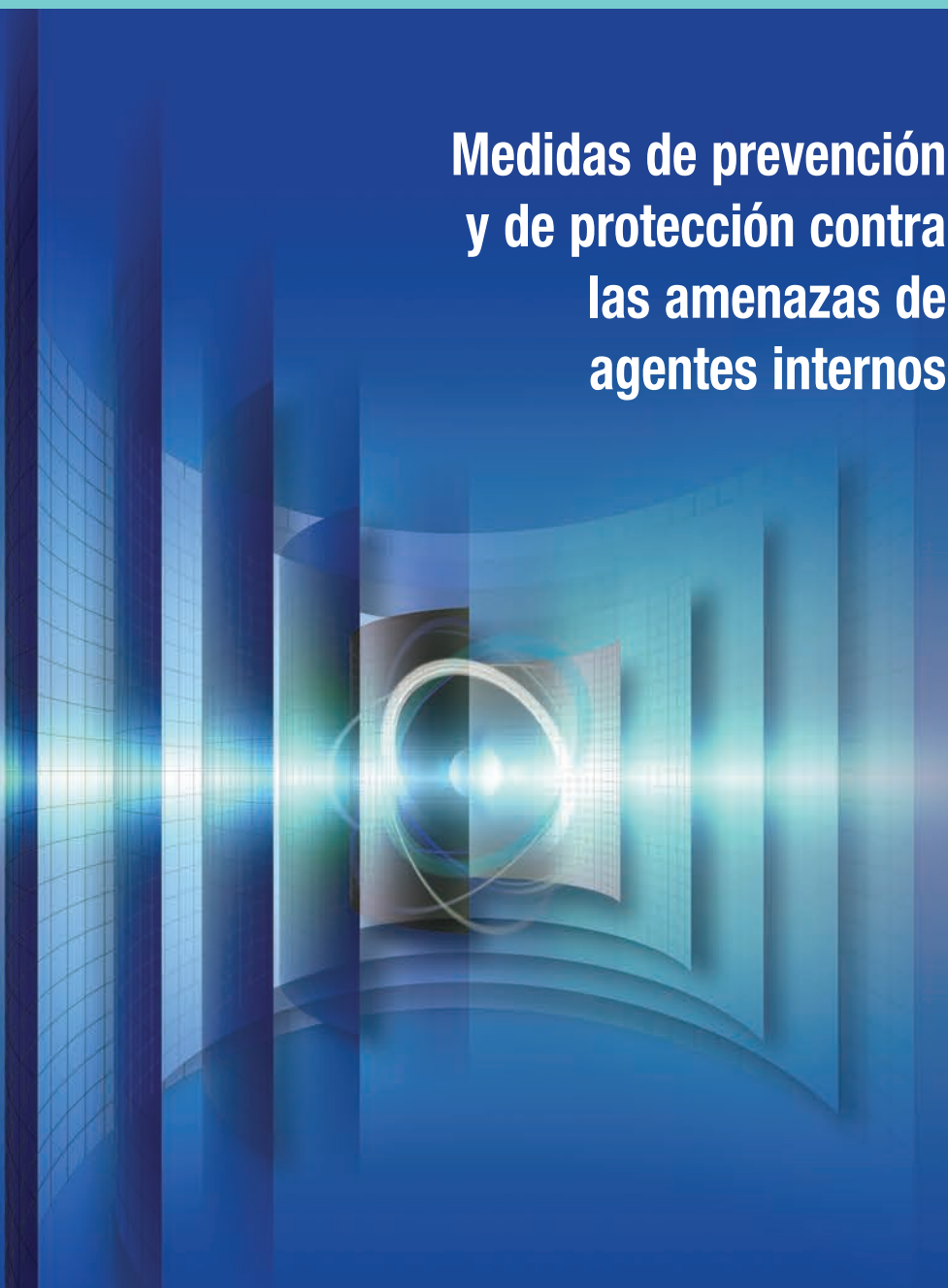
Colección de Seguridad Física Nuclear del OIEA N° 8-G (Rev. 1)

Guía de aplicación

Medidas de prevención y de protección contra las amenazas de agentes internos



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.

MEDIDAS DE PREVENCIÓN Y DE PROTECCIÓN CONTRA LAS AMENAZAS DE AGENTES INTERNOS

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

AFGANISTÁN
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
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
TRINIDAD Y TABAGO
TÚNEZ
TURKMENISTÁN
TURQUÍA
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 8-G (Rev. 1)

MEDIDAS DE PREVENCIÓN Y DE PROTECCIÓN CONTRA LAS AMENAZAS DE AGENTES INTERNOS

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
Febrero de 2022
STI/PUB/1858

MEDIDAS DE PREVENCIÓN Y DE PROTECCIÓN CONTRA LAS AMENAZAS DE AGENTES INTERNOS
OIEA, VIENA, 2022
STI/PUB/1858
ISBN 978–92–0–314621–0 (papel) | ISBN 978–92–0–314721–7 (PDF) | 978–92–0–308822–0 (EPUB)
ISSN 2521–1803

PRÓLOGO

El principal objetivo que asigna al OIEA su Estatuto es el de "acelerar y aumentar la contribución de la energía atómica a la paz, la salud y la prosperidad en el mundo entero". Nuestra labor supone a un tiempo prevenir la propagación de las armas nucleares y asegurar que la tecnología nuclear esté disponible con fines pacíficos en ámbitos como la salud o la agricultura. Es esencial que todos los materiales nucleares y otros materiales radiactivos, así como las instalaciones que los albergan, sean gestionados en condiciones de seguridad y estén debidamente protegidos contra todo acto delictivo o acto no autorizado intencional.

Aunque la seguridad física nuclear es una responsabilidad que incumbe a cada Estado, la cooperación internacional es básica para ayudar a los Estados a implantar y mantener regímenes eficaces de seguridad física nuclear. La función central que desempeña el OIEA para facilitar esta cooperación y prestar asistencia a los Estados goza de gran predicamento, fiel exponente de la amplitud de su composición, su mandato, sus singulares conocimientos técnicos y su dilatado historial de prestación de asistencia técnica a los Estados y asesoramiento especializado y práctico.

Desde 2006, el OIEA viene publicando obras de la *Colección de Seguridad Física Nuclear* para ayudar a los Estados a instituir regímenes nacionales eficaces de seguridad física nuclear. Estas publicaciones son un complemento de los instrumentos jurídicos internacionales existentes en la materia, 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 o el Código de Conducta sobre la Seguridad Tecnológica y Física de las Fuentes Radiactivas.

En la elaboración de estas orientaciones participan activamente expertos de los Estados Miembros del OIEA, lo que garantiza que den cuenta de un sentir consensuado sobre las buenas prácticas en materia de seguridad física nuclear. El Comité de Orientación sobre Seguridad Física Nuclear del OIEA, establecido en marzo de 2012 e integrado por representantes de los Estados Miembros, examina y aprueba los borradores de las publicaciones de la *Colección de Seguridad Física Nuclear* a medida que se van elaborando.

El OIEA seguirá trabajando con sus Estados Miembros para que los beneficios derivados del uso pacífico de la tecnología nuclear se hagan realidad y deparen mayores cotas de salud, bienestar y prosperidad a las poblaciones del mundo entero.

NOTA EDITORIAL

Este informe no aborda cuestiones de responsabilidad, jurídica o de otra índole, por actos u omisiones por parte de persona alguna.

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.

ÍNDICE

1. INTRODUCCIÓN

ANTECEDENTES

1.1. La *Colección de Seguridad Física Nuclear del OIEA* proporciona orientación a los Estados para ayudarlos a aplicar, examinar y, si fuese preciso, reforzar un régimen de seguridad física nuclear nacional. La colección proporciona asimismo orientación a los Estados sobre el cumplimiento de sus obligaciones y compromisos con respecto a instrumentos internacionales vinculantes y no vinculantes. Las publicaciones de la subcategoría Nociones Fundamentales de Seguridad Física Nuclear (*Colección de Seguridad Física Nuclear del OIEA* Nº 20 [1]) establecen el objetivo y los elementos esenciales de todo el régimen de seguridad física nuclear. Las publicaciones de la subcategoría Recomendaciones indican a qué debería responder un régimen de seguridad física nuclear en la protección física de los materiales y las instalaciones nucleares [2], los materiales radiactivos e instalaciones conexas [3], y los materiales nucleares y otros materiales radiactivos no sometidos al control reglamentario [4]. Estas publicaciones, así como muchas otras de la *Colección de Seguridad Física Nuclear del OIEA* (referencias [5-12]), reconocen las particulares amenazas que podrían plantear los agentes internos, así como la necesidad de aplicar medidas específicas contra las amenazas de agentes internos y de evaluar esas medidas en consecuencia.

1.2. Esta publicación es una actualización de *Preventive and Protective Measures against Insider Threats* (*Colección de Seguridad Física Nuclear del OIEA* Nº 8), publicada por el OIEA en 2008[1]. La presente revisión se ha llevado a cabo para mejorar la armonización de esta guía de aplicación con las Nociones Fundamentales de Seguridad Física Nuclear y con las Recomendaciones publicadas después de 2008, para incluir remisiones a otras guías de aplicación pertinentes publicadas desde ese año y para añadir más detalles respecto a algunos temas sobre la base de la experiencia del OIEA y de los Estados Miembros en la utilización del volumen Nº 8 de la *Colección de Seguridad Física Nuclear del OIEA*.

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).

OBJETIVO

1.3. El objetivo de esta guía de aplicación es proporcionar una orientación actualizada a los Estados, sus autoridades competentes y explotadores[2], remitentes y transportistas sobre la selección, aplicación y evaluación de las medidas para hacer frente a las amenazas de agentes internos. En las amenazas contra las instalaciones nucleares pueden participar adversarios externos o internos, o ambos en connivencia (colaboración, con otro adversario interno o con un adversario externo, que tiene por objeto un propósito ilegal o doloso).

ALCANCE

1.4. Esta obra trata sobre la prevención de la retirada no autorizada de materiales nucleares y del sabotaje de materiales e instalaciones nucleares por parte de agentes internos, así como la protección ante ambos actos. La publicación es aplicable a todo tipo de instalación nuclear —en particular, centrales nucleares, reactores de investigación y otras instalaciones del ciclo del combustible nuclear (como pueden ser las plantas de enriquecimiento, las plantas de reprocesamiento, las plantas de fabricación de combustible o las instalaciones de almacenamiento)— ya sea en diseño, rediseño, construcción, puesta en servicio, explotación, parada o clausura.

1.5. Las orientaciones que contiene respecto a las amenazas de agentes internos también pueden aplicarse a la prevención y la protección contra la retirada no autorizada y el sabotaje de materiales radiactivos e instalaciones conexas [3]; a la seguridad física en el transporte de materiales nucleares y radiactivos [6, 13], y a la prevención y detección de materiales nucleares y otros materiales radiactivos no sometidos a control reglamentario, así como a la respuesta a ellos [4]. Asimismo, las orientaciones pueden aplicarse a la seguridad de la información sobre las instalaciones que posean u obtengan otras partes interesadas, incluida la autoridad competente [8].

1.6. A los efectos de esta publicación, el acceso de agentes internos a una instalación incluye el acceso físico a lugares y materiales; el acceso interno o

[2] El término "explotador" se utiliza para describir una entidad (persona u organización) autorizada a explotar una instalación nuclear o radiológica, o autorizada a utilizar, almacenar o transportar material nuclear y/o radioactivo. Esa entidad es titular, por lo general, de una licencia u otro documento de autorización expedido por una autoridad competente, o es contratista del titular de dicha autorización.

remoto autorizado a computadoras o redes, y el acceso a información de carácter estratégico sobre la instalación.

1.7. Aunque en esta publicación no se abordan consideraciones de seguridad, las medidas de prevención y de protección descritas deberían aplicarse de una forma equilibrada, que sea compatible con las consideraciones de seguridad y que tenga en cuenta la protección radiológica de los trabajadores. Las medidas de seguridad física y las de seguridad tecnológica deberían concebirse y aplicarse de forma integrada para generar sinergias entre estas dos esferas, y de tal manera que las medidas de seguridad física no comprometan la seguridad tecnológica ni las medidas de seguridad tecnológica comprometan la seguridad física [1].

ESTRUCTURA

1.8. Tras esta introducción, la publicación se articula en cuatro secciones. La sección 2 presenta las amenazas de agentes internos y las formas de clasificar a esos agentes. La sección 3 indica los blancos y los sistemas de las instalaciones que deben protegerse frente a actos dolosos de agentes internos. La sección 4 analiza la aplicación a nivel de la instalación de las medidas de prevención y de protección para hacer frente a las amenazas de agentes internos. La sección 5 trata la evaluación de las medidas que se examinan en la sección 4.

