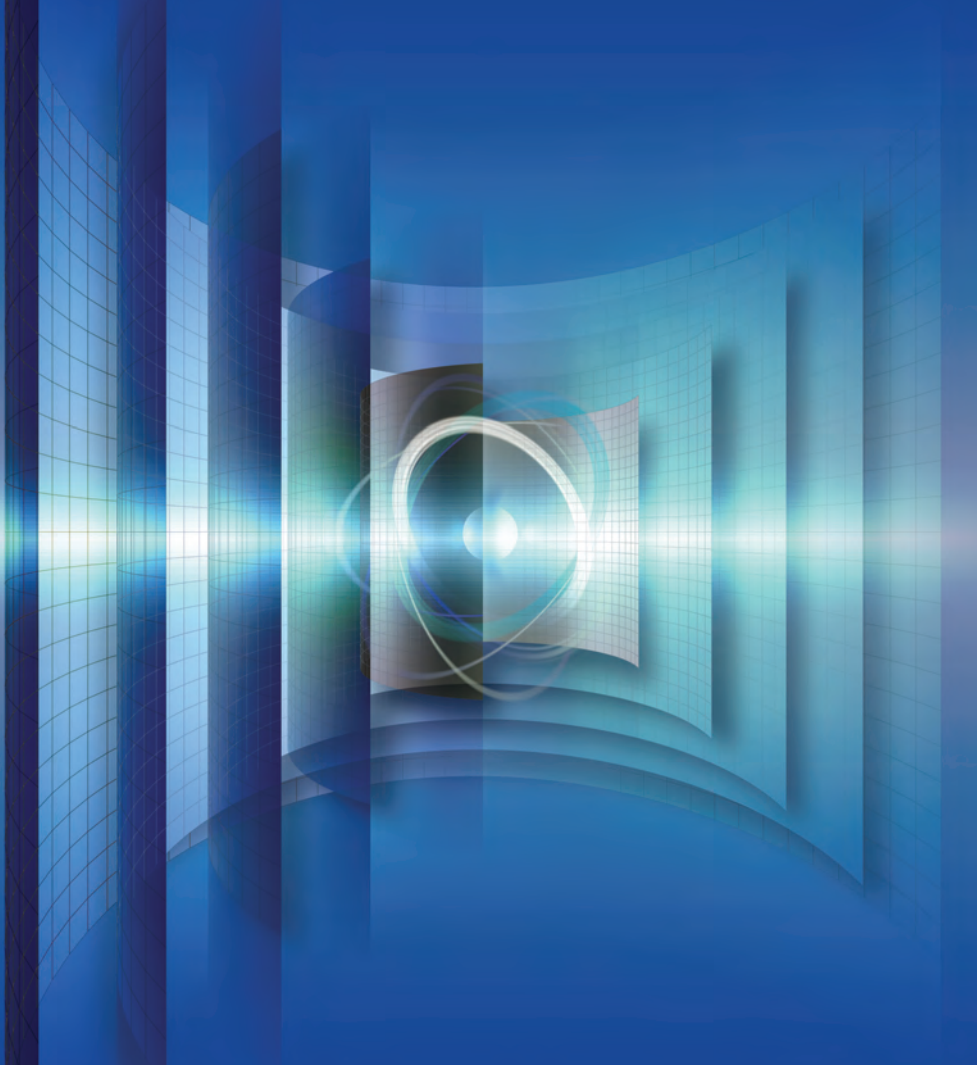
Colección de Seguridad Física Nuclear del OIEA N° 42 G

Guía de Aplicación

Seguridad informática al servicio de la seguridad física 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 INFORMÁTICA
AL SERVICIO DE LA SEGURIDAD FÍSICA NUCLEAR

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

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

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

COLECCIÓN DE SEGURIDAD FÍSICA NUCLEAR DEL OIEA
Nº 42-G

SEGURIDAD INFORMÁTICA AL SERVICIO DE LA SEGURIDAD FÍSICA NUCLEAR

GUÍA DE APLICACIÓN

ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA
VIENA, 2023

DERECHOS DE AUTOR

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

Impreso por el OIEA en Austria
Octubre 2023
STI/PUB/1918

SEGURIDAD INFORMÁTICA AL SERVICIO DE LA SEGURIDAD FÍSICA NUCLEAR
OIEA, VIENA, 2023
STI/PUB/1918
ISBN 978–92–0–121120–0 (paperback : alk. paper) | ISBN 978–92–0–121220–7 (pdf) | ISBN 978–92–0–121320–4 (epub) | ISBN 978–92–0–121420–1 (mobipocket)
ISSN 1816–9317

PREFACIO

Rafael Mariano Grossi
Director General

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

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

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

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

El OIEA también utiliza las orientaciones que figuran en la Colección de Seguridad Física Nuclear del OIEA cuando presta asistencia a los Estados

Miembros mediante sus misiones de examen y servicios de asesoramiento. Esto ayuda a los Estados Miembros en la aplicación de estas orientaciones y permite el intercambio de experiencias y conocimientos valiosos. Las observaciones recibidas sobre estas misiones y servicios, así como las enseñanzas extraídas de los eventos y la experiencia en el uso y la aplicación de las orientaciones sobre seguridad física, se tienen en cuenta durante su revisión periódica.

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

NOTA EDITORIAL

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

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

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

El OIEA no es responsable de la continuidad o exactitud de las URL de los sitios web externos o de terceros en Internet a que se hace referencia en esta publicación y no garantiza que el contenido de dichos sitios web sea o siga siendo preciso o adecuado.

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. Los sistemas computerizados desempeñan un papel esencial en todos los aspectos del funcionamiento tecnológico y físicamente seguro de las instalaciones y actividades en que se utilizan, almacenan y transportan materiales nucleares y otros materiales radiactivos, incluido el mantenimiento de la protección física, y en las medidas de detección y respuesta relacionadas con los materiales no sometidos a control reglamentario. Por lo tanto, todos esos sistemas computerizados han de estar protegidos contra actos delictivos o actos intencionales no autorizados. Se prevé que la utilización de sistemas computerizados en todos los aspectos de las operaciones, incluidas la seguridad física nuclear y la seguridad tecnológica nuclear, aumentará a medida que la tecnología avance.

1.2. En las Nociones Fundamentales de Seguridad Física Nuclear [1] se destaca la importancia de la seguridad de la información, incluida la seguridad informática, en un régimen de seguridad física nuclear, y la necesidad de que en las actividades de garantía se determinen y aborden las cuestiones y los factores que pueden afectar a la capacidad de proporcionar una seguridad física nuclear adecuada, comprendida la cibernética.

1.3. La seguridad de la información de carácter estratégico es un componente del elemento esencial 3 de un régimen nacional de seguridad física nuclear. En la referencia [1] se indica que: “El marco legislativo y reglamentario, y las medidas administrativas asociadas […] prevén el establecimiento de reglamentos y requisitos para proteger la confidencialidad de la *información de carácter estratégico* y para proteger los *recursos de información de carácter estratégico*”. La seguridad de la información de carácter estratégico y de los recursos de información de carácter estratégico conlleva la protección de la confidencialidad, la integridad y la disponibilidad de esa información y de esos recursos. En la Enmienda de la Convención sobre la Protección Física de los Materiales Nucleares [2] también se establece la protección de la confidencialidad de la información como su Principio Fundamental L.

1.4. El párrafo 4.10 de las *Recomendaciones de seguridad física nuclear sobre la protección física de los materiales y las instalaciones nucleares* (INFCIRC/225/Rev.5) [3] dice lo siguiente:

> "Debería velarse por que los sistemas computarizados utilizados para la protección física, la seguridad nuclear y la contabilidad y el control de los materiales nucleares no se vean comprometidos (por ejemplo, por ataques cibernéticos, manipulación o falsificación) de conformidad con la *evaluación de amenazas* o la *amenaza base de diseño*".

1.5. En las *Recomendaciones de seguridad física nuclear sobre materiales radiactivos e instalaciones conexas* [4] y las *Recomendaciones de seguridad física nuclear sobre materiales nucleares y otros materiales radiactivos no sometidos a control reglamentario* [5] también se hace hincapié en la necesidad de evitar el acceso no autorizado a la información de carácter estratégico y de protegerla para que no quede comprometida. En el anexo I se ofrecen orientaciones de la categoría "Recomendaciones" destinadas a complementar las recomendaciones sobre seguridad informática de las referencias [3 a 5] a la espera de una futura revisión de esas publicaciones.

1.6. Cuando se utilizan sistemas computerizados para procesar, transmitir y almacenar información de carácter estratégico en formato digital, es necesario proteger suficientemente su confidencialidad, integridad y disponibilidad mediante la aplicación de medidas de seguridad informática a lo largo del ciclo de vida de esos recursos digitales. La seguridad informática incluye las medidas necesarias para prevenir y detectar los ciberataques, para responder ante ellos y para devolver los sistemas computerizados a su estado anterior.

1.7. En el marco de las amenazas para la seguridad física nuclear, los ciberataques se han definido como un medio para atacar los sistemas computerizados con el fin de llevar a cabo o facilitar actos dolosos, ya sea directamente o en combinación con medios más convencionales, como el acceso físico y los agentes internos. Esos actos podrían dar lugar a la retirada no autorizada de materiales nucleares u otros materiales radiactivos o a sabotajes que podrían tener consecuencias radiológicas inaceptables. Los ciberataques también se podrían utilizar para facilitar otros actos delictivos o actos intencionales no autorizados, como el tráfico ilícito de materiales nucleares u otros materiales radiactivos no sometidos a control reglamentario.

1.8. Por lo tanto, a fin de hacer frente a toda la gama de amenazas potenciales para la seguridad física nuclear, un régimen de seguridad física nuclear tiene

que incluir los medios para contrarrestar las amenazas que tienen o pueden acabar teniendo las destrezas para dirigir ciberataques contra los sistemas computerizados. Además, las amenazas para la seguridad física nuclear que no tienen esas destrezas pueden inducir a las personas que sí las tienen a colaborar (por ejemplo, mediante dinero o coacciones).

1.9. Mantener una seguridad informática eficaz en las instalaciones que manipulan materiales nucleares u otros materiales radiactivos, y en las actividades conexas, como el transporte, es un reto de envergadura, debido a la amenaza sustancial y en rápida evolución. Muchos de los elementos esenciales de un régimen estatal de seguridad física nuclear dependen de los sistemas computerizados o se basan en ellos y, por lo tanto, dependen de una seguridad informática eficaz.

OBJETIVO

1.10. El objetivo de esta publicación es proporcionar orientación sobre el desarrollo y la aplicación de la seguridad informática como componente integral de la seguridad física nuclear.

1.11. La presente guía de aplicación está destinada a las personas encargadas de formular políticas, las autoridades competentes, los explotadores, los remitentes, los transportistas y otras personas con responsabilidades en materia de seguridad física nuclear y seguridad tecnológica nuclear.

ALCANCE

1.12. Las orientaciones de la presente publicación se aplican a los aspectos de seguridad informática de la seguridad física nuclear y a sus interfaces con la seguridad tecnológica nuclear y con otros elementos del régimen de seguridad física nuclear de un Estado, como la protección física de los materiales nucleares y de las instalaciones nucleares, la seguridad de los materiales radiactivos y de las instalaciones y actividades conexas y la detección de sucesos relacionados con la seguridad física nuclear y la respuesta a estos. El alcance de la publicación incluye los sistemas computerizados que podrían afectar negativamente a la seguridad física nuclear o a la seguridad tecnológica nuclear si se vieran comprometidos.

1.13. En la presente publicación se abordan aspectos generales de la seguridad informática aplicables a todos los ámbitos de la seguridad física nuclear, incluida la seguridad física de los materiales nucleares y las instalaciones nucleares, de los

materiales radiactivos y las instalaciones conexas y de los materiales nucleares y otros materiales radiactivos no sometidos a control reglamentario. En las publicaciones 33-T y 17-T (Rev. 1) de la *Colección de Seguridad Física Nuclear del OIEA*, a saber, *Computer Security of Instrumentation and Control Systems at Nuclear Facilities* [6] y *Computer Security Techniques for Nuclear Facilities* [7], figuran orientaciones más detalladas en materia de seguridad informática en relación con la seguridad física de las instalaciones nucleares, incluidos ejemplos concretos de aplicación técnica de las medidas de seguridad informática y de gestión de riesgos de seguridad informática.

1.14. En la presente publicación se hace referencia a las orientaciones sobre seguridad de la información de las Nociones Fundamentales de Seguridad Física Nuclear [1] y a las Recomendaciones de Seguridad Física Nuclear [3 a 5], pero no se ofrecen orientaciones detalladas sobre ese tema en general. En la publicación 23-G de la *Colección de Seguridad Física Nuclear del OIEA, Seguridad física de la información nuclear* [8], se brinda orientación sobre la seguridad física de la información nuclear y la delimitación y protección de la información de carácter estratégico sensible y los recursos de información de carácter estratégico.

