para casos de emergencia nuclear o radiológica, Colección de Normas de Seguridad del OIEA* Nº GSR Part 7, OIEA, Viena, 2018.

[12] OFICINA DE COORDINACIÓN DE ASUNTOS HUMANITARIOS DE LAS NACIONES UNIDAS, OFICINA INTERNACIONAL DEL TRABAJO, ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, ORGANIZACIÓN DE LAS NACIONES UNIDAS PARA LA ALIMENTACIÓN Y LA AGRICULTURA, ORGANIZACIÓN MUNDIAL DE LA SALUD, ORGANIZACIÓN PANAMERICANA DE LA SALUD, *Disposiciones de preparación para emergencias nucleares o radiológicas*, *Colección de Normas de Seguridad del OIEA* Nº GS-G-2.1, OIEA, Viena, 2010.

[13] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Protección física de los materiales y las instalaciones nucleares (aplicación del documento INFCIRC/225/Rev. 5)*, *Colección de Seguridad Física Nuclear del OIEA* Nº 27-G, OIEA, Viena, 2019.

[14] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Seguridad física de los materiales radiactivos durante su uso y almacenamiento y de las instalaciones conexas*, *Colección de Seguridad Física Nuclear del OIEA* Nº 11-G (Rev. 1), OIEA, Viena, 2022.

[15] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *La seguridad física de los materiales radiactivos durante su transporte*, *Colección de Seguridad Física Nuclear del OIEA* Nº 9-G (Rev. 1), OIEA, Viena, 2022.

[16] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Seguridad física de los materiales nucleares durante el transporte*, *Colección de Seguridad Física Nuclear del OIEA* Nº 26-G, OIEA, Viena, 2021.

GLOSARIO

amenaza base de diseño. Atributos y características de posibles adversarios internos y/o externos que podrían iniciar una retirada no autorizada o actos de sabotaje que se toman como base para el diseño y la evaluación de un sistema de protección física.

declaración de amenaza representativa. Atributos y características de posibles adversarios internos y/o externos que podrían iniciar una retirada no autorizada o actos de sabotaje con miras a utilizarlos para formular requisitos prescriptivos para la protección de los materiales y/o las instalaciones definidos.

evaluación de la amenaza. Evaluación de las amenazas —basada en la información disponible de los servicios de inteligencia, las fuerzas del orden y fuentes de libre acceso— que describe las motivaciones, intenciones y capacidades de esas amenazas.

declaración de amenaza. Descripción de los adversarios creíbles (incluidos atributos y características) en forma de amenaza base de diseño o declaración de amenaza representativa elaborada a partir de la evaluación nacional de amenazas para la seguridad física nuclear.

PEDIDOS DE PUBLICACIONES

Las publicaciones de pago del OIEA pueden adquirirse a través de los proveedores que se indican a continuación o en las principales librerías locales.

Los pedidos de publicaciones gratuitas deben hacerse directamente al OIEA. Al final de la lista de proveedores se proporcionan los datos de contacto.

AMÉRICA DEL NORTE

Bernan / Rowman & Littlefield
15250 NBN Way, Blue Ridge Summit, PA 17214, EE. UU.
Teléfono: +1 800 462 6420 • Fax: +1 800 338 4550
Correo electrónico: orders@rowman.com • Sitio web: www.rowman.com/bernan

Renouf Publishing Co. Ltd
22-1010 Polytek Street, Ottawa, ON K1J 9J1, CANADÁ
Teléfono: +1 613 745 2665 • Fax: +1 613 745 7660
Correo electrónico: order@renoufbooks.com • Sitio web: www.renoufbooks.com

RESTO DEL MUNDO

Póngase en contacto con su proveedor local de preferencia o con nuestro distribuidor principal:

Eurospan Group
Gray's Inn House
127 Clerkenwell Road
Londres EC1R 5DB
Reino Unido

Pedidos comerciales y consultas:
Teléfono: +44 (0)176 760 4972 • Fax: +44 (0)176 760 1640
Correo electrónico: eurospan@turpin-distribution.com

Pedidos individuales:
www.eurospanbookstore.com/iaea

Para más información:
Teléfono: +44 (0)207 240 0856 • Fax: +44 (0)207 379 0609
Correo electrónico: info@eurospangroup.com • Sitio web: www.eurospangroup.com

Los pedidos de publicaciones, tanto de pago como gratuitas, pueden enviarse directamente a:

Dependencia de Mercadotecnia y Venta
Organismo Internacional de Energía Atómica
Vienna International Centre, PO Box 100, 1400 Viena, Austria
Teléfono: +43 1 2600 22529 o 22530 • Fax: +43 1 26007 22529
Correo electrónico: sales.publications@iaea.org • Sitio web: https://www.iaea.org/es/publicaciones

La presente publicación proporciona una metodología paso a paso para realizar una evaluación nacional de amenazas para la seguridad física nuclear que comprenda aspectos de seguridad física e informática y para formular, usar y mantener amenazas base de diseño y declaraciones de amenazas representativas. Va dirigida a los Estados, las autoridades competentes (incluido el órgano regulador), las organizaciones de apoyo técnico y científico pertinentes y los explotadores de instalaciones y actividades relacionadas con materiales nucleares y otros materiales radiactivos, incluidos los remitentes y los transportistas.

ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA
VIENA