2. DETECCIÓN DE LAS AMENAZAS DE AGENTES INTERNOS

2.1. El término "adversario" se utiliza para describir a toda persona que realice o intente realizar un acto doloso. Un adversario puede ser un agente interno o externo.

2.2. El término "agente interno" se utiliza para describir a personas

> "con acceso autorizado a [los materiales nucleares,] las *instalaciones conexas* o *actividades conexas*, o a la *información de carácter estratégico* o *los recursos de información de carácter estratégico*, que podría[n] cometer, o facilitar la comisión de, actos delictivos o actos intencionales no autorizados que estén relacionados con *materiales nucleares*, *otros materiales radiactivos*, *instalaciones conexas* o *actividades conexas*, o

que vayan dirigidos contra ellos, u otros actos que el Estado determine que tienen un impacto negativo en la seguridad física nuclear" [1].

El término "adversario externo" se utiliza para describir a todo adversario que no sea un agente interno.

ATRIBUTOS DE LOS AGENTES INTERNOS

2.3. Los agentes internos poseen al menos uno de los siguientes atributos, que les proporcionan ventajas frente a los adversarios externos cuando intentan realizar actividades dolosas:

a) Acceso: los agentes internos tienen acceso autorizado a las zonas, los equipos y la información necesarios para realizar su trabajo. El acceso abarca el acceso físico a las instalaciones nucleares; a los materiales nucleares y a los sistemas, componentes y equipos conexos, y a los sistemas informáticos. También incluye el acceso informático remoto a una instalación, como, por ejemplo, el acceso a los sistemas y las redes informáticos que controlan los procesos, proporcionan seguridad, contienen información de carácter estratégico o contribuyen de algún otro modo a la seguridad física nuclear. El explotador no debería permitir el acceso remoto a los sistemas críticos, como son los sistemas relacionados con la seguridad.
b) Autoridad: los agentes internos tienen autorización para realizar operaciones en el marco de las funciones que se les han asignado y también pueden tener autoridad para dar instrucciones a otros empleados. Esta autoridad puede utilizarse para apoyar actos dolosos, entre ellos, actos físicos o informáticos, como la manipulación de archivos o de procesos digitales.
c) Conocimientos: los agentes internos pueden poseer conocimientos sobre la instalación, las actividades o los sistemas conexos, que pueden ir desde un conocimiento limitado hasta un conocimiento experto. Entre los conocimientos que pueden tener se incluyen los que podrían permitir a un agente interno eludir o frustrar los sistemas de protección física específicos y otros sistemas de la instalación que contribuyen a la seguridad física nuclear, como pueden ser los sistemas de seguridad y los de contabilidad y control de materiales nucleares (CCMN), los procedimientos operacionales y las capacidades de respuesta.

Estos atributos también pueden incluir el acceso a información de carácter estratégico o a recursos de información de carácter estratégico, o estar en posesión

de esa información, comprendida la relativa al transporte o la circulación de materiales nucleares [13].

2.4. Un agente interno puede no poseer los tres atributos a la vez, pero aun así podría tener la capacidad suficiente para llevar a cabo un acto doloso. Por ejemplo, un miembro del personal directivo de la oficina central puede tener un acceso físico limitado a una instalación, pero podría tener la autoridad de emitir una orden falsificada de entrega a un lugar externo. Los adversarios internos pueden utilizar una autoridad simulada o conocimientos para facilitar o promover la comisión de un acto doloso. Un adversario interno puede actuar de forma independiente o en connivencia con otro adversario interno o externo.

2.5. Debido a sus capacidades de acceso, autoridad y conocimientos, los agentes internos tienen la oportunidad de seleccionar el blanco más vulnerable y el mejor momento para intentar o realizar un acto doloso. A fin de maximizar la probabilidad de éxito, un adversario interno podría cometer un acto doloso a lo largo de un período de tiempo prolongado. Esta táctica podría consistir en a) la manipulación ilícita del equipo de protección física o el de seguridad para preparar un acto de sabotaje, b) la falsificación de registros para poder retirar sin autorización, de manera reiterada y sin ser detectado cantidades pequeñas de material nuclear de categoría inferior que tiene una protección menos sólida que la aplicada a material nuclear de categorías superiores, o c) la retirada sin autorización de material nuclear en cantidades inferiores a los umbrales de detección del sistema de mediciones. Los agentes internos pueden tener oportunidad de cometer un acto doloso cuando una instalación se encuentra en condiciones normales o anormales, por ejemplo durante períodos de mantenimiento, o durante el traslado del material nuclear, y pueden elegir el momento más favorable para hacerlo [14].

MOTIVACIONES DE LOS AGENTES INTERNOS

2.6. Los agentes internos pueden tener distintas motivaciones para promover actos dolosos, como dinero, convicciones, venganza, ego, coacción o una combinación de estos factores.

2.7. Un agente interno puede desarrollar de forma independiente una motivación suficiente para realizar un acto doloso, entre otras cosas, como resultado de un problema de salud mental. También puede ser reclutado por un adversario externo que busque explotar su acceso, autoridad o conocimientos. Se podría forzar a un agente interno a cometer un acto doloso mediante coacción (por ejemplo, chantaje).

2.8. Un agente interno podría ocupar cualquier posición dentro de una organización, desde el nivel más alto hasta el más bajo. Los agentes internos de todos los niveles pueden tener una motivación suficiente para realizar un acto doloso. El personal que no está empleado directamente por el explotador, el remitente o el transportista, pero que tiene de forma periódica un acceso autorizado a la instalación o a sus sistemas (por ejemplo, proveedores, primeros actuantes, contratistas, inspectores de órganos reguladores u otras autoridades competentes) también debería contemplarse como posible amenaza interna.

CATEGORÍAS DE AGENTES INTERNOS

2.9. Un agente interno involuntario es un agente interno sin la intención ni la motivación de cometer un acto doloso que es explotado por un adversario sin que dicho agente interno involuntario sea consciente de ello. Por ejemplo, en un ataque informático, un agente interno involuntario puede no ser consciente de que determinadas acciones (por ejemplo, hacer clic en un enlace doloso de un correo electrónico que se presenta fraudulentamente como si procediera de una fuente fiable) pueden proporcionar información o acceso autenticado a un adversario.

2.10. Un adversario interno es un agente interno que comete actividades dolosas siendo consciente de ello, con premeditación y motivación. Un adversario interno puede ser pasivo o activo, y un adversario interno activo puede ser violento o no violento. Esta categorización es útil con fines de evaluación, como puede ser para la elaboración de perfiles de adversarios en la evaluación de amenazas o la amenaza base de diseño (ABD), o cuando se crean escenarios para ensayar las medidas de seguridad física nuclear en el marco de un proceso de evaluación del sistema de seguridad física nuclear.

2.11. Un adversario interno pasivo ayuda a otro adversario proporcionándole información para que la utilice en la realización de un acto doloso. Un adversario interno pasivo no participaría en el acto doloso de ninguna otra manera y probablemente dejaría de participar si hubiera una probabilidad alta de ser descubierto.

2.12. Un adversario interno activo y no violento utiliza la ocultación o el engaño para facilitar o realizar un acto doloso y puede proporcionar información a otro adversario. Por ejemplo, un adversario interno activo y no violento puede intentar cometer un robo repentino o prolongado de material nuclear o puede ayudar a adversarios externos a realizar un acto doloso desactivando o ignorando las alarmas o abriendo las puertas. Es probable que un adversario interno activo y no

violento pusiera fin al acto doloso si existe una probabilidad alta de ser descubierto (esto es, este tipo de adversario interno podría arriesgarse a ser detectado pero no es probable que se arriesgase a ser descubierto).

2.13. Un adversario interno activo y violento es similar a un adversario interno activo y no violento, pero también está dispuesto a utilizar la fuerza física contra el personal para facilitar o cometer un acto doloso. En función de las circunstancias, un agente interno puede pasar de no violento a violento.

RECONOCIMIENTO DE POSIBLES AMENAZAS DE AGENTES INTERNOS

2.14. La orientación contenida en esta sección puede ser útil para que el explotador identifique posibles amenazas de agentes internos y debería utilizarse junto con otros procesos de reconocimiento de amenazas de agentes internos, como el desarrollo de escenarios plausibles en el marco de una evaluación del sistema de seguridad física nuclear.

2.15. La referencia [2] recomienda que "[l]as autoridades estatales competentes, utilizando diversas fuentes de información creíble, [definan] la *amenaza* y las capacidades conexas en forma de una *evaluación de amenazas* y, si procede, una *amenaza base de diseño*."[3] El Estado debería tener en cuenta los atributos, las motivaciones y las categorías de los agentes internos y describir toda amenaza de agentes internos que sea creíble en la evaluación nacional de amenazas o en la ABD.

2.16. Una evaluación de amenazas y riesgos también puede ayudar a determinar posibles amenazas de agentes internos. Además de la información general sobre las amenazas de agentes internos contenida en la evaluación nacional de amenazas o en la ABD, en la evaluación específica de la instalación debería tenerse en cuenta la información sobre las amenazas locales en el entorno de la zona en la que dicha instalación se encuentra. Esta información puede poner de manifiesto condiciones relevantes (por ejemplo, los niveles de delincuencia) o situaciones del exterior de la instalación (como puede ser la actitud general de la comunidad o la presencia de grupos hostiles organizados) que pueden ser favorables para los adversarios internos.

---

[3] La ABD se refiere a los "[a]tributos y características de posibles *agentes internos* y/o adversarios externos que podrían intentar una *retirada no autorizada* o *actos de sabotaje*, que se toman como base para el diseño y evaluación de un *sistema de protección física*" [2].

2.17. Las posibles amenazas de agentes internos también pueden determinarse especificando qué agentes internos tienen acceso autorizado remoto o *in situ* a los sistemas de la instalación a través de las redes informáticas. Los sistemas modernos de las instalaciones, incluidos los que contribuyen a la seguridad física nuclear, se basan en controles y redes informáticos. Estos sistemas deberían estar protegidos contra los ataques informáticos, como se describe en la referencia [7]. Debería tenerse en cuenta el personal con acceso a estos sistemas a la hora de determinar las amenazas de agentes internos.

3. DETERMINACIÓN DEL BLANCO

3.1. La determinación del blanco, como se describe en la referencia [15], precisa qué materiales y equipos requieren protección frente a adversarios. Los blancos pueden incluir materiales nucleares, y zonas, edificios, equipos, componentes, información, sistemas y funciones conexos. En las referencias [2-4, 8, 15, 16] se ofrece orientación sobre la determinación de blancos en relación con instalaciones y con materiales nucleares y radiactivos.

3.2. Los activos (por ejemplo, los sistemas de vigilancia, los pórticos detectores) que no se consideran blancos pero que son críticos para la protección de los blancos identificados también pueden requerir protección. Un adversario interno podría eludir o comprometer esos activos para cometer un acto doloso.

BLANCOS RELACIONADOS CON RETIRADAS NO AUTORIZADAS

3.3. Los materiales nucleares que pueden ser blancos de retiradas no autorizadas pueden asignarse a una de tres categorías (I-III) según su atractivo relativo y las características del material nuclear, así como las posibles consecuencias de su utilización en un dispositivo nuclear explosivo. Esta categorización se define en el cuadro 1 de la referencia [2]. Debería contemplarse también la retirada no autorizada de materiales nucleares o radiactivos para la construcción de un dispositivo de dispersión radiactiva [3]. Además de los materiales nucleares y otros materiales radiactivos, los blancos de un robo pueden incluir información de carácter estratégico y recursos de información de carácter estratégico.

3.4. La determinación de los blancos potenciales de una retirada no autorizada de material nuclear por parte de un adversario interno debería tener en cuenta la

posibilidad tanto de un robo repentino como de un robo prolongado. El "robo repentino" es la retirada no autorizada de un blanco o de una cantidad significativa de material nuclear en un solo acto. El "robo prolongado" es la sustracción reiterada y no autorizada de cantidades potencialmente pequeñas de material nuclear, ya sea de un solo lugar o de varios.

3.5. Un adversario interno podría recurrir al robo prolongado de material nuclear para pasar desapercibido, retirando repetidamente pequeñas cantidades de material por debajo de la cantidad mínima detectable por los sistemas de CCMN y de protección física. El robo prolongado puede ejecutarse retirando el material nuclear de la instalación con cada adquisición o acumulándolo en un lugar oculto para retirarlo de la instalación más adelante, posiblemente de manera repentina. En la determinación del blanco debería tenerse en cuenta la posibilidad de que un adversario interno pueda recopilar una cantidad de material nuclear equivalente a una categoría superior reuniendo cantidades suficientes de material nuclear de categoría inferior. Factores como el elemento químico, la forma física del material, el modo de uso, la cantidad que se utiliza durante el procesamiento y la cantidad almacenada también deberían abordarse en la determinación del blanco al sopesar si son posibles y creíbles los escenarios de robo prolongado. Asimismo, deberían formularse consideraciones similares para los escenarios de robo repentino.

BLANCOS DE ACTOS DE SABOTAJE

3.6. Los blancos de actos de sabotaje en una instalación se establecen analizando la posibilidad de que el inventario de material radiactivo y los desechos de la instalación, entre ellos, los materiales nucleares y las fuentes radiactivas [3], den lugar a consecuencias radiológicas inaceptables o elevadas. Las referencias [2, 15] ofrecen más detalles sobre las medidas de seguridad física nuclear que deberían adoptarse en la protección contra los actos de sabotaje y al realizar un análisis de los blancos de sabotaje.

3.7. La determinación de posibles combinaciones de acciones (escenarios) que un adversario interno podría llevar a cabo para deteriorar las estructuras, los sistemas y los componentes de las instalaciones y que podrían tener consecuencias radiológicas inaceptables o elevadas debería formar parte del proceso de determinación de blancos.

DETERMINACIÓN DE LOS SISTEMAS QUE CONTRIBUYEN A LA SEGURIDAD FÍSICA NUCLEAR

3.8. En los procesos de determinación de los blancos deberían tenerse en cuenta todos los sistemas que podrían requerir una protección adicional frente a las amenazas de agentes internos. Los sistemas de protección física, los sistemas de CCMN y los sistemas de control de la seguridad y los procesos deberían considerarse blancos potenciales de actos dolosos, en particular, los promovidos por un adversario interno.

3.9. Un adversario interno puede tener acceso autorizado a la instalación o a la información sobre esta, y podría atacar otras estructuras, sistemas o componentes para perpetrar indirectamente un ataque, enmascarar actos dolosos o ayudar a un adversario externo. Dependiendo de la instalación o de la operación, el adversario interno puede aprovechar los sistemas informáticos (por ejemplo, las redes de oficinas o las computadoras de comunicación podrían utilizarse para obtener información de carácter estratégico).

3.10. Si los sistemas informáticos de una instalación se ven comprometidos, ello podría afectar negativamente la seguridad tecnológica, la seguridad física de los materiales nucleares o la mitigación de accidentes. El explotador debería evaluar y proteger los sistemas informáticos que contengan información relacionada con la seguridad tecnológica o la seguridad física en función del riesgo y de las posibles consecuencias de la divulgación de esa información. Esta evaluación debería tener como objetivo determinar cuáles son los sistemas informáticos críticos que pueden ser más vulnerables a un acto doloso y cuya pérdida podría dar lugar a un suceso relacionado con la seguridad física nuclear.

3.11. El explotador debería sopesar la posibilidad de impartir capacitación adicional a los empleados y contratistas con acceso a los sistemas de carácter estratégico para aumentar la concienciación respecto de la seguridad física. Los adversarios externos pueden tomar como blancos a los agentes internos con acceso a una instalación, a la información de carácter estratégico y los recursos de información de carácter estratégico o a las redes de la instalación a fin de obtener ayuda para facilitar o camuflar actividades dolosas.

4. MEDIDAS CONTRA POSIBLES AMENAZAS DE AGENTES INTERNOS

4.1. Las medidas de seguridad física nuclear utilizadas en la protección contra las amenazas de agentes internos deberían incluir medidas tanto de prevención como de protección. El término "medidas de prevención" se refiere a las medidas utilizadas para reducir el número de posibles adversarios internos antes de que se les conceda el acceso, para reducir al mínimo las oportunidades de que un agente interno lleve a cabo un acto doloso si se le concede el acceso o para evitar que un posible adversario interno lleve a cabo un acto doloso. El término "medidas de protección" se refiere a las medidas utilizadas para detectar o demorar los actos dolosos, responder a ellos o mitigar sus consecuencias.

4.2. Las presentes orientaciones no comprenden todas las medidas que podrían utilizarse contra la amenaza de agentes internos. Sin embargo, el uso de medidas de prevención y de protección puede ayudar a contrarrestar las amenazas de agentes internos si la amenaza se define adecuadamente, el proceso de determinación del blanco es exhaustivo y las medidas se aplican y evalúan eficazmente.

4.3. Las autoridades competentes deberían recopilar la información relativa a las medidas utilizadas contra las amenazas de agentes internos y a los incidentes en los que intervienen adversarios internos en actos dolosos para analizar las tendencias, los puntos débiles y las buenas prácticas. Si procede, la información debería compartirse con los organismos internacionales autorizados para mejorar la comprensión del alcance y la naturaleza del reto de seguridad física que plantean los adversarios internos.

ENFOQUE GENERAL DE LA APLICACIÓN

4.4. Como se indica en la referencia [2], los requisitos de seguridad física nuclear deberían basarse en un enfoque graduado, teniendo en cuenta la evaluación de la amenaza en cada momento, el atractivo relativo y la naturaleza de los materiales, y las posibles consecuencias asociadas a la retirada no autorizada de material nuclear o a actos de sabotaje de materiales o instalaciones nucleares. En la referencia [15] se ofrecen orientaciones generales sobre la aplicación de un enfoque graduado para proteger los materiales y las instalaciones nucleares contra las amenazas internas y externas.

4.5. La aplicación de medidas de seguridad física nuclear para la protección frente a las amenazas de agentes internos implica la selección de una combinación de medidas de prevención y de protección[4] y su aplicación con un enfoque graduado. Es importante que las medidas seleccionadas se apliquen y se evalúen eficazmente para que tengan el efecto deseado. No todas las medidas son apropiadas para toda instalación u operación.

4.6. Deberían aplicarse capas de medidas de prevención y de protección siguiendo el concepto de la defensa en profundidad, de tal manera que los adversarios internos tengan que superar o eludir múltiples capas de medidas o de tecnologías para lograr sus objetivos. Estas capas pueden ser medidas administrativas (por ejemplo, procedimientos, instrucciones, normas de control del acceso o normas de confidencialidad), medidas técnicas o una combinación de ambas. Ambos tipos de medidas deberían integrar a personas y equipos.

4.7. El explotador debería preparar un plan de seguridad física como parte de su solicitud para obtener una licencia, como se describe en la referencia [2], y cerciorarse de que describe las medidas necesarias para hacer frente a las amenazas de agentes internos, entre ellas, las medidas para responder a las amenazas internas a la seguridad informática y de la información (por ejemplo, un ciberataque perpetrado por un adversario interno [7, 8]). El explotador debería tener en cuenta las amenazas de agentes internos durante el diseño, la evaluación, la aplicación y el mantenimiento de los sistemas de seguridad física nuclear a nivel de la instalación.

4.8. El plan de seguridad física debería definir cómo se aplican los sistemas de seguridad física nuclear en la instalación e indicar las medidas utilizadas para proteger los blancos determinados frente a las amenazas de agentes internos. El plan debería contener información sobre estas medidas. Por ejemplo, las medidas técnicas podrían incluir medidas de contención y vigilancia destinadas a detectar y demorar a un adversario interno, medidas para monitorizar y asegurar las redes y los dispositivos conexos, y medidas para hacer respetar el control del acceso. Las medidas administrativas podrían incluir procedimientos, instrucciones, sanciones administrativas, la regla de la actuación por pareja, normas de confidencialidad y comprobaciones administrativas, así como inspecciones planificadas, no planificadas o no anunciadas de la aplicación de las medidas de prevención y de protección. Las inspecciones deberían realizarlas el explotador o equipos independientes. El plan de seguridad física debería especificar cómo se evaluarán las medidas (véase la sección 5).

---

[4] Algunas medidas pueden tener efectos tanto de prevención como de protección.

4.9. Los sistemas de seguridad física de las instalaciones en funcionamiento quizás precisen una modernización para poder dar respuesta a amenazas internas cambiantes.

APLICACIÓN DE MEDIDAS CONTRA LAS AMENAZAS DE AGENTES INTERNOS

4.10. En la protección frente a las amenazas de agentes internos deberían utilizarse tanto medidas de prevención como medidas de protección. Las medidas de prevención pueden utilizarse de la siguiente manera:

a) para reducir posibles amenazas de agentes internos antes de permitir el acceso a las personas, descubriendo comportamientos o características no deseables que puedan dar indicios de una motivación;
b) para reducir aún más las potenciales amenazas de agentes internos después de que estos hayan obtenido acceso, descubriendo comportamientos o características no deseables que puedan dar indicios de una motivación, y
c) para reducir al mínimo las oportunidades de cometer actos dolosos limitando el acceso, la autoridad y los conocimientos de los agentes internos.

Las medidas de protección pueden utilizarse de la siguiente manera:

1) para detectar y demorar actos dolosos y darles respuesta, y
2) para mitigar o reducir al mínimo las consecuencias de un suceso relacionado con la seguridad física nuclear y, en su caso, localizar o recuperar el material.

En la figura 1 se muestra cómo se pueden utilizar estas medidas para hacer frente a las amenazas de los agentes internos.

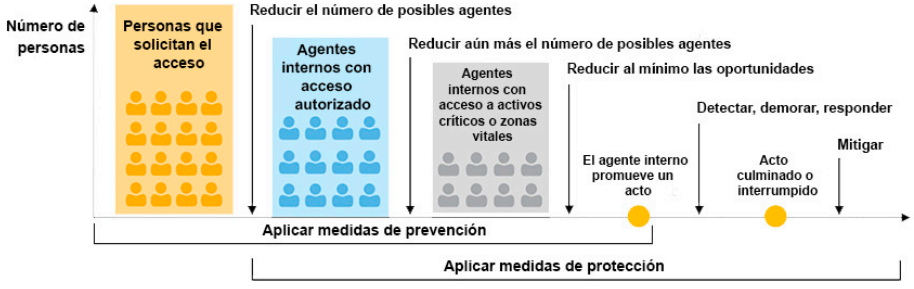


Fig. 1. Pasos en la utilización de las medidas de prevención y de protección frente a posibles amenazas de agentes internos.

4.11. Muchas de las medidas enumeradas en las dos secciones que figuran a continuación pueden considerarse tanto de prevención como de protección. En el proceso de selección y evaluación, debería contemplarse el valor potencial de cada medida propuesta tanto para la protección como para la prevención.

Aplicación de las medidas preventivas

4.12. El objetivo de las medidas de prevención es reducir el número de posibles amenazas de agentes internos y restringir al máximo las oportunidades de que estos cometan un acto doloso. Las medidas preventivas deberían aplicarse antes de la contratación, durante el período de servicio y en el momento del cese. Además, las medidas de prevención incluyen la garantía de la calidad y medidas específicas de seguridad informática. Los explotadores deberían aplicar las medidas preventivas descritas en esta sección.

Medidas que deberían aplicarse antes de la contratación

4.13. Se debería someter a las personas que soliciten un puesto de trabajo que requiera el acceso a una instalación a la verificación de su identidad y documentos personales, y a la evaluación de su probidad.

4.14. La verificación de la identidad se utiliza para confirmar que los datos personales de un individuo determinado son correctos y auténticos.

4.15. La verificación de los documentos personales se utiliza para comprobar la autenticidad de los detalles del historial profesional de un solicitante, su formación académica y la posesión del conjunto de aptitudes requeridas para la labor que deberá desempeñar. La verificación y validación de los documentos y las cualificaciones pueden realizarse poniéndose en contacto con los empleadores anteriores, las instituciones de enseñanza y las referencias.

4.16. Las evaluaciones de la probidad se utilizan como evaluación inicial (durante el proceso de contratación) y como evaluaciones continuas (regularmente a lo largo del período de servicio) de la integridad, honestidad y fiabilidad de una persona. En la referencia [2] se recomienda lo siguiente:

> "Teniendo en cuenta las leyes, los reglamentos o las políticas estatales sobre privacidad de la persona y requisitos laborales, el Estado debería definir la política de probidad destinada a determinar las circunstancias en que es necesario establecer la probidad y la manera en que se demuestra, utilizando para ello un *enfoque graduado*".

4.17. Las evaluaciones deberían examinar si la persona observa la ley y cumple las normas de la instalación, así como todo comportamiento o factor motivacional preocupante. Por ejemplo, la evaluación debería tratar de determinar si existen factores motivacionales, tales como problemas o presiones financieras (por ejemplo, deudas o recortes salariales), convicciones preocupantes, deseos de venganza (por ejemplo, que la persona perciba que se cometió una injusticia en su contra), dependencia física (como puede ser de drogas, alcohol o sexo), afecciones psicológicas o psiquiátricas, grave insatisfacción con la vida privada o profesional u otros factores que hagan que la persona sea susceptible a coacciones para cometer un acto doloso. Estos factores motivacionales pueden detectarse mediante un examen de información contenida en fuentes como los antecedentes penales, las referencias personales y profesionales, el historial profesional, los registros financieros, las redes sociales en línea y de otro tipo, las historias clínicas o los informes sobre el desempeño laboral, así como de la información sobre el comportamiento que hayan observado sus colegas.

4.18. La legislación nacional podría restringir, para un Estado, el alcance o la realización de la verificación de la identidad y de los documentos personales, así como la evaluación de la probidad.

Medidas que deberían aplicarse durante el servicio

4.19. Los agentes internos que hayan superado las comprobaciones previas a la contratación y hayan recibido autorización para acceder, entre otras cosas, a activos críticos, información de carácter estratégico y zonas vitales, deberían estar sujetos a las medidas descritas en los párrafos siguientes.

4.20. Deberían formularse y aplicarse procedimientos de escolta. Las personas que tengan acceso autorizado y a las que no se requiera llevar escolta para el acceso deberían escoltar a las zonas vitales o interiores a aquellas cuya probidad no se haya establecido o cuyas funciones no requieran una evaluación de probidad (por ejemplo, el personal temporal de reparación, el personal administrativo, el personal de mantenimiento, los trabajadores de la construcción o los visitantes). El escolta debería saber qué acciones han recibido aprobación, en particular, a qué zonas y sistemas puede acceder la persona escoltada y qué actividades está autorizada a realizar.

4.21. Durante la vigencia de su contrato, debería someterse regularmente a los agentes internos a revaluaciones de su probidad. Hay comportamientos y factores motivacionales preocupantes que pueden no haber sido evidentes con anterioridad o que pueden surgir con el tiempo. Por ejemplo, debería contemplarse la posibilidad

de realizar pruebas aleatorias para detectar el consumo de estupefacientes o alcohol durante un turno de trabajo, como forma de garantizar la fiabilidad de un trabajador. El alcance de las comprobaciones de la probidad debería graduarse en función del nivel de acceso y autoridad que el agente interno tenga sobre la instalación y sus activos. Por ejemplo, los agentes internos que se encargan de la administración de la red, que facilitan el acceso remoto a los recursos de información de carácter estratégico y que trabajan con materiales nucleares deberían someterse a controles de probidad más frecuentes y exhaustivos que quienes trabajan en recursos humanos.

4.22. Los empleados cuya evaluación de probidad se haya visto modificada por circunstancias personales podrían ver reducido temporalmente su nivel de acceso o podrían ser apartados de las responsabilidades de gestión hasta que sean evaluados de nuevo. Para conservar la probidad de los empleados, son de utilidad los programas de concienciación en materia de seguridad física, la satisfacción laboral y los incentivos a los empleados, que se comentan más adelante.

4.23. Debería preservarse la confidencialidad de la información de carácter estratégico para que solo puedan acceder a ella quienes necesiten conocerla. Obtener información sobre blancos sensibles o sobre procedimientos o medidas de seguridad física (por ejemplo, la ubicación del inventario de materiales nucleares o los planes y horarios de transporte) podría facilitar que los agentes internos lograsen cometer un acto doloso. Debería mantenerse un registro de las personas que acceden a la información de carácter estratégico en el que conste la fecha y la hora en que se accede a la información, y protegerlo para impedir las modificaciones. La información relativa a las posibles vulnerabilidades de los sistemas de seguridad física nuclear debería tener un nivel elevado de protección y compartimentarse (como se describe en el párrafo 4.30), ya que esta información podría facilitar ulteriormente una retirada no autorizada o un acto de sabotaje.

4.24. Debería controlarse el acceso a las instalaciones nucleares, los materiales nucleares, los sistemas de las instalaciones nucleares y la información de carácter estratégico. Debería establecerse y aplicarse un proceso documentado para la autorización y revocación de dicho acceso. Este proceso debería aplicarse a toda persona que requiera acceso remoto o *in situ* a una instalación o a sus operaciones, entre ellas, el transporte. Los datos personales podrían verificarse con documentos de identificación emitidos por las autoridades y datos biométricos (como puede ser el reconocimiento de la retina, de las huellas de la palma de la mano, de las huellas dactilares o el reconocimiento facial). El proceso debería regirse por normas estrictas de necesidad de saber y necesidad de acceder, según concrete la autoridad competente. Debería permitirse el acceso sin escolta únicamente a las

zonas a las que una persona necesite acceder para concluir el trabajo asignado. El número de personas con acceso autorizado a las zonas designadas debería mantenerse en el mínimo imprescindible.

4.25. El tratamiento o la circulación de materiales nucleares y otros materiales radiactivos debería autorizarse con antelación para reducir al mínimo las oportunidades de retirada no autorizada de materiales y detectar las actividades no autorizadas [6, 13]. Por ejemplo, el explotador de la instalación debería disponer de un procedimiento escrito en el que se especifique quién puede retirar los materiales nucleares de una cámara de almacenamiento para su uso en el tratamiento, cuándo se puede retirar y cómo se debería autorizar y registrar la retirada. Un calendario de actividades diario o semanal, coordinado y aprobado por el personal de operaciones, puede reducir las oportunidades de que el personal que normalmente realiza esas actividades pueda llevarlas a cabo sin autorización.

4.26. Las zonas físicas, las funciones, el tiempo y la información deberían compartimentarse de manera que sea poco probable que un agente interno tenga acceso, autoridad o conocimientos suficientes para llevar a cabo un acto doloso. La compartimentación aumenta el esfuerzo que necesitaría un agente interno para cometer un acto doloso y la probabilidad de que, para culminarlo, tenga que realizar actividades que van más allá de las que tiene autorizadas normalmente.

4.27. El explotador de la instalación debería tratar de garantizar que las zonas físicas estén compartimentadas de manera que un solo agente interno no tenga acceso a todos los sistemas, componentes y equipos con los que podría culminar un acto doloso. Debería limitarse el número de personas con acceso a toda zona que requiera protección. Para determinar qué personal tiene la necesidad de acceder a las zonas compartimentadas deberían definirse unas normas de aplicación a todas ellas. Estas normas deberían examinarse y modificarse cuando se cambien los procesos o las configuraciones dentro de la zona compartimentada. Además, debería limitarse estrictamente el número de personas a las que se permite el acceso a cada una de esas zonas. Deberían realizarse inspecciones y ensayos de funcionamiento para garantizar que en los procesos se observan las normas de acceso.

4.28. La segregación de tareas compartimenta las actividades laborales de los agentes internos para limitar la capacidad de cada uno de ellos de obtener el acceso autorizado, la autoridad o el conocimiento suficientes para llevar a cabo un acto doloso. La segregación de tareas incluye la aplicación del principio del mínimo privilegio a los sistemas informáticos, mediante el cual a un agente

interno se le asignan únicamente aquellos derechos de acceso que son esenciales para su trabajo.

4.29. El tiempo debería compartimentarse limitando el acceso autorizado para diferentes períodos de actividad de una instalación (por ejemplo, horas de trabajo, mantenimiento, paradas o condiciones no rutinarias). Concretamente, el acceso de un agente interno a una zona crítica debería limitarse a sus turnos.

4.30. La información debería compartimentarse dividiendo la almacenada tanto en papel como electrónicamente en fragmentos controlados por separado y utilizando medidas administrativas y técnicas para controlar el acceso a ella. El objetivo de la compartimentación de la información es evitar que los agentes internos reúnan toda la que fuese necesaria para intentar cometer un acto doloso. A la hora de compartimentar la información, deberían aplicarse las normas de necesidad de saber del personal para la información de carácter estratégico.

4.31. Deberían respetarse los procedimientos operacionales normalizados. Estos procedimientos son instrucciones escritas que rigen las tareas recurrentes de acuerdo con especificaciones aprobadas a fin de producir un resultado específico. Los procedimientos operacionales normalizados reducen la variación al mínimo y favorecen la garantía de calidad con la aplicación congruente de un proceso dentro de una organización, con independencia de los cambios de personal. Los procedimientos operacionales normalizados pueden ayudar a detectar, y por tanto a prevenir, los actos dolosos de un adversario interno, ya que proporcionan valores de referencia para actividades predeterminadas con los que detectar más fácilmente desviaciones del procedimiento que otros pueden cuestionar.

4.32. Debería elaborarse y aplicarse un programa de concienciación en materia de seguridad física para el personal y los contratistas. Dicho programa contribuye a la cultura de la seguridad física nuclear de la organización y puede ayudar a prevenir las amenazas de agentes internos si se integran en la cultura de seguridad física nuclear de la instalación los conocimientos sobre esas amenazas. Todo el personal, con independencia de su cargo o función, debería tener conocimiento de las amenazas y posibles consecuencias de los actos dolosos, y de lo que puede hacer para reducir el riesgo de que se produzcan. Los programas de concienciación en materia de seguridad física pueden reducir el riesgo de chantaje, coacción, extorsión y demás amenazas a los empleados y sus familias, y deberían instar a que se informe de las posibles intimidaciones al personal directivo de seguridad. Los programas de concienciación en materia de seguridad física deberían elaborarse de forma coordinada con los programas de concienciación en materia

de seguridad tecnológica para generar culturas de seguridad física y de seguridad tecnológica eficaces y complementarias.

4.33. El programa de concienciación sobre la seguridad física debería incluir políticas claras de seguridad física, medidas de aplicación de las prácticas en la materia y formación continua. El objetivo de esa formación es establecer un entorno en el que todos los empleados conozcan las políticas y los procedimientos de seguridad física, de modo que sean capaces de ayudar a detectar y notificar comportamientos sospechosos o erróneos, así como actos no autorizados. En la formación deberían incluirse métodos para evaluar los conocimientos de seguridad física y la eficacia de la formación en la materia, así como procesos para la mejora continua o el readiestramiento. Además de preparar al personal para la posibilidad de un incidente físico en la instalación o contra los activos de esta, la formación debería prepararlo para la posibilidad de un ciberataque.

4.34. Debería elaborarse y aplicarse un programa de aptitud para el trabajo. El personal directivo debería estar capacitado para advertir comportamientos preocupantes en un empleado y comunicarlos a la persona adecuada. Pueden contemplarse los programas de aptitud para el trabajo como medio para monitorizar la salud de los empleados de forma periódica. El explotador de las instalaciones también puede estudiar la posibilidad de ofrecer asistencia a los empleados que se encuentren en situaciones difíciles (como pueden ser situaciones financieras, médicas o psicológicas).

4.35. Deberían notificarse e investigarse los incidentes que susciten preocupación por la seguridad física (es decir, los incidentes que ocurran en una instalación y que entrañen infracciones o irregularidades relacionadas con las políticas, los procedimientos o los sistemas de seguridad física de la instalación). La notificación e investigación de dichos incidentes pueden ayudar a las instalaciones a formular medidas correctivas y a prevenir las amenazas de agentes internos. Un incidente puede ser causado por un agente interno como precursor de un acto doloso, ya sea para preparar el acto o para ensayar la respuesta de un sistema. La investigación minuciosa de estos incidentes podría servir para disuadir a los agentes internos y podría revelar qué personal pudiera ser un adversario interno.

4.36. Los empleados deberían disponer de buenas condiciones de trabajo, incentivos y reconocimiento. Las buenas condiciones de trabajo, los incentivos y el reconocimiento son ingredientes importantes para mantener y potenciar la moral y la lealtad de los empleados, lo que contribuye a una cultura de la seguridad física eficaz.

4.37. Los agentes internos deberían ser conscientes de que las contravenciones deliberadas de las instrucciones de trabajo, los reglamentos o las leyes serán penalizadas. La posibilidad de que se adopten medidas disciplinarias o se inicie un proceso judicial podría disuadir a los agentes internos de cometer actos dolosos. Además, exigir a los explotadores que informen a la autoridad competente de intentos de comisión o de conclusión efectiva de actos dolosos podría servir de base, tras una evaluación adecuada, para el intercambio de información entre explotadores, y para las modificaciones necesarias de los requisitos reglamentarios.