ESTRUCTURA

1.15. Después de esta introducción, en la sección 2 se presentan la terminología y los conceptos clave. En la sección 3 se establecen las funciones y responsabilidades del Estado en relación con la seguridad informática en el régimen de seguridad física nuclear, y en la sección 4 se establecen las funciones y responsabilidades de las entidades competentes. En la sección 5 se describen las actividades del Estado a la hora de establecer una estrategia de seguridad informática al servicio de la seguridad física nuclear, y en la sección 6 se describen las actividades para aplicar la estrategia. En la sección 7 se describen los elementos y las medidas de un programa de seguridad informática[1]. En la sección 8 se describen las actividades para mantener la seguridad informática. En el apéndice figuran importantes consideraciones técnicas relativas a las interfaces con la seguridad tecnológica nuclear.

[1] Algunas organizaciones pueden denominar plan de seguridad informática al programa de seguridad informática.

1.16. En el anexo I se proponen orientaciones, de la categoría “Recomendaciones”, sobre seguridad informática para un régimen nacional de seguridad física nuclear, con las que son coherentes las orientaciones de aplicación de la presente publicación. Como apoyo a las orientaciones de la publicación, en los anexos II a IV se ofrecen ejemplos de posibles medidas de aplicación. El anexo II ofrece una visión general de los perfiles de las ciberamenazas. En el anexo III se ofrecen distintos ejemplos de asignación de responsabilidades de seguridad informática en el régimen de seguridad física nuclear y, en el anexo IV, un ejemplo de marco de competencias en materia de seguridad informática.

2. CONCEPTOS Y CONTEXTO

TERMINOLOGÍA CLAVE

2.1. Las organizaciones de un Estado crean, procesan, manejan y almacenan muchos tipos de información. Parte de esa información, como los secretos militares o la información personal de los ciudadanos, puede considerarse que tiene un carácter suficientemente delicado como para necesitar una protección específica. El Estado podrá establecer leyes nacionales de seguridad de la información en las que se precise y clasifique la información y se definan los requisitos específicos de protección, incluidos los relativos a los datos en formato digital y a los sistemas computerizados conexos. La información que forma parte del régimen de seguridad física nuclear del Estado estará sujeta a esos requisitos, y puede ser necesario proteger otra información adicional, o aumentar la protección de determinados tipos de información que, si se viera comprometida, podría ayudar a un adversario a llevar a cabo un acto doloso contra una instalación o actividad u otro acto delictivo o intencional no autorizado que guarde relación con materiales nucleares u otros materiales radiactivos. Por información de carácter estratégico se entiende la información, sea cual sea su forma, comprendidos los programas informáticos, cuya revelación, modificación, alteración o destrucción no autorizadas o la denegación de cuya utilización podría comprometer la seguridad física nuclear [1]. En la figura 1 se ilustran los conceptos y las relaciones entre los recursos de información de carácter estratégico, los sistemas computerizados y los recursos digitales de carácter estratégico. Estos conceptos se describen más adelante.

2.2. Los recursos de información de carácter estratégico se definen [1] como cualquier equipo o componente utilizado para almacenar, procesar, controlar

o transmitir información de carácter estratégico. La información de carácter estratégico puede estar en formato digital o en cualquier otro formato.

2.3. Los sistemas computerizados son tecnologías que crean, procesan, computan, comunican o almacenan información digital, proporcionan acceso a ella o realizan, prestan o controlan servicios relacionados con esa información. Esos sistemas pueden incluir computadoras de sobremesa, computadoras portátiles, tabletas y otras computadoras personales, teléfonos inteligentes, computadoras centrales, servidores, dispositivos de instrumentación y control digitales, controladores lógicos programables, impresoras, dispositivos de red y componentes y dispositivos integrados. También pueden incluir servicios virtuales, como la computación en nube o las máquinas virtuales. Asimismo, pueden existir como un solo componente o como una colección de recursos digitales.

2.4. Los sistemas computerizados desempeñan muchas funciones en un Estado. Puede haber sistemas computerizados en el régimen de seguridad física nuclear que proporcionen valiosas funciones institucionales y de comunicación, pero que no tengan carácter estratégico en relación con la seguridad física nuclear y, por lo tanto, queden fuera del alcance de las orientaciones de la presente publicación.

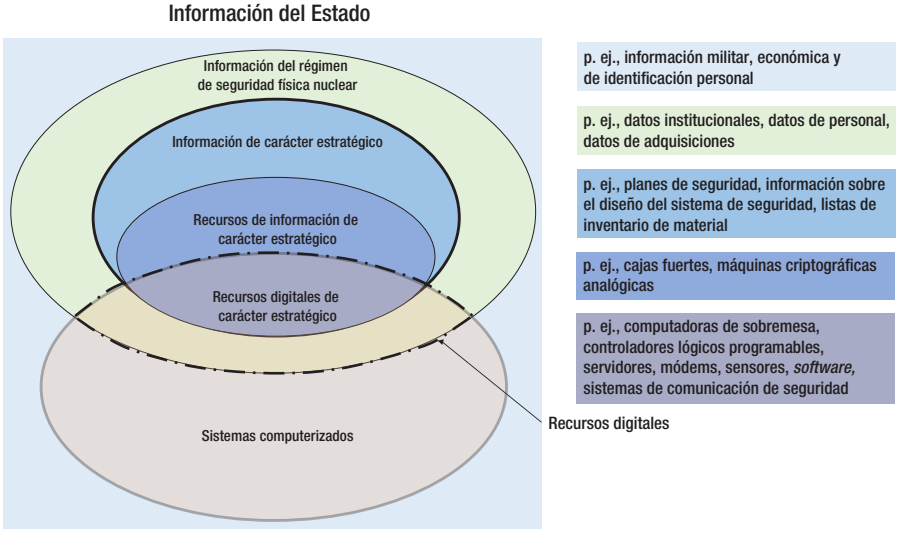


Fig. 1. Sistemas de información y sistemas computerizados en el Estado y en el régimen de seguridad física nuclear.

2.5. Los recursos de información de carácter estratégico tienen que protegerse para evitar que la información de carácter estratégico que almacenan, procesan, controlan o transmiten se vea comprometida. Los enfoques de protección variarán según el tipo de recurso en cuestión y la forma de la información. En la referencia [8] se aborda principalmente la protección de la información escrita en papel y otra información en forma de "copia impresa". Los recursos digitales son sistemas computerizados (o partes de ellos) que están asociados al régimen de seguridad física nuclear de un Estado o que se encuentran dentro de él. Por "recurso digital de carácter estratégico" se entienden los recursos de información de carácter estratégico que son sistemas computerizados (o forman parte de ellos). Los recursos digitales de carácter estratégico necesitan medidas de seguridad informática para su protección.

2.6. Los recursos digitales de carácter estratégico respaldan sistemas que realizan funciones de seguridad tecnológica nuclear, seguridad física nuclear y contabilidad y control de materiales nucleares, o que almacenan y procesan información de carácter estratégico relacionada con esas funciones. Los recursos digitales de carácter estratégico y, por tanto, las funciones esenciales que desempeñan, pueden ser vulnerables a los ciberataques y pueden ser un objetivo específico de los adversarios. Si se produjera un ataque de ese tipo y los recursos digitales de carácter estratégico se vieran comprometidos, podría haber repercusiones negativas en la seguridad nuclear física y tecnológica. Si los recursos digitales de carácter estratégico se vieran comprometidos, la situación resultante podría contribuir o dar lugar, por ejemplo, a los siguientes escenarios:

a) Un sabotaje que provoque consecuencias radiológicas inaceptables o consecuencias radiológicas graves si se vieran afectadas zonas vitales;
b) La retirada no autorizada de materiales nucleares u otros materiales radiactivos;
c) Capacidades degradadas para la prevención, la detección y la respuesta en caso de sucesos relacionados con la seguridad física nuclear;
d) Pérdida, alteración o denegación del acceso a información de carácter estratégico.

2.7. Dependiendo de la situación, el *software* puede tener que ser tratado como información o como parte integrante de un sistema computerizado, o como ambas cosas. Por ejemplo, en su fase inicial de diseño, el *software* puede ser una expresión de alto nivel de un algoritmo de procesamiento, de modo que es mejor tratarlo como información. En su forma operacional (es decir, ejecutable), el *software* formará parte intrínseca de su sistema computerizado conexo, sin el cual

el sistema no funciona, y la mayoría de los ciberataques tendrán como objetivo aprovechar la vulnerabilidad de ese *software*.

2.8. La seguridad informática es un aspecto particular de la seguridad de la información que se ocupa de la protección de los sistemas computerizados para evitar que se vean comprometidos. Quedan comprendidos todos los sistemas interconectados y las redes de las que esos sistemas forman parte. Tanto "seguridad de la tecnología de la información" como "ciberseguridad" se consideran, a los efectos de la presente publicación, sinónimos de "seguridad informática" y no se utilizan. La seguridad informática es un subconjunto de la seguridad de la información, como se indica en la referencia [8]. La seguridad de la información y la seguridad informática suelen compartir objetivos, metodología y terminología.

2.9. En vista de la interconectividad de las redes informáticas y del flujo de información, también se necesitan medidas de seguridad informática para proteger los recursos digitales de carácter estratégico contra las amenazas que explotan otros recursos digitales y otros sistemas computerizados. La aplicación de un enfoque graduado de medidas de seguridad graduadas que englobe todos los recursos digitales proporciona una defensa en profundidad contra los ciberataques.

DETERMINACIÓN DE LOS RECURSOS DIGITALES DE CARÁCTER ESTRATÉGICO

2.10. Los propietarios o diseñadores de sistemas computerizados deberían utilizar un proceso sistemático a fin de precisar las funciones que realizan sus recursos digitales necesarios para la seguridad nuclear física y tecnológica, los recursos digitales de carácter estratégico conexos y el efecto potencial en la seguridad nuclear física y tecnológica si los recursos digitales de carácter estratégico se vieran comprometidos. Al llevar a cabo esa labor, deberían comprender que un sistema computerizado que no contenga en sí mismo recursos digitales de carácter estratégico podría, con todo, si se viera comprometido o acabara infectado por un programa malicioso[2], repercutir en los recursos digitales de carácter estratégico de otros sistemas.

[2] Los programas maliciosos (*malware*) son las formas de código informático diseñado intencionalmente para realizar un acto doloso. Por ejemplo, pueden facilitar el robo de información de carácter estratégico, comprometer el diseño de un sistema computerizado o comprometer una función realizada por un sistema computerizado.

2.11. La seguridad informática tiene como objetivo mantener los atributos de confidencialidad, integridad y disponibilidad de los recursos digitales de carácter estratégico y de la información de carácter estratégico que contienen. Los recursos digitales de carácter estratégico y su información de carácter estratégico respaldan el correcto funcionamiento de las funciones que sustentan el régimen de seguridad física nuclear. Según la información de carácter estratégico que contenga, y de la función del sistema que realice cada recurso digital de carácter estratégico, se deberían considerar las necesidades de protección de cada uno de esos atributos.

2.12. El primer paso de un proceso sistemático debería consistir en determinar las funciones que respaldan directamente uno o más aspectos de la seguridad física nuclear (por ejemplo, la protección física, la contabilidad y el control de los materiales nucleares y la gestión de la información de carácter estratégico) y la seguridad tecnológica nuclear. A continuación, deberían determinarse cuáles son los sistemas computerizados y los recursos digitales que los componen que respaldan esas funciones.

2.13. Posteriormente, debería realizarse un análisis inicial de las consecuencias de que los recursos digitales dentro de dichos sistemas se vieran comprometidos a fin de determinar los recursos que, si se quedaran comprometidos en un ciberataque, podrían influir en las funciones necesarias del sistema y, por tanto, repercutir negativamente en la seguridad física nuclear. Los recursos digitales que podrían causar efectos adversos si se vieran comprometidos son los recursos digitales de carácter estratégico. Ese proceso se ilustra en la figura 2. El análisis inicial debería realizarse sin tener en cuenta las medidas de seguridad informática existentes, con el objeto de determinar cuál sería el efecto más grave si los recursos digitales se vieran comprometidos.

2.14. El proceso debería incluir también la evaluación de los sistemas de apoyo, o de los equipos no asociados directamente a las funciones de seguridad nuclear tecnológica y física, para determinar si un ciberataque en esos sistemas o equipos podría afectar directa o indirectamente a las funciones de seguridad nuclear tecnológica y física. Los recursos digitales que se podrían conectar temporalmente a un recurso digital de carácter estratégico también deberían ser evaluados para su posible clasificación como recursos digitales de carácter estratégico. Algunos ejemplos de esos sistemas pueden ser las computadoras con fines de mantenimiento y los equipos de prueba digitales.

2.15. Las organizaciones pueden elegir entre diferentes estrategias para gestionar los recursos digitales de carácter estratégico. Pueden agrupar los recursos digitales de carácter estratégico —por ejemplo, los que pertenecen al mismo sistema o

los que son de naturaleza similar— y gestionar todos los recursos digitales de carácter estratégico en un grupo de forma colectiva. Por lo tanto, un sistema computerizado que realice una función importante puede tratarse como un recurso digital de carácter estratégico o como un conjunto de componentes de recursos digitales de carácter estratégico. Esa agrupación debería ayudar a garantizar que se brinden niveles similares de protección a los recursos digitales de carácter estratégico que, en caso de verse comprometidos, conllevarían consecuencias potenciales similares. Una vez definidos y clasificados los recursos digitales de carácter estratégico en función de las consecuencias potenciales si se vieran comprometidos, se puede aplicar un enfoque graduado, mediante la defensa en profundidad.

2.16. Los requisitos de confidencialidad, integridad y disponibilidad de cada recurso digital de carácter estratégico deberían determinarse por conducto de la evaluación de su contribución a la seguridad nuclear física y tecnológica y a las consecuencias potenciales del mal funcionamiento de ese recurso digital de carácter estratégico tras un ciberataque. Esa determinación puede requerir el juicio de un experto en la materia, a partir de principios y procesos analíticos.

2.17. Hasta que no se haya evaluado un sistema computerizado para determinar si es o no un recurso digital de carácter estratégico (o si contiene recursos digitales de carácter estratégico), ese sistema debería tratarse como “no asignado”. Las medidas de seguridad informática para los recursos no asignados deberían ser, por lo general, muy estrictas, como un enfoque prudente, puesto que se desconocen

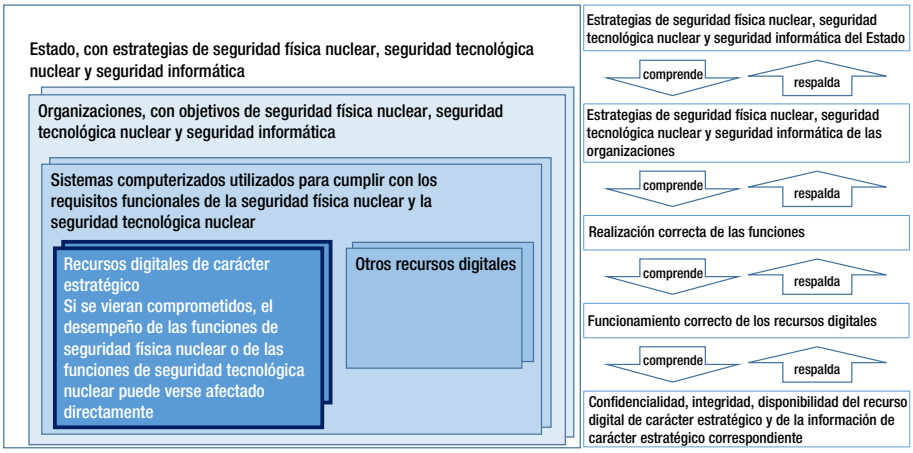


Fig. 2. Diagrama conceptual de un recurso digital de carácter estratégico dentro del sistema computerizado de una organización.

los efectos potenciales de un ciberataque. Se debería considerar la posibilidad de prohibir o restringir la utilización de esos recursos dentro del régimen de seguridad física nuclear. Por ejemplo, se puede prohibir la utilización de los dispositivos privados del personal, como teléfonos móviles y tabletas, dentro de las instalaciones nucleares, y se puede prohibir la conexión de computadores de terceros a los sistemas de una instalación nuclear hasta que se evalúen por completo. La definición adecuada de lo que constituye un recurso digital de carácter estratégico, de su extensión, límites e interfaces, y de los niveles aceptables de dependencia de otros recursos digitales, son aspectos fundamentales para crear un diseño seguro que exigen un juicio experto a partir de principios de seguridad informática e ingeniería de sistemas. Por ejemplo, si se modifica el diseño general del sistema para transferir las funciones entre los recursos digitales de carácter estratégico y otros recursos digitales, puede simplificarse la definición de los recursos digitales de carácter estratégico y, por ende, pueden simplificarse las medidas de seguridad informática conexas.

2.18. Cabe prestar especial atención si se utilizan recursos digitales de carácter estratégico de servicios virtuales por contrato, como la computación en la nube, dado que esos servicios incluyen elementos que no están bajo el control directo del propietario de los datos. Por ejemplo, un recurso digital de carácter estratégico consistente en una aplicación o servicio basado en la nube se basará en el *software* y el *hardware* conexos que se encuentran bajo el control del operador de la nube (por ejemplo, el almacenamiento en la nube). En esos casos, debería haber requisitos contractuales estrictos sobre cuestiones como el control de acceso, la disponibilidad, la segregación de datos, la destrucción de datos, la interfaz de comunicación, el *software*, el *hardware* y los procesos administrativos, con el fin de garantizar que la aplicación esté adecuadamente protegida contra el acceso y la manipulación no autorizados. La contratación del suministro de recursos digitales de carácter estratégico a otra organización (es decir, la subcontratación) no elimina la responsabilidad del propietario u operador del proceso en cuanto a la protección de ese recurso digital de carácter estratégico.

2.19. Los recursos digitales de carácter estratégico pueden incluir componentes de sistemas de tecnología de la información y sistemas de tecnología operacional. Las medidas de seguridad informática adecuadas para esos componentes dependerán del tipo de sistema y de su función. Sin embargo, a menudo existen interfaces entre los sistemas de tecnología de la información y los de tecnología operacional, y el conjunto de medidas de seguridad informática aplicadas a los distintos sistemas debería tener en cuenta esas interfaces.

2.20. Se han aplicado procesos, que suelen denominarse “modelos de ciclo de vida”, para garantizar que los recursos digitales de carácter estratégico cumplen sus requisitos especializados. Los modelos de ciclo de vida describen las actividades de desarrollo, funcionamiento, mantenimiento y retirada de los recursos digitales de carácter estratégico, así como las relaciones entre esas actividades. La seguridad informática ha de tenerse en cuenta en todas las fases del ciclo de vida de los recursos digitales de carácter estratégico. Las instalaciones, las funciones, los sistemas, los componentes, los recursos digitales de carácter estratégico y otros recursos digitales pueden tener su propio ciclo de vida, con interacciones entre ellos. El ciclo de vida teórico para el desarrollo de sistemas, establecido en relación con los sistemas de instrumentación y control, puede utilizarse como base para el ciclo de vida de los sistemas computerizados, incluidos los recursos digitales de carácter estratégico, y debería considerarse en el contexto de la vida útil de una instalación.

CIBERATAQUE

2.21. El término “ciberataque” se utiliza para describir un acto doloso con la intención de robar, alterar o destruir un objetivo específico, o impedir el acceso a este, mediante el acceso no autorizado a un sistema computerizado susceptible (o mediante acciones dentro de él). Los ciberataques ponen en peligro la confidencialidad, la integridad o la disponibilidad[3] (o una combinación de estas propiedades) de la información de carácter estratégico dentro de un recurso digital de carácter estratégico, o del propio recurso digital de carácter estratégico, y pueden utilizarse para llevar a cabo o facilitar un acto doloso contra una instalación o actividad u otro acto delictivo o intencional no autorizado que guarde relación con materiales nucleares u otros materiales radiactivos. Un concepto estrechamente relacionado es el de ataque no selectivo, en el que, por ejemplo, se pueden introducir inadvertidamente códigos maliciosos no selectivos en sistemas y redes informáticos. Un ataque de ese tipo también podría incidir negativamente en la seguridad física nuclear.

2.22. Un ciberataque puede llevarse a cabo por conducto de un acceso físico directo a la información o a los recursos de información o a través de un acceso electrónico, o mediante una combinación de ambos, y puede ser llevado a cabo directamente por un adversario o por un agente interno (o con su ayuda)

[3] Se supone que la protección de otras propiedades, como la autenticación y el no rechazo, está incluida en la protección de la confidencialidad, la integridad y la disponibilidad.

influenciado deliberadamente o no por un adversario. Los ciberataques, una vez detectados, deberían tratarse como incidentes de seguridad informática.

2.23. Los incidentes de seguridad informática ocasionados por los ciberataques pueden dar lugar a otros incidentes de seguridad informática y, en última instancia, a sucesos relacionados con la seguridad física nuclear, ya sea directamente o como parte de una secuencia de actividades dolosas, que pueden incluir otros ciberataques, o el acceso físico no autorizado o la explotación de agentes internos, o una mezcla en un ataque combinado.

LA SEGURIDAD INFORMÁTICA EN LA SEGURIDAD FÍSICA NUCLEAR

2.24. El régimen de seguridad física nuclear aborda los tres ámbitos tratados en las referencias [3 a 5], y la seguridad informática respalda los objetivos de seguridad física nuclear en cada uno de esos ámbitos. El papel de la seguridad informática en cada uno de esos ámbitos se describe brevemente en las siguientes secciones.

Materiales nucleares e instalaciones nucleares

2.25. La protección física de los materiales nucleares y de las instalaciones nucleares depende de las medidas de seguridad para lograr los siguientes objetivos [3]:

a) proteger contra la retirada no autorizada;
b) localizar y recuperar materiales nucleares desaparecidos;
c) proteger contra el sabotaje;
d) mitigar o reducir al mínimo los efectos del sabotaje.

2.26. Los sistemas computerizados de las instalaciones nucleares respaldan las funciones de control de procesos, seguridad tecnológica nuclear, seguridad física nuclear y contabilidad y control de materiales nucleares. Para la ejecución de cada una de esas funciones se utilizan recursos digitales de carácter estratégico que podrían seleccionarse a fin de facilitar un ataque independiente o utilizarse en combinación con un ataque físico (por ejemplo, un ataque combinado). La seguridad informática es necesaria para proteger estos sistemas computerizados de los ciberataques.

Material radiactivo e instalaciones conexas

2.27. El material radiactivo se utiliza en todo el mundo para una gran variedad de propósitos, incluidos muchos en los que no hay presencia de materiales nucleares. Los sistemas computerizados se utilizan de forma creciente en esos sectores con fines de seguridad tecnológica, seguridad física y realización de operaciones. Las medidas de seguridad, incluidas las de seguridad informática, son necesarias a fin de evitar el acceso no autorizado o la adquisición de ese material para un acto doloso, o el sabotaje de ese material y de las instalaciones conexas.

2.28. El marco legislativo y reglamentario debería reflejar el hecho de que el registro nacional de fuentes radiactivas o materiales radiactivos contendrá normalmente información de carácter estratégico que ha de protegerse. La seguridad informática es necesaria en este ámbito para proteger la confidencialidad, la integridad y la disponibilidad de la información de carácter estratégico y de los recursos de información de carácter estratégico, incluidos los recursos digitales de carácter estratégico; por ejemplo, para respaldar la confidencialidad y la integridad de los registros de fuentes y la disponibilidad de los datos necesarios para responder a los incidentes.

Materiales nucleares y otros materiales radiactivos no sometidos a control reglamentario

2.29. Los materiales no sometidos a control reglamentario son los materiales nucleares u otros materiales radiactivos presentes en cantidad suficiente que deberían estar sometidos a control reglamentario pero no lo están, bien porque los controles han fallado por algún motivo o porque esos controles nunca existieron. La seguridad de los materiales nucleares y otros materiales radiactivos no sometidos a control reglamentario se logra mediante la acción coordinada de las autoridades competentes para llevar a cabo las funciones que se les han asignado de prevención, detección y respuesta en caso de sucesos relacionados con la seguridad física nuclear. Los recursos digitales de carácter estratégico componen o respaldan muchos de los sistemas utilizados para realizar esas funciones.

2.30. La seguridad informática es necesaria en este ámbito, por ejemplo, para proteger la confidencialidad de la información de carácter estratégico, la integridad de los sistemas de detección, la confidencialidad, la integridad y la disponibilidad de los sistemas de transmisión de datos, y la disponibilidad de las medidas de apoyo a la respuesta, como las comunicaciones y la investigación forense nuclear.

AMENAZAS, FACTORES DE VULNERABILIDAD Y MEDIDAS DE SEGURIDAD INFORMÁTICA

Amenazas

2.31. Una amenaza es una persona o grupo de personas con motivación, intención y capacidad para cometer un acto doloso. La persona que realiza o intenta realizar un acto doloso es un adversario.

2.32. Comprender las amenazas y los riesgos asociados a los posibles ciberataques es esencial para desarrollar una seguridad informática eficaz en el contexto de la seguridad física nuclear. Hay que comprender, entre otros aspectos, la motivación, las intenciones, las capacidades y las tácticas que puede tener una amenaza para la seguridad física nuclear a la hora de planificar y llevar a cabo un ciberataque. En el anexo II figuran algunos ejemplos de caracterización general de las amenazas para la seguridad física nuclear que pueden recurrir a los ciberataques.

Factores de vulnerabilidad

2.33. Los factores de vulnerabilidad de un sistema computerizado o de una red son atributos operacionales que hacen que el sistema esté abierto a la explotación o sea susceptible a una determinada amenaza. Estas deficiencias pueden ser de carácter administrativo, físico o técnico. A través de la explotación de los factores de vulnerabilidad, un adversario puede obtener acceso no autorizado o el control de un recurso digital de carácter estratégico. Las consecuencias asociadas a la explotación de un factor de vulnerabilidad en un recurso digital de carácter estratégico pueden ser desde insignificantes hasta graves, dependiendo de su capacidad potencial para incidir negativamente en el funcionamiento del recurso digital de carácter estratégico y su función.

2.34. La complejidad del *hardware* y del *software* de los sistemas computerizados aumenta continuamente, al igual que el número de sistemas computerizados y su interconectividad. Esa complejidad aumenta el reto de mantener un conocimiento cabal de los sistemas y, por ende, de mantener los conocimientos necesarios para gestionar la seguridad. El número de factores de vulnerabilidad de un sistema puede estar relacionado con su complejidad y, por lo tanto, los sistemas solo deberían ser tan complejos como sea necesario para su función prevista.

2.35. La explotación de los factores de vulnerabilidad recién descubiertos constituye la base de muchos ciberataques exitosos. Por ejemplo, los “ataques de día cero” son situaciones en que el adversario explota un factor de vulnerabilidad

que es desconocido para el defensor. Además, la rápida evolución de las nuevas tecnologías informáticas ofrece oportunidades para que la naturaleza de los factores de vulnerabilidad cambie, con nuevas clases enteras de vulnerabilidad que solo se hacen evidentes después de que esas nuevas tecnologías hayan sido adoptadas y sean operacionales.

2.36. Debido a la complejidad de algunos sistemas computerizados y a la posibilidad de que haya factores de vulnerabilidad ocultos en ellos, es posible que las medidas de seguridad informática disponibles no sean suficientes a fin de reducir el riesgo a un nivel aceptable para su empleo en aplicaciones específicas de seguridad nuclear física y tecnológica. Cuando las medidas no puedan reducir el riesgo a un nivel aceptable, deberían considerarse enfoques alternativos (por ejemplo, un diseño diferente o una asignación distinta de las funciones).

Enfoque graduado y defensa en profundidad para la seguridad informática

2.37. Las medidas de seguridad informática pueden ser técnicas, físicas o administrativas, o una combinación de ellas. Se debería elegir una combinación de medidas de control mediante un enfoque basado en el conocimiento de los riesgos, que se aplique mediante un enfoque graduado y la defensa en profundidad, a fin de lograr una seguridad informática adecuada. Las medidas específicas de seguridad informática aplicadas pueden ser una combinación de algunas medidas prescritas por orientaciones de categoría superior o requisitos estatales, y otras pueden venir determinadas por un explotador a través de su propio proceso de conocimiento de riesgos.

2.38. Los niveles de seguridad informática son una forma de indicar el alcance y el rigor de la seguridad que se considera necesaria para los diferentes recursos digitales de carácter estratégico. Cada nivel de un enfoque graduado necesitará un conjunto diferente de medidas de protección para satisfacer los requisitos de seguridad de ese nivel. Los requisitos más estrictos se aplican a los recursos digitales de carácter estratégico más críticos. Este principio aparece ilustrado en la figura 3.

2.39. Una forma práctica de aplicar un enfoque graduado consiste en agrupar los sistemas computerizados y los recursos digitales de carácter estratégico conexos en zonas de seguridad informática y aplicar medidas de seguridad informática graduadas para cada zona en función de los requisitos de protección (es decir, el nivel de seguridad). A continuación, se asigna un nivel de seguridad informática a cada zona específica en función del impacto potencial de los ciberataques en las funciones, los sistemas y los recursos digitales de carácter estratégico de la zona.

2.40. El uso de los niveles de seguridad informática, representado en la figura 3, es un enfoque graduado que implica determinar cuáles son los requisitos de seguridad informática proporcionales a las posibles consecuencias de un ciberataque exitoso. Las siguientes consideraciones podrían orientar la aplicación de ese método:

a) Los requisitos de protección de mayor nivel se aplicarían a los recursos digitales de carácter estratégico que podrían provocar las consecuencias más graves si se vieran comprometidos, incluidos los sucesos relacionados con la seguridad física nuclear más significativos.
b) Los requisitos de protección de menor nivel se aplicarían a los sistemas computerizados que tienen funciones relacionadas con la seguridad física nuclear, pero que no se consideran recursos digitales de carácter estratégico.
c) Los requisitos genéricos se aplicarían a todos los niveles de seguridad y a los sistemas computerizados con funciones relacionadas con la seguridad física nuclear, y pueden abordarse mediante medidas de seguridad informática comunes a los sistemas computerizados de otros ámbitos.

2.41. Las medidas de seguridad informática también son necesarias para los sistemas computerizados que no se consideran recursos digitales de carácter estratégico. Dada la interconectividad de las redes informáticas y el flujo de información, es necesario aplicar un enfoque por capas de requisitos de seguridad informática graduados que englobe todos los sistemas computerizados para

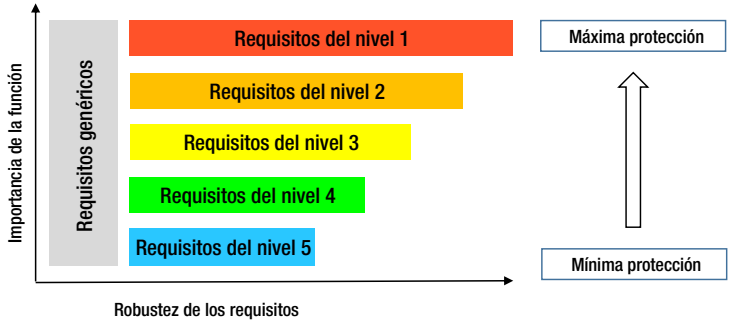


Fig. 3. Ilustración del enfoque graduado mediante la utilización del concepto de nivel de seguridad informática.

proporcionar una defensa en profundidad contra los ciberataques. En el ejemplo anterior, es probable que los sistemas computerizados de las zonas con requisitos de nivel 4 y nivel 5 no figuren clasificados como recursos digitales de carácter estratégico, pero que se apliquen medidas de protección a los sistemas de estas zonas para proporcionar distintas capas de defensa a fin de evitar que haya intrusiones en los recursos digitales de carácter estratégico de las zonas con niveles superiores o que esos se vean comprometidos.

2.42. La defensa en profundidad para la seguridad informática implica establecer distintas capas defensivas de medidas de seguridad informática que tendrían que fallar o ser eludidas para que un ciberataque progrese y afecte negativamente a un recurso digital de carácter estratégico. La combinación adecuada de medidas de seguridad informática complementarias y superpuestas proporciona una defensa en profundidad. La defensa en profundidad se consigue no solo implantando distintas capas defensivas, sino también aplicando medidas de seguridad informática con fines de prevención, detección, protección, respuesta, mitigación de los efectos y facilitación de la recuperación en caso de ataque a un recurso digital de carácter estratégico. Por ejemplo, si se produjera un fallo en la prevención (por ejemplo, la vulneración de una política que prohíba el uso de medios de almacenamiento portátiles) o si se eludieran los mecanismos de protección (por ejemplo, por un nuevo virus no reconocido como ciberataque), seguirían existiendo mecanismos para detectar cualquier alteración no autorizada en un recurso digital de carácter estratégico afectado y responder ante ella.

2.43. Una defensa en profundidad eficaz también significa que, por su diseño, ningún fallo de una medida de seguridad informática de una capa debería invalidar o hacer ineficaz más de una capa. Por ejemplo, la explotación de una vulnerabilidad crítica dentro de un dispositivo de protección utilizado habitualmente podría permitir que se eludieran distintas capas de defensa, a menos que la defensa en profundidad proporcionara una diversidad de dispositivos, configuraciones u otras medidas. La diversidad de las medidas de seguridad informática debería gestionarse de manera que haya un equilibrio entre la defensa en profundidad proporcionada y la complejidad del sistema.

2.44. La defensa en profundidad puede depender de un diseño del sistema que comprenda zonas de diferentes niveles de seguridad informática, a menudo visualizadas como anillos concéntricos. Un principio general es que solo deberían existir conexiones directas entre zonas de seguridad informática adyacentes.

2.45. La eficacia de la defensa en profundidad también puede aumentar si las diferentes partes de la organización operativa tienen funciones y responsabilidades

complementarias en materia de seguridad informática, con una separación efectiva de funciones, de manera que cualquier error cometido por una persona pueda ser advertido por otra y corregido.

2.46. La determinación de las amenazas y los factores de vulnerabilidad y la evaluación de riesgos facilitan la base del conocimiento de los riesgos para determinar las medidas de seguridad proporcionadas. En ese contexto, el riesgo es la posibilidad de que se produzcan efectos adversos en los recursos digitales de carácter estratégico y, por consiguiente, en la seguridad nuclear física y tecnológica, como consecuencia de las amenazas para la seguridad física nuclear que explotan los factores de vulnerabilidad, de modo que es una función de la probabilidad de un ataque y de la gravedad de sus consecuencias. La relación entre estos términos se puede explicar de la siguiente manera en el contexto de la seguridad informática, como se ilustra en la figura 4:

a) Los propietarios de los sistemas computerizados del régimen de seguridad física nuclear tratan de evitar los sucesos relacionados con la seguridad física nuclear y, por lo tanto, tratan de minimizar los riesgos de incidentes de seguridad informática que podrían contribuir a los sucesos relacionados con la seguridad física nuclear.
b) Las amenazas para la seguridad física nuclear pueden tener la intención de provocar sucesos relacionados con la seguridad física nuclear y pueden tener como objetivo los recursos digitales de carácter estratégico para comprometerlos o sabotearlos.
c) En consecuencia, las amenazas para la seguridad nuclear pueden iniciar actividades que exploten los factores de vulnerabilidad, lo que entraña riesgos de seguridad informática para los recursos digitales de carácter estratégico; esos riesgos pueden derivar en sucesos relacionados con la seguridad física nuclear.
d) Los propietarios imponen medidas de seguridad informática para reducir los riesgos de seguridad informática de los recursos digitales de carácter estratégico.
e) Un enfoque basado en el conocimiento de los riesgos puede incluir la consideración de la probabilidad de determinados incidentes de seguridad informática a la hora de determinar las medidas de seguridad informática proporcionadas. Los riesgos pueden reducirse eliminando la amenaza, imponiendo medidas de seguridad informática que disminuyan la probabilidad de que un ataque dé lugar a un incidente de seguridad informática, o limitando o mitigando la gravedad del efecto del incidente de seguridad informática.

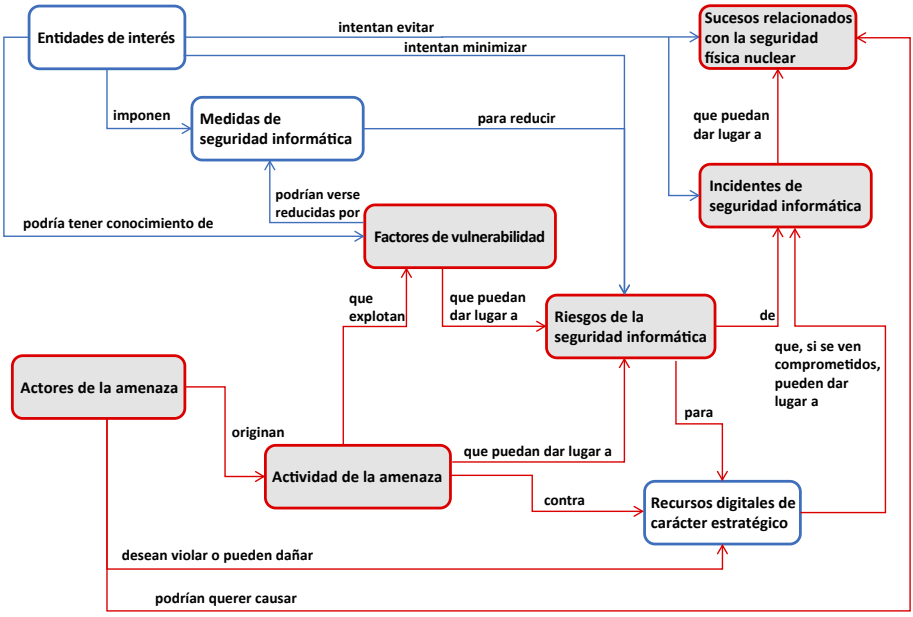


Fig. 4. Enfoque basado en el conocimiento de los riesgos para las medidas de seguridad informática (adaptado de la norma ISO/IEC 27005:2018) [9].

f) La determinación de los riesgos y su gestión conexa deberían ser procesos continuos que respondan a los cambios en los factores de riesgo.

Responsabilidades en materia de seguridad informática en un régimen de seguridad física nuclear

2.47. Muchas organizaciones dentro de un régimen de seguridad física nuclear utilizan sistemas computerizados para funciones como el procesamiento de la información, la seguridad física nuclear, la seguridad tecnológica nuclear y la contabilidad y el control de los materiales nucleares.

2.48. Cada una de esas organizaciones es responsable de proteger la información de carácter estratégico que contienen esos sistemas y los recursos digitales de carácter estratégico conexos.

2.49. En la figura 5 se ilustra una representación de las organizaciones de un régimen de seguridad física nuclear que pueden tener responsabilidades en materia de seguridad informática. Entre ellas se encuentran las autoridades

competentes[4] y los explotadores[5], que tienen responsabilidades en materia de seguridad informática en el régimen de seguridad física nuclear que se asignan a través de los requisitos jurídicos y reglamentarios nacionales.

2.50. El Estado puede tener una o varias autoridades competentes designadas para la seguridad informática, que puede ser diferente de las autoridades competentes con responsabilidades en materia de seguridad física nuclear. Además, las autoridades competentes pueden tener requisitos de seguridad informática dictados por requisitos jurídicos y normas nacionales ajenos al régimen de seguridad física nuclear.

2.51. Los proveedores, contratistas y suministradores incluyen organizaciones que facilitan bienes y servicios a las autoridades competentes y los explotadores, pero cuyas responsabilidades en materia de seguridad informática (por ejemplo, proteger la información de carácter estratégico y los recursos digitales de carácter estratégico conexos) pueden derivarse no de los requisitos jurídicos y reglamentarios nacionales, sino de las condiciones especificadas en sus contratos con las autoridades competentes y los explotadores.

2.52. Las funciones y responsabilidades relacionadas con la seguridad informática del Estado, las autoridades competentes y los explotadores, así como las de los proveedores, contratistas y suministradores, se explican de forma más pormenorizada en las secciones 3 y 4.

COMPETENCIAS Y CAPACIDADES EN MATERIA DE SEGURIDAD INFORMÁTICA

2.53. La seguridad informática eficaz y sólida se aplica, se mantiene y se sustenta gracias a un personal competente y de confianza con una gestión eficaz y un liderazgo activo y bien fundamentado. Cada organización del régimen de seguridad física nuclear debería, según sus funciones y responsabilidades particulares, desarrollar y mantener competencias y capacidades de seguridad informática.

---

[4] Las autoridades competentes incluyen asimismo a la policía, las fuerzas de rescate, la guardia fronteriza y las fuerzas de defensa que tienen un papel en la seguridad de las instalaciones y actividades y en la detección y respuesta en caso de incidentes relacionados con materiales nucleares y otros materiales radiactivos no sometidos a control reglamentario.

[5] En la presente publicación, se entiende por “explotadores” la gama de entidades con licencia en un régimen de seguridad física nuclear, incluidos los explotadores de instalaciones y actividades con materiales nucleares u otros materiales radiactivos, los remitentes y los transportistas.

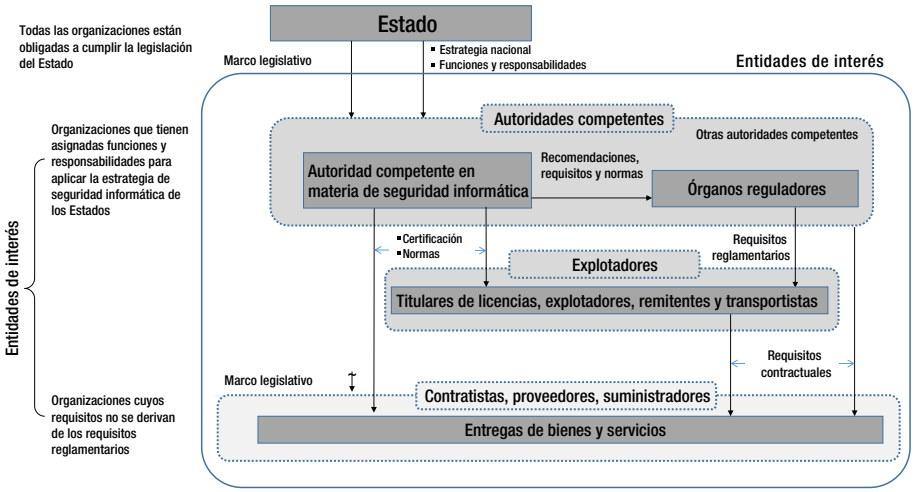


Fig. 5. Organizaciones con responsabilidades en materia de seguridad informática en un régimen de seguridad física nuclear.

3. FUNCIONES Y RESPONSABILIDADES DEL ESTADO

3.1. El Estado debería elaborar y mantener una estrategia nacional de seguridad informática como parte de su régimen de seguridad física nuclear (en adelante, "la estrategia"). El Estado debería designar a una autoridad competente como responsable principal de la elaboración de la estrategia.

CONSIDERACIONES LEGISLATIVAS Y REGLAMENTARIAS

3.2. El Estado debería garantizar que la seguridad informática se aborde adecuadamente en un marco legislativo y reglamentario que sea aplicable y coherente con el régimen de seguridad física nuclear. El Estado debería incorporar a su legislación nacional los requisitos adecuados para la seguridad informática que garanticen la correcta aplicación de la seguridad informática en el marco de la seguridad física nuclear.

3.3. El Estado debería asegurarse de que su legislación tipifica como delito los ciberataques a los sistemas computerizados del régimen de seguridad física nuclear. Es posible que a los fines de la seguridad informática sean necesarias disposiciones legislativas especiales para tener en cuenta las características singulares de algunos delitos y *modus operandi* asociados a los ciberataques.

3.4. El Estado debería garantizar que las sanciones por actos delictivos o actos intencionales no autorizados contra los recursos digitales de carácter estratégico que podrían poner en peligro la seguridad física nuclear formen parte de su marco legislativo o reglamentario.

3.5. El Estado debería considerar ejemplos de otras leyes e instrumentos jurídicos internacionales (como las convenciones) para ayudarle a definir la seguridad informática y su aplicación en relación con la seguridad física nuclear. Esos ejemplos pueden ser:

a) Leyes relativas a los delitos informáticos.
b) Leyes en materia de terrorismo.
c) Leyes sobre la protección de las infraestructuras nacionales críticas.
d) Leyes que obligan a divulgar información.
e) Leyes en materia de privacidad y manejo de información personal.
f) Instrumentos internacionales, como convenios, en materia de ciberdelincuencia.

3.6. El Estado debería revisar y actualizar continuamente su marco legislativo y reglamentario para incluir disposiciones relativas a las ciberamenazas y los factores de vulnerabilidad nuevos y emergentes.

3.7. El Estado debería designar una autoridad competente principal en materia de seguridad informática[6], con la responsabilidad de supervisar y observar las leyes y los reglamentos de seguridad informática aplicados al régimen de seguridad física nuclear (en lo sucesivo, “autoridad competente en materia de seguridad informática”).

3.8. El Estado puede optar por aplicar un marco legislativo y reglamentario en materia de seguridad informática que no se limite al régimen de seguridad física nuclear, y el ámbito de aplicación de algunas leyes y reglamentos puede trascender el régimen de seguridad física nuclear. En esos casos, la autoridad competente en materia de seguridad informática debería velar por que el marco sea suficiente para la seguridad física nuclear y, en caso contrario, el Estado debería complementar

[6] Un Estado puede asignar esa responsabilidad a diferentes autoridades competentes en diferentes contextos; por ejemplo, la autoridad competente responsable de la seguridad informática en las instalaciones nucleares puede ser diferente de la responsable de la seguridad informática en las consultas médicas o en la vigilancia de las fronteras. En la presente publicación, se entiende por “autoridad competente” cualquier autoridad responsable en un contexto determinado.

ese marco con los requisitos necesarios de forma coherente con el régimen de seguridad física nuclear.

3.9. El Estado debería garantizar que las autoridades competentes dispongan de suficientes recursos financieros, humanos y técnicos para cumplir con sus responsabilidades de interpretar y aplicar correctamente sus obligaciones legales relativas a la seguridad informática en el régimen de seguridad física nuclear del Estado.

AUTORIDAD COMPETENTE EN MATERIA DE SEGURIDAD INFORMÁTICA EN EL RÉGIMEN DE SEGURIDAD FÍSICA NUCLEAR

3.10. Dependiendo de la organización del Estado, la autoridad competente en materia de seguridad informática en el régimen de seguridad física nuclear puede ser o no el órgano regulador de la seguridad física nuclear. Del mismo modo, las responsabilidades relativas a la seguridad informática dentro del Estado pueden ser compartidas por varias organizaciones, pero el Estado debería designar una autoridad competente específica para que tenga la responsabilidad de la seguridad informática en cada esfera concreta del régimen de seguridad física nuclear. Por ejemplo, la autoridad competente para la seguridad informática de las centrales nucleares puede ser diferente de la autoridad competente para la seguridad informática de las operaciones de vigilancia de fronteras.

3.11. Cuando hay más de una autoridad competente en materia de seguridad informática en el régimen de seguridad física nuclear, o es diferente de la autoridad competente responsable de la seguridad física nuclear, el Estado debería establecer y mantener un organismo o mecanismo de coordinación adecuado para garantizar la claridad de la responsabilidad y la rendición de cuentas de todos los aspectos de la seguridad informática en relación con todas las autoridades competentes.

3.12. El Estado debería precisar cuáles son todas las autoridades competentes[7] y explotadores con funciones y responsabilidades relacionadas con la seguridad informática en el régimen de seguridad física nuclear y garantizar que cada una de esas organizaciones esté bajo la supervisión de la autoridad competente apropiada en materia de seguridad informática del régimen de seguridad física nuclear.

---

[7] Las autoridades competentes que deberían considerarse incluyen, según el caso, cualquier organismo o mecanismo de coordinación, las fuerzas del orden, las autoridades aduaneras y de control de fronteras, los organismos de inteligencia y seguridad y los organismos de salud y medio ambiente.

3.13. El Estado debería exigir a las autoridades competentes y a los explotadores indicados que formulen y apliquen los programas de seguridad informática de acuerdo con la estrategia.

3.14. El Estado debería definir y asignar responsabilidades de seguridad informática a todas las entidades pertinentes del régimen de seguridad física nuclear.

3.15. En el anexo III figura una lista de ejemplos de responsabilidades en materia de seguridad física nuclear de la que pueden deducirse atribuciones en materia de seguridad informática, según la naturaleza del régimen de seguridad física nuclear del Estado y sus recursos digitales de carácter estratégico.

3.16. Algunas organizaciones de apoyo pueden no estar sujetas a la autoridad de los órganos reguladores del Estado, pero tienen un papel fundamental en la consecución de los objetivos de seguridad física nuclear por lo que respecta a la seguridad informática. Las responsabilidades y los requisitos de seguridad informática de esas organizaciones pueden definirse a través de acuerdos contractuales como los que se utilizan con proveedores, contratistas y suministradores. El Estado puede asignar requisitos de seguridad informática (por ejemplo, en relación con el diseño, los resultados y la capacitación del personal) para sistemas computerizados específicos y para proveedores, contratistas y suministradores del régimen de seguridad física nuclear, en consonancia con lo establecido en la estrategia.

INTERFACES CON OTROS ÁMBITOS

3.17. El Estado debería garantizar que las interfaces entre la seguridad informática y otros ámbitos sean eficaces. Para ello puede ser necesaria una acción del Estado al margen del ámbito de la seguridad informática (por ejemplo, establecer requisitos en los otros ámbitos).

3.18. El Estado debería asegurarse de que la estrategia defina las interfaces entre la seguridad informática y todos los demás ámbitos pertinentes para que las respectivas autoridades competentes y los explotadores comprendan sus funciones y responsabilidades en relación con esas interfaces.

Seguridad tecnológica nuclear

3.19. La seguridad física nuclear y la seguridad tecnológica nuclear tienen en común el objetivo de proteger a las personas, los bienes, la sociedad y el medio

ambiente. Las medidas de seguridad física y de seguridad tecnológica tienen que formularse y aplicarse en forma integrada para poder generar sinergia entre las dos esferas y, además, de un modo en que las medidas de seguridad física no comprometan la seguridad tecnológica y las medidas de seguridad tecnológica no comprometan la seguridad física [1].

3.20. La seguridad informática desempeña un papel importante en la interfaz entre la seguridad física nuclear y la seguridad tecnológica nuclear, especialmente en vista de la creciente dependencia de los sistemas computerizados en todos los aspectos operacionales de las instalaciones nucleares.

3.21. El Estado debería tener en cuenta la reglamentación de seguridad física nuclear y de seguridad tecnológica nuclear a la hora de elaborar la reglamentación de seguridad informática y garantizar que esta se aplique de forma coherente.

3.22. Cualquier función de seguridad tecnológica nuclear que esté ligada a un sistema computerizado o se sustente en él dependerá de la integridad y la disponibilidad de la información conexa (incluido el *software*) —y, en su caso, de su confidencialidad— para su correcto funcionamiento. Por lo tanto, la seguridad informática debería aplicarse como parte integrante de los procesos del ciclo de vida de los sistemas computerizados utilizados para la seguridad física nuclear, para garantizar que los requisitos de seguridad informática y de seguridad tecnológica nuclear se aborden conjuntamente.

3.23. Debería existir una relación coherente y racional entre las clases de seguridad tecnológica y los niveles de seguridad informática asignados a los recursos digitales, para garantizar que un recurso digital asignado a una clase de seguridad concreta cuente con la protección de seguridad informática adecuada, pero no existe necesariamente una simple equivalencia entre las clases de seguridad tecnológica y los niveles de seguridad informática. Además, algunos recursos digitales que no tienen una clasificación formal de seguridad pueden, sin embargo, revestir importancia para la seguridad tecnológica desde el punto de vista de la seguridad física y, por tanto, constituir recursos digitales de carácter estratégico. La determinación del nivel de seguridad informática adecuado dependerá de la función del sistema y del recurso digital concreto en el contexto del sistema y de la organización. Para esa determinación serán necesarias las competencias y capacidades adecuadas, mediante un juicio basado en principios convenidos.

3.24. La aplicación de las medidas de seguridad informática no debería influir negativamente en los resultados, la eficacia, la fiabilidad o el funcionamiento de las funciones de seguridad tecnológica nuclear.

3.25. En el apéndice se describen otras consideraciones para el Estado a la hora de abordar las interfaces con la seguridad tecnológica nuclear.

Protección física

3.26. Los sistemas de protección física, como los que proporcionan control de acceso físico, detección y monitorización de la seguridad física y funciones de alarma y respuesta, suelen basarse en sistemas computerizados. Si esos sistemas computerizados se vieran comprometidos de forma dolosa (es decir, la confidencialidad, la integridad o la disponibilidad de la información que contienen se vieran comprometidas), el funcionamiento del sistema de protección física podría quedar degradado y facilitar las acciones físicas destinadas a la retirada no autorizada de materiales o al sabotaje. La seguridad informática debería aplicarse como parte integrante de los procesos del ciclo de vida de los sistemas computerizados que se utilicen para las funciones o sistemas de protección física.

3.27. Los sistemas de protección física, como el control de acceso físico, también pueden contribuir de forma valiosa a la seguridad informática, y deberían tenerse en cuenta a la hora de proteger los sistemas computerizados.

3.28. Algunos Estados pueden tratar la seguridad informática como parte integrante de la protección física, de acuerdo con la definición que figura en la referencia [3]. En la presente publicación se trata la seguridad informática como un tema aparte, distinto de la protección física, para aclarar y subrayar las diferencias. La naturaleza de la interfaz con la protección física dependerá de las circunstancias de cada Estado.

3.29. La aplicación de las medidas de seguridad informática no debería influir negativamente en los resultados, la eficacia, la fiabilidad o el funcionamiento del sistema de protección física.

Tecnología de la información y funciones tecnológicas operacionales

3.30. Las responsabilidades de la gestión y la seguridad de los sistemas de tecnología de la información y de las tecnologías operacionales (incluidos los sistemas de control industrial y los sistemas de control e instrumentación) suelen recaer en distintos departamentos de una organización. La interfaz y la colaboración eficaces entre esos grupos son esenciales para una seguridad integral. Los ciberataques anteriores han conllevado el uso de los sistemas de tecnología de la información como recurso de reconocimiento y medio de ataque contra las tecnologías operacionales.

3.31. Podría haber diferencias de procedimientos, vocabulario y evaluación de riesgos entre los responsables de los sistemas computerizados y los responsables de las tecnologías operacionales. La colaboración eficaz entre ellos es esencial para evitar malentendidos y una aplicación incoherente de las medidas de seguridad informática.

Servicios de inteligencia

3.32. El Estado debería garantizar que los servicios de inteligencia proporcionen el apoyo adecuado para contribuir o mantener una evaluación nacional de las amenazas precisa y actualizada que incluya las amenazas de ciberataques contra el régimen de seguridad física nuclear. Deberían existir protocolos y procesos para respaldar la transferencia de información sobre las ciberamenazas a las entidades pertinentes del régimen de seguridad física nuclear, según proceda, con miras a garantizar una seguridad informática adecuada contra las amenazas cambiantes.

3.33. El Estado debería garantizar que los servicios de inteligencia conozcan el papel de la seguridad informática en el régimen de seguridad física nuclear, incluido el conocimiento de los tipos de recursos digitales de carácter estratégico que puedan existir y su importancia.

Organizaciones de respuesta

3.34. El Estado debería garantizar que todas las autoridades competentes y los explotadores dispongan de sistemas y medidas de seguridad física nuclear para detectar y evaluar los incidentes de seguridad informática que tengan consecuencias reales o potenciales para la seguridad física nuclear, y que se notifiquen dichos incidentes a las autoridades competentes pertinentes con el fin de que puedan iniciarse las acciones de respuesta adecuadas.

3.35. Los planes de contingencia deberían incluir disposiciones para responder a ciberataques y ataques combinados.

Asistencia y cooperación internacionales (incluido el intercambio de información)

3.36. Se alienta a los Estados a que cooperen entre sí y con las organizaciones internacionales, cuando proceda, para asegurar los recursos digitales de carácter estratégico y la información de carácter estratégico conexa y para detectar las amenazas de ciberataque, especialmente las amenazas verosímiles de sabotaje de materiales nucleares o de una instalación nuclear (por ejemplo, de conformidad

con el artículo 5.3) de la Convención sobre la Protección Física de los Materiales Nucleares, en su forma enmendada [2]). La creación de confianza y la mejora de la seguridad informática pueden lograrse compartiendo y analizando oportunamente la información relativa a los factores de vulnerabilidad, las amenazas y los incidentes de seguridad informática. La confidencialidad de esa información debería protegerse adecuadamente.

3.37. El Estado debería establecer mecanismos seguros y controlados de intercambio de información para coordinar la respuesta a los ciberataques contra el régimen de seguridad física nuclear del Estado. Se alienta la cooperación y la asistencia internacionales para apoyar la investigación de los ciberataques y el enjuiciamiento de los delincuentes.

3.38. Se alienta al Estado a que contrate periódicamente servicios de asesoramiento o evaluación para valorar su estrategia y los programas de seguridad informática y su aplicación en el régimen de seguridad física nuclear del Estado.

4. FUNCIONES Y RESPONSABILIDADES DE LAS AUTORIDADES COMPETENTES Y DE LOS EXPLOTADORES

4.1. La seguridad informática es una cuestión transversal para las autoridades competentes y los explotadores de un régimen de seguridad física nuclear. Todas esas organizaciones tienen algún nivel de responsabilidad en la protección de los recursos digitales de carácter estratégico.

4.2. Las autoridades competentes y los explotadores son a la vez generadores y usuarios de información de carácter estratégico, que a menudo es procesada, almacenada o integrada en los recursos digitales de carácter estratégico bajo su control. Las autoridades competentes y los explotadores deberían aplicar medidas de seguridad informática para proteger esos recursos digitales de carácter estratégico y la información de carácter estratégico conexa.

4.3. Las autoridades competentes y los explotadores deberían determinar cuáles son sus recursos digitales de carácter estratégico, caracterizarlos en función del efecto potencial sobre la seguridad física nuclear y la seguridad tecnológica nuclear que causaría que se vieran comprometidos y definir en sus programas de

seguridad informática el nivel de las medidas de seguridad informática necesarias para cada uno de esos recursos digitales de carácter estratégico.

4.4. Las autoridades competentes y los explotadores deberían aplicar medidas de seguridad informática para proteger la confidencialidad, la integridad y la disponibilidad de los recursos digitales de carácter estratégico y la información de carácter estratégico que contienen. Por ejemplo, las medidas de seguridad informática deberían tener las siguientes características:

a) Deberían concebirse para impedir el acceso no autorizado, por parte de personas, procesos o equipos, a los recursos digitales de carácter estratégico (de acuerdo con un enfoque graduado).
b) Deberían garantizar que no se introduzcan códigos o datos maliciosos en los recursos digitales de carácter estratégico.
c) Deberían integrarse en los acuerdos de gestión de la cadena de suministro.

4.5. Las autoridades competentes y los explotadores deberían utilizar un proceso formal para garantizar que solo el personal que se considere competente y digno de confianza esté autorizado a realizar actividades relacionadas con la seguridad informática.

4.6. Las autoridades competentes y los explotadores deberían permitir que el personal cuya fiabilidad no haya sido determinada realice esas actividades solo en casos excepcionales y únicamente cuando existan sólidas medidas de seguridad compensatorias para prevenir o detectar actos no autorizados.

4.7. Las autoridades competentes y los explotadores deberían evaluar y gestionar las interfaces relacionadas con la seguridad informática entre la seguridad nuclear física y tecnológica [4] de manera que se garantice que las medidas de seguridad física y las medidas de seguridad tecnológica no se perjudiquen entre sí y que, en la medida de lo posible, se apoyen mutuamente.

4.8. Cada autoridad competente y explotador debería mantener un programa de seguridad informática en que se describa cómo va a proporcionar una seguridad informática adecuada, según las exigencias del Estado y su autoridad competente en materia de seguridad informática. Si hay varias organizaciones que comparten recursos digitales de carácter estratégico o dependen de los recursos de las demás, todas las responsabilidades o dependencias comunes deberían reflejarse en sus respectivos programas de seguridad informática.

4.9. Las autoridades competentes y los explotadores deberían evaluar periódicamente sus medidas de seguridad informática para asegurarse de que cumplen los requisitos reglamentarios. El período entre esas evaluaciones debería fijarse de manera que se tenga en cuenta con prontitud cualquier cambio en la amenaza u otros factores que influyan en el riesgo. Esas actividades de evaluación pueden incluir auditorías, revisiones, pruebas de los resultados y simulacros, según proceda. Las autoridades competentes y los explotadores también deberían realizar autoevaluaciones cuando se modifiquen los sistemas computerizados, para considerar si las modificaciones podrían introducir nuevos factores de vulnerabilidad o crear nuevos recursos digitales de carácter estratégico.

COLABORACIÓN CON PROVEEDORES, CONTRATISTAS Y SUMINISTRADORES

4.10. Las autoridades competentes y los explotadores deberían imponer requisitos contractuales a los proveedores, contratistas y suministradores para que apliquen medidas de seguridad informática acordes con su función. En los requisitos contractuales deberían especificarse las medidas de seguridad informática para garantizar que ninguna actividad de las partes proporcione una vía para el ciberataque a la otra, y que la información de carácter estratégico de ambas partes esté debidamente protegida.

4.11. Las autoridades competentes y los explotadores, así como sus proveedores, contratistas y suministradores, deberían mantener protocolos y procedimientos para la comunicación oportuna de información sobre incidentes de seguridad informática.

AUTORIDAD COMPETENTE EN MATERIA DE SEGURIDAD INFORMÁTICA

4.12. La autoridad competente en materia de seguridad informática debería definir los requisitos, las normas y las recomendaciones en materia de seguridad informática adaptados a cada autoridad competente u explotador, sobre la base de un enfoque graduado y basado en el conocimiento de los riesgos.

4.13. La autoridad competente en materia de seguridad informática debería garantizar que esos requisitos reflejen la estrategia, así como los requisitos operacionales y de seguridad particulares y las capacidades y competencias demostradas de la autoridad competente o del explotador correspondiente.

4.14. La autoridad competente en materia de ciberseguridad debería utilizar un enfoque basado en el conocimiento de los riesgos [1], que se aplique mediante un enfoque graduado y la defensa en profundidad, a fin de lograr una seguridad informática adecuada.

4.15. Cada autoridad competente debería garantizar que todas las operaciones a lo largo del ciclo de vida de los recursos digitales de carácter estratégico de las que es responsable (por ejemplo, el diseño, la aplicación, el mantenimiento y la disposición final) se controlen, supervisen y documenten adecuadamente.

4.16. Cada autoridad competente debería verificar el cumplimiento continuado de su normativa de seguridad informática mediante evaluaciones periódicas y, cuando sea necesario, garantizar la adopción de medidas correctivas.

4.17. La autoridad competente en materia de seguridad informática puede prescribir medidas específicas de seguridad informática para que las autoridades competentes o los explotadores las apliquen basándose en su evaluación de los riesgos (es decir, un enfoque prescriptivo). Como alternativa, la autoridad competente en materia de seguridad informática puede definir requisitos de seguridad informática basados en los resultados, lo que permite a las autoridades competentes o a los explotadores utilizar un enfoque basado en el conocimiento de los riesgos para determinar las medidas de seguridad informática proporcionadas. La autoridad competente en materia de seguridad informática también puede emplear una combinación de los dos enfoques.

4.18. Los criterios para la selección de un enfoque prescriptivo o un enfoque basado en los resultados (o una combinación adecuada de ambos) dependerán del marco legislativo y la estructura organizativa del Estado y de otros factores, como los siguientes:

a) La competencia del explotador para interpretar los requisitos basados en los resultados y para diseñar, aplicar y evaluar un sistema eficaz de seguridad física nuclear;
b) El número y la variedad de instalaciones y explotadores que se regirán por la normativa, y la medida en que los requisitos prescriptivos pueden limitar la flexibilidad del explotador para desarrollar medidas adecuadas;
c) La gravedad de las consecuencias potenciales de los actos dolosos que se quieren prevenir o para los que se establece la protección [10].

Enfoque prescriptivo

4.19. En el enfoque prescriptivo, la autoridad competente en materia de seguridad informática establece las medidas específicas de seguridad informática que considera necesarias para cumplir sus objetivos concretos de seguridad informática.

4.20. Las ventajas del enfoque prescriptivo incluyen la simplicidad en la aplicación tanto para la autoridad competente en materia de seguridad informática como para la autoridad competente o explotador correspondiente, la eliminación de la necesidad de compartir información de carácter estratégico y la facilidad de inspección y evaluación. El uso del enfoque prescriptivo tal vez sea especialmente apropiado en los casos en que es bajo el grado de amenaza y de consecuencias potenciales. El enfoque prescriptivo también puede ser más apropiado en los casos en que la realización de una evaluación detallada de las amenazas o el establecimiento de una amenaza base de diseño no sea viable.

4.21. El enfoque prescriptivo puede carecer de flexibilidad para abordar circunstancias específicas. Además, con ese enfoque, la autoridad competente pertinente no tiene la responsabilidad de garantizar que las medidas de seguridad informática aplicadas sean suficientes; la responsabilidad principal de hacer frente a los riesgos incumbe a la autoridad competente en materia de seguridad informática, puesto que ella prescribe exactamente las medidas de seguridad informática necesarias para contrarrestar la amenaza de ciberataque. La autoridad competente o el explotador pertinente solo tienen la responsabilidad de aplicar las medidas de seguridad informática prescritas.

Enfoque basado en los resultados

4.22. En el enfoque basado en los resultados, la autoridad competente en materia de seguridad informática define los objetivos de seguridad informática y exige a las autoridades competentes o a los explotadores que diseñen y apliquen medidas de seguridad informática que cumplan esos objetivos, para alcanzar un nivel de eficacia determinado en la protección contra los ciberataques y proporcionar respuestas de contingencia.

4.23. El enfoque basado en los resultados permite a las autoridades competentes o a los explotadores proponer una combinación específica de medidas de seguridad informática para la organización. La adecuación de esas medidas se comprueba mediante la evaluación de las amenazas o la amenaza base de diseño, a fin de garantizar que el conjunto de medidas basadas en los resultados cumple los objetivos. Una ventaja del enfoque basado en los resultados es que reconoce que

se puede lograr una seguridad informática eficaz con muchas combinaciones distintas de medidas de seguridad informática, y que cada organización y sus circunstancias operacionales pueden ser diferentes.

4.24. El enfoque basado en los resultados depende de que tanto la autoridad competente en materia de seguridad informática como las autoridades competentes o los explotadores tengan suficientes competencias y capacidades en materia de seguridad informática para establecer los requisitos y aplicar las medidas de seguridad informática. El enfoque basado en los resultados puede conllevar que el Estado proporcione a las respectivas autoridades competentes y a los explotadores información de carácter estratégico de la evaluación de las amenazas o de la amenaza base de diseño.

Enfoque combinado

4.25. El enfoque combinado incluye elementos del enfoque prescriptivo y del enfoque basado en los resultados. Hay muchas formas de aplicar el enfoque combinado, por ejemplo, las dos que figuran a continuación:

a) El Estado puede exigir la aplicación de un enfoque basado en los resultados en circunstancias en que el impacto potencial sea grave o muy grave, mientras que permite la aplicación de un enfoque prescriptivo cuando el impacto potencial sea bajo o muy bajo.
b) El Estado puede imponer un conjunto de requisitos prescriptivos que deberían seguirse para abarcar determinados aspectos de la seguridad informática (por ejemplo, la protección de la información de carácter estratégico), al tiempo que complementa las medidas de seguridad informática para abarcar los demás aspectos derivados mediante el enfoque basado en los resultados.

4.26. La principal ventaja del enfoque combinado es la flexibilidad que ofrece. Las limitaciones de un enfoque combinado son similares a las asociadas a los enfoques basado en los resultados y prescriptivo y dependen de la aplicación específica. Sin embargo, un enfoque combinado bien ejecutado puede proporcionar un equilibrio adecuado y reducir los efectos de las limitaciones asociadas a cada enfoque.

ÓRGANO REGULADOR

4.27. El órgano regulador[8] de la seguridad física nuclear debería establecer requisitos reglamentarios para las medidas de seguridad informática con el fin de proteger los recursos digitales de carácter estratégico y la información de carácter estratégico conexa. El órgano regulador debería garantizar, a través de la reglamentación, que las entidades pertinentes desempeñen sus responsabilidades en materia de seguridad informática de acuerdo con los requisitos reglamentarios.

4.28. El órgano regulador debería garantizar que su reglamentación sea lo suficientemente flexible como para adaptarse a la naturaleza y circunstancias cambiantes de los sistemas computerizados, los ciberataques y las medidas de seguridad informática.

4.29. Se propone que el órgano regulador publique una guía de su reglamentación de seguridad informática para ayudar a las entidades pertinentes en su aplicación. La guía debería examinarse de forma periódica para garantizar que aborda adecuadamente las ciberamenazas y los objetivos de la reglamentación.

4.30. El órgano regulador debería garantizar que la seguridad informática forme parte de la evaluación y la concesión de licencias u otros procedimientos para otorgar autorización a los titulares.

4.31. El órgano regulador debería asegurarse de que cada explotador tenga un programa de seguridad informática que describa sus medidas de seguridad informática.

4.32. El órgano regulador debería verificar el cumplimiento continuado de los requisitos reglamentarios y las condiciones de la licencia en materia de seguridad informática mediante inspecciones periódicas y, cuando sea necesario, recurrir a acciones coercitivas para garantizar que se adopten las medidas correctivas oportunas.

---

[8] Puede haber más de un órgano regulador dentro de un Estado, cada uno de los cuales es responsable de la seguridad física nuclear en diferentes contextos; por ejemplo, el órgano regulador responsable de la seguridad física nuclear en las instalaciones nucleares puede ser diferente del responsable de la seguridad física nuclear en las industrias que utilizan fuentes radiactivas. En la presente publicación, se entiende por “órgano regulador” cualquier órgano que tenga responsabilidad en un contexto determinado. El órgano regulador de la seguridad física nuclear puede ser también la autoridad competente en materia de seguridad informática, en cuyo caso también se le aplican las orientaciones de la subsección anterior.

5. ESTABLECIMIENTO DE LA ESTRATEGIA DE SEGURIDAD INFORMÁTICA

ESTRATEGIA DE SEGURIDAD INFORMÁTICA PARA EL RÉGIMEN DE SEGURIDAD FÍSICA NUCLEAR

5.1. En la estrategia[9] se establecen los objetivos de seguridad informática de alto nivel del régimen de seguridad física nuclear del Estado, los cuales figurarán en documentos de rango inferior que se utilizarán para aplicar la estrategia. La estrategia ha de ser aplicable, factible y auditable.

5.2. La estrategia debería incluir los siguientes elementos:

a) un método para evaluar las amenazas, incluida la definición de posibles escenarios de ciberataques;
b) un método para determinar los objetivos de seguridad informática;
c) un método para especificar las competencias y los niveles de capacidad en materia de seguridad informática;
d) la asignación de funciones y responsabilidades en materia de seguridad informática a todas las autoridades competentes y explotadores (y posiblemente a los proveedores, contratistas y suministradores);
e) la delimitación y el establecimiento de nuevas organizaciones o la adaptación de las funciones de seguridad informática para las organizaciones existentes en las que existen deficiencias de capacidad;
f) enfoques para la ejecución, integración y coordinación de las actividades de seguridad informática de las autoridades competentes y los explotadores, y
g) medidas para mantener las capacidades de seguridad informática en el régimen de seguridad física nuclear.

5.3. En las secciones 5 a 8 se proporciona más orientación sobre estos puntos, que deberían documentarse en la estrategia.

[9] El Estado puede optar por incluir determinada información de carácter estratégico en los apéndices de la estrategia, de modo que la distribución de esa información pueda limitarse de una forma más conveniente.

5.4. En la presente sección se describen las actividades preparatorias que el Estado y su autoridad competente en materia de seguridad informática deberían llevar a cabo para establecer la estrategia, entre ellas las siguientes:

a) realizar una evaluación de las amenazas;
b) evaluar la repercusión en la seguridad física nuclear de un ciberataque a los recursos digitales de carácter estratégico;
c) determinar si se utiliza el enfoque prescriptivo o el enfoque basado en los resultados, o una combinación de ambos, para regular la seguridad informática, y
d) especificar un marco de capacidades y competencias en seguridad informática;
e) ejecutar (integrar y coordinar) las actividades de seguridad informática de las autoridades competentes y de los explotadores.

EVALUACIÓN DE LAS CIBERAMENAZAS PARA EL RÉGIMEN DE SEGURIDAD FÍSICA NUCLEAR

5.5. El Estado debería mantener una evaluación actualizada de las amenazas para su régimen de seguridad física nuclear [1, 5]. Esa información puede utilizarse con el fin de elaborar una declaración nacional de amenazas o una amenaza base de diseño.

5.6. En la evaluación de las amenazas al Estado o la amenaza base de diseño se debería incluir a los posibles adversarios que utilicen ciberataques, incluido el posible uso de agentes internos en esos ataques, y los ataques combinados.

5.7. Los ciberataques permiten al adversario iniciar un acto doloso desde fuera del emplazamiento objetivo o incluso desde fuera de la jurisdicción nacional del emplazamiento objetivo. Por lo tanto, el Estado debería considerar las amenazas internacionales en su evaluación.

5.8. El Estado debería asegurarse de que la evaluación de las amenazas relativas a ciberataques (evaluación de las ciberamenazas) se actualiza con asiduidad. La frecuencia de revisión de la evaluación de las amenazas debería reflejar la rápida evolución de las tecnologías, los avances en los sistemas computerizados, los factores de vulnerabilidad recién descubiertos y la naturaleza cambiante de los posibles ciberataques y los correspondientes enfoques de seguridad informática.

5.9. El Estado debería garantizar que los cambios en la evaluación de las amenazas relativas a los ciberataques se comuniquen a las autoridades competentes y a los explotadores pertinentes de manera oportuna y segura.

5.10. El Estado debería adoptar todas las medidas razonables para tener en cuenta la naturaleza cambiante de la ciberamenaza, y fomentar las medidas de seguridad informática que anticipen dichos cambios o se adapten fácilmente a ellos y, por tanto, sigan siendo eficaces.

5.11. Además de los servicios nacionales de inteligencia, otras autoridades competentes, los explotadores, los proveedores, los contratistas y los suministradores pueden poseer información que puede servir de aportación a la evaluación de las amenazas.

5.12. El Estado podrá definir protocolos para el intercambio seguro de información sobre amenazas, incluidas las comunicaciones directas entre organizaciones.

5.13. No se puede esperar que las autoridades competentes y los explotadores brinden protección contra todos los niveles de amenaza. A partir de un determinado nivel de amenaza, se espera que el Estado responda en apoyo de la autoridad competente o del explotador (figura 6). Para las autoridades competentes y los explotadores que utilizan una amenaza base de diseño, esto suele denominarse "suceso que sobrepasa la amenaza base de diseño".

5.14. El Estado debería asegurarse de que la evaluación de las amenazas o la amenaza base de diseño en relación con la seguridad informática proporcionen suficientes detalles para las posteriores evaluaciones de riesgos, que a su vez se traducirán en la aplicación adecuada y eficaz de la seguridad informática en todo el régimen de seguridad física nuclear del Estado.

5.15. El Estado, a través de la autoridad competente en materia de seguridad informática, debería precisar los criterios, los procesos y los recursos para responder a los ciberataques contra las autoridades competentes y los explotadores y sus proveedores, contratistas y suministradores. Esos procesos deberían incluir protocolos de comunicación seguros con la organización de respuesta.

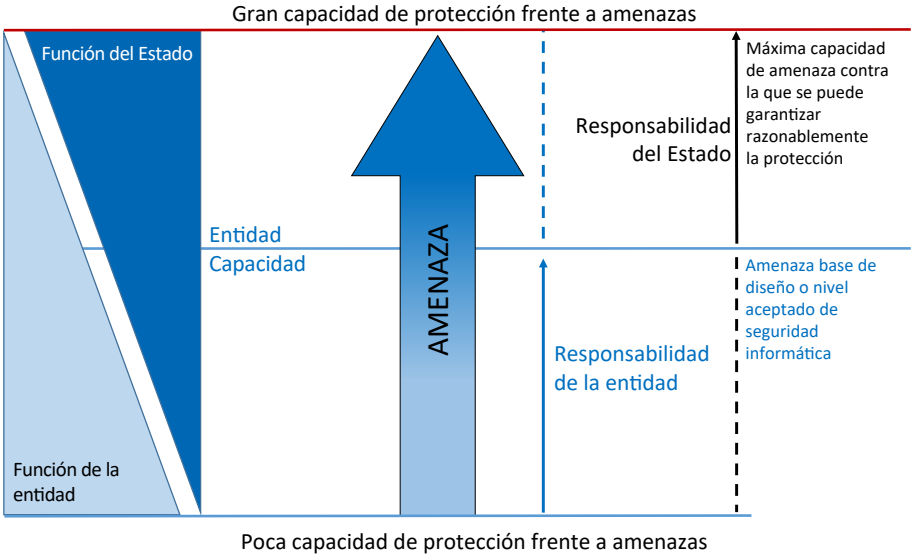


Fig. 6. Funciones y responsabilidades de protección frente a amenazas.

ASIGNACIÓN A UNA AUTORIDAD COMPETENTE DE LA EVALUACIÓN DE LAS CIBERAMENAZAS

5.16. El Estado debería garantizar que se realice una evaluación de las amenazas de ciberataques de forma asidua y oportuna. El Estado debería asignar esa función a una autoridad competente con experiencia en la determinación y evaluación de ciberamenazas. La autoridad competente encargada de la evaluación de las ciberamenazas puede ser diferente de la autoridad competente en materia de seguridad informática.

5.17. En el desempeño de sus funciones, la autoridad competente para la evaluación de las ciberamenazas debería consultar y cooperar con todas las autoridades competentes y los explotadores indicados por el Estado que tengan funciones y responsabilidades en la evaluación de la ciberamenaza y que tengan competencias y capacidades en un proceso formalizado de evaluación de las ciberamenazas. La autoridad competente debería dirigir el proceso de coordinación y combinación de las distintas aportaciones a la evaluación de las amenazas de ciberataque.

5.18. La autoridad competente para la evaluación de las ciberamenazas debería ser responsable de garantizar que la evaluación de la ciberamenaza proporcione suficientes detalles para las posteriores evaluaciones del riesgo que se utilizarán con el fin de concebir una aplicación adecuada y eficaz de las medidas de seguridad informática en todo el régimen de seguridad física nuclear del Estado.

EVALUACIÓN DEL IMPACTO DERIVADO DEL MAL FUNCIONAMIENTO DE LOS RECURSOS DIGITALES DE CARÁCTER ESTRATÉGICO

5.19. La autoridad competente en materia de seguridad informática debería determinar, para cada autoridad competente y explotador pertinente, la gravedad de las posibles consecuencias de los ciberataques que tienen que prevenir mediante medidas eficaces de seguridad informática.

5.20. La evaluación de la gravedad de las consecuencias debería basarse en las características y los atributos inherentes a los recursos digitales de carácter estratégico. Las autoridades competentes y los explotadores deberían considerar la gravedad de las consecuencias independientemente de su probabilidad y del tipo de ciberataque que podría provocarlas.

5.21. En la figura 7 se ilustran los diferentes niveles de impacto de los distintos tipos de sucesos relacionados con la seguridad física nuclear en los ámbitos de la seguridad física nuclear que abarcan las referencias [3 a 5]. La autoridad competente en materia de seguridad informática debería determinar la gravedad de las consecuencias y evaluar la idoneidad de las medidas de seguridad informática para garantizar la prevención o mitigación de esas consecuencias.

5.22. La autoridad competente en materia de seguridad informática podría determinar, en colaboración con otras autoridades competentes, el nivel de protección que debería exigirse para cada nivel de gravedad de las consecuencias.

5.23. Para aplicar una seguridad informática eficaz es necesaria una serie de competencias y niveles de capacidad que se adapten a las funciones y responsabilidades de cada autoridad competente, explotador, proveedor, contratista y suministrador. En los casos en que sean necesarias decisiones y acciones basadas en el juicio, los niveles de capacidad tendrán que ser necesariamente más altos. Una seguridad informática eficaz incluye la especificación de esas competencias y niveles de capacidad para cada autoridad competente, explotador, proveedor,

contratista y suministrador, y la obtención de garantías de que esas competencias y niveles de capacidad se mantienen y aplican.

5.24. La autoridad competente en materia de seguridad informática debería establecer un marco de competencias y niveles de capacidad de seguridad informática. En el anexo IV figura un marco a modo de ejemplo.

5.25. El marco debería garantizar que las competencias y los niveles de capacidad en materia de seguridad informática exigidos a cada autoridad competente, explotador, proveedor, contratista y suministrador sean los adecuados para cumplir con sus respectivas responsabilidades en materia de seguridad informática. En otras publicaciones de la *Colección de Seguridad Física Nuclear del OIEA* [3, 11] se ofrecen más orientaciones sobre la definición de las funciones, la formulación y el mantenimiento de las competencias dentro de las organizaciones y la creación de capacidades en relación con las organizaciones y las personas.

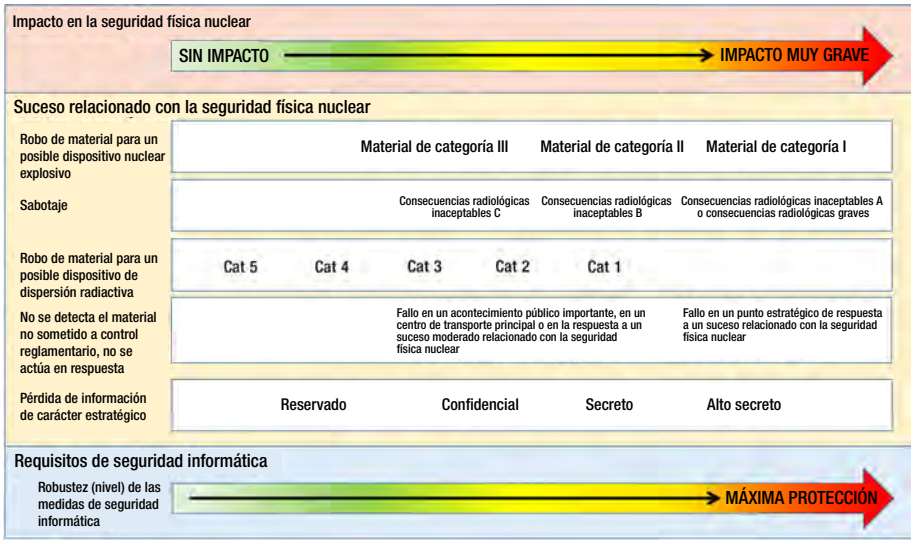


Fig. 7. Ilustración de la gravedad variable de las consecuencias de diferentes tipos de sucesos relacionados con la seguridad física nuclear (las escalas de impacto son independientes y la gravedad de cada impacto debe evaluarse de forma independiente).

MÉTODO DE EVALUACIÓN DE RIESGOS PARA DETERMINAR LAS MEDIDAS DE SEGURIDAD INFORMÁTICA

5.26. La aplicación de medidas de seguridad informática debería basarse en un enfoque de conocimiento de los riesgos. La autoridad competente en materia de seguridad informática debería definir un método de evaluación de riesgos o una secuencia de métodos mediante los cuales las organizaciones responsables lleven a cabo las siguientes tareas:

a) determinar si cada sistema computerizado ofrece una función pertinente para el régimen de seguridad física nuclear;
b) determinar si cada recurso digital es un recurso digital de carácter estratégico, y
c) realizar un análisis de riesgos de seguridad informática a fin de determinar la robustez de las medidas de seguridad informática necesarias para ese recurso digital de carácter estratégico u otro recurso digital, como se ilustra en la figura 3.

5.27. El método debería tener en cuenta lo siguiente:

a) cualquier legislación o reglamento pertinente;
b) la importancia de las funciones del recurso digital de carácter estratégico, incluida la importancia de proteger la confidencialidad, la integridad y la disponibilidad del recurso digital de carácter estratégico y de su información de carácter estratégico, tanto para la seguridad física nuclear como para la seguridad tecnológica nuclear (es decir, su clasificación de seguridad);
c) una evaluación de las consecuencias de los ciberataques contra ese recurso digital de carácter estratégico;
d) el entorno operativo del recurso digital de carácter estratégico;
e) la definición y evaluación de las amenazas de interés para las autoridades competentes y los explotadores, así como para sus proveedores, contratistas y suministradores, y para el recurso digital de carácter estratégico según la evaluación de las amenazas o amenaza base de diseño o declaración de amenazas de carácter nacional;
f) el atractivo del recurso digital de carácter estratégico para las amenazas para la seguridad física nuclear, y
g) los factores de vulnerabilidad intrínsecos del recurso digital de carácter estratégico.

5.28. La autoridad competente en materia de seguridad informática puede modificar los resultados de la evaluación de riesgos en función del impacto potencial en

caso de que el recurso digital de carácter estratégico se vea comprometido, en concreto si ello da lugar a alguno de los siguientes aspectos:

a) la función del recurso digital de carácter estratégico se vuelve indeterminada;
b) el recurso digital de carácter estratégico da lugar a comportamientos o acciones inesperadas;
c) fallo del recurso digital de carácter estratégico, y
d) el recurso digital de carácter estratégico funciona como estaba previsto (es decir, es tolerante a los fallos).

5.29. La evaluación de riesgos debería considerar todos los aspectos de la seguridad física de forma colectiva para hacer frente a los ataques combinados, que pueden combinar la protección física (incluido el personal, especialmente los agentes internos) y los ciberataques a la seguridad informática. En consecuencia, quienes realicen la evaluación de riesgos deberían tener acceso a personas con todas las competencias pertinentes, como las relacionadas con la protección física y la seguridad informática al servicio de la seguridad nuclear física y tecnológica.

6. APLICACIÓN DE LA ESTRATEGIA DE SEGURIDAD INFORMÁTICA

6.1. En la presente sección se describen las responsabilidades de la autoridad competente en materia de seguridad informática a la hora de asignar funciones y responsabilidades de seguridad informática a las autoridades competentes o a los explotadores.

6.2. Esas funciones y responsabilidades deberían documentarse en la estrategia o en los documentos de apoyo.

6.3. La autoridad competente en materia de seguridad informática puede establecer requisitos en forma de normas, requisitos reglamentarios a través de un órgano regulador, o requisitos contractuales para proveedores, contratistas o suministradores, y puede facilitar documentos de orientación para indicar cómo deben cumplirse esos requisitos.

ASIGNACIÓN DE RESPONSABILIDADES EN MATERIA DE SEGURIDAD INFORMÁTICA

6.4. La autoridad competente en materia de seguridad informática debería velar por que se asignara a todas las autoridades competentes y a los explotadores que utilicen recursos digitales de carácter estratégico la responsabilidad principal de la seguridad informática de esos recursos digitales de carácter estratégico y de cualquiera de sus demás recursos digitales que podrían afectar negativamente a la seguridad física nuclear o a la seguridad tecnológica nuclear si se vieran comprometidos.

6.5. La autoridad competente en materia de seguridad informática debería garantizar que todas las autoridades competentes, los explotadores, los proveedores, los contratistas y los suministradores que participen en el ciclo de vida de los recursos digitales de carácter estratégico tengan asignadas las responsabