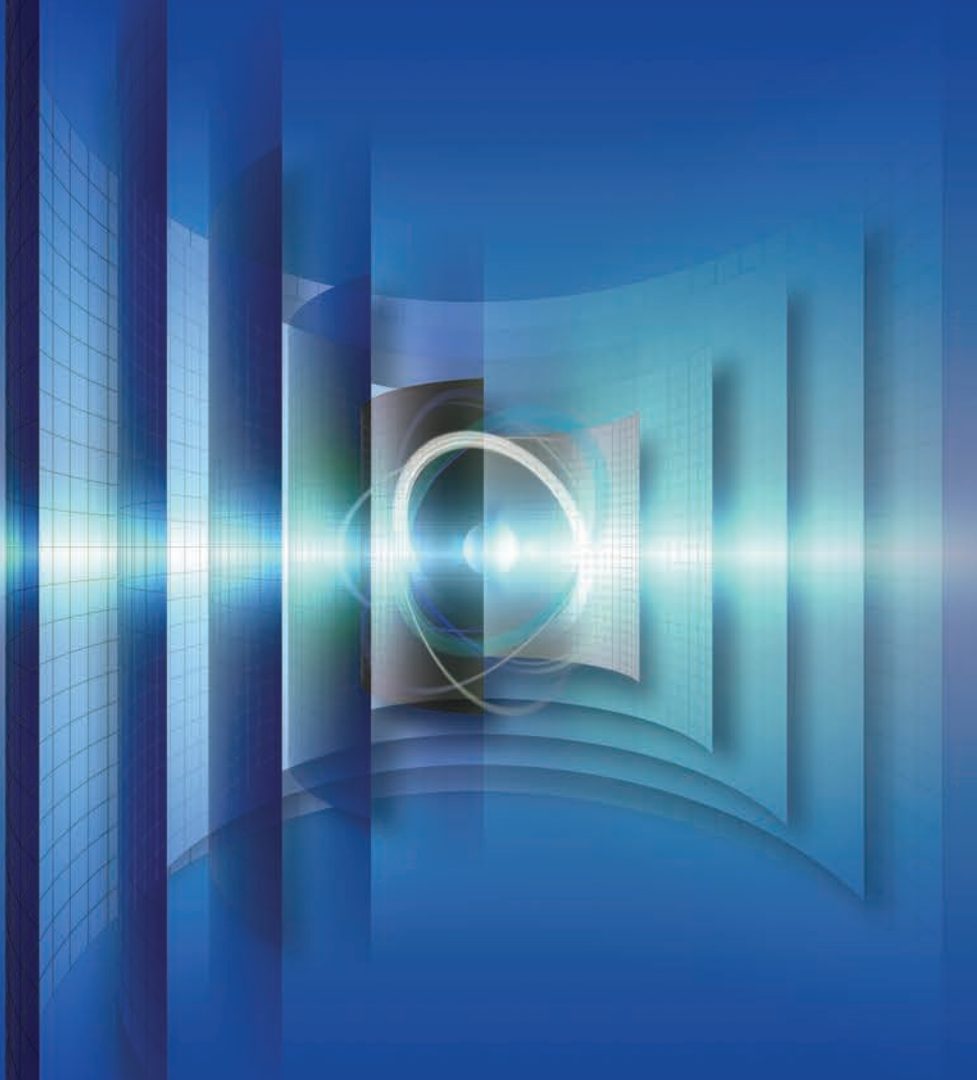
Colección de Seguridad Física Nuclear del OIEA Nº 23-G

Guía de Aplicación

Seguridad física de la información nuclear



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.

SEGURIDAD FÍSICA DE LA INFORMACIÓN NUCLEAR

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
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
EX REPÚBLICA YUGOSLAVA DE MACEDONIA
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
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
SAN MARINO
SANTA SEDE
SAN VICENTE Y LAS GRANADINAS
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 23-G

SEGURIDAD FÍSICA DE LA INFORMACIÓN NUCLEAR

GUÍA DE APLICACIÓN

ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA
VIENA, 2018

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
http://www.iaea.org/books

Impreso por el OIEA en Austria
Diciembre de 2018
STI/PUB/1677

SEGURIDAD FÍSICA DE LA INFORMACIÓN NUCLEAR
OIEA, VIENA, 2018
STI/PUB/1677
ISBN 978–92–0–305417–1
ISSN 2521–1803

PREFACIO

por Yukiya Amano
Director General

El principal objetivo del OIEA, en virtud de su Estatuto, es "acelerar y aumentar la contribución de la energía atómica a la paz, la salud y la prosperidad en el mundo entero". Nuestro trabajo tiene el doble propósito de prevenir la propagación de las armas nucleares y fomentar la disponibilidad de la tecnología nuclear para fines pacíficos en sectores como la salud y la agricultura. Es esencial que todos los materiales nucleares y otros materiales radiactivos, así como las instalaciones en que se encuentren, se gestionen de manera segura y se protejan debidamente contra todo acto delictivo o acto intencional no autorizado.

La seguridad física nuclear es responsabilidad de cada Estado, pero la cooperación internacional es fundamental para ayudar a los Estados a establecer y mantener un régimen de seguridad física nuclear eficaz. El papel central del OIEA en la facilitación de esa cooperación y la prestación de asistencia a los Estados es ampliamente reconocido. La función del OIEA refleja su amplia composición, su mandato, su competencia técnica sin paralelo y su larga experiencia en la provisión de asistencia técnica y orientación práctica especializada a los Estados.

Desde 2006, el OIEA publica volúmenes de la *Colección de Seguridad Física Nuclear* para ayudar a los Estados a establecer regímenes de seguridad física nuclear eficaces. Estas publicaciones complementan los instrumentos jurídicos internacionales relativos a la 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.

Las orientaciones se elaboran con la activa participación de expertos de los Estados Miembros del OIEA y, por lo tanto, reflejan el consenso sobre las buenas prácticas en la 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 proyectos de publicación de la *Colección de Seguridad Física Nuclear* a medida que se elaboran.

El OIEA seguirá trabajando con sus Estados Miembros con miras a lograr que los beneficios de la tecnología nuclear con fines pacíficos estén disponibles para mejorar la salud, el bienestar y la prosperidad de las personas en el mundo entero.

NOTA EDITORIAL

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

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

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

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

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

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

ÍNDICE

1. INTRODUCCIÓN

ANTECEDENTES

1.1. El objetivo general del régimen de seguridad física nuclear de un Estado es proteger a las personas, los bienes, la sociedad y el medio ambiente contra las consecuencias nocivas de un suceso relacionado con la seguridad física nuclear [1]. Los grupos o personas que desean planificar o cometer actos dolosos relacionados con materiales nucleares u otros materiales radiactivos, o con las instalaciones conexas, pueden sacar partido del acceso a la información de carácter estratégico. Por consiguiente, esa información se debería identificar, clasificar y asegurar con las medidas adecuadas. Es de carácter estratégico la información, en cualquiera de sus formas, incluidos los programas informáticos, cuya divulgación, modificación, alteración, destrucción o denegación de uso no autorizada pueda comprometer la seguridad física nuclear.

1.2. La confidencialidad es la propiedad de la información en virtud de la cual esta no se facilita ni revela a personas, entidades o procesos no autorizados. La seguridad física de la información supone garantizar no solo su confidencialidad, sino también su exactitud y exhaustividad (su integridad) y su accesibilidad o posibilidad de uso cuando se solicite (su disponibilidad).

1.3. La garantía de la seguridad física de la información de carácter estratégico es un requisito indispensable en todos los aspectos de la seguridad física nuclear, y los sistemas y medidas para lograr una seguridad física efectiva de la información son elementos fundamentales del régimen de seguridad física nuclear de un Estado.

1.4. En las Nociones Fundamentales de Seguridad Física Nuclear [1] y en las tres publicaciones de la categoría Recomendaciones de la *Colección de Seguridad Física Nuclear* [2 a 4] se reconoce la importancia de garantizar la seguridad física de la información de carácter estratégico. En la presente Guía de Aplicación se analizan más a fondo las declaraciones de alto nivel contenidas en esas publicaciones, con el fin de ofrecer más detalles sobre lo que se debería hacer.

OBJETIVO

1.5. La presente publicación contiene orientaciones sobre la aplicación del principio de la confidencialidad y sobre los aspectos más amplios de la

seguridad física de la información. Existen muchas orientaciones nacionales e internacionales acerca del establecimiento y la gestión de marcos de seguridad física para distintos tipos de información, tanto en forma de orientación de alto nivel como de normas detalladas. Esta publicación no pretende sustituir esas orientaciones; su objetivo es, en cambio, ayudar a los Estados a cerrar la brecha entre sus normas gubernamentales e industriales sobre la seguridad física de la información en general, los conceptos y consideraciones particulares que se aplican a la seguridad física nuclear, y las disposiciones y condiciones especiales que rigen en el caso de los materiales nucleares y otros materiales radiactivos.

1.6. El objetivo de la presente publicación es ofrecer orientación sobre:

a) el establecimiento de un marco eficaz para garantizar la confidencialidad, integridad y disponibilidad de la información de carácter estratégico (sección 3), con inclusión de la legislación y reglamentación necesarias;
b) la determinación de la información que puede considerarse de carácter estratégico (sección 4);
c) las consideraciones aplicables al intercambio y la divulgación de la información de carácter estratégico (sección 5);
d) las directrices y metodologías para garantizar la confidencialidad, integridad y disponibilidad (sección 6).

ÁMBITO DE APLICACIÓN

1.7. La presente publicación trata sobre la seguridad física de la información de carácter estratégico en los usos civiles de los materiales nucleares y otros materiales radiactivos y las instalaciones y actividades conexas, y se centra en la información de carácter estratégico referente a los materiales e instalaciones sometidos a control reglamentario.

1.8. La seguridad física nuclear relacionada con los materiales nucleares y otros materiales radiactivos no sometidos a control reglamentario también puede entrañar información de carácter estratégico que se deba proteger. En tales casos, la orientación general proporcionada en esta publicación debería utilizarse en la medida en que sea aplicable.

1.9. La presente publicación está destinada a todos aquellos que tienen responsabilidades relacionadas con la seguridad física de la información de carácter estratégico, a saber:

a) las autoridades competentes, incluidos los órganos reguladores;
b) el personal directivo de las instalaciones, empresas y organizaciones que participan en el uso, almacenamiento o transporte de materiales nucleares u otros materiales radiactivos;
c) las entidades explotadoras de las instalaciones y su personal, especialmente el personal de seguridad;
d) los contratistas y otras partes que trabajen para las autoridades, las organizaciones o las entidades explotadoras de las instalaciones;
e) cualquier otra entidad que pueda haber obtenido acceso legítimo a información de carácter estratégico.

ESTRUCTURA

1.10. Después de esta introducción, en la sección 2 se presentan varios términos y conceptos clave que se utilizarán en esta publicación. En la sección 3 se describen los elementos necesarios que, en su conjunto, constituyen un marco para la seguridad física de la información de carácter estratégico en un Estado, y en las secciones 4 a 6 se examinan esos elementos uno por uno. La sección 4 trata de las consideraciones que permiten determinar si una información es de carácter estratégico y, por lo tanto, se debe proteger. En la sección 5 se exponen las consideraciones relativas al intercambio y la divulgación de la información de carácter estratégico, y en la sección 6 se describen con más detalle las medidas que se deben aplicar a nivel de la instalación para proteger esa información. En el anexo I se presenta un ejemplo de un marco de clasificación. En el anexo II se ofrece un ejemplo de un sistema de categorización de la seguridad para la información relacionada con la seguridad física nuclear. En el anexo III se propone un formato y un contenido para un programa de capacitación y sensibilización.

2. CONCEPTOS Y CONTEXTO

2.1. En la presente sección se aclara el significado de algunos términos importantes empleados en esta publicación y se indica cómo se aplican los conceptos clave de la seguridad física de la información al contexto de la seguridad física nuclear. Las definiciones de estos y otros términos pertinentes se recogen en el glosario que figura al final de esta publicación.

INFORMACIÓN

2.2. La información es conocimiento, independientemente de la forma en que exista o se exprese. Comprende ideas, conceptos, sucesos, procesos, pensamientos, hechos y patrones. Puede registrarse en un material como el papel, una película o un medio magnético u óptico, o conservarse en sistemas electrónicos. La información puede representarse y comunicarse de mil maneras distintas. En la esfera nuclear hay una enorme cantidad de información, en muchas formas diferentes. Los activos de información son el equipo o los componentes (incluidos los medios) que se utilizan para almacenar, procesar, controlar o transmitir la información.

2.3. A los efectos de su tratamiento y de la seguridad física, la información puede agruparse en objetos de información. Estos se definen como todos los elementos de información que tienen valor para una organización. Por lo general, un objeto de información comprende un conjunto de datos, información o conocimientos que tienen un mismo uso, propósito o riesgo asociado, o una misma forma de almacenamiento o transmisión.

2.4. Es importante entender que la información relacionada con la seguridad física nuclear puede tener valor (posiblemente de diferente índole y magnitud) para cualquiera de las entidades siguientes o para todas ellas:

a) el Estado;
b) las autoridades competentes;
c) las entidades explotadoras de las instalaciones (incluidos terceros, como los proveedores);
d) un posible adversario (personas y entidades organizadas);
e) los medios de comunicación;
f) el público.

DETERMINACIÓN Y PROTECCIÓN DE LA INFORMACIÓN DE CARÁCTER ESTRATÉGICO

2.5. La información de carácter estratégico es aquella cuya divulgación (o modificación, alteración, destrucción o denegación de uso) no autorizada podría comprometer la seguridad física nuclear o ayudar de otra manera a perpetrar un acto doloso contra una instalación u organización nuclear o contra un transporte de materiales nucleares. Esa información puede referirse, por ejemplo, a los arreglos adoptados para la seguridad física nuclear en una instalación, los sistemas,

estructuras y componentes de una instalación, el recorrido y los pormenores de un transporte de materiales nucleares u otros materiales radiactivos, o los detalles sobre el personal de una organización.

2.6. La determinación de la información que cumple con esta definición es uno de los pasos clave en el establecimiento de un programa de seguridad física de la información para garantizar la confidencialidad. En la sección 4 se ofrece orientación más detallada y completa sobre este tema, y en el anexo II se presentan algunos ejemplos ilustrativos.