Medidas que deberían aplicarse en el momento del cese

4.38. El acceso y la autoridad de una persona, incluido el acceso a las computadoras, deberían anularse en el momento en que cese de su puesto, empleo o contrato. Deberían instaurarse procedimientos de cese que comprendan la revocación del acceso físico a las instalaciones; un acuerdo de no divulgación para proteger la información de carácter estratégico, y la modificación de las claves criptográficas, las contraseñas y los códigos de acceso.

Política y programas de garantía de calidad

4.39. La política de garantía de calidad de la instalación y sus programas de seguridad física nuclear deberían abordar las amenazas de los agentes internos, descritas en la evaluación de las amenazas o en la ABD. Como se indica en el párrafo 3.52 de la referencia [2]:

> "La política y los programas de garantía de calidad en materia de protección física deberían asegurar que el *sistema de protección física* sea diseñado, puesto en funcionamiento, explotado y mantenido en condiciones que le permitan responder eficazmente a la *evaluación de amenazas* o la *amenaza base de diseño*, y que cumpla los reglamentos del Estado, incluidos los requisitos de carácter preceptivo y/o los basados en el comportamiento".

4.40. En los programas de garantía de la calidad deberían contemplarse todos los sistemas de las instalaciones que contribuyen a la seguridad física nuclear a fin de garantizar una protección adecuada contra las amenazas de los agentes internos. La garantía de la calidad debería requerir la gestión de la configuración de los sistemas de seguridad física nuclear para cerciorarse de que siguen cumpliendo los criterios funcionales que se persiguen y para comprender las posibles consecuencias de los cambios que puedan realizarse en los sistemas, como pueden ser los que realice un agente interno.

Medidas para los sistemas informáticos

4.41. Si bien algunas medidas, como la necesidad de escolta, pueden ser eficaces para limitar el acceso de los agentes internos a los materiales nucleares y radiactivos, no proporcionan una protección suficiente contra las posibles amenazas de los agentes internos a los sistemas informáticos y de red; las medidas de seguridad física de la información pueden ofrecer esa protección [7, 8]. Por ejemplo, terceros y proveedores pueden tener acceso físico a información y activos de carácter estratégico en el emplazamiento durante el desarrollo y mantenimiento de los sistemas informáticos y de red. Aunque estos terceros y proveedores pueden querer mantener el acceso remoto durante todas las etapas del ciclo de vida de los sistemas informáticos y de red, dicho acceso debería concederse únicamente en aplicación de un enfoque basado en el conocimiento de los riesgos [1].

4.42. El explotador de la instalación debería definir y aplicar una política que trate el uso aceptable de los sistemas informáticos. Esta política puede definir el uso aprobado de los sistemas informáticos, describir las expectativas del empleador en la monitorización del uso aprobado de esos sistemas, proporcionar capacitación e indicar de forma explícita acciones prohibidas en los sistemas informáticos. El explotador de la instalación también debería contemplar el uso de medidas técnicas para hacer cumplir la política de sistemas o mejorarla. Por ejemplo, el explotador de la instalación podría definir una política de medios sociales e impartir capacitación informatizada sobre el uso de estos medios para reducir la probabilidad de que los adversarios utilicen a los empleados como agentes internos involuntarios.

Aplicación de medidas de protección

4.43. El objetivo de las medidas de protección contra las amenazas de agentes internos es detectar y demorar los actos dolosos, y responder a ellos, después de que se hayan iniciado, y puede incluir la mitigación de las consecuencias y la recuperación de materiales nucleares o radiactivos. Al diseñar y aplicar las medidas de protección, se debería procurar que estas respalden tanto las operaciones como la seguridad de las instalaciones, y que no tengan un efecto adverso en ellas. En caso de conflicto, en particular, con la seguridad tecnológica, debería alcanzarse una solución en la que el riesgo global para los trabajadores y la población se reduzca al mínimo y se mantenga una seguridad física nuclear suficiente.

4.44. Las medidas de protección contra las amenazas de los agentes internos deberían aplicarse utilizando un enfoque graduado para los blancos determinados. Además de la protección contra la retirada no autorizada, como se indica en el

párrafo 5.12 de la referencia [2]: "El *explotador* debería diseñar un *sistema de protección física* que sea eficaz contra los escenarios de *sabotaje* definidos y que ofrezca el nivel de protección exigido para la *instalación nuclear* y el *material nuclear*". Los escenarios de sabotaje deberían abarcar hipótesis de participación de uno o más adversarios internos. Las secciones siguientes abordan las medidas de protección contra las amenazas de los agentes internos que deberían contemplarse durante el diseño de un sistema de seguridad física nuclear.

Medidas de detección

4.45. La detección de los intentos de comisión de actos dolosos por adversarios externos se centra en detectar la penetración de cualquiera de las medidas de protección de una instalación. Por el contrario, en el caso de los agentes internos, estos podrían eludir o anular ciertas medidas de protección física y de CCMN gracias a su acceso autorizado, su autoridad y sus conocimientos. Los explotadores deberían aplicar múltiples y diversas medidas de protección para estos sistemas con el fin de detectar posibles actos dolosos realizados por agentes internos y ofrecer la información necesaria para su investigación y análisis. El explotador de la instalación debería investigar toda la información proporcionada por estas medidas de detección de manera exhaustiva. Al examinar en su conjunto señales que, por separado, parecen insignificantes, pueden revelarse indicios de un acto doloso.

4.46. Una investigación podría incluir el examen de las imágenes grabadas y de los datos de monitorización de la red, la verificación de los dispositivos de indicación de manipulación ilícita o de los datos de medición asociados a los materiales nucleares, la inspección de los registros de acceso o la realización de un inventario de emergencia. La investigación y el análisis del posible acto doloso debería encomendarse a personal cualificado. El tiempo necesario para concluir la investigación y el análisis tras la detección afecta directamente a la capacidad del explotador de la instalación para responder oportunamente a un acto doloso.

4.47. Las actividades sospechosas o no autorizadas deberían detectarse e investigarse porque pueden indicar que un acto doloso se encuentra en una fase exploratoria o preparatoria. Por ejemplo, un agente interno podría intentar sortear los procedimientos (entre otras cosas, introduciendo artículos prohibidos en una zona), tratar de acceder a una zona a la que no está autorizado (por ejemplo, entrando por una puerta de emergencia), activar una alarma para observar los tiempos y el carácter de la respuesta o intentar obtener información de carácter estratégico o que está sometida a la norma de necesidad de saber y a la que no se le ha concedido acceso.

4.48. Es preciso que las medidas de protección para detectar las amenazas internas estén diseñadas para determinar y evaluar correctamente los actos sospechosos o dolosos e informar de ellos. Las medidas de detección de las amenazas de agentes internos a nivel de la instalación suelen comprender medidas relacionadas con el control del acceso, el rastreo del personal, la detección de artículos prohibidos, la vigilancia, los sistemas de CCMN y la seguridad informática. En las siguientes secciones se analizan estos tipos de medidas.

Control del acceso

4.49. El explotador debería establecer y documentar normas y procedimientos estrictos de control del acceso para los materiales nucleares, el equipo utilizado para el tratamiento o la manipulación de los materiales nucleares y los datos sobre los materiales o sistemas nucleares pertinentes para la seguridad tecnológica o la seguridad física. La aplicación estricta de las normas y procedimientos de control del acceso reduce al mínimo el acceso de los agentes internos a los materiales, sistemas y equipos. Las normas y procedimientos de control del acceso también pueden actuar como elemento disuasorio debido a la posibilidad de detectar o descubrir a un agente interno que intenta acceder a material, equipos o datos para los que no está autorizado.

4.50. Las normas y procedimientos de control del acceso deberían ser aplicables a una variedad de circunstancias, entre ellas, la autorización del acceso a zonas con materiales nucleares y el control de materiales nucleares en condiciones rutinarias y no rutinarias, como pueden ser las situaciones de emergencia reales o simuladas. Por ejemplo, las normas de control del acceso podrían aplicarse al control y la distribución de las combinaciones de llaves y cerraduras en los sistemas manuales de control del acceso y a la impresión de pases, la inscripción de números de identificación personal, la recopilación de datos biométricos y el control de cerraduras en los sistemas electrónicos.

4.51. El explotador debería proteger del acceso no autorizado a) al equipo que genera los pases, b) al equipo de apoyo y los repuestos conexos y c) a los sistemas utilizados para conceder permisos de acceso. El explotador de la instalación debería aplicar controles estrictos al acceso al equipo de seguridad física o al equipo que contribuye a la seguridad física, la calibración y el mantenimiento. El explotador también debería instaurar procedimientos para garantizar que este equipo permanezca intacto. Por ejemplo, para garantizar que no ha sido manipulado, el personal autorizado debería someter el equipo a ensayos después de que se haya realizado el mantenimiento y antes de que el equipo entre nuevamente en servicio.

4.52. Deberían definirse normas de control del acceso para visitantes y acompañantes, y para condiciones anómalas, como la respuesta a emergencias y las paradas del sistema.

4.53. Antes de autorizar el acceso a toda zona cuyo acceso esté controlado, deberían verificarse criterios específicos, como la necesidad de saber del personal y la determinación de su probidad. La instauración de normas para el control del acceso debería coordinarse con las organizaciones de CCMN, operaciones, seguridad y protección física.

4.54. Todo acceso o intento de acceso a lugares físicos sensibles y sistemas informáticos con información de carácter estratégico deberían hacerse constar en los registros de control del acceso. Los actos dolosos cometidos por agentes internos pueden descubrirse al monitorizar o inspeccionar esos registros de control del acceso. Por ejemplo, las inspecciones de los registros de control del acceso pueden descubrir sucesos tales como un acceso no programado a la cámara de almacenamiento, todos los intentos fallidos de entrada con número de identificación personal, una autentificación biométrica fallida para una tarjeta de identificación autorizada u otros indicios de intentos de entrada por parte de personas no autorizadas. Una vez descubierta, la irregularidad o actividad sospechosa puede evaluarse como un posible acto doloso. Durante el diseño o la actualización del sistema deberían contemplarse las medidas de detección y los procedimientos conexos utilizados para monitorizar e inspeccionar los registros de control del acceso como medidas técnicas y administrativas para el control del acceso.

4.55. También deberían mantenerse registros del control del acceso de todas las personas que acceden a las zonas vitales o que pueden acceder o están en posesión de llaves, tarjetas de claves y demás credenciales de utilidad para acceder a otros sistemas, entre ellos, los sistemas informáticos que controlan el acceso a las zonas interiores, las zonas vitales y otras zonas con materiales nucleares [2].

4.56. Si se documentan adecuadamente, los registros de control del acceso pueden utilizarse durante la investigación de un acto doloso para acotar la lista de posibles sospechosos. Las solicitudes de acceso autorizado a las zonas o sistemas de seguridad física que guarden relación con la seguridad tecnológica o la seguridad física, ya sean aprobadas o denegadas, también deberían examinarse e inspeccionarse a fin de encontrar posibles actividades dolosas.

Rastreo del personal

4.57. El rastreo de los movimientos y la ubicación del personal dentro de una instalación permite al explotador detectar un intento de violación o una violación de las normas de control del acceso, como la salida de varias personas de la instalación utilizando una única tarjeta de control del acceso. La tecnología existente permite rastrear a las personas en tiempo real o *a posteriori*, registrando los lugares y las zonas que visitan cada día, junto con la hora y la duración correspondientes a cada visita.

4.58. Saber que una instalación tiene un sistema de rastreo puede disuadir a los agentes internos de llevar a cabo actividades no autorizadas. Además, los registros de rastreo y los de control del acceso pueden utilizarse durante la investigación de un acto doloso con fines de evaluación, o después de un incidente para generar una lista inicial de sospechosos.

Detección de artículos prohibidos

4.59. Como se recomienda en el párrafo 4.43 de la referencia [2]:

> "Al entrar tanto en la *zona protegida* como en la *zona interior*, los vehículos, personas y bultos deberían ser objeto de un registro para *detectar* y prevenir los accesos no autorizados y la introducción de artículos prohibidos. Los vehículos, personas y bultos que abandonen la *zona interior* deberían ser objeto de un registro para *detectar* y prevenir *retiradas no autorizadas*".

4.60. El explotador debería identificar y documentar los artículos prohibidos en las zonas limitadas, las zonas protegidas, las zonas interiores y las zonas vitales. Los artículos prohibidos pueden comprender herramientas y materiales no autorizados, como computadoras, teléfonos móviles, tabletas y otros medios o dispositivos de tecnología de la información con cámaras; material de blindaje contra la radiación; armas, o explosivos. Estos artículos podrían utilizarse para acceder o causar daños a sistemas o equipos sensibles, o a sus componentes, o para favorecer la retirada no autorizada o el sabotaje de materiales nucleares. Una instalación puede especificar otros artículos prohibidos para proteger, frente a adversarios internos, la información o sus sistemas de protección física, de CCMN, de seguridad y operacionales.

4.61. El explotador debería investigar inmediatamente la detección de artículos prohibidos que entren o salgan de una zona como un posible acto doloso cometido por un agente interno. Al prepararse para realizar un acto doloso, un adversario

interno podría poner a prueba el sistema de detección de artículos prohibidos para comprobar la sensibilidad de los detectores o la solidez de los procedimientos de evaluación. Deberían indicarse, evaluarse, notificarse e investigarse las detecciones sospechosas o repetidas de artículos prohibidos.

4.62. Las medidas para la detección de artículos prohibidos comprenden los registros manuales del personal, la inspección de bultos y vehículos (tanto periódica como aleatoria); el uso de detectores de metales, máquinas de rayos X y detectores de radiación, y el uso de perros u otros tipos de detectores de sustancias químicas y explosivos. Estas medidas deberían tener en cuenta las características específicas de la instalación y las amenazas contra las que se requiere protección según la evaluación de las amenazas o la ABD, si procede.

4.63. El explotador debería formular y aplicar políticas que señalen cuáles son los artículos prohibidos y los procedimientos de búsqueda y detección conexos. El personal que realice registros o utilice equipos para detectar artículos prohibidos debería estar capacitado para utilizar el equipo y responder adecuadamente al descubrir un artículo prohibido. Las respuestas pueden comprender, entre otras medidas, confirmar una excepción autorizada, detener al adversario interno potencial o grabar el suceso para detectar posibles actos dolosos más adelante.

4.64. El rigor de los registros y la determinación de los lugares en los que realizarlos deberían ser acordes a la sensibilidad de la zona en la que se activó el registro y proximidad de la zona al blanco. Los registros deberían llevarse a cabo cerca de las zonas en las que se activaron. Deberían realizarse registros periódicos y aleatorios para disuadir en mayor grado la retirada no autorizada o el sabotaje de materiales nucleares y radiactivos. También deberían realizarse registros en condiciones de evacuación de emergencia, particularmente durante los ejercicios.

4.65. Durante el registro detallado de un vehículo de transporte antes de la carga y el envío, deberían aplicarse procedimientos de monitorización para velar por que las personas que realizan el registro no puedan introducir elementos prohibidos que faciliten la comisión de un acto doloso.

4.66. Deberían utilizarse detectores de radiación fijos o portátiles para inspeccionar a las personas, los paquetes o los vehículos que entren y salgan de zonas protegidas, interiores y vitales, a fin de detectar la retirada no autorizada de materiales nucleares. Deberían colocarse detectores de metales junto a los detectores de radiación en las entradas y salidas peatonales para aumentar la eficacia de la detección de la radiación, ya que podría utilizarse material de

blindaje para impedir que se detecten los rasgos radiactivos al retirar materiales nucleares de la instalación.

4.67. Los procedimientos para aprobar las excepciones a la introducción de artículos prohibidos o controlados (por ejemplo, fuentes de calibración radiactivas) en la instalación deberían establecerse de forma específica [3].

Vigilancia

4.68. Las medidas de vigilancia pueden utilizarse para supervisar sin interrupción las actividades de las personas dentro de las zonas designadas de la instalación en las que podría producirse un acto doloso, de modo que se descubran, notifiquen y evalúen las actividades no autorizadas.

4.69. La vigilancia incluye la observación visual, el seguimiento de las secuencias de vídeo en directo o el examen de las secuencias grabadas recogidas por los sistemas de vigilancia automatizados. La vigilancia puede ser útil no solo como medida de detección, sino también para la disuasión e investigación de posibles actos dolosos realizados por un agente interno.

4.70. El personal que realice actividades de vigilancia debería ser capaz de detectar actos autorizados y no autorizados y debería contar con los medios para informar de manera rápida y segura cuando observe actividades no autorizadas.

4.71. En caso de que se informe de una actividad no autorizada, las imágenes de vigilancia grabadas pueden servir para evaluar correctamente un acto doloso o señalar a los posibles sospechosos. La evaluación sin demora de los actos dolosos puede ser difícil sin la información de la vigilancia.

4.72. Como se recomienda en el párrafo 4.48 de la referencia [2], "cuando una *zona interior* esté ocupada, se debería poder *detectar* un acto no autorizado mediante una vigilancia constante (por ejemplo, aplicando la *regla de la actuación por pareja*)". Debería sopesarse la posibilidad de aplicar medidas de vigilancia durante operaciones como el mantenimiento y, en particular, durante las operaciones de embalaje, envío y transferencia [14]. La vigilancia puede llevarse a cabo a través de compañeros de trabajo, personal directivo, sistemas de vigilancia automatizados o una combinación de estos factores.

4.73. El explotador debería instaurar y ejecutar comprobaciones periódicas para confirmar que el control de los materiales u otras medidas de protección

se aplican de acuerdo con los procedimientos establecidos y que el equipo se utiliza correctamente.

4.74. Cuando la regla de la actuación por pareja sea el método de vigilancia seleccionado para una zona (por ejemplo, para una zona que contenga material de la categoría I), las dos personas autorizadas y con conocimientos deberían ocupar una ubicación física desde la que puedan verse claramente la una a la otra y a los materiales nucleares. Además, cada una de estas personas debería estar capacitada y técnicamente cualificada para detectar actividades no autorizadas o procedimientos incorrectos. Para que la vigilancia visual sea eficaz, las personas que observan deberían ser capaces de reconocer las actividades no autorizadas, evaluar correctamente la situación e informar de las actividades al personal de respuesta adecuado a tiempo para que este pueda evitar la retirada no autorizada. Si se aplica la regla de la actuación por pareja en este tipo de vigilancia, los dos individuos autorizados deberán tener la capacitación adecuada, estar situados en una ubicación con una visión clara del material y de la otra persona y ser capaces de detectar procedimientos no autorizados o incorrectos [1].

4.75. Además, la regla de la actuación por pareja solo es eficaz cuando los individuos no bajan la guardia, como puede ocurrir al trabar una amistad o relacionarse durante mucho tiempo. Siempre que sea posible, el personal directivo debería asegurar la rotación de los miembros de cada equipo de parejas. La aplicación de la regla de la actuación por pareja para el acceso a las zonas designadas puede disuadir a los adversarios internos y favorecer una detección oportuna. Además, la regla de la actuación por pareja puede contribuir a la protección frente a los adversarios internos que manipulen ilícitamente los sistemas de protección física. Debería informarse de los intentos de anular la regla de la actuación por pareja e investigarse los casos.

Sistemas de contabilidad y control de materiales nucleares

4.76. La contribución de los sistemas de CCMN a la seguridad física nuclear radica principalmente en su capacidad para mantener el conocimiento preciso de los tipos, las cantidades y las ubicaciones de los materiales nucleares de la instalación; para realizar un inventario físico eficaz de los materiales nucleares, y, en algunos casos, para garantizar que las actividades realizadas en relación con el material nuclear han sido debidamente autorizadas [9]. Existen múltiples medidas con las que un sistema de CCMN puede contribuir a detectar las amenazas de agentes internos. Estas medidas se describen con más detalle en la referencia [9].

4.77. También deberían aplicarse rigurosamente las medidas de CCMN y de detección de otro tipo para impedir la retirada no autorizada de materiales nucleares adicionales de una instalación por parte de un adversario interno, o con su ayuda, mientras se está realizando un envío autorizado. Otras medidas de detección pueden incluir a) la regla de la actuación por pareja durante la preparación del traslado, b) mediciones de los materiales, c) dispositivos de indicación de manipulación ilícita, d) comprobaciones de documentos, e) monitores de radiación y f) procedimientos operacionales normalizados.

Medidas de detección para sistemas informáticos

4.78. Para detectar actos dolosos deberían utilizarse medidas técnicas que abarquen tanto los equipos como los programas informáticos. Estas medidas pueden incluir las siguientes actividades de ejemplo:

a) Determinar valores de referencia para el tráfico de red de los activos informáticos de carácter estratégico y caracterizarlos, y realizar la inspección siguiendo los valores de referencia.
b) Aplicar herramientas de detección de intromisiones para detectar patrones anómalos en el comportamiento de los usuarios.
c) Monitorizar, inspeccionar y evaluar los sistemas informáticos para comprobar el cumplimiento de las políticas y procedimientos por parte de los agentes internos y detectar acciones sospechosas. Por ejemplo, el explotador podría establecer objetivos falsos y vigilarlos para detectar intentos de acceso no autorizado a información de carácter estratégico, a fin de descubrir a potenciales adversarios internos garantizando al mismo tiempo que no se revelan datos sensibles.
d) Restringir las posibles vías de acceso a los datos para que solo el personal autorizado pueda utilizarlas, y garantizar que estén controladas y monitorizadas para protegerlas de un uso doloso. Esto podría comprender la monitorización, el bloqueo físico, la prohibición del uso de medios extraíbles y dispositivos móviles para limitar el acceso a los sistemas sensibles por parte de agentes internos o el uso de zonas de seguridad informática para aislar los sistemas de seguridad física nuclear y sus redes de las redes de otras instalaciones [7].

Medidas de demora

4.79. La multitud de diferentes capas de protección física o medidas de procedimiento, entre ellas, la compartimentación y la segregación de tareas, pueden dificultar el avance de un adversario interno al requerir una variedad

de herramientas y competencias, proporcionando así tiempo y oportunidades adicionales para la detección. Al demorar de ese modo el acto doloso, podría detectarse a un adversario interno y frustrar su intento. La demora también puede disuadir a los agentes internos de intentar cometer actos dolosos.

4.80. Las medidas aplicadas en las proximidades de los equipos o materiales nucleares (como son los amarres, las sujeciones o las cerraduras) pueden ser medidas de demora eficaces contra adversarios internos en zonas bajo vigilancia continua o en conjunción con otras medidas de detección adecuadas. Dichas medidas de demora deberían diseñarse de manera que sea difícil para un agente interno utilizarlas para demorar la respuesta a un acto doloso, en especial, un acto de sabotaje.

4.81. Conservar los materiales nucleares en un lugar seguro puede demorar más a un agente interno que intente cometer un acto doloso. La extracción simultánea de materiales nucleares del almacenamiento seguro para la producción o el uso debería limitarse a la cantidad mínima necesaria para esos fines, y deberían tomarse medidas para controlar los materiales nucleares entre los pasos del proceso. Cuando los materiales no puedan trasladarse a un lugar de almacenamiento seguro durante las horas no laborables, deberían aplicarse medidas adicionales de protección física y vigilancia hasta que el material sea adecuadamente devuelto y almacenado en un lugar seguro normal.

4.82. La anulación de ciertos tipos de medidas de demora puede obligar a los adversarios internos a utilizar herramientas, recursos, logística, capacitación y competencias más complejos. Estos recursos más elaborados pueden no estar disponibles en la instalación, por lo que el adversario interno debería introducirlos en ella o aprenderlos en otro lugar.

4.83. Los diseños de seguridad de los sistemas que los dotan de una autoprotección (como son los equipos de reserva, la parada automática de los equipos o el cierre automático de válvulas) pueden obligar al adversario interno a superar equipos y sistemas múltiples, redundantes y dispersos. Estas funcionalidades pueden demorar un acto doloso y frustrarlo. En la medida de lo posible, el acceso a la información sobre los diseños de seguridad de los sistemas debería restringirse por la necesidad de saber a fin de evitar que se utilice para cometer un acto doloso.

Medidas de demora en los sistemas informáticos

4.84. Las medidas de seguridad física aplicadas para demorar a los adversarios pueden no ser eficaces para proteger los sistemas informáticos debido al acceso

remoto a algunos sistemas informáticos y a la conectividad entre ellos. Por ejemplo, un agente interno con derechos de acceso a sistemas informáticos sensibles podría ser capaz de comprometer activos físicamente distantes de forma remota y simultánea. Puede que las demoras tampoco sean eficaces frente a un adversario interno que pueda utilizar las credenciales existentes para obtener derechos de acceso. Por lo tanto, las medidas destinadas a los sistemas informáticos deberían hacer hincapié en la prevención y, en mayor medida, en la detección y la respuesta.

4.85. El diseño y la adopción de zonas de seguridad informática y de niveles de seguridad informática en una instalación pueden aumentar la complejidad necesaria para llevar a cabo un acto doloso con sistemas informáticos y aportar controles de seguridad que también pueden incrementar la probabilidad de detección [7].

Medidas de respuesta

4.86. Tanto el personal de operaciones como el de seguridad física pueden responder a una irregularidad (como las diferencias de inventario o una puerta abierta que debería estar cerrada). Normalmente, el personal de operaciones responde a una irregularidad para investigar su causa. Si se sospecha que una irregularidad se debe a un acto doloso, debería advertirse al personal de seguridad física, que debería responder de ser necesario. Estos son algunos ejemplos:

a) La respuesta a un adversario interno pasivo debería depender del momento en que se produzca la detección (cuando se obtiene la información, cuando esta se transmite o cuando se finaliza la investigación).
b) La respuesta a un adversario interno activo y no violento debería confiarse al personal de operaciones o de seguridad, en función del momento en que se produzca la detección, ya que un adversario interno activo y no violento dejará de realizar un acto doloso si se ve confrontado o desafiado.
c) La respuesta a un adversario interno activo y violento debería ser la misma que la aplicada a un adversario externo.

4.87. En comparación con un adversario externo, un adversario interno es más difícil de descubrir y puede no ser fácilmente reconocido como amenaza en ninguna parte de la instalación. Además, un acto doloso cometido por un adversario interno puede consistir en varios actos distantes en el tiempo y el espacio. Por lo tanto, a menos que el adversario interno sea descubierto al detectar un acto sospechoso o doloso, puede ser difícil de señalar posteriormente entre los demás agentes internos.

4.88. Para poder dar una respuesta eficaz, es necesario detectar un robo prolongado antes de que el adversario interno acumule la cantidad pretendida de materiales dentro o fuera del emplazamiento. Los escenarios deberían contemplar los sistemas y las medidas de seguridad física existentes en el edificio y en las posibles zonas de balance de materiales, así como los procedimientos específicos de seguridad física nuclear que podrían aplicarse para detectar actividades no autorizadas relacionadas con materiales nucleares con la suficiente antelación para poder dar una respuesta eficaz. En el caso de las instalaciones en las que pudieran producirse robos prolongados, deberían analizarse los escenarios para determinar la probabilidad de detección si el material a) se extrajera del emplazamiento cada vez que se robara una cantidad del mismo o b) se acumulara en la instalación o dentro de una zona de tratamiento para sacarlo del emplazamiento de una sola vez en un robo repentino.

4.89. Un adversario interno podría realizar en un orden inesperado o con períodos de inactividad entre los distintos actos un conjunto de actos que, en última instancia, tienen como objetivo la retirada no autorizada o el sabotaje. Por ejemplo, un adversario interno podría cometer un solo acto y luego esperar a ver si es detectado. Esto puede complicar la respuesta de seguridad física necesaria para descubrir y detener al adversario interno y aumentar la importancia de la investigación. La investigación puede requerir la colaboración de especialistas en operaciones para analizar el suceso anómalo o irregular a fin de predecir qué otros actos dolosos podrían intentarse.

4.90. Los agentes internos con acceso a una instalación deberían recibir capacitación para detectar actos dolosos y responder a ellos, de modo que se protejan y transmitan las alarmas de acuerdo con un conjunto de procedimientos formalizados. Estos procedimientos deberían documentarse y utilizarse como parte de la capacitación que el explotador ofrezca para concienciar al personal de la instalación en materia de seguridad física. Los procedimientos de respuesta deberían basarse en el supuesto de que, entre quienes participan en la respuesta, podría haber un adversario. Por ejemplo, un adversario interno podría informar de una emergencia ficticia para distraer a los demás y evitar que detecten un acto doloso, o ser parte del equipo de respuesta y utilizar un ejercicio de emergencia o crear una emergencia para encubrir un acto doloso.

Medidas de respuesta en los sistemas informáticos

4.91. En el caso de incidentes de seguridad informática que puedan afectar negativamente a los sistemas que contribuyen a la seguridad física nuclear, las actividades de respuesta deberían coordinarse con el personal de respuesta de

seguridad física nuclear y documentarse. Por ejemplo, el personal de seguridad física del emplazamiento y el personal de seguridad informática deberían responder coordinadamente si se detecta que un agente interno realiza cambios no autorizados en el control del acceso, ya que dichos cambios podrían facilitar una retirada no autorizada o un sabotaje. En caso de que se produzca un incidente de seguridad informática de este tipo, también debería sopesarse la aplicación de medidas compensatorias con la participación de la seguridad física del emplazamiento y otras organizaciones pertinentes de la instalación.

ELEMENTOS INTEGRALES QUE REFUERZAN LAS MEDIDAS DE PREVENCIÓN Y PROTECCIÓN

La cultura de la seguridad física nuclear

4.92. La base de la cultura de la seguridad física nuclear es el reconocimiento de que existe una amenaza creíble y de que la seguridad física nuclear es importante [11].

4.93. La cultura de la seguridad física nuclear desempeña un papel fundamental para garantizar que los individuos, las organizaciones y las instituciones se mantengan vigilantes y que se tomen medidas duraderas para contrarrestar las amenazas de los agentes internos. La eficacia de las medidas de prevención y protección contra las amenazas de agentes internos depende de las actitudes, los comportamientos y las actuaciones de los individuos [17].

4.94. El personal directivo debería promover una sólida cultura de la seguridad física nuclear para contrarrestar las amenazas de agentes internos y externos. La cultura de la seguridad física nuclear genera las condiciones globales para que el personal aplique medidas tanto preventivas como de protección. La cultura de la seguridad física nuclear de una instalación debería favorecer la lealtad y el cumplimiento de las políticas de seguridad. Por ejemplo, el personal directivo debería hacer hincapié en la responsabilidad de los empleados de informar sobre actividades inusuales o comportamientos sospechosos sin temor a sufrir medidas disciplinarias [11].

Planes de contingencia

4.95. Como se indica en el párrafo 3.58 de la referencia [2]:

> "El Estado debería establecer un *plan de contingencia*. La *autoridad competente* del Estado debería velar por que el *explotador* elabore *planes de contingencia* para contrarrestar eficazmente *la evaluación de amenazas* o la *amenaza base de diseño* teniendo en cuenta las acciones de las *fuerzas de respuesta*".

El párrafo 3.62 de la referencia [2] afirma que "El *explotador* debería iniciar su *plan de contingencia* tras la *detección* y la evaluación de cualquier *acto doloso*". El párrafo 5.44 de la referencia [2] señala que "El *plan de contingencia* debería incluir medidas centradas en prevenir nuevos daños, lograr la seguridad de la *instalación nuclear* y proteger el equipo y el personal de emergencia".

4.96. Los planes de contingencia elaborados por el Estado y el explotador deberían abordar las medidas para responder tanto a las amenazas de agentes internos como externos. Las medidas de protección contra las amenazas de agentes internos deberían coordinarse con los planes de contingencia conforme a los procedimientos acordados. El plan de contingencia debería exigir el control y registro del personal que evacúa un edificio durante una emergencia real o simulada en busca de contaminación y materiales nucleares para protegerlos contra las amenazas de agentes internos.

4.97. Las medidas que se tomen en respuesta a la sospecha o confirmación de actos dolosos cometidos por adversarios internos pueden ser diferentes a las que se tomen como respuesta a actos dolosos de adversarios externos.

Programa de mantenimiento y recuperación del sistema

4.98. Un programa de mantenimiento y recuperación para todos los sistemas de seguridad física nuclear de la instalación que deban protegerse puede mitigar las consecuencias de un acto doloso cometido por un adversario interno. El programa de mantenimiento debería incluir la capacidad de reparar rápidamente los sistemas operativos y demás sistemas esenciales, sustituir rápidamente las piezas dañadas y aplicar las medidas compensatorias necesarias. La reparación y la sustitución rápidas limitan la duración de la parada del sistema y el tiempo disponible para todo acto doloso ulterior, y pueden mitigar las consecuencias del acto doloso del adversario interno.

4.99. Los explotadores deberían sopesar la posibilidad de proteger las piezas de repuesto (por ejemplo, instalando barreras, almacenando las piezas lejos del sistema instalado y monitorizando con frecuencia el lugar de almacenamiento), de modo que a un adversario interno le resulte difícil destruir o poner en peligro las piezas instaladas y las piezas de repuesto de los equipos esenciales.

4.100. Los procedimientos operacionales y para la recuperación de los sistemas de seguridad física y operacionales de las instalaciones deberían validarse y ejecutarse para contribuir a garantizar la rápida recuperación de estos sistemas, así como para proteger el equipo y al personal de emergencia.

4.101. Los procedimientos aplicados para la protección de los equipos determinados deberían incluir una respuesta adecuada a las paradas —como la aplicación de medidas compensatorias, la investigación de la causa de la parada y la aplicación de un sistema de reparación rápida (restablecimiento del servicio)— para la protección frente a la posibilidad de un acto doloso no evaluado y en curso.

4.102. Deberían ponerse en práctica procesos seguros de copia de seguridad y recuperación para los sistemas informáticos sensibles que desempeñan funciones operacionales o de seguridad física nuclear. Los archivos del sistema utilizados para los procesos de recuperación deberían almacenarse en una zona independiente con control de acceso.

5. EVALUACIÓN DE LAS MEDIDAS

OBJETIVOS Y VISIÓN GENERAL DEL PROCESO DE EVALUACIÓN

5.1. La evaluación de la eficacia de las medidas de prevención y de protección contra las amenazas de agentes internos es un componente clave de una evaluación de riesgos destinada a identificar los sistemas vulnerables a las amenazas de agentes internos. La evaluación debería utilizar escenarios de amenazas creíbles basados en la evaluación de la amenaza o la ABD.

5.2. Los resultados de la evaluación deberían compararse con los criterios de eficacia de las medidas de prevención y de protección previamente establecidos. La autoridad competente suele determinar estos criterios sobre la base de las posibles consecuencias de un acto doloso cometido por un adversario interno y su probabilidad de culminarlo. El explotador debería documentar cómo cumple estos

criterios en su plan integral de seguridad física, que comprende los planes para proteger los sistemas de CCMN y de protección física.

5.3. La evaluación de la eficacia de las medidas de prevención y de protección debería basarse en el plan de seguridad física del explotador. Si la evaluación indica que las medidas de prevención y de protección definidas en el plan de seguridad física no cumplen los criterios, deberían introducirse mejoras y la evaluación debería repetirse hasta que se cumplan los criterios.

5.4. En la evaluación, el explotador debería tener en cuenta la facilidad relativa de cometer un acto doloso y el nivel de riesgo asociado al posible acto doloso. Por ejemplo, un acto doloso puede tener consecuencias que se consideren aceptables pero ser relativamente fácil de realizar (como puede ser la alteración no autorizada del nivel de detección de un pórtico detector de radiación); por ello, dicho acto puede considerarse inaceptable y requerir una medida correctiva. Por otra parte, el riesgo puede considerarse aceptable pero estar cerca del umbral de lo inaceptable. Por ejemplo, un adversario interno podría retirar de una zona de tratamiento de categoría III pequeñas cantidades de materiales nucleares que suponen poco riesgo, pero, si esta retirada no autorizada se repitiera, la cantidad total retirada podría alcanzar una cantidad contemplada en una categoría superior. Este caso no debería ignorarse, y las prácticas de gestión prudentes se decantarían por adoptar medidas de protección adicionales.

5.5. La eficacia de las medidas de prevención y de protección debería revaluarse periódicamente, en particular, cuando se produzcan cambios en la evaluación de la amenaza o la ABD, en las medidas de prevención y de protección o en los procesos y las condiciones de funcionamiento.

5.6. Los requisitos relativos a los criterios y el funcionamiento de los sistemas de CCMN se determinan en el marco del contexto general de la seguridad física nuclear y pueden ser especialmente útiles para evaluar la eficacia del sistema de seguridad física nuclear frente a las amenazas de agentes internos. Estos requisitos referidos a los criterios y el funcionamiento deberían abordar los diferentes tipos de materiales nucleares y los plazos para la detección de la retirada no autorizada de materiales nucleares.

5.7. Para evaluar la eficacia del sistema de seguridad física nuclear frente a las amenazas de agentes internos pueden utilizarse diferentes métodos (por ejemplo, inspecciones y evaluaciones, ensayos del funcionamiento, control de calidad de las mediciones o análisis de escenarios). El análisis de escenarios es un método eficaz de evaluación frente a las amenazas de agentes internos. Los ensayos

del funcionamiento sustentan el proceso de análisis de escenarios al aportar información como la probabilidad de detección y de respuesta posterior. Deberían elaborarse y aplicarse planes para la realización de ensayos del funcionamiento a fin de comprobar la preparación de los empleados, las instalaciones y las autoridades competentes para responder a un posible acto doloso cometido por un adversario interno.

EVALUACIÓN DE LAS MEDIDAS PREVENTIVAS

5.8. La aplicación de las medidas preventivas debería evaluarse para velar por que sea conforme a su diseño. Aunque es difícil de evaluar cuantitativamente, las medidas preventivas pueden ser eficaces para reducir la factibilidad de las amenazas de agentes internos. Las medidas preventivas deberían evaluarse con ensayos del funcionamiento de los procedimientos para determinar si estos son adecuados para hacer frente a la amenaza y si los empleados los siguen.

5.9. La oportunidad de que un adversario interno realice un acto doloso puede reducirse al mínimo mermando la posibilidad de que este agente interno obtenga el acceso, la autoridad o los conocimientos necesarios para lograr cometer un acto doloso. Los escenarios creíbles para la evaluación incorporarán el grado y la forma en que la oportunidad se reduce al mínimo. Debería realizarse un examen para determinar qué medidas preventivas existen y si se aplican correctamente.

EVALUACIÓN DE LAS MEDIDAS DE PROTECCIÓN

5.10. La eficacia de las medidas utilizadas para detectar y demorar los actos dolosos y responder a ellos (medidas de protección) puede analizarse cuantitativa o cualitativamente. La probabilidad de detección y la rapidez de la respuesta suelen ser cuantificables y pueden servir de base para evaluar la eficacia de las medidas de protección.

5.11. Una forma de evaluar la eficacia de las medidas de protección contra las amenazas de agentes internos es elaborar escenarios creíbles, en los que se incluyan hipótesis en las que estos actúen en connivencia con otros adversarios internos o con adversarios externos, según el caso. Con estos escenarios, se puede evaluar la eficacia de las medidas de protección para contrarrestar esas hipótesis.

5.12. La elaboración de escenarios implica definir la combinación de acciones necesarias para que un adversario interno cometa un acto doloso. Los explotadores

deberían considerar la posibilidad de elaborar los escenarios conectando los blancos determinados (véase la sección 3) con un adversario interno definido (véase la sección 2). El conjunto de acciones que un adversario interno tendría que emprender para lograr su objetivo debería definirse teniendo en cuenta la evaluación de la amenaza o la ABD. Estos conjuntos de acciones deberían incluir las que se realizarían y los lugares donde se llevarían a cabo, y deberían determinarse todas las medidas de protección con las que podrían topar los adversarios internos al ejecutarlas. Dado que los adversarios internos pueden llevar a cabo las acciones necesarias para cometer un acto doloso durante un período prolongado, y dado que las acciones pueden no seguir una secuencia predecible, el concepto de trayectoria o cronología puede o no ser relevante para el análisis.

5.13. Para los escenarios de sabotaje, deberían indicarse las acciones que, de llevarse a cabo, iniciarían una secuencia de sucesos que daría lugar a consecuencias radiológicas inaceptables. Los escenarios de sabotaje deberían incluir ataques contra blancos únicos y múltiples.

5.14. Para los escenarios que impliquen la retirada no autorizada de materiales nucleares, debería determinarse qué acciones habría que lograr ejecutar para retirar los materiales nucleares de la instalación. Los escenarios que impliquen la retirada no autorizada de materiales nucleares deberían contemplar tanto el robo prolongado como el repentino e incluir situaciones en las que el adversario abandona la instalación directamente con los materiales nucleares y otras en las que esconde los materiales en la instalación para retirarlos más tarde en circunstancias más favorables. Los escenarios deberían tener en cuenta los ataques a los sistemas informáticos y acciones para comprometerlos, combinaciones de ataques físicos y ciberataques, y ataques de adversarios internos violentos y no violentos.

5.15. Las estrategias que pueden utilizar los adversarios internos para frustrar las medidas de protección también deberían considerarse como parte del proceso de elaboración del escenario. El explotador puede formular estas estrategias teniendo en cuenta la oportunidad que el acceso, la autoridad y el conocimiento podrían ofrecer a un adversario interno para frustrar las medidas de detección y demora. También deberían contemplarse los posibles actos de los adversarios internos para reducir la eficacia de la respuesta. Las condiciones de emergencia que provocan la evacuación de las instalaciones pueden crear oportunidades para que un adversario interno realice un acto doloso, y deberían tenerse en cuenta en la elaboración del escenario.

5.16. Una vez elaborados los escenarios detallados de las amenazas de agentes internos, la eficacia de las medidas de protección puede evaluarse considerando

el impacto acumulado de la detección y la demora, así como la respuesta y la mitigación de las consecuencias del escenario. Para un adversario interno activo y no violento, la eficacia de la respuesta dependerá de la probabilidad de que se interrumpa o neutralice[5] un acto doloso.

5.17. El proceso de evaluación debería repetirse para los escenarios creíbles que requieran un análisis más profundo. Las conclusiones sobre la eficacia de las medidas de protección deberían basarse en los resultados de todas las evaluaciones realizadas.

EVALUACIÓN DE LAS MEDIDAS CONTRA LA ACTUACIÓN DE AGENTES INTERNOS EN CONNIVENCIA

5.18. El desarrollo de escenarios suficientes que aborden la actuación de dos o más adversarios internos en connivencia es un reto debido a las numerosas combinaciones de agentes internos con diferente acceso, autoridad y conocimiento que hay que contemplar. La evaluación de la eficacia de las medidas que ayudan a prevenir la actuación en connivencia (como pueden ser la compartimentación, la vigilancia o las medidas preventivas) puede ser un buen enfoque.

EVALUACIÓN DE LAS MEDIDAS CONTRA EL ROBO PROLONGADO

5.19. La evaluación de las medidas contra el robo prolongado puede enfocarse de la misma manera que la evaluación de las medidas contra el robo repentino. Sin embargo, la evaluación de las medidas contra el robo prolongado también debería tener en cuenta las dificultades adicionales que encuentra el adversario interno al intentar sustraer sin autorización pequeñas cantidades de materiales durante un período de tiempo prolongado. Estas complejidades comprenden la realización de inventarios periódicos, la posibilidad de que se detecten diferencias de inventario, el rastreo de los registros, la ocultación de las cantidades de materiales acumuladas y la necesidad de salvar los pórticos detectores de radiación. El método de evaluación también debería considerar el aumento de la probabilidad de detección cuando la misma acción se repite varias veces.

---

[5] Que el acto doloso se "interrumpa" significa que la respuesta se produce a tiempo de impedir su comisión. En el caso de un adversario interno activo y violento, que un acto doloso se "neutralice" significa que la fuerza de respuesta detiene o impide el ataque de forma permanente. En el caso de un adversario interno activo y no violento, la neutralización se produce cuando se descubre al adversario interno.

EVALUACIÓN DE LAS MEDIDAS CONTRA EL SABOTAJE

5.20. La evaluación de las medidas contra el sabotaje realizado por un adversario interno puede utilizar el mismo proceso que la evaluación de las medidas contra el robo repentino y prolongado, y puede aludir al enfoque del modelo lógico (árbol de fallos o árbol de sucesos) proporcionado en la referencia [16].

5.21. Los escenarios de sabotaje que se evalúen deberían incluir escenarios tanto de sabotaje directo de materiales nucleares como de sabotaje indirecto (es decir, sabotaje de los sistemas de la instalación) que puedan tener consecuencias radiológicas inaceptables. La evaluación de los escenarios de sabotaje debería contemplar escenarios con personas sin acceso directo a los materiales o al equipo.

5.22. Para llevar a cabo un acto de sabotaje, el adversario interno no tendría que salir necesariamente de la instalación para cometer el acto doloso. No obstante, también se aplicaría la evaluación de las medidas de prevención y protección frente a todo agente interno que salga de la instalación.

EVALUACIÓN DE LA PROTECCIÓN CONTRA LAS AMENAZAS DE AGENTES INTERNOS DE UNA INSTALACIÓN

5.23. El proceso de evaluación de la protección contra las amenazas de agentes internos de una instalación comienza con la caracterización de los agentes internos según sus atributos, motivaciones y categorías para determinar las posibles amenazas de agentes internos. El siguiente paso es la determinación del blanco, que implica una evaluación de los activos que hay que proteger contra una retirada no autorizada o acto de sabotaje. El resultado de esta evaluación es una lista priorizada de blancos.

5.24. Deberían aplicarse medidas preventivas siguiendo el concepto de defensa en profundidad y un enfoque graduado para reducir al mínimo las oportunidades de que se ejecuten las amenazas detectadas y de que los blancos determinados sean objeto de actos dolosos.

5.25. Deberían indicarse medidas de protección para blancos en zonas protegidas, interiores o vitales siguiendo un orden de prioridad. La profundidad de las medidas para detectar y demorar la amenaza de los agentes internos y responder a ella debería aumentarse con los resultados de la evaluación.

5.26. Las medidas de prevención y de protección contra el sabotaje y la retirada no autorizada de materiales nucleares deberían evaluarse utilizando un método como la formulación de escenarios creíbles. Los escenarios deberían ser coherentes con la evaluación de la amenaza o la ABD y pueden comprender ataques físicos, ciberataques o una combinación de ambos en la instalación, en las rutas de transporte y dentro de las cadenas de suministro.

5.27. Debería revaluarse el sistema periódicamente para corroborar que las medidas se aplican de forma efectiva y se mantienen. La revaluación puede programarse en ciclos o puede activarse a consecuencia de cambios en la amenaza o en la instalación y su explotación.

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/Rev.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] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Seguridad física de las fuentes radiactivas*, *Colección de Seguridad Física Nuclear del OIEA* Nº 11, OIEA, Viena, 2019.

[6] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *La seguridad física en el transporte de materiales radiactivos*, *Colección de Seguridad Física Nuclear del OIEA* Nº 9, OIEA, Viena, 2013.

[7] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Seguridad informática en las instalaciones nucleares*, *Colección de Seguridad Física Nuclear del OIEA* Nº 17, OIEA, Viena, 2013.

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

[9] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Empleo de la contabilidad y el control de materiales nucleares con fines de seguridad física nuclear en las instalaciones*, *Colección de Normas de Seguridad del OIEA* Nº 25-G, OIEA, Viena, 2019.

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, IAEA Nuclear Security Series No. 4, IAEA, Vienna (2007).

[11] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Cultura de la seguridad física nuclear*, *Colección de Seguridad Física Nuclear del OIEA* Nº 7, OIEA, Viena, 2017.

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

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Material in Transport, IAEA Nuclear Security Series No. 26-G, IAEA, Vienna (2015).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Establishing a System for Control of Nuclear Material for Nuclear Security Purposes at a Facility during Use, Storage and Movement, IAEA Nuclear Security Series No. 32-T, IAEA, Vienna (2019).

[15] 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.

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Identification of Vital Areas at Nuclear Facilities, IAEA Nuclear Security Series No. 16, IAEA, Vienna (2012).

[17] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Autoevaluación de la cultura de la seguridad física nuclear en instalaciones y actividades*, *Colección de Seguridad Física Nuclear del OIEA* Nº 28, OIEA, Viena, 2019.

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

Esta obra es una actualización del volumen Nº 8 de la *Colección de Seguridad Física Nuclear del OIEA*, publicado originalmente en 2008. La revisión se ha llevado a cabo para mejorar la armonización de esta Guía de Aplicación con las Nociones Fundamentales de Seguridad Física Nuclear y con las Recomendaciones publicadas después de 2008, para incluir remisiones a otras Guías de Aplicación pertinentes publicadas desde 2008 y para añadir más detalles respecto a algunos temas sobre la base de la experiencia del OIEA y de los Estados Miembros con la utilización del Nº 8 de la *Colección de Seguridad Física Nuclear del OIEA*. Esta publicación ofrece una orientación actualizada a los Estados, a sus autoridades competentes y explotadores, y a remitentes y transportistas sobre la selección, aplicación y evaluación de las medidas para hacer frente a las amenazas de agentes internos. Es aplicable a todo tipo de instalación nuclear, en particular, centrales nucleares, reactores de investigación y otras instalaciones del ciclo del combustible nuclear (por ejemplo, plantas de enriquecimiento, plantas de reprocesamiento, plantas de fabricación de combustible e instalaciones de almacenamiento), ya sea para su diseño, construcción, puesta en servicio, explotación, parada o clausura.

ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA
VIENA