2.7. La seguridad física de la información de carácter estratégico es necesaria porque el acceso fácil a información que no esté protegida de forma adecuada puede ayudar a los adversarios a planificar o cometer actos dolosos con un esfuerzo o riesgo relativamente bajo. Por ejemplo, si un adversario que estuviera planificando un atentado a una instalación se apoderara del plan de protección física de esta, tendría conocimiento de los obstáculos que debería superar, los efectivos y las armas de las fuerzas de guardia, el tamaño de las fuerzas de respuesta y el tiempo aproximado que tardarían en acudir. También se enteraría de los blancos importantes dentro de la instalación, su ubicación y las medidas adoptadas para protegerlos. Del mismo modo, si un adversario que deseara robar materiales nucleares durante su transporte lograra apoderarse —debido a una protección insuficiente— de un dispositivo que le diera acceso a información detallada sobre el transporte planificado, podría planear el atentado de manera mucho más eficaz. Así pues, la posesión de esa información o de esos activos de información por un adversario aumentaría sus probabilidades de éxito.

2.8. El acceso a la información de carácter estratégico y a los objetos de información de carácter estratégico no debería ser mayor que lo necesario para desempeñar las actividades de una organización. Por consiguiente, la divulgación debería limitarse solo a las personas que estén debidamente autorizadas a acceder a la información, y a las circunstancias en que ese acceso sea necesario. Las reglas de la ‘necesidad de conocer’ y la ‘necesidad de poseer’ son fundamentales para la seguridad física de la información de carácter estratégico. Estas reglas deberían guiar la gestión y el control de los derechos de acceso a la información. Los derechos de acceso deberían examinarse periódicamente, y cuando surja la necesidad.

2.9. Para mantener la confidencialidad es preciso aplicar medidas de seguridad física a cierta información de carácter estratégico y a los activos de información de carácter estratégico (el equipo o los componentes, incluidos los medios, que procesen, manipulen, almacenen o transmitan información de carácter estratégico)

a fin de que no caigan en manos de personas u organizaciones no autorizadas, ya sea externas o internas. En la publicación titulada *Preventive and Protective Measures against Insider Threats* (Medidas de prevención y protección contra las amenazas internas) [5] se ofrece orientación sobre las medidas adecuadas para combatir las amenazas internas. Las medidas de seguridad física deberían basarse en un análisis de los riesgos, y este análisis debería mantenerse actualizado mediante un proceso de exámenes periódicos.

SEGURIDAD FÍSICA DE LA INFORMACIÓN

2.10. La seguridad física de la información, tal como se describe en la presente publicación, se refiere al sistema, programa o conjunto de normas establecidos para garantizar la confidencialidad, integridad y disponibilidad de la información en cualquiera de sus formas. Como mínimo, comprende:

a) la seguridad física de la información en sus soportes materiales (por ejemplo, en papel o medios electrónicos);
b) la seguridad física de los sistemas informáticos, a veces denominada seguridad informática, seguridad de la tecnología de la información (TI) o ciberseguridad (en la publicación *Seguridad informática en las instalaciones nucleares* [6] del OIEA figura más orientación a este respecto);
c) la seguridad física de los activos de información (p. ej., el equipo de almacenamiento y procesamiento de información, y los sistemas y redes de comunicación);
d) la seguridad física de la información sobre los empleados de una instalación y sobre terceros (como los contratistas y proveedores) que pueda comprometer la seguridad de los elementos anteriores;
e) la seguridad física de la información intangible (como los conocimientos).

2.11. Aunque a menudo solo se menciona la confidencialidad, las organizaciones deberían velar por que su programa de seguridad física de la información garantice los tres atributos. La pérdida de la integridad o de la disponibilidad puede repercutir negativamente en la seguridad física nuclear del mismo modo que la pérdida de la confidencialidad, por ejemplo si los usuarios autorizados no tienen acceso oportuno a la información necesaria para cumplir sus deberes (pérdida de la disponibilidad), o si esa información ha sido alterada hasta el punto de inducirlos a error (pérdida de la integridad).

2.12. La seguridad física de la información debería considerarse y aplicarse en el contexto del marco de seguridad física global, porque tiene una estrecha

interdependencia con otros dominios de la seguridad, como la protección física y la seguridad física del personal. Por ejemplo, las medidas de protección física pueden utilizarse para proteger información y activos de información de carácter estratégico, y las medidas de confidencialidad aumentan la dificultad y la incertidumbre de un atentado contra los sistemas de protección física para un adversario. Las lagunas o deficiencias en cualquiera de las esferas de la seguridad física pueden menoscabar la seguridad en las otras esferas, por lo que es indispensable utilizar un enfoque integral que aborde todos los aspectos juntos.

2.13. La seguridad física de la información debería tomar en consideración también el equilibrio necesario entre la seguridad física y otros objetivos, como la seguridad tecnológica, la apertura y la transparencia, y los aspectos operacionales. En la *Colección de Normas de Seguridad del OIEA* se proporciona orientación sobre la seguridad tecnológica.

3. MARCO PARA LA SEGURIDAD FÍSICA DE LA INFORMACIÓN DE CARÁCTER ESTRATÉGICO

3.1. La protección de la información de carácter estratégico de forma fragmentada, en cada instalación por separado, no dará buenos resultados. Se requiere un marco nacional eficaz que prevea la adopción de amplias medidas de seguridad física en todas las instalaciones, emplazamientos y organizaciones (gubernamentales y no gubernamentales) que manejen información de carácter estratégico. El Estado debería crear este marco nacional y, para ello, establecer:

a) la responsabilidad del Estado;
b) un marco jurídico y de reglamentación;
c) una orientación nacional;
d) políticas de seguridad física;
e) sistemas de clasificación.

Las políticas de cada organización también contribuirán al marco global.

RESPONSABILIDADES

3.2. La responsabilidad de velar por la existencia y el funcionamiento eficaz del régimen completo de seguridad física nuclear de un Estado recae en el gobierno

de ese Estado. La garantía de la seguridad física de la información de carácter estratégico es parte integrante del régimen de seguridad física nuclear que el Estado debería aplicar.

3.3. Por lo general, los Estados tienen organizaciones u organismos responsables de la seguridad física nacional global, que en lo sucesivo se denominarán autoridades nacionales de seguridad. Las autoridades nacionales de seguridad suelen tener la responsabilidad de definir la política nacional fundamental en todos los aspectos de la seguridad física. Las políticas e instrucciones de seguridad física emitidas por las autoridades nacionales de seguridad son a menudo de carácter general y no están concebidas específicamente para la seguridad física nuclear. Sin embargo, las autoridades nacionales de seguridad de numerosos Estados tienen políticas y orientaciones para proteger la información de carácter estratégico, por ejemplo, la de uso gubernamental o militar.

3.4. Las autoridades competentes pertinentes del Estado deberían elaborar y publicar políticas y requisitos específicos para la seguridad física de la información de carácter estratégico en las instalaciones y actividades relacionadas con materiales nucleares y otros materiales radiactivos. Por lo general, esas políticas y requisitos se basarán en la política y los requisitos nacionales de seguridad física que hayan establecido las autoridades nacionales de seguridad y estarán en consonancia con ellos, pero tendrán en cuenta la índole especial de las actividades relacionadas con esos materiales. Las autoridades competentes deberían mantener asimismo un estrecho enlace con las autoridades nacionales de seguridad a fin de elaborar la evaluación nacional de la amenaza, o la amenaza base de diseño (en la publicación *Development, Use and Maintenance of the Design Basis Threat* (Elaboración, uso y mantenimiento de la amenaza base de diseño) [7] figura más información a este respecto).

3.5. Cada organización debería establecer su política y sus planes y procedimientos internos para garantizar la confidencialidad, integridad y disponibilidad de toda información de carácter estratégico relacionada con la seguridad física nuclear que posea o maneje, y para proteger los activos de información de carácter estratégico conexos, en cumplimiento de la política de seguridad física nacional y de las leyes y requisitos nacionales pertinentes. Todos los empleados deberían ser plenamente conscientes de la necesidad de garantizar la seguridad física de la información, y aplicar las normas y procedimientos de seguridad física de la información de sus organizaciones.

MARCO JURÍDICO Y DE REGLAMENCIÓN PARA LA SEGURIDAD FÍSICA DE LA INFORMACIÓN DE CARÁCTER ESTRATÉGICO

3.6. Los requisitos para el mantenimiento de la seguridad física nuclear dentro de las fronteras de un Estado deberían aplicarse a todos los ministerios, departamentos, organismos y otras organizaciones que se ocupen de los asuntos que el Estado haya definido como necesarios para la seguridad física nuclear nacional. El Estado puede imponer estos requisitos mediante leyes, reglamentos u otros instrumentos jurídicos vinculantes. Los requisitos para la seguridad física nuclear de un Estado deberían incluir los requisitos de seguridad física de la información. Además, debería existir legislación que defina las sanciones o castigos que se impondrán a las personas u organizaciones que incumplan esos requisitos de seguridad física de la información. Esa legislación podrá contener secciones que definan la gravedad de determinados tipos de violación de la confidencialidad o de otros atributos de la información, y las sanciones correspondientes.

3.7. Las facultades reguladoras de las autoridades competentes deberían permitirles imponer obligaciones a quienes mantengan información de carácter estratégico. Las leyes que se promulguen a tal efecto deberían prever sanciones o castigos para los casos de divulgación no autorizada. La legislación debería establecer asimismo la obligación de los ministerios, departamentos, organismos y otras organizaciones del Estado de proporcionar a las autoridades competentes todo el apoyo necesario para que puedan cumplir su tarea de garantizar la seguridad física de la información de carácter estratégico.

PREPARACIÓN DE LA ORIENTACIÓN NACIONAL

3.8. La política estatal sobre la seguridad física de la información debería definir el tipo de información que el Estado desea proteger, e indicar cómo se garantizará su seguridad física. Esto se establece, por lo general, en un manual de seguridad física preparado por las autoridades nacionales de seguridad del Estado (u otra autoridad adecuada). Un manual de este tipo puede no contener ninguna mención directa de la información de carácter estratégico para la seguridad física nuclear. Sin embargo, especificará las diferentes clases de información e indicará su grado de sensibilidad y, en consecuencia, el nivel de seguridad física que se habrá de aplicar, y cómo se deberían marcar los objetos de información para que su nivel de sensibilidad esté perfectamente claro.

3.9. La orientación detallada sobre la información que haya de considerarse de carácter estratégico debería ser proporcionada por las autoridades competentes pertinentes, en estrecha consulta con las autoridades nacionales de seguridad y con la participación de los usuarios de los materiales nucleares y otros materiales radiactivos. Tal orientación se basará normalmente en las disposiciones de la evaluación nacional de la amenaza, si esta existe, y debería ser coherente con ellas. Este tipo de orientación, que a veces se denomina política de clasificación, suele dividir las clases de información en una serie de temas conexos, e indica la importancia relativa de una determinada información y, por consiguiente, en qué medida tiene carácter estratégico, y el grado de seguridad física que se debe aplicar.

3.10. A nivel de la organización, la importancia de una determinada información puede indicarse en el plan de seguridad física de esta, que debería describir de qué manera se habrá de proteger la diferente información de carácter estratégico de conformidad con la legislación y los reglamentos nacionales.

POLÍTICAS DE SEGURIDAD FÍSICA

3.11. Además de publicar políticas de seguridad física de la información que cumplan con los requisitos nacionales, las autoridades competentes deberían describir en detalle cómo se habrán de aplicar esos requisitos a las instalaciones y actividades que se relacionen con materiales nucleares y otros materiales radiactivos.

3.12. La política de seguridad física nuclear del Estado debería apoyar firmemente la seguridad física de la información. Para ello, debería alentar la publicación y el mantenimiento de una política de seguridad física de la información completa y apropiada, que sea aplicable a todas las instalaciones y actividades que se relacionen con materiales nucleares y otros materiales radiactivos, así como a cualquier otro emplazamiento en que se conserve información de carácter estratégico. El objetivo de la política será garantizar la protección de la información de carácter estratégico contra cualquier forma de vulneración.

3.13. Toda organización e instalación que maneje información de carácter estratégico debería luego elaborar su propia política específica de seguridad física de la información, sobre la base de la que hayan publicado las autoridades competentes, cuando sea el caso. Esta política debería darse a conocer en toda la organización, de una forma que sea pertinente, accesible y comprensible para los usuarios previstos. En la sección 6 se ofrecen más orientaciones sobre

el establecimiento de un programa de gestión de la seguridad física de la información, incluidas las políticas correspondientes.

SISTEMAS DE CLASIFICACIÓN DE LA INFORMACIÓN

3.14. Para aplicar sistemas de seguridad física de la información y los controles correspondientes se requieren recursos y tiempo. No es posible ni conveniente asegurar de la misma manera toda la información de un emplazamiento o instalación. Una parte de la información no tendrá carácter estratégico y no requerirá ninguna medida de protección particular. Incluso en el caso de la información de carácter estratégico, los diferentes objetos de información pueden precisar diferentes niveles de seguridad física. Por consiguiente, es importante determinar cuál es la información que tiene carácter estratégico y qué nivel de seguridad física se debe aplicar. Las autoridades competentes de cada Estado deberían definir la información sobre los materiales nucleares, otros materiales radiactivos y las instalaciones y actividades conexas que tiene carácter estratégico. Con respecto al transporte internacional, el Estado debería determinar cuál información se habrá de proteger, teniendo en cuenta, posiblemente, la coherencia con los otros Estados que participen en el transporte internacional.

3.15. Para establecer el valor de un determinado activo de información se recomienda utilizar un enfoque basado en el riesgo, que tome en consideración los daños y las consecuencias que puedan dimanar de su vulneración. Es importante señalar que toda vulneración de la información en una instalación puede afectar a otras instalaciones que posean activos de información similares; por consiguiente, los daños y las consecuencias que se consideren deberían incluir los efectos que se puedan producir en la seguridad física nuclear de otras instalaciones, y no sólo los que afecten a un emplazamiento específico. Debería prestarse especial atención a las acumulaciones de información y a los posibles puntos de fallo (por ejemplo, los activos de información que dependan de una única red o de un único suministro de electricidad). Los resultados de esta evaluación podrían utilizarse para determinar el nivel de seguridad física requerido para cada objeto de información, de conformidad con el sistema de clasificación que utilice cada Estado.

3.16. Debería establecerse y mantenerse un sistema nacional de clasificación que agrupe la información en distintas categorías, de modo tal que la divulgación no autorizada de cualquiera de los elementos de información de una misma categoría tenga consecuencias parecidas y que, por lo tanto, toda la información de una categoría particular se deba someter a los mismos requisitos de seguridad

física. Este sistema debería ser nacional, y no específico de una determinada industria o elaborado por una instalación particular. En muchos casos, los Estados ya tienen sistemas de clasificación de este tipo, pero esos sistemas pueden no abordar el caso específico de la información relativa a la seguridad física nuclear. El sistema se basa en un enfoque que tiene en cuenta el riesgo, y en que las posibles consecuencias de la divulgación no autorizada de la información determinan la categoría en que esta se clasificará y los requisitos de seguridad física correspondientes.

3.17. Deberían estudiarse cuidadosamente el número de categorías de clasificación que se establecerán y los beneficios que reportará su utilización. Los sistemas muy complejos pueden ser engorrosos y poco prácticos, mientras que los muy sencillos pueden proporcionar una clasificación demasiado imprecisa. También habría que proceder con cuidado al asignar un nivel de clasificación a los objetos de información. La clasificación en una categoría de seguridad más estricta que la que realmente se justifica puede generar gastos adicionales innecesarios, mientras que la clasificación en un nivel inferior al requerido puede exponer la información a un riesgo de vulneración inaceptable. La clasificación en una categoría demasiado alta puede también estar en conflicto con las políticas de transparencia o crear una situación en que la clasificación pierda utilidad para los usuarios de la información.

3.18. Un sistema de clasificación de la información de carácter estratégico, con categorías que indiquen la sensibilidad de cada objeto de información particular, podría comprender los siguientes niveles[1]:

a) SECRETO;
b) CONFIDENCIAL;
c) RESERVADO.

3.19. Otras etiquetas pueden indicar las restricciones a la distribución de la información que dimanen de su clasificación, por ejemplo:

a) prohibida la distribución ulterior;
b) distribución controlada por el autor;
c) para uso oficial;

---

[1] En muchos Estados existe además el nivel ESTRICTAMENTE SECRETO, pero en la mayoría de ellos este nivel no se utiliza casi nunca en el sector civil. Por lo general se aplica en los sectores militares y de armamentos.

d) distribución reservada;
e) disponible para uso público.

3.20. En el anexo I se dan ejemplos de las definiciones de los niveles de clasificación SECRETO, CONFIDENCIAL y RESERVADO.

4. DETERMINACIÓN DE LA INFORMACIÓN DE CARÁCTER ESTRATÉGICO

4.1. El primer paso para clasificar y proteger la información es determinar cuál se considera de carácter estratégico.

4.2. Debería estudiarse la posibilidad de establecer controles de seguridad física por lo menos para los siguientes tipos de información, que podrían afectar a la seguridad física nuclear[2]:

a) los detalles de los sistemas de protección física y de cualquier otra medida de seguridad física que se haya establecido para los materiales nucleares, otros materiales radiactivos y las instalaciones y actividades conexas, incluida la información sobre las fuerzas de guardia y de respuesta;
b) la información relativa a la cantidad y forma de los materiales nucleares u otros materiales radiactivos que se utilicen o mantengan almacenados, incluida la información sobre la contabilidad de los materiales nucleares;
c) la información relativa a la cantidad y forma de los materiales nucleares u otros materiales radiactivos que se transporten;
d) los detalles sobre los sistemas informáticos, incluidos los sistemas de comunicación, que procesen, manejen, almacenen o transmitan información que sea directa o indirectamente importante para la seguridad tecnológica y física;
e) los planes de contingencia y de respuesta para los sucesos relacionados con la seguridad física nuclear;
f) la información personal sobre los empleados, proveedores y contratistas;
g) la información sobre las evaluaciones de la amenaza y las alertas de seguridad;

[2] Esta lista no pretende incluir todas las posibilidades, pero debería proporcionar un punto de partida para el examen.

h) los detalles sobre la tecnología de carácter estratégico;
i) los detalles sobre las vulnerabilidades o los puntos débiles de los elementos arriba mencionados;
j) la información histórica sobre cualquiera de los elementos arriba mencionados.

4.3. Una parte de esta información, por ejemplo la información personal, puede estar sujeta también a requisitos de seguridad específicos establecidos en otras leyes nacionales o en las políticas de las empresas.

4.4. En el anexo II figuran ejemplos de tipos específicos de información correspondientes a las categorías enumeradas en el párrafo 4.2, con una indicación de si se consideran normalmente información de carácter estratégico o no, y por qué motivo.

5. INTERCAMBIO Y DIVULGACIÓN DE LA INFORMACIÓN DE CARÁCTER ESTRATÉGICO

5.1. En muchos casos existirá una necesidad legítima de intercambiar información de carácter estratégico de manera continua, por ejemplo entre los organismos adecuados de un Estado, entre las organizaciones que manipulan materiales nucleares u otros materiales radiactivos y las autoridades competentes pertinentes, o entre diferentes Estados. De igual modo, a veces será necesario comunicar información de carácter estratégico a otras organizaciones o al público, en circunstancias particulares. Tanto el intercambio como la divulgación deberían gestionarse de modo que la información de carácter estratégico no caiga inadvertidamente en manos de quienes no necesiten conocerla.

INTERCAMBIO DE INFORMACIÓN

5.2. A veces es preciso compartir cierta información de carácter estratégico con los organismos autorizados del Estado o con empresas y organizaciones que necesitan conocer esa información. Ese intercambio de información puede generar aumentos de la eficiencia que no se darían si cada entidad tuviera que elaborar y manejar la información independientemente de las demás. También hay ocasiones en que el hecho de no intercambiar información puede menoscabar

la seguridad física o debilitar la planificación, el diseño y la aplicación globales de las medidas de seguridad física. Además, puesto que en muchos casos la responsabilidad por la seguridad física nuclear no recae en un único organismo, empresa u organización, puede ser preciso con frecuencia que quienes comparten la responsabilidad por la seguridad física intercambien información. Por ejemplo, a menudo es necesario, para la seguridad física nacional, que las autoridades competentes transmitan información de carácter estratégico a las autoridades nacionales de seguridad y viceversa, como en el caso de los cambios en las evaluaciones de la amenaza o de la información sobre los sucesos relacionados con la seguridad física, que deberían comunicarse oportunamente a las partes pertinentes para que sea posible ajustar las medidas de seguridad e intercambiar experiencias operacionales, como base para la mejora continua. Además de las consideraciones relativas a la seguridad física, el intercambio de información puede ser necesario también para apoyar otros objetivos, como las necesidades operacionales, comerciales y de evaluación de la seguridad global.

5.3. La naturaleza y el alcance del intercambio de esa información deberían basarse en primer lugar en el cumplimiento de la legislación o los reglamentos nacionales, y luego en un equilibrio entre los beneficios que reporte el intercambio y las necesidades de seguridad física. Las normas para el traspaso de información entre esas autoridades deberían regirse por los procedimientos de seguridad física que se apliquen en cada Estado. El establecimiento de un enfoque común dentro del Estado puede evitar la divulgación inapropiada de información de carácter estratégico.

5.4. A menudo es necesario también intercambiar cierta información con otros Estados u organizaciones internacionales pertinentes. En tales casos, debería existir un acuerdo que garantice que el receptor protegerá esa información de carácter estratégico en un grado compatible con los requisitos que aplique el propietario de la información. La seguridad física de la información puede garantizarse mediante un tratado o acuerdo bilateral o multilateral que defina de qué manera se protegerá la información para evitar su divulgación. Tales acuerdos describirán normalmente las medidas de protección que habrán de aplicarse a la información de carácter estratégico correspondiente a los diferentes niveles de clasificación de cada Estado. También deberían tener en cuenta de qué manera los requisitos particulares de un Estado (como la legislación sobre la libertad de información, véase el párr. 5.6) pueden afectar al manejo de la información de carácter estratégico de otros Estados.

DIVULGACIÓN DE INFORMACIÓN

Necesidad de divulgación

5.5. La mayoría de los Estados tienen leyes que tratan sobre la seguridad física de la información de importancia para los intereses nacionales. Tales leyes especifican las sanciones que se impondrán a las personas, sean nacionales del Estado o no, que infrinjan las leyes sobre la confidencialidad de esa información. Además, generalmente hay legislación que regula el acceso de las personas a la información oficial del gobierno, y puede haber mecanismos para resolver los desacuerdos entre el gobierno y otras partes con respecto a la información que pueda retenerse para proteger la seguridad nacional.

5.6. Varios Estados tienen legislación sobre la libertad de información u otras leyes que permiten a los particulares solicitar acceso a información que obre en poder de las autoridades. Por lo general, la única información que pueden retener las autoridades es la de las clases incluidas en las exenciones especificadas, como la información relacionada con la defensa nacional o la información privada y personal. En algunos Estados, un elemento que lleve una marca de clasificación no estará automáticamente exento del deber de divulgación.

5.7. Otras leyes y reglamentos pueden exigir la divulgación de ciertos tipos de información, que a veces incluirán información de carácter estratégico. Un ejemplo de ello es la legislación ambiental que exige la comunicación pública de determinada información. Se debería velar por que esas leyes eximan de esta obligación a la información que pueda afectar a la seguridad nacional o a la seguridad física de terceros.

Preparación de orientaciones sobre la divulgación

5.8. Deberían elaborarse orientaciones específicas para ayudar a las organizaciones e instalaciones a decidir cuál información de carácter estratégico se puede divulgar. Al preparar esas orientaciones, el organismo gubernamental encargado consultará normalmente con otros departamentos del gobierno y con las organizaciones pertinentes. Mediante la indicación del tipo de información que se considere inapropiado divulgar, las orientaciones deberían tener por objeto prevenir la divulgación no autorizada de información de carácter estratégico (véase también el anexo II).

5.9. Los Estados deberían examinar la necesidad de proporcionar orientación específica sobre los siguientes aspectos:

a) el grado de sensibilidad de ciertos tipos de información de carácter estratégico, sobre la base de las consecuencias de su divulgación;
b) los tipos de información que se pueden divulgar, en qué circunstancias, a quién y por cuáles métodos en particular;
c) las condiciones aplicables a la divulgación de información;
d) los procesos para examinar el posible carácter estratégico de la información antes de su presentación al público, por ejemplo en ponencias hechas en conferencias, publicaciones en sitios web o especificaciones técnicas;
e) las medidas que deberían adoptarse en caso de divulgación no autorizada de información de carácter estratégico, ya sea intencional o involuntaria, o de otro tipo de incumplimiento de los requisitos de seguridad física de la información.

5.10. Las orientaciones deberán irse modificando. Las circunstancias evolucionan, y la información que en un momento dado pueda considerarse de carácter estratégico y no adecuada para la divulgación podría ser mucho menos delicada y más apta para la divulgación en un momento posterior (o viceversa). Por consiguiente, las orientaciones deberían examinarse y actualizarse en forma periódica, y cuando se produzcan cambios importantes en la política o las circunstancias.

5.11. En general, reducir el nivel de seguridad física aplicado a una información particular, cuando proceda, no planteará problemas. En cambio, reclasificar la información en una categoría más estricta puede ser imposible o ineficaz, si ya ha sido objeto de una divulgación más amplia. Esto debería tenerse en cuenta al efectuar la clasificación inicial, considerando el equilibrio adecuado entre la confidencialidad y precaución, por una parte, y la disponibilidad y transparencia, por otra. Debería establecerse un marco cronológico predeterminado para el examen periódico de las clasificaciones, pero también deberían introducirse modificaciones cada vez que sea necesario, por ejemplo, cuando ocurran cambios significativos en las circunstancias.

5.12. Todas las solicitudes de divulgación de información de carácter estratégico que reciba una organización deberían examinarse aplicando las mismas orientaciones o criterios y, si es posible, tramitarse por conducto de una única oficina central de la organización. Una técnica que se utiliza comúnmente para obtener acceso indebido a información de carácter estratégico consiste en presentar múltiples solicitudes a diferentes personas o dependencias de una misma organización. Si esas solicitudes se tramitan por separado, sin coordinación alguna, es posible que se den respuestas diferentes y se revele información de carácter estratégico que de otro modo no se habría divulgado.

6. MARCO DE GESTIÓN DE LA CONFIDENCIALIDAD

6.1. En la sección 3 se describe el marco de alto nivel para la seguridad física de la información de carácter estratégico. En la presente sección se examinan con más detalle los componentes que ha de incluir un marco de ese tipo en una instalación u organización, situándolos en el contexto del sistema de gestión.

6.2. Debería existir un sistema de gestión que establezca las políticas y los objetivos y que permita alcanzar estos últimos de manera eficiente y eficaz. Un sistema de gestión integrado (véanse la publicación Nº GS-R-3 de la *Colección de Normas de Seguridad del OIEA*, *Sistema de gestión de instalaciones y actividades* [8], y las orientaciones correspondientes) es un elemento de apoyo fundamental para una cultura de la seguridad física nuclear. Muchas de las actividades que tienen lugar en las instalaciones se controlan mediante sistemas de gestión. En una situación ideal, estos integran los elementos económicos, ambientales y relativos a la seguridad física y tecnológica, la salud y la calidad en un único proceso de gestión o en un conjunto de sistemas integrados que se refuerzan mutuamente. La seguridad física de la información debería integrarse al sistema de gestión que exista en la instalación u organización para garantizar la confidencialidad, integridad y disponibilidad de la información.

6.3. La garantía de la confidencialidad, integridad y disponibilidad de la información de carácter estratégico exige una asignación eficaz de las funciones y responsabilidades, una clasificación que indique la información que es de carácter estratégico y se debe proteger, el motivo por el que se debe proteger y en qué nivel de seguridad (véase la sección 4), decisiones sobre la forma de proteger esa información, la aplicación de las medidas de seguridad necesarias y una respuesta (incluida la recuperación) en caso de vulneración, robo o pérdida de esa información.

6.4. El marco de gestión que se explica en los párrafos siguientes se aplica a todos los niveles de gestión de las organizaciones que poseen o manejan información de carácter estratégico.

RESPONSABILIDADES

6.5. La administración tiene la responsabilidad global de velar por que exista un sistema de seguridad física de la información eficaz en toda la instalación u

organización, a fin de proteger la información de carácter estratégico. Todo el personal que maneje información de carácter estratégico tendrá la responsabilidad de garantizar su seguridad física de conformidad con la legislación nacional correspondiente y con las políticas y procedimientos de la organización.

Responsabilidades de la administración

6.6. Las responsabilidades de la administración comprenden normalmente lo siguiente:

a) asumir la responsabilidad global de la seguridad física de la información de carácter estratégico y de los activos de información de carácter estratégico;
b) velar por que se cumplan las leyes y los reglamentos pertinentes;
c) asignar las responsabilidades por la seguridad física en la organización;
d) impartir una capacitación y formación efectivas sobre la seguridad física;
e) velar por que se establezca una política eficaz de seguridad física de la información;
f) proporcionar suficientes recursos para aplicar un programa eficaz de seguridad física de la información;
g) velar por el desarrollo del programa de seguridad física de la información y de los planes y procedimientos conexos;
h) garantizar una eficaz gestión del cambio en relación con los planes, procedimientos y políticas;
i) velar por que periódicamente se realicen auditorías, exámenes y revisiones de las políticas y procedimientos de seguridad física de la información.

Responsabilidades relativas a la clasificación

6.7. Las autoridades competentes pertinentes deberían impartir orientación sobre la categoría que se haya de asignar a un objeto de información mediante la publicación de una guía o de orientaciones para la clasificación. Este documento agrupará la información relativa a determinados temas e indicará la sensibilidad de la información. Quienes generen información de carácter estratégico deberían utilizar una guía de este tipo cuando adopten decisiones sobre el nivel de clasificación adecuado.

6.8. Una vez que la información se haya divulgado, quienes reciban o tengan en su poder algún objeto de información de carácter estratégico no deberían modificar el nivel de clasificación aplicado a la información sin la autorización de su autor. Quienes reciban o posean copias podrán y, si corresponde, deberán impugnar el nivel de clasificación aplicado. Por ejemplo, si la autoridad competente recibe

de un explotador información que se ha clasificado incorrectamente según la legislación aplicable, debería dar instrucciones al explotador para que modifique la clasificación.

6.9. Cuando la organización en que se produjo la información haya dejado de existir, la responsabilidad recaerá en su sucesor. Si no es posible localizar a un sucesor, el poseedor del objeto de información de carácter estratégico podrá, si procede, modificar su nivel de clasificación, previa consulta con las autoridades competentes que corresponda.

6.10. Si se modifica el nivel de clasificación aplicado a un objeto de información o a un tipo de objeto de información, el cambio debería, en lo posible, notificarse a todos los que puedan resultar afectados. Esto puede incluir a quienes posean la información en ese momento o la hayan poseído en el pasado, así como a quienes puedan utilizarla en el futuro.

PLAN DE SEGURIDAD FÍSICA

6.11. Todas las organizaciones que manejen información de carácter estratégico deberían tener un plan de seguridad física. Este plan debería contener una sección detallada consagrada específicamente a la seguridad física de la información de carácter estratégico. Los requisitos pertinentes del plan de seguridad física deberían comunicarse a los empleados y contratistas que trabajen para la organización. Es esencial que los empleados y contratistas comprendan sus responsabilidades.

POLÍTICA Y PROCEDIMIENTOS DE SEGURIDAD FÍSICA

Plan de seguridad física de la información

6.12. La responsabilidad por la seguridad física de la información debería integrarse en la jerarquía de políticas y procedimientos de una organización. Como mínimo, esto debería incluir lo siguiente:

a) Una definición de la seguridad física de la información y una declaración de sus objetivos generales, su ámbito de aplicación y su importancia.
b) Una definición de las funciones y responsabilidades, incluido el establecimiento de un coordinador que dirija y gestione la seguridad física de la información.

c) El cumplimiento de los requisitos de seguridad física de la información, incluidos los jurídicos, reglamentarios y contractuales.
d) El establecimiento de un plan de gestión del riesgo para reducir los riesgos a un nivel aceptable, definido por el Estado, aplicando controles adecuados sobre la base de una evaluación del riesgo. En el caso de una instalación nuclear, el plan de gestión del riesgo debería ser aprobado por la autoridad competente u otra autoridad que designe el Estado.
e) La vigilancia y el examen periódicos de los arreglos establecidos para velar por que la política, las normas y procedimientos sigan siendo pertinentes y eficaces.
f) La labor de formación y capacitación necesaria para velar por que el personal, los contratistas y otros empleados tengan el conocimiento de la política, los procedimientos y la práctica que sea adecuado y necesario para el cumplimiento de sus funciones y comprendan cabalmente sus responsabilidades (incluidas sus obligaciones jurídicas).
g) Las consecuencias (es decir, las penas o sanciones) del incumplimiento de los requisitos de seguridad física de la información o de la negligencia culpable en la protección de la información de carácter estratégico.
h) Documentación de referencia que respalde la política, por ejemplo procedimientos más detallados para determinados sistemas o normas de seguridad física que los usuarios deban respetar.

Aspectos del plan de seguridad física de la información que se aplican específicamente a la información de carácter estratégico

6.13. Con respecto específicamente a la protección de la información de carácter estratégico, el plan debería incluir también:

a) el ciclo de vida de la información: una definición de los procesos utilizados para crear, identificar, clasificar, marcar, manejar, utilizar, almacenar, transmitir, reclasificar, reproducir y destruir la información de carácter estratégico;
b) los requisitos de seguridad física aplicables a la información de carácter estratégico, con la debida consideración de los objetivos de la confidencialidad, integridad y disponibilidad de la información;
c) la restricción del acceso a la información de carácter estratégico y a los activos de información de carácter estratégico a quienes necesiten ese acceso para desempeñar sus funciones, quienes posean la autoridad necesaria y quienes se hayan sometido a una verificación de la probidad acorde con el nivel de clasificación de la información;

d) la transmisión de la información de carácter estratégico de un modo que reduzca a un nivel aceptable el riesgo de vulneración o de interceptación, modificación o perturbación no autorizadas.

Procedimientos para el manejo de la información de carácter estratégico

6.14. La gestión efectiva de los riesgos derivados de las amenazas a la confidencialidad, integridad y disponibilidad de la información exigirá la elaboración de medidas eficaces contra esas amenazas. Este proceso entrañará necesariamente una combinación de controles de la seguridad física correspondientes a los ámbitos de la seguridad física de la información, la protección física y la seguridad física del personal.

6.15. La seguridad física del personal, que incluye las verificaciones de la probidad, garantiza que solo tengan acceso a la información de carácter estratégico las personas que el Estado considere suficientemente dignas de confianza. Para la información clasificada en una categoría relativamente baja, la organización debería decidir si se requiere o no algún control de quienes necesiten acceso a ella; en caso afirmativo, podría ser suficiente un control limitado de los antecedentes de la persona. Para el acceso a información de una categoría más alta, se requerirá un conjunto más amplio de controles de los antecedentes de la persona para determinar su probidad. El proceso de seguridad física del personal debería incluir también la firma de un acuerdo de no divulgación entre la persona y la autoridad competente o la organización respectiva.

6.16. La protección física combina a menudo un cierto grado de control estricto del acceso por medio de un perímetro de seguridad con uno o más niveles de otras medidas de protección física más próximas a los activos de información, como cajas fuertes u otros lugares seguros. Pueden utilizarse los mismos principios para garantizar la protección física de la información y de los activos de información.

6.17. Las medidas de seguridad física de la información incluyen controles técnicos, administrativos y de procedimiento aplicados a lo largo de todo el ciclo de vida de los objetos de información, que abarca su creación, manejo, almacenamiento, transmisión, reproducción y destrucción. Entre otras cosas, las medidas de seguridad física de la información comprenden lo siguiente:

a) la gestión administrativa para dirigir, mantener y desarrollar la seguridad física de la información (incluidos los servicios prestados por terceros);
b) la seguridad física del personal, particularmente en las fases de la contratación y al comienzo y el final del empleo;

c) la seguridad física de las zonas en que se utilizan, manejan o mantienen información de carácter estratégico o activos de información de carácter estratégico;
d) la seguridad física en el manejo de la información digital y manual: la seguridad física de las estaciones de trabajo, la protección contra virus y programas dañinos, la supresión y destrucción de información y los procesos manuales;
e) la seguridad física de la red de comunicaciones (teléfonos, correos electrónicos, Internet y redes de área local): política, autentificación de los usuarios, identificación del equipo, controles de la segregación, la conexión y el encaminamiento, y vigilancia;
f) la seguridad física del equipo: control del acceso, registro de la utilización, gestión de las piezas de repuesto, unidades de apoyo del equipo de importancia crítica, dispositivos de apoyo para el suministro de electricidad, documentación y mantenimiento, cableado y seguridad física de los medios de comunicación;
g) la seguridad física de los programas informáticos: control del acceso, registro de las actividades de los usuarios y superusuarios, gestión de los respaldos, contratación del mantenimiento, gestión de la configuración y las versiones, uso de programas informáticos legales y registrados, ensayos de la vulnerabilidad y pruebas de comportamiento de los sistemas en condiciones de error;
h) la seguridad física del uso de los sistemas de información: control de los derechos de los usuarios, reconocimiento y verificación de los usuarios, conexión a servicios, sistemas y equipos, gestión de contraseñas, supervisión del uso, y la regla de las dos personas (es decir, del control por dos personas) para las operaciones de importancia crítica;
i) la clasificación y los procedimientos correspondientes para el manejo de la información;
j) la protección de la privacidad.

6.18. El manejo de la información de carácter estratégico debería regirse por procedimientos que sean conformes con lo prescrito en la sección sobre seguridad física de la información que figure en la política y orientación nacional sobre la seguridad física, incluida toda interpretación que hayan establecido al respecto las autoridades competentes del Estado. En el plan de seguridad física de la información deberían describirse las normas de desempeño mínimo en los distintos niveles de seguridad. Un ejemplo de ello sería la metodología criptográfica utilizada para la transmisión electrónica de la información.

Sistema de gestión de los derechos

6.19. Debería existir un sistema de gestión que establezca el control de cómo, cuándo y por qué motivos debería autorizarse el acceso de determinados titulares o usuarios de información de carácter estratégico a la información de carácter estratégico y a los activos de información de carácter estratégico. El sistema de gestión de los derechos incluye normalmente:

a) una estructura definida de responsabilidades para la gestión de las autorizaciones;
b) procesos definidos para la función que esté autorizada a designar quién tiene derecho a acceder a la información y los activos de información de carácter estratégico;
c) procesos definidos para verificar, controlar y supervisar la función de asignación del acceso;
d) procesos definidos para determinar cuánto tiempo debería durar una autorización a acceder a información y activos de información de carácter estratégico;
e) procesos definidos para revocar una autorización a acceder a información y activos de información de carácter estratégico;
f) procesos definidos para mantener la plena rastreabilidad de la gestión de los derechos en todos los pasos de la cadena de gestión por la que se autorice el acceso a información y activos de información de carácter estratégico.

Exámenes periódicos

6.20. Las políticas, los planes y los procedimientos de seguridad física deberían evolucionar con arreglo a los cambios en las circunstancias. Una forma eficaz de velar por que se mantengan actualizados puede ser establecer un plazo para su examen en el propio documento de política. Si se produjera un cambio fundamental en las circunstancias que pudiera dar lugar a una modificación de la política, por ejemplo un cambio en la legislación, podría realizarse un examen antes de la fecha prevista. La estructura de los exámenes debería aplicarse a la política en todos los niveles en que haya responsabilidades relativas a la seguridad física nuclear.

CULTURA DE LA SEGURIDAD FÍSICA

6.21. El desarrollo, fomento y mantenimiento de una robusta cultura de la seguridad física nuclear es un elemento esencial de un régimen de seguridad

física nuclear. Esto es especialmente cierto en el caso de la seguridad física de la información, en que las personas y los procesos suelen ser el factor clave para proteger la información.

6.22. Como parte de una cultura efectiva de la seguridad física nuclear [9], todas las organizaciones, los empleados y los contratistas deberían tener una comprensión completa de sus responsabilidades relativas a la seguridad física y de la importancia de esas responsabilidades. Es esencial que los empleados y contratistas reciban una capacitación y formación sobre la seguridad física que sea acorde con sus responsabilidades y necesidades respectivas.

6.23. Los empleados y contratistas que tengan responsabilidades específicas en materia de seguridad física y los que tengan acceso a información de carácter estratégico, así como la administración en todos los niveles de una organización, deben recibir capacitación e instrucciones específicas con respecto a sus responsabilidades. También es importante que otras categorías de empleados (como los mensajeros, el personal de seguridad y el personal administrativo) que manejen información de carácter estratégico sin tener necesariamente conocimiento de su contenido reciban capacitación sobre la seguridad física relacionada específicamente con sus responsabilidades.

6.24. Las actividades aisladas de capacitación sobre la seguridad física de la información no refuerzan adecuadamente la preparación y, a la larga, pueden permitir que se instaure una actitud de complacencia entre los empleados. Toda persona que maneje información de carácter estratégico, con inclusión de todo el personal directivo, los empleados y los contratistas, debería recibir capacitación continua en el trabajo y asistir periódicamente a cursos de actualización de los conocimientos. Deberían llevarse registros de la capacitación oficial que hayan recibido y aprobado todos los empleados y contratistas. Es especialmente importante que cualquier cambio en las normas y procedimientos de seguridad física se dé a conocer a todos los empleados y contratistas pertinentes tan pronto como sea posible. En el anexo III se propone un formato y un contenido para un programa de capacitación y sensibilización.

ARREGLOS DE SEGURIDAD FÍSICA DE LA INFORMACIÓN CONCERTADOS CON TERCEROS

6.25. Una autoridad competente o una organización necesitarán a veces que un tercero les preste servicios o les suministre bienes que entrañen información de carácter estratégico. Estos arreglos deberían concertarse utilizando acuerdos

jurídicos tales como una licencia o un contrato, e incluir acuerdos de no divulgación. En los arreglos con terceros puede ser necesario confiar al cuidado de estos información que sea de carácter estratégico. Para no poner en peligro esa información, debería existir una política o legislación nacional que regule los arreglos que entrañen información de carácter estratégico, y las organizaciones e instalaciones que suscriban esos contratos deberían estar obligadas a aplicarla.

6.26. Incumbirá a las organizaciones contratantes, cuando negocien esas relaciones con terceros, asegurarse de que toda información de carácter estratégico que se confíe a esas partes esté protegida de manera satisfactoria. Las medidas de seguridad que se adopten para proteger la información de carácter estratégico deberían ser proporcionadas a los riesgos y conformes a la política establecida.

6.27. En este contexto, las autoridades competentes y las organizaciones deberían cerciorarse de que los terceros:

a) tengan procesos y procedimientos de seguridad física de la información que, como mínimo, sean equivalentes a los requisitos establecidos en los arreglos de seguridad física de la propia organización;
b) tengan un coordinador que dirija y gestione la seguridad física en la empresa contratante;
c) posean un sistema que garantice que todo el personal con acceso a la información de carácter estratégico que obre en su poder se haya sometido a una verificación de la probidad a un nivel apropiado;
d) velen por que el acceso a la información y los activos de información de carácter estratégico se limite solo a las personas que tengan realmente necesidad de conocerla y cuenten con la autorización de seguridad adecuada;
e) transmitan la información de manera conforme con la legislación nacional y la política local y de modo tal que la información no se exponga a ningún tipo de vulneración;
f) velen por que la información no se ponga en conocimiento de ninguna parte o persona no autorizadas;
g) velen por que todo el personal tenga un conocimiento adecuado de la política y la práctica de la seguridad física y comprenda plenamente sus responsabilidades (incluidas sus obligaciones jurídicas);
h) cuenten con procedimientos para hacer frente a los sucesos relacionados con la seguridad física de la información;
i) velen por que los arreglos de seguridad física adoptados en sus locales sean inspeccionados periódicamente por las autoridades competentes o

las organizaciones contratantes, de conformidad con las disposiciones del acuerdo, para verificar que se cumplan los requisitos de seguridad establecidos en el acuerdo.

INSPECCIONES Y AUDITORÍAS

6.28. La realización sistemática de actividades de garantía es esencial para mantener un programa de seguridad física de la información. Es preciso tener la garantía de que los programas de seguridad física establecidos en las organizaciones que poseen información de carácter estratégico, incluidos los terceros con los que trabajen, cumplen en todos los aspectos con la política y los reglamentos nacionales. Cuando proceda, las medidas de seguridad física de la información deberían ser examinadas por las autoridades competentes antes de que se apruebe oficialmente su uso. La garantía puede lograrse mediante inspecciones o auditorías oficiales periódicas de la organización o instalación. Las auditorías son normalmente una actividad interna de la organización, mientras que las inspecciones pueden ser tanto internas como externas. Además, las inspecciones pueden ser anunciadas o no anunciadas (es decir, con o sin previo aviso).

6.29. Las inspecciones internas y las auditorías corren a cargo de la propia organización y tienen por objeto determinar si el programa de seguridad física cumple con el plan de seguridad física de la información aprobado y verificar su conformidad con los requisitos reglamentarios. Estas inspecciones permiten a la organización controlar su propio cumplimiento con una frecuencia mayor que la de las inspecciones externas. Además, las inspecciones o auditorías realizadas por personal que está familiarizado con los requisitos, procedimientos y sistemas internos permiten detectar oportunidades de introducir mejoras que difieren de las que se pueden descubrir en una inspección externa.

6.30. Las inspecciones externas son realizadas por las autoridades competentes u otras organizaciones externas autorizadas. La finalidad de estas inspecciones es evaluar el grado de cumplimiento de la política de seguridad física de la información del Estado. Las inspecciones externas ofrecen una evaluación independiente de las inspecciones que efectúa la propia organización. Cuando se empleen auditores externos, deberán tenerse en cuenta los aspectos de la confidencialidad y la probidad.

6.31. Los resultados de las inspecciones y auditorías deberían poner de relieve las esferas específicas en que se puedan adoptar medidas o introducir mejoras. Las

medidas preventivas y correctivas que se considere adecuado adoptar deberían llevar aparejado un calendario con plazos concretos para la rectificación o la aplicación. Una vez ejecutadas estas medidas de rectificación y aplicación, se debería efectuar un seguimiento y una evaluación de la eficacia.

INCIDENTES DE SEGURIDAD FÍSICA DE LA INFORMACIÓN

6.32. La vulneración de un objeto de información puede dar lugar a violaciones de la seguridad física. Dos tipos de violación de la seguridad que suponen una vulneración de la información son las filtraciones y las pérdidas. Las filtraciones suelen estar asociadas a una vulneración de la confidencialidad, en que, de forma deliberada o accidental, se produce una divulgación no autorizada de información. Las pérdidas se relacionan por lo general con una vulneración de la información que se debe a un robo, o al hecho de no haber garantizado adecuadamente la seguridad física, de la información o los activos de información.

6.33. Los incidentes de seguridad física de la información pueden entrañar también una pérdida de la disponibilidad o integridad de la información, causada por acciones ya sea involuntarias o intencionales. La disponibilidad puede perderse, por ejemplo, a causa de un fallo de un sistema de información (como una base de datos) o de una denegación dolosa de su uso (por una sobrecarga intencional de una red de información con un tráfico excesivo de datos). La pérdida de integridad puede deberse, por ejemplo, al daño de un sistema de información, la corrupción de una base de datos o la alteración no autorizada de la información durante la transmisión.

6.34. La notificación a las autoridades competentes de los incidentes o violaciones importantes de la seguridad física nuclear, incluidas las violaciones de la seguridad física de la información, debería ser obligatoria y estar prescrita en las leyes o reglamentos del Estado. Las leyes o reglamentos deberían especificar también las sanciones o penas en que se incurrirá si no se efectúa esa notificación.

6.35. Los jefes de las organizaciones e instalaciones deberían velar por que existan los arreglos oficiales de rendición de cuentas necesarios para que todo incidente de seguridad física de la información sea señalado inmediatamente a su atención de modo que se puedan adoptar medidas correctivas y, cuando corresponda, el incidente se notifique a las autoridades competentes. La vergüenza no debería

ser nunca un motivo para no notificar un incidente de seguridad física de la información a ningún nivel. Los incidentes deberían comunicarse de inmediato para que se puedan adoptar medidas correctivas y determinar las tendencias.

INVESTIGACIONES

6.36. Todos los incidentes de seguridad física de la información deben investigarse. Deberían definirse políticas y procedimientos que rijan la investigación de esos incidentes. La investigación debería tener por objeto determinar si el incidente de seguridad física tiene un efecto menor o importante en la seguridad y confidencialidad de la información. Las autoridades competentes podrán entonces adoptar el curso de acción apropiado. Un ejemplo de un incidente menor puede ser el hecho de no guardar un documento bajo llave o en la forma prescrita, sin que por ello se pierda o vulnere ninguna información. Un incidente importante puede ser, por ejemplo, el robo de un plan de seguridad física que se traduzca en una amenaza estratégica para la organización.

6.37. Una investigación debería comprender lo siguiente:

a) Un estudio a fondo de las circunstancias del incidente para determinar su alcance, escala y efecto.
b) Una evaluación de las consecuencias del incidente y del grado de vulneración que pueda haberse producido.
c) Una evaluación de la necesidad de medidas ulteriores o de indagaciones más amplias, que podrían incluir a otros organismos.
d) La recomendación de medidas correctivas o la adopción de medidas para contener o reducir al mínimo las consecuencias.
e) Un informe de los resultados de la investigación, que indique:
    i) la causa probable del incidente;
    ii) el grado de vulneración observado;
    iii) el efecto o los efectos probables de esa vulneración;
    iv) posibles recomendaciones para mejorar el programa de seguridad física con el fin de evitar otros incidentes parecidos;
    v) la recomendación de otras medidas que se justifique adoptar a raíz del incidente;
    vi) las enseñanzas que deban extraer las partes interesadas.

6.38. Las autoridades competentes deberían llevar un registro del número y tipo de incidentes de seguridad física de la información notificados. Se deberían determinar los incidentes recurrentes o las tendencias en los fallos de la seguridad, que pueden indicar la necesidad de cambios en la política de seguridad física o de mejoras en los procedimientos o programas correspondientes. Los programas de sensibilización deberían incluir información actualizada sobre las tendencias y los cambios a fin de mantener una cultura de la seguridad física apropiada entre los empleados y contratistas. Las organizaciones e instalaciones deberían también llevar sus propios registros.

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] OFICINA EUROPEA DE POLICÍA, ORGANISMO INTERNACIONAL DE ENERGIA ATÓMICA, ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL, ORGANIZACIÓN INTERNACIONAL DE POLICÍA CRIMINAL-INTERPOL, 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, ORGANIZACIÓN MUNDIAL DE ADUANAS, *Recomendaciones de Seguridad Física Nuclear sobre Materiales Nucleares y otros Materiales Radiactivos no sometidos a Control Reglamentario, Colección de Seguridad Física Nuclear del OIEA* Nº 15, OIEA, Viena (2012).

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

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

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

[8] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Sistema de gestión de instalaciones y actividades*, *Colección de Normas de Seguridad del OIEA* Nº GS-R-3, OIEA, Viena (2011).

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

Anexo I

SISTEMA DE CLASIFICACIÓN Y DEFINICIONES

I–1. En este anexo se presenta un ejemplo de un marco de clasificación. Los distintos Estados podrán concebir y utilizar cualquier sistema de clasificación adecuado que indique el grado de sensibilidad de la información sobre la seguridad física nuclear. Las definiciones que se dan a continuación representan un sistema en cuatro niveles similar al que utilizan muchos Estados Miembros. El cuarto nivel, correspondiente a la información ESTRICTAMENTE SECRETA, no se describe en este documento, porque la experiencia ha demostrado que en el sector nuclear civil es muy improbable que algún activo de información se clasifique en ese nivel. Obsérvese también que, aunque al hablar de información se piensa principalmente en documentos o conocimientos, los equipos u otros objetos físicos también pueden estar clasificados, si es posible obtener de ellos información protegida mediante la observación visual de su aspecto interno o externo o de su estructura, funcionamiento, ensayo, aplicación o uso.

SECRETO

I–2. La vulneración de una información o un material clasificado como SECRETO podría tener las siguientes consecuencias:

a) un aumento de la tensión internacional;
b) un grave daño a las relaciones entre gobiernos;
c) una amenaza directa a la vida, o un serio detrimento del orden público o de la seguridad o libertad de las personas;
d) un grave menoscabo de la eficacia operacional o de la seguridad física de las fuerzas nacionales de seguridad, o de la eficacia ininterrumpida de operaciones de inteligencia o de seguridad muy importantes;
e) un daño material sustancial a las finanzas o los intereses económicos y comerciales nacionales;
f) su posible utilización por una persona o un grupo para la planificación de un acto doloso que pueda causar un daño grave a una instalación en que haya materiales nucleares u otros materiales radiactivos, o a un transporte de esos materiales.

CONFIDENCIAL

I–3. La vulneración de una información o un material clasificado como CONFIDENCIAL podría tener las siguientes consecuencias:

a) un daño a las relaciones diplomáticas;
b) un detrimento de la seguridad o libertad de las personas;
c) un menoscabo de la eficacia operacional o la seguridad física de las fuerzas nacionales de seguridad, o de la eficacia de operaciones de inteligencia o de seguridad importantes;
d) un efecto negativo sustancial en las finanzas o los intereses económicos y comerciales nacionales;
e) un menoscabo sustancial de la viabilidad financiera de organizaciones importantes;
f) la obstaculización de la investigación de delitos graves, o la facilitación de su perpetración;
g) una seria obstaculización de la elaboración o aplicación de políticas gubernamentales importantes;
h) el cierre u otra perturbación sustancial de operaciones nacionales importantes;
i) su posible utilización por una persona o un grupo para la planificación de un acto doloso que pueda causar un daño serio a una instalación en que haya materiales nucleares u otros materiales radiactivos, o a un transporte de esos materiales.

RESERVADO

I–4. La vulneración de una información o un material clasificado como RESERVADO podría tener las siguientes consecuencias:

a) un efecto adverso en las relaciones diplomáticas;
b) un sufrimiento considerable para las personas;
c) una mayor dificultad para mantener la eficacia operacional o la seguridad física de las fuerzas nacionales de seguridad;
d) una pérdida financiera o una pérdida de posibilidades de ingresos, o una obtención más fácil de ganancias o ventajas indebidas, por personas o empresas;
e) un perjuicio a la investigación de delitos;
f) la facilitación de la comisión de delitos;

g) una violación de los debidos compromisos de mantener la confidencialidad de la información proporcionada por terceros;
h) la obstaculización de la elaboración o el funcionamiento efectivos de políticas gubernamentales;
i) la violación de restricciones reglamentarias a la divulgación de información;
j) una posición de desventaja para el gobierno en negociaciones comerciales o políticas con otros;
k) un menoscabo de la correcta gestión del sector público y sus operaciones;
l) su posible utilización por una persona o un grupo para la planificación de un acto doloso que pueda causar un daño significativo a una instalación en que haya materiales nucleares u otros materiales radiactivos, o a un transporte de esos materiales.

I–5. En lo que respecta a la aplicación de estos niveles de clasificación al control de la información nuclear de carácter estratégico, debería examinarse de qué manera la divulgación no autorizada de esa información podría ayudar a un posible adversario a realizar lo siguiente:

a) Seleccionar un blanco para un robo o un acto de sabotaje de materiales nucleares u otros materiales radiactivos, equipos o instalaciones.
b) Planificar o cometer un robo o un acto de sabotaje de materiales nucleares u otros materiales radiactivos, equipos o instalaciones:
    i) diseño de los sistemas de seguridad;
    ii) planos de construcción;
    iii) métodos y procedimientos para la transferencia, contabilidad y manipulación de materiales nucleares u otros materiales radiactivos;
    iv) planes, procedimientos y capacidades de seguridad física.
c) Medir el éxito de un robo o un acto de sabotaje de materiales nucleares u otros materiales radiactivos, equipos o instalaciones:
    i) consecuencias efectivas o hipotéticas de un acto de sabotaje de determinados equipos o instalaciones esenciales.
d) Producir ilegalmente un dispositivo nuclear explosivo, un dispositivo de dispersión radiactiva o un dispositivo de exposición a la radiación:
    i) información sobre el diseño que ayude a desarrollar un dispositivo;
    ii) localización de los materiales requeridos para fabricar un dispositivo;
    iii) localización de un arma nuclear.
e) Dispersar materiales nucleares u otros materiales radiactivos en el medio ambiente:
    i) localización, forma y cantidad de los materiales.

Anexo II

EJEMPLOS DE INFORMACIÓN DE CARÁCTER ESTRATÉGICO

II–1. En este anexo se presenta un ejemplo de un sistema de categorización de la seguridad física de la información relacionada con la seguridad física nuclear. El Estado debería decidir el nivel de clasificación exacto que se asignará a cada elemento de esa información. En el cuadro II–1 se dan ejemplos de tipos de información de carácter estratégico, con una indicación de los aspectos sensibles de cada información. En los casos en que no se recomienda la divulgación, el cuadro señala los motivos e indica si se justifica proteger la información.

II–2. Las categorías de información que se presentan en el cuadro II–1 son solo una indicación de la información que puede considerarse de carácter estratégico. No pretenden representar un modelo o una lista exhaustiva. Las categorías que sea pertinente incluir en un cuadro nacional de este tipo se determinarán sobre la base de una evaluación específica del Estado.

II–3. En cada fila del cuadro, la primera columna contiene un ejemplo de un tipo de información. La segunda columna indica si esa categoría se aplica habitualmente a materiales nucleares e instalaciones nucleares (N), a otros materiales radiactivos y las instalaciones conexas (R), o a ambos (N, R). La tercera columna indica si la información puede o no considerarse de carácter estratégico. En la última columna se explica por qué la información tiene o no ese carácter y se indican los motivos por los que se debería proteger o no proteger.

II–4. Con respecto a la clasificación de una información como de carácter estratégico y a su posible asignación a una categoría de seguridad, debería tomarse en consideración si la información ya es de dominio público, o si ha estado expuesta anteriormente a alguna vulneración real o potencial. Si es así, puede ser inútil asignarle y tratar de gestionar un nivel de clasificación.

II–5. Asimismo, habrá que pensar en designar como de carácter estratégico la información que no tenga este carácter pero que, en combinación con otra que tampoco lo tenga, pueda revelar información de carácter estratégico.

CUADRO II–1. SISTEMA HIPOTÉTICO DE CATEGORIZACIÓN DE LA SEGURIDAD FÍSICA PARA LA INFORMACIÓN RELACIONADA CON LA SEGURIDAD FÍSICA NUCLEAR

Categoría	Ámbito	Carácter estratégico	Motivos para la protección o no protección
1. SEGURIDAD FÍSICA DE MATERIALES E INSTALACIONES			
1.1. Reglamentos y orientaciones			
A. Reglamentos nacionales de seguridad física que rigen el uso de materiales nucleares u otros materiales radiactivos	N, R	No	Esta información es normalmente de dominio público.
B. Orientaciones sobre esos reglamentos, publicadas por la autoridad competente u otro organismo gubernamental	N, R	Sí	Aunque es posible que no todas estas orientaciones sean de carácter estratégico, un documento de esta naturaleza podría contener detalles sobre las normas, los tipos de equipo que se deban utilizar, los procedimientos y las operaciones de seguridad física en una instalación. Estos detalles podrían ser útiles para un adversario que planifique un acto doloso.
1.2. Políticas nacionales de seguridad física nuclear			
A. Políticas generales del gobierno sobre asuntos que se relacionan con materiales nucleares u otros materiales radiactivos	N, R	No	Esta información es normalmente de dominio público.
B. Política detallada sobre aspectos específicos de la seguridad física	N, R	Sí	Podría dar una indicación del tipo de obstáculos con que se pueden encontrar los adversarios, y permitirles así planificar la adquisición de información más detallada.

CUADRO II–1. SISTEMA HIPOTÉTICO DE CATEGORIZACIÓN DE LA SEGURIDAD FÍSICA PARA LA INFORMACIÓN RELACIONADA CON LA SEGURIDAD FÍSICA NUCLEAR (continuación)

Categoría	Ámbito	Carácter estratégico	Motivos para la protección o no protección
1.3. Planes de seguridad física de las instalaciones	N, R	Sí	Normalmente contienen descripciones detalladas de las medidas de seguridad física existentes en el emplazamiento y detalles precisos de dónde se encuentra almacenado el material. En el caso de las instalaciones nucleares, los planes también contienen detalles de otras áreas esenciales para el funcionamiento del emplazamiento.
1.4. Informes de seguridad física			
A. Informes de los estudios, inspecciones y evaluaciones de la seguridad física y otros informes sobre las medidas de protección física o seguridad técnica aplicadas en un emplazamiento o instalación	N, R	Sí	El acceso a estos informes puede proporcionar a un adversario detalles sobre la ubicación del material, las medidas adoptadas para protegerlo y las vulnerabilidades que puedan haberse descubierto, y ayudarle así a eludir las medidas y controles de seguridad.
B. Informes que describen elementos de importancia crítica y/o que destacan las mejoras necesarias en la seguridad física, también en áreas vitales (si se aplica)	N, R	Sí	La información de este tipo podría ser útil para un adversario que desee eludir los arreglos de seguridad física, y podría ayudarle a seleccionar una instalación.
C. Resultados de investigaciones sobre la seguridad física en un emplazamiento o instalación, incluidas las investigaciones de filtraciones y pérdidas de información de carácter estratégico	N, R	Sí	La información de este tipo podría ser útil para un adversario que desee eludir los arreglos de seguridad física, y puede ayudarle a seleccionar una instalación.

CUADRO II–1. SISTEMA HIPOTÉTICO DE CATEGORIZACIÓN DE LA SEGURIDAD FÍSICA PARA LA INFORMACIÓN RELACIONADA CON LA SEGURIDAD FÍSICA NUCLEAR (continuación)

Categoría	Ámbito	Carácter estratégico	Motivos para la protección o no protección
D. Informes que describen las vulnerabilidades del sistema de gestión de la seguridad física y las consecuencias de los fallos	N, R	Sí	La información de este tipo podría ser útil para un adversario que desee eludir los arreglos de seguridad física.
1.5. Detalles de la construcción			
A. Detalles de la construcción y la disposición física de los lugares en que puedan almacenarse o procesarse materiales, incluidos los proyectos o planos, en cualquier soporte, que muestren los elementos de protección física de interés para la prevención de actos dolosos	N, R	Sí	Los mapas o planos oficiales de los emplazamientos podrán ser divulgados a discreción de la administración de cada emplazamiento, a condición de que no contengan ninguna descripción de los detalles de las funciones de un edificio, los materiales almacenados en él o la ubicación de las vallas de seguridad física internas, o de las otras medidas de seguridad física que se apliquen en el edificio.
B. Detalles de la construcción de las áreas vitales en las centrales nucleares y otras instalaciones nucleares	N	Sí	La información de este tipo puede ser útil para un adversario que desee eludir los arreglos de seguridad física, y podría ayudarle a seleccionar los blancos de un acto de sabotaje.
1.6. Sistemas de protección			
A. Detalles de las medidas de protección física utilizadas, como las alarmas, las cámaras de vigilancia, los controles del acceso, el personal de seguridad física, etc.	N, R	Sí	

CUADRO II–1. SISTEMA HIPOTÉTICO DE CATEGORIZACIÓN DE LA SEGURIDAD FÍSICA PARA LA INFORMACIÓN RELACIONADA CON LA SEGURIDAD FÍSICA NUCLEAR (continuación)

Categoría	Ámbito	Carácter estratégico	Motivos para la protección o no protección
B. Los tipos y la ubicación de los sensores de los sistemas de detección de intrusiones y de las cámaras de vigilancia correspondientes, incluidos los diagramas de los circuitos, la localización de los suministros de energía eléctrica esenciales, el recorrido de los cables, y los programas de mantenimiento y ensayo de este equipo	N, R	Sí	Cualquier detalle de esta naturaleza sería útil para un adversario que desee eludir los sistemas de seguridad física de una instalación.
1.7. Detalles de los sistemas automáticos de control del acceso, incluida la localización de los servidores de las computadoras y los servidores de reserva y de sus suministros de electricidad	N, R	Sí	No debería divulgarse ningún detalle que pueda ayudar a un adversario, externo o interno, a eludir el sistema de control del acceso.
1.8. Almacenes: procedimientos de seguridad física para la entrega, la recepción y el control del suministro de materiales; nombres de las personas autorizadas a tener las llaves; arreglos para la vigilancia y la protección	N, R	Sí	Podrían ser útiles para un adversario que planifique un acto doloso.
1.9. Mapas generales que indican la posición y los límites de una instalación, pero que no dan detalles de lo que existe en ella	N, R	No	Las aplicaciones cartográficas de libre acceso en Internet dan esta información con toda claridad.

CUADRO II–1. SISTEMA HIPOTÉTICO DE CATEGORIZACIÓN DE LA SEGURIDAD FÍSICA PARA LA INFORMACIÓN RELACIONADA CON LA SEGURIDAD FÍSICA NUCLEAR (continuación)

Categoría	Ámbito	Carácter estratégico	Motivos para la protección o no protección
1.10. Otros aspectos relacionados con la protección física, como la localización, la configuración, la dotación de personal y el equipo de la estación central de alarmas; la localización de la estación de alarmas secundaria; el tipo de barrera del área interna	N, R	Sí	Cualquier detalle de esta naturaleza sería muy útil para un adversario que desee eludir los sistemas de seguridad física de una instalación nuclear.
2. INFORMACIÓN RELACIONADA CON LA CANTIDAD Y FORMA DE LOS MATERIALES			
2.1. Información sobre la cantidad, el tipo y la forma de los materiales nucleares, incluidas las fuentes, que se reciben o mantienen en lugares especificados de todas las categorías de emplazamientos y centrales nucleares, incluidos los lugares exactos en que se conserva el combustible gastado	N	Sí	Este tipo de información podría ayudar a un adversario que planifique un atentado a seleccionar los blancos.
2.2. Producción — capacidad nominal, producción efectiva y datos históricos sobre la producción de una instalación sometida a las salvaguardias del OIEA	N	No	Esta información de alto nivel, especialmente en el caso de las centrales nucleares, suele ser de dominio público.

CUADRO II–1. SISTEMA HIPOTÉTICO DE CATEGORIZACIÓN DE LA SEGURIDAD FÍSICA PARA LA INFORMACIÓN RELACIONADA CON LA SEGURIDAD FÍSICA NUCLEAR (continuación)

Categoría	Ámbito	Carácter estratégico	Motivos para la protección o no protección
2.3. Inventarios, ya sea nacionales o locales, de otros materiales radiactivos (incluidos los materiales en desuso), con indicación de las cantidades, los tipos, las formas y la ubicación exacta	R	Sí	Este tipo de información podría ayudar a un adversario a seleccionar los blancos cuando planifique un atentado para robar materiales radiactivos. Debería examinarse cuál información sobre esos inventarios ya es de dominio público. Toda esa información podrá considerarse de carácter no estratégico. Los procesos basados en el riesgo ayudarán a determinar cuáles elementos deberían considerarse de carácter estratégico.
3. MATERIAL EN TRÁNSITO (INCLUIDOS LOS MOVIMIENTOS DENTRO UN EMPLAZAMIENTO)			
3.1. Información sobre los movimientos de materiales nucleares de las categorías I, II, III	N	Sí	Esta información podría ayudar a seleccionar los blancos cuando se planifiquen actos dolosos que se relacionen con materiales nucleares en tránsito.
3.2. Vehículos de alta seguridad			
A. Acceso visual al interior de la cabina y el compartimento de carga	N	Sí	
B. Características de seguridad física del diseño y la construcción de los vehículos	N	Sí	

CUADRO II–1. SISTEMA HIPOTÉTICO DE CATEGORIZACIÓN DE LA SEGURIDAD FÍSICA PARA LA INFORMACIÓN RELACIONADA CON LA SEGURIDAD FÍSICA NUCLEAR (continuación)

Categoría	Ámbito	Carácter estratégico	Motivos para la protección o no protección
C. Diseño y función de las alarmas, los dispositivos de inmovilización, y los diseños clave de dispositivos de bloqueo especiales	N	Sí	Los vehículos de alta seguridad son vehículos especialmente diseñados para transportar materiales nucleares en condiciones de seguridad. Estos vehículos transportan materiales nucleares, y toda información del tipo indicado en esta sección podría ser útil para un adversario que planifique un intento de robo o sabotaje de materiales nucleares en tránsito.
D. Llaves de los compartimentos de carga, llaves de repuesto y claves de las cerraduras con combinación, cuando existan	N	Sí	
E. Sistema de rastreo de vehículos, cuando esté instalado en un vehículo de alta seguridad; funcionamiento del sistema y comunicaciones	N	Sí	
3.3. Contenedores de materiales nucleares en tránsito			
A. Grado de resistencia de los contenedores de transporte al ataque por diversos medios	N	Sí	Esta información sería útil para un adversario que planifique un acto de sabotaje con el fin de provocar una emisión de materiales nucleares, o que planifique un robo de materiales nucleares durante el transporte.

CUADRO II–1. SISTEMA HIPOTÉTICO DE CATEGORIZACIÓN DE LA SEGURIDAD FÍSICA PARA LA INFORMACIÓN RELACIONADA CON LA SEGURIDAD FÍSICA NUCLEAR (continuación)

Categoría	Ámbito	Carácter estratégico	Motivos para la protección o no protección
B. Especificaciones y datos del diseño de los contenedores	N	No	La información sobre el diseño de estos contenedores, sin detalles sobre la construcción, suele estar disponible en Internet.
C. Información sobre el diseño de contenedores específicos (contenedores con protección especial)	N	Sí	Sería útil para un adversario que planifique un acto de sabotaje con el fin de provocar una emisión de materiales nucleares, o que planifique un robo de materiales durante el transporte.
3.4. Bultos de transporte: Información sobre el diseño de los bultos de transporte	N	Sí	Sería útil para un adversario que planifique un acto de sabotaje con el fin de provocar una emisión de materiales nucleares, o que planifique un robo de materiales durante el transporte.
3.5. Información sobre los movimientos de otros materiales radiactivos	R	Sí	Este tipo de información, particularmente si se refiere al transporte de fuentes de radiación potentes, podría ser útil para planificar un robo.

CUADRO II–1. SISTEMA HIPOTÉTICO DE CATEGORIZACIÓN DE LA SEGURIDAD FÍSICA PARA LA INFORMACIÓN RELACIONADA CON LA SEGURIDAD FÍSICA NUCLEAR (continuación)

Categoría		Ámbito	Carácter estratégico	Motivos para la protección o no protección
4. SISTEMAS DE TECNOLOGÍA DE LA INFORMACIÓN Y SISTEMAS INFORMÁTICOS IMPORTANTES PARA LA SEGURIDAD FÍSICA Y TECNOLÓGICA				
4.1.	Detalles de los sistemas de TI en que se almacena y procesa información de carácter estratégico, incluidos los sistemas que se utilizan para fines de seguridad física, la arquitectura de los sistemas, los detalles de las medidas aplicadas para la seguridad física de las computadoras y la localización de los medios de respaldo	N, R	Sí	Esta información sería útil para un adversario que planifique un acto doloso en una instalación.
4.2.	Detalles sobre el control del acceso, los sistemas de detección de intrusiones, los sistemas de monitorización con alarmas, los sistemas de evaluación y vigilancia y otras funciones y dispositivos de seguridad física; información sobre la localización del equipo de reserva y los programas informáticos de respaldo	N, R	Sí	Esta información sería útil para un adversario que planifique un acto doloso en una instalación.
4.3.	Detalles sobre los sistemas de TI relacionados con la seguridad tecnológica o con sistemas informáticos importantes para la seguridad tecnológica, que incluyan las ubicaciones, las funciones, los planes de mejoras, el suministro de electricidad y los respaldos	N, R	Sí	Estos sistemas tienen funciones de vigilancia operacional y de control. Su vulneración podría permitir a un adversario, como mínimo, perturbar el funcionamiento de una instalación y, en el peor de los casos, provocar una perturbación que conduzca a la emisión de materiales radiactivos.

CUADRO II–1. SISTEMA HIPOTÉTICO DE CATEGORIZACIÓN DE LA SEGURIDAD FÍSICA PARA LA INFORMACIÓN RELACIONADA CON LA SEGURIDAD FÍSICA NUCLEAR (continuación)

Categoría	Ámbito	Carácter estratégico	Motivos para la protección o no protección
5. FUERZAS DE GUARDIA Y DE RESPUESTA			
5.1. Fuerzas de guardia de una instalación			
A. Dotación general y capacidades de las fuerzas de guardia existentes	N	No	El hecho de dar a conocer la existencia de estas fuerzas puede tranquilizar al público, y podría ser un factor disuasivo.
B. Dotación y capacidades existentes en un emplazamiento particular	N	Sí	Este tipo de información podría ser útil para un adversario que planifique una incursión en un emplazamiento nuclear con el fin de cometer un robo o un acto de sabotaje, y podría socavar la capacidad de responder a un atentado de manera eficaz.
C. Efectivos en cada turno de un emplazamiento	N	Sí	
D. Armas y otro equipo especial de que disponen las fuerzas de guardia, y número de personas capacitadas en el uso de armas de fuego en las fuerzas de guardia de un emplazamiento particular	N	Sí	
E. Fuerzas de respuesta: localización, capacidades, armas, vehículos especiales de respuesta y planificación de los tiempos en un emplazamiento	N	Sí	Toda información que pueda ayudar a un adversario a estimar de antemano la escala de la respuesta y las capacidades disponibles en una unidad operacional táctica debería estar protegida contra la divulgación.
F. Planes de despliegue	N	Sí	

CUADRO II–1. SISTEMA HIPOTÉTICO DE CATEGORIZACIÓN DE LA SEGURIDAD FÍSICA PARA LA INFORMACIÓN RELACIONADA CON LA SEGURIDAD FÍSICA NUCLEAR (continuación)

Categoría	Ámbito	Carácter estratégico	Motivos para la protección o no protección
5.2. Escoltas para los movimientos de materiales nucleares			
A. Despliegue y capacidades de la escolta	N	Sí	
B. Radiofrecuencias utilizadas para la comunicación con las fuerzas de respuesta o las fuerzas de policía locales	N	Sí	Esta información podría ser útil para un adversario que planifique un atentado contra un convoy.
6. CONTABILIDAD DE LOS MATERIALES NUCLEARES			
6.1. Descripción			
A. Declaraciones sobre los principios generales de la contabilidad de materiales	N	No	Los principios generales de este tipo son de dominio público.
B. Cuestionario y descripción de la información de diseño, y localización de las áreas de balance de materiales y los puntos clave de medición	N	Sí	Esta información detallada sobre la localización y las cantidades de los materiales nucleares podría ser útil para un adversario que planifique un acto doloso.
C. Forma física y química de la medición de los materiales en los puntos clave de medición	N	Sí	

CUADRO II–1. SISTEMA HIPOTÉTICO DE CATEGORIZACIÓN DE LA SEGURIDAD FÍSICA PARA LA INFORMACIÓN RELACIONADA CON LA SEGURIDAD FÍSICA NUCLEAR (continuación)

Categoría	Ámbito	Carácter estratégico	Motivos para la protección o no protección
6.2. Mediciones y datos de la instrumentación			
A. Precisión y exactitud de las técnicas de laboratorio estándar	N	No	Esta información suele ser de dominio público.
B. Datos que revelan la sensibilidad de las mediciones o los límites de las alarmas para el material no contabilizado (MNC) en una determinada instalación	N	Sí	Los datos sobre la precisión y exactitud de las mediciones efectivas o típicas en los emplazamientos, ya sea agregados o desglosados, podrían ser útiles para un adversario que planifique un robo de materiales.
6.3. Flujo de los materiales nucleares y datos de inventarios mantenidos en los sistemas de TI, en forma impresa o en cualquier tipo de medio de almacenamiento	N	Sí	Esta información podría revelar detalles exactos de la localización y los movimientos de materiales nucleares.
6.4. Material no contabilizado			
A. Cifras anuales del MNC de un emplazamiento que no revelan el área de balance de materiales de que se trata	N	No	En muchos Estados, las cifras anuales agregadas del material no contabilizado son públicas o pueden hacerse públicas.
B. MNC en las áreas de balance de materiales o los puntos clave de medición	N	Sí	

CUADRO II–1. SISTEMA HIPOTÉTICO DE CATEGORIZACIÓN DE LA SEGURIDAD FÍSICA PARA LA INFORMACIÓN RELACIONADA CON LA SEGURIDAD FÍSICA NUCLEAR (continuación)

Categoría	Ámbito	Carácter estratégico	Motivos para la protección o no protección
C. Detalles de las investigaciones sobre un MNC en particular, a menos que se haya aprobado oficialmente su publicación	N	Sí	Sin embargo, la información detallada sobre las cifras o los resultados de investigaciones del MNC podría ayudar a un adversario a seleccionar una instalación específica para cometer un atentado y, por lo tanto, debería considerarse de carácter estratégico.
D. Límite de error del MNC u otra indicación específica de la incertidumbre de las cifras sobre el MNC	N	Sí[a]	
7. SOLICITUDES DEL PROCESO DE CONCESIÓN DE LICENCIAS Y PERMISOS			
7.1. Solicitudes del proceso de concesión de licencias y permisos que no contienen información detallada sobre las medidas de seguridad física ni sobre el tipo, la forma y la cantidad de los materiales	N, R	No	El contenido de estas solicitudes variará según el marco jurídico y de reglamentación que exista y según el uso final previsto. Si las solicitudes contienen información de carácter estratégico que pueda ser útil para un adversario, deberían tratarse como información de carácter estratégico.
7.2. Solicitudes del proceso de concesión de licencias y permisos que contienen información detallada sobre, por ejemplo, las medidas de seguridad física y el tipo, la forma y la cantidad de los materiales	N, R	Sí	El contenido de estas solicitudes variará según el marco jurídico y de reglamentación que exista y según el uso final previsto. Si las solicitudes contienen información de carácter estratégico que pueda ser útil para un adversario, deberían tratarse como información de carácter estratégico.

[a] En algunos Estados, el límite de error del MNC no se considera información de carácter estratégico.

CUADRO II–1. SISTEMA HIPOTÉTICO DE CATEGORIZACIÓN DE LA SEGURIDAD FÍSICA PARA LA INFORMACIÓN RELACIONADA CON LA SEGURIDAD FÍSICA NUCLEAR (continuación)

Categoría	Ámbito	Carácter estratégico	Motivos para la protección o no protección
8. JUSTIFICACIONES DE LA SEGURIDAD, DOCUMENTOS DE INGENIERÍA Y OTRA INFORMACIÓN AMBIENTAL O SOBRE LA SEGURIDAD TECNOLÓGICA			
8.1. Justificaciones de la seguridad de todas las clases			Aunque la mayor parte de la información sobre las justificaciones de la seguridad puede hacerse pública en aras de la transparencia, cierta información puede considerarse de carácter estratégico a los efectos de la seguridad física nuclear.
A. Detalles sobre los peligros posibles u otra información que pueda utilizarse como indicador indirecto para evaluar el impacto de una emisión, o detalles sobre los efectos de las emisiones	N, R	Sí	
B. Detalles sobre los puntos fuertes y débiles de los procesos, estructuras y sistemas de protección diseñados para contener, controlar o proteger materiales nucleares u otros materiales radiactivos	N, R	Sí	El tipo de información detallada que figura en las justificaciones de la seguridad podría ayudar a un adversario a elegir los blancos y planificar una operación.
C. Detalles sobre el acceso al proceso de producción, tanto el control del acceso físico como la retirada de materiales del proceso para fines de control y monitorización	N, R	Sí	

CUADRO II–1. SISTEMA HIPOTÉTICO DE CATEGORIZACIÓN DE LA SEGURIDAD FÍSICA PARA LA INFORMACIÓN RELACIONADA CON LA SEGURIDAD FÍSICA NUCLEAR (continuación)

Categoría	Ámbito	Carácter estratégico	Motivos para la protección o no protección
9. PLANES Y EJERCICIOS DE CONTIGENCIA Y RESPUESTA			
9.1. Contingencia y respuesta			
A. La existencia de un plan de contingencia y de respuesta	N, R	No	El hecho de dar a conocer la existencia de planes puede tranquilizar al público, y podría ser un factor disuasivo.
B. Contenido detallado de un plan de contingencia y de respuesta	N, R	Sí	Los detalles del plan podrían indicar las capacidades, las limitaciones y los tiempos de respuesta y, por lo tanto, ser útiles para un adversario en la planificación de un atentado.
9.2. Planes de contingencia para la seguridad física, con información detallada	N, R	Sí	Estos documentos contienen información sobre las medidas de seguridad física establecidas, las capacidades de los contingentes de las fuerzas policiales o de guardia y la respuesta probable a un incidente de seguridad física.
9.3. Ejercicios			
A. La información de que se realizará o se ha realizado un ejercicio	N, R	No	El hecho de dar a conocer la existencia de ejercicios puede tranquilizar al público, pero la información no debe contener detalles que puedan ayudar a un adversario, como la fecha/hora/lugar de un ejercicio futuro.

CUADRO II–1. SISTEMA HIPOTÉTICO DE CATEGORIZACIÓN DE LA SEGURIDAD FÍSICA PARA LA INFORMACIÓN RELACIONADA CON LA SEGURIDAD FÍSICA NUCLEAR (continuación)

Categoría	Ámbito	Carácter estratégico	Motivos para la protección o no protección
B. Detalles sobre los ejercicios de seguridad física en un emplazamiento, como el escenario utilizado, los aspectos del plan de seguridad que se ponen a prueba, la participación de una fuerza de respuesta y los resultados del ejercicio	N, R	Sí	Proporcionan a los adversarios información sobre la naturaleza, el tamaño, las capacidades y los tiempos de reacción de las fuerzas de respuesta, los detalles de las fuerzas de respuesta armadas, la naturaleza de la táctica empleada y el plan de señales.
C. Detalles de los ejercicios de seguridad tecnológica	N, R	No	Los ejercicios de seguridad tecnológica se realizan con frecuencia de manera abierta y transparente. Por lo general pueden considerarse de carácter no estratégico, siempre que no revelen información detallada sobre las medidas de seguridad física.
10. INFORMACIÓN PERSONAL			
10.1. Información personal			
A. Información dimanante de las verificaciones de la probidad	N, R	Sí	La información de esta naturaleza podría utilizarse para el chantaje o la extorsión. La mayoría de los reglamentos nacionales sobre la privacidad impondrán la protección obligatoria de este tipo de información.
B. Información contenida en archivos del personal	N, R	Sí	

CUADRO II–1. SISTEMA HIPOTÉTICO DE CATEGORIZACIÓN DE LA SEGURIDAD FÍSICA PARA LA INFORMACIÓN RELACIONADA CON LA SEGURIDAD FÍSICA NUCLEAR (continuación)

Categoría	Ámbito	Carácter estratégico	Motivos para la protección o no protección
11. INVENTARIO DE DESECHOS RADIACTIVOS			
11.1. Información sobre los desechos radiactivos			
A. Información general sobre los inventarios que no contiene ningún detalle que pueda ser utilizado, como la existencia de desechos almacenados en un emplazamiento particular, o las cantidades totales de desechos, sin su ubicación	N	No	Esta información es por lo general de dominio público y no describe detalles específicos que puedan ser útiles para un adversario.
B. Información que pueda utilizarse en un acto doloso o que permita identificar un edificio específico de una instalación y el material que se encuentra en él	N	Sí	Proporciona información sobre los posibles blancos a un adversario que planifique un acto de sabotaje.
12. CLAUSURA			
12.1. Planes para la clausura de una planta	N, R	No	Los planes de clausura de las instalaciones suelen ser de dominio público.
12.2. Desechos derivados de la clausura[b]			

[b] Esto se refiere principalmente a los materiales contaminados de la instalación, no a los desechos radiactivos de los procesos realizados durante el funcionamiento normal de la instalación.

CUADRO II–1. SISTEMA HIPOTÉTICO DE CATEGORIZACIÓN DE LA SEGURIDAD FÍSICA PARA LA INFORMACIÓN RELACIONADA CON LA SEGURIDAD FÍSICA NUCLEAR (continuación)

Categoría	Ámbito	Carácter estratégico	Motivos para la protección o no protección
A. La información de que se construirá un depósito, y en qué lugar	N, R	No	Esta información suele ser de dominio público.
B. Detalles de la construcción, las medidas de seguridad física y la cantidad o el tipo de materiales que se almacenarán en los nuevos edificios para el tratamiento y almacenamiento de los desechos y el material contaminado generados en las actividades de procesamiento durante la clausura	N, R	Sí	Pueden proporcionar información útil para la selección de los blancos a un adversario que planifique actos de sabotaje.
13. EVALUACIONES DE LA AMENAZA E INFORMACIÓN SOBRE LAS ALERTAS DE SEGURIDAD FÍSICA			
13.1. Evaluaciones de la amenaza emitidas por el Estado, las autoridades nacionales de seguridad u otras autoridades competentes	N, R	Sí	Por lo general forman parte del material de seguridad nacional, como la información de inteligencia nacional.
13.2. Detalles sobre la amenaza base de diseño	N	Sí	Por lo general forman parte del material de seguridad nacional, como la información de inteligencia nacional.
13.3. Detalles del estudio de determinación de las áreas vitales	N	Sí	Podrían ayudar a un adversario a determinar los blancos y realizar un atentado.

CUADRO II–1. SISTEMA HIPOTÉTICO DE CATEGORIZACIÓN DE LA SEGURIDAD FÍSICA PARA LA INFORMACIÓN RELACIONADA CON LA SEGURIDAD FÍSICA NUCLEAR (continuación)

Categoría	Ámbito	Carácter estratégico	Motivos para la protección o no protección
13.4. Razones del establecimiento de un determinado estado de alerta de seguridad física y de los cambios que se introduzcan en él	N, R	Sí	Por lo general forman parte del material de seguridad nacional, como la información de inteligencia nacional.
14. TECNOLOGÍA NUCLEAR			
14.1. Información técnica detallada sobre la producción o el procesamiento de materiales nucleares (por ejemplo, el procesamiento o reprocesamiento de uranio enriquecido)	N	Sí	La información de este tipo podría ser útil para un adversario.
14.2. Diseños o nuevas tecnologías presentadas para la obtención de una licencia (por ejemplo, tecnología de reactores avanzados, etc.)	N	Sí	Aunque los detalles de estas tecnologías pueden estar a disposición del público, algunos pormenores del diseño o la tecnología podrían ayudar a un adversario a planificar un acto doloso. Esta información podrá examinarse para determinar si contiene elementos de carácter estratégico.
14.3. Información detallada que pueda ayudar a desmontar dispositivos para acceder a fuentes o ayudar de otra manera a eludir las medidas de seguridad física	R	Sí	Esta información podría ser útil para un adversario que intente extraer material radiactivo.

CUADRO II–1. SISTEMA HIPOTÉTICO DE CATEGORIZACIÓN DE LA SEGURIDAD FÍSICA PARA LA INFORMACIÓN RELACIONADA CON LA SEGURIDAD FÍSICA NUCLEAR (continuación)

Categoría	Ámbito	Carácter estratégico	Motivos para la protección o no protección
14.4. Estudios de la vulnerabilidad de los diseños tecnológicos	N, R	Sí	Aunque los estudios académicos pueden estar a disposición del público, toda información detallada que revele las vulnerabilidades y que pueda ser aprovechada por un adversario debería estar protegida contra la divulgación no autorizada.
15. INFORMACIÓN HISTÓRICA			
15.1. Información histórica que sigue siendo de interés y teniendo carácter estratégico, tanto si está clasificada como si no	N, R	Sí	Aun siendo antigua, la información de este tipo puede ser útil para un adversario.

Anexo III

PROGRAMA MODELO DE SENSIBILIZACIÓN SOBRE LA SEGURIDAD FÍSICA

III–1. En este anexo se presenta un ejemplo de un marco para el establecimiento de un programa de sensibilización sobre la seguridad física y de su contenido. Al seleccionar el contenido de un programa de sensibilización sobre la seguridad física de la información, el director de seguridad física de una organización debería examinar la pertinencia específica de los aspectos y métodos aquí señalados y adaptar el programa en consecuencia.

CAPACITACIÓN SOBRE LA SEGURIDAD FÍSICA

III–2. La capacitación puede dividirse en general en cuatro categorías:

a) La capacitación de sensibilización, que aumenta el conocimiento de las amenazas y vulnerabilidades y el reconocimiento de la necesidad de proteger los datos, la información y los medios para procesarlos (el conocimiento sobre la seguridad física informática y de la información).
b) La capacitación temática, que comprende cursos sobre aspectos específicos de la seguridad física destinados a todo el personal (procedimientos para el manejo de materiales clasificados y para los incidentes de seguridad física de la información).
c) La capacitación profesional, que por lo general es una formación técnica detallada para personal con responsabilidades particulares, como los administradores de sistemas, los desarrolladores de programas informáticos, los administradores de redes, los guardias de seguridad, y los encargados de la clasificación y desclasificación de los documentos, entre otros.
d) La capacitación en seguridad física especializada, que es una formación específica para expertos, por lo general del nivel directivo, en las esferas de la gestión del riesgo, la prevención de incidentes y la respuesta a incidentes, entre otras.

III–3. El programa podría incluir contenido que aumente el conocimiento de los siguientes temas:

a) Una visión general de la infraestructura nacional de seguridad física.

b) Los aspectos de la seguridad física de la información y por qué son importantes para la seguridad física nuclear.
c) El sistema nacional de clasificación.
d) Los principios de la seguridad física, por ejemplo 'la necesidad de conocer' y 'la necesidad de poseer'.
e) Las amenazas actuales para la seguridad física que pueden derivarse de acciones deliberadas de:
   i) servicios de inteligencia hostiles, respecto del espionaje y la transferencia de tecnología;
   ii) organizaciones subversivas;
   iii) otras personas y grupos, como los agentes de información y los periodistas investigadores que intentan obtener acceso no autorizado a información de carácter estratégico o a emplazamientos e instalaciones nucleares;
   iv) personas con información privilegiada.
f) La amenaza que plantean las organizaciones adversarias y los actos de sabotaje, teniendo en cuenta la amenaza que suponen en el mundo actual los grupos extremistas.
g) Los riesgos y las consecuencias de las pérdidas o filtraciones internas de información de carácter estratégico, tal vez por un comportamiento involuntario o para crear una situación embarazosa, junto con la traición deliberada por motivos políticos o para apoyar el terrorismo.
h) Las conductas o actividades que pueden ser de utilidad para los posibles adversarios o aumentar el riesgo de una vulneración, tales como:
   i) el comportamiento vulnerable, como las distracciones en el mantenimiento de la seguridad física y el chismorreo;
   ii) el comportamiento inconsciente que puede atraer la atención de agentes hostiles, y las precauciones necesarias en las actividades cotidianas, por ejemplo, en los contactos sociales, los viajes, la correspondencia, y la relación con los conocidos.
i) La información sobre incidentes de seguridad física concretos o los nuevos tipos de enfoques utilizados por los agentes hostiles, que deberían divulgarse rápidamente.
j) La importancia de notificar de inmediato toda circunstancia sospechosa y todo punto débil percibido en los procedimientos de seguridad física o comportamiento vulnerable evidente de los colegas; los medios para hacerlo de manera confidencial deberían ser del conocimiento de todos.
k) El efecto, y el interés para las personas, de leyes y reglamentos nacionales tales como los que regulan el secreto, la lucha contra el terrorismo, la seguridad física, la protección de los datos y la libertad de información, y las sanciones y los castigos en que incurren los transgresores.

l) La explicación de los niveles de autorización para la seguridad física; la forma en que se realizan las verificaciones de la probidad; por qué son necesarias en los sectores nuclear y radiológico; y los niveles de acceso asociados a los diferentes niveles de autorización y probidad — y cómo se relaciona todo esto con las amenazas para la seguridad física arriba mencionadas.

m) La denegación de servicios (por ejemplo, la denegación del acceso de una organización a la información que necesita, con inclusión de acciones tales como el robo) o la destrucción, que violan la disponibilidad.

n) La modificación no autorizada de la información, o la interferencia con esta, que violan la integridad.

o) La divulgación no autorizada, que viola la confidencialidad.

III–4. El programa podría incluir contenidos que capaciten a los participantes en los siguientes temas:

a) La seguridad física de la información relativa a los materiales nucleares y otros materiales radiactivos y a las instalaciones.

b) Las buenas prácticas y los procedimientos de seguridad física, con inclusión de:
   i) el uso correcto de las marcas de clasificación;
   ii) la protección física, la seguridad física del personal y la seguridad física de la información, como los documentos, las comunicaciones y las computadoras;
   iii) ejemplos prácticos de la aplicación de las normas y procedimientos de seguridad física en las tareas que los empleados desempeñen o vayan a desempeñar;
   iv) las medidas que se deban adoptar cuando se sospeche o descubra una violación de la seguridad física.

OTROS MÉTODOS PARA PROMOVER LA SEGURIDAD FÍSICA

III–5. Además de un programa de capacitación fundamental, hay varios otros métodos para señalar los mensajes de sensibilización sobre la seguridad física a la atención de los empleados y contratistas:

a) Los boletines sobre seguridad física publicados periódicamente por las autoridades nacionales de seguridad. Estos pueden contener temas de actualidad y asesoramiento sobre una serie de aspectos de la seguridad física.

b) Los carteles que recuerdan a las personas las amenazas para la seguridad física y los principales controles que se deben aplicar para hacerles frente. El efecto de esos carteles tiende a ser temporal, por lo que no solo deberían colocarse en lugares muy visibles, sino también cambiarse con frecuencia.

c) Las etiquetas adhesivas que recuerdan a los empleados su responsabilidad personal de mantener la seguridad física cuando utilizan determinados equipos.

d) Los avisos que recuerdan aspectos de la seguridad física en la fase de puesta en marcha (inicialización) de un sistema informático, y que el usuario debe aceptar antes de que la computadora concluya la inicialización o dé inicio a una sesión. (Los sistemas pueden registrar esas aceptaciones, de modo que los usuarios no pueden negar que vieron los avisos.)

e) Los avisos, boletines y circulares de seguridad física elaborados por los directores de seguridad física para recordar al personal determinadas normas de seguridad y combatir la posible complacencia, entre otras cosas.

f) La información sobre los casos de violación de la seguridad física y las enseñanzas extraídas de ellos.

g) La advertencia a las personas sobre amenazas específicas o concretas a la seguridad física y el asesoramiento sobre las formas de combatirlas.

h) La creación de un canal de comunicación con las personas sobre los asuntos de seguridad física en general.

i) La puesta a prueba periódica de los conocimientos de las personas sobre la seguridad física.

j) La intranet de una organización, que también puede ser una herramienta valiosa para transmitir o promover el mensaje de la seguridad física, en la medida en que la naturaleza y sensibilidad del material se mantenga dentro del nivel de clasificación acreditado para la red.

GLOSARIO

activos de información de carácter estratégico. Todo equipo o componente que se utilice para almacenar, procesar, controlar o transmitir información de carácter estratégico. Por ejemplo, son activos de información de carácter estratégico los sistemas de control, las redes, los sistemas de información y cualquier otro medio electrónico o físico.

autoridad competente. Organización o institución gubernamental que ha sido designada por un Estado para desempeñar una o varias funciones de seguridad física nuclear.

confidencialidad. Propiedad en virtud de la cual una información no se pone a disposición o en conocimiento de personas, entidades o procesos no autorizados.

disponibilidad. Propiedad en virtud de la cual un objeto puede ser consultado y utilizado por una entidad autorizada que lo solicite.

información de carácter estratégico. Información, en cualquiera de sus formas, incluidos los programas informáticos, cuya divulgación, modificación, alteración, destrucción o denegación de uso no autorizada podría comprometer la seguridad física nuclear.

integridad. Propiedad de una información que indica que esta es exacta y completa.

material radiactivo. Todo material que, en virtud de lo dispuesto en la legislación o la reglamentación nacional o por un órgano regulador, está sometido a control reglamentario a causa de su radiactividad.

materiales nucleares. Todo material que sea un material fisionable especial o un material básico, según las definiciones que figuran en el artículo XX del Estatuto del OIEA.

necesidad de conocer. Regla en virtud de la cual las personas, los procesos y los sistemas solo pueden tener acceso a la información, los medios y los activos que son necesarios para la ejecución de las funciones que están autorizados a desempeñar.

necesidad de poseer. Regla en virtud de la cual las personas solo pueden tener físicamente en su poder los activos de información que son necesarios para el desempeño eficaz de su trabajo.

objeto de información. Conocimiento o datos que tienen valor para la organización.

otro material radiactivo. Todo material radiactivo que no es un material nuclear.

seguridad física de la información. Preservación de la confidencialidad, integridad y disponibilidad de la información.

vulneración. Violación de la confidencialidad, pérdida de la integridad o pérdida de la disponibilidad, accidentales o deliberadas, de un objeto de información.

PEDIDOS DE PUBLICACIONES

En los siguientes países, 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.

ALEMANIA

Goethe Buchhandlung Teubig GmbH
Schweitzer Fachinformationen
Willstätterstrasse 15, 40549 Dusseldorf, ALEMANIA
Teléfono: +49 (0) 211 49 874 015 • Fax: +49 (0) 211 49 874 28
Correo electrónico: kundenbetreuung.goethe@schweitzer-online.de • Sitio web: www.goethebuch.de

CANADÁ

Renouf Publishing Co. Ltd
22-1010 Polytek Street, Ottawa, ON K1J 9J1, CANADÁ
Teléfono: +1 613 745 2665 • Fax: +1 643 745 7660
Correo electrónico: order@renoufbooks.com • Sitio web: www.renoufbooks.com

Bernan / Rowman & Littlefield
15200 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

ESTADOS UNIDOS DE AMÉRICA

Bernan / Rowman & Littlefield
15200 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
812 Proctor Avenue, Ogdensburg, NY 13669-2205, EE.UU.
Teléfono: +1 888 551 7470 • Fax: +1 888 551 7471
Correo electrónico: orders@renoufbooks.com • Sitio web: www.renoufbooks.com

FEDERACIÓN DE RUSIA

Scientific and Engineering Centre for Nuclear and Radiation Safety
107140, Moscú, Malaya Krasnoselskaya st. 2/8, bld. 5, FEDERACIÓN DE RUSIA
Teléfono: +7 499 264 00 03 • Fax: +7 499 264 28 59
Correo electrónico: secnrs@secnrs.ru • Sitio web: www.secnrs.ru

FRANCIA

Form-Edit
5 rue Janssen, PO Box 25, 75921 París CEDEX, FRANCIA
Teléfono: +33 1 42 01 49 49 • Fax: +33 1 42 01 90 90
Correo electrónico: formedit@formedit.fr • Sitio web: www.form-edit.com

INDIA

Allied Publishers

1st Floor, Dubash House, 15, J.N. Heredi Marg, Ballard Estate, Bombay 400001, INDIA
Teléfono: +91 22 4212 6930/31/69 • Fax: +91 22 2261 7928
Correo electrónico: alliedpl@vsnl.com • Sitio web: www.alliedpublishers.com

Bookwell

3/79 Nirankari, Delhi 110009, INDIA
Teléfono: +91 11 2760 1283/4536
Correo electrónico: bkwell@nde.vsnl.net.in • Sitio web: www.bookwellindia.com

ITALIA

Libreria Scientifica "AEIOU"

Via Vincenzo Maria Coronelli 6, 20146 Milán, ITALIA
Teléfono: +39 02 48 95 45 52 • Fax: +39 02 48 95 45 48
Correo electrónico: info@libreriaaeiou.eu • Sitio web: www.libreriaaeiou.eu

JAPÓN

Maruzen-Yushodo Co., Ltd

10-10 Yotsuyasakamachi, Shinjuku-ku, Tokio 160-0002, JAPÓN
Teléfono: +81 3 4335 9312 • Fax: +81 3 4335 9364
Correo electrónico: bookimport@maruzen.co.jp • Sitio web: www.maruzen.co.jp

REPÚBLICA CHECA

Suweco CZ, s.r.o.

Sestupná 153/11, 162 00 Praga 6, REPÚBLICA CHECA
Teléfono: +420 242 459 205 • Fax: +420 284 821 646
Correo electrónico: nakup@suweco.cz • Sitio web: www.suweco.cz

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: www.iaea.org/books

18-00937S

OBJECTIVE AND ESSENTIAL ELEMENTS OF A STATE'S NUCLEAR SECURITY REGIME
IAEA Nuclear Security Series No. 20
STI/PUB/1590 (15 pp.; 2013)
ISBN 978–92–0–137810–1
Price: €20.00

NUCLEAR SECURITY RECOMMENDATIONS ON NUCLEAR AND OTHER RADIOACTIVE MATERIAL OUT OF REGULATORY CONTROL
IAEA Nuclear Security Series No. 15
STI/PUB/1488 (33 pp.; 2011)
ISBN 978–92–0–112210–0
Price: €23.00

NUCLEAR SECURITY RECOMMENDATIONS ON RADIOACTIVE MATERIAL AND ASSOCIATED FACILITIES
IAEA Nuclear Security Series No. 14
STI/PUB/1487 (27 pp.; 2011)
ISBN 978–92–0–112110–3
Price: €22.00

NUCLEAR SECURITY RECOMMENDATIONS ON PHYSICAL PROTECTION OF NUCLEAR MATERIAL AND NUCLEAR FACILITIES (INFCIRC/225/REVISION 5)
IAEA Nuclear Security Series No. 13
STI/PUB/1481 (57 pp.; 2011)
ISBN 978–92–0–111110–4
Price: €28.00

La seguridad física de la información de carácter estratégico es un principio fundamental de la seguridad física nuclear. La información de carácter estratégico es aquella cuya divulgación (o modificación, alteración, destrucción o denegación de uso) no autorizada podría comprometer la seguridad física nuclear o contribuir de otro modo a la comisión de un acto doloso contra una instalación u organización nuclear o contra un transporte de materiales nucleares. En la presente Guía de Aplicación se definen los conceptos básicos de la seguridad física de la información que pueden aplicarse a la seguridad física nuclear, con el fin de ayudar a los Estados Miembros y a las organizaciones a cumplir sus responsabilidades en este ámbito y elaborar un marco de seguridad física de la información.

ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA
VIENA
ISBN 978–92–0–305417–1
ISSN 2521–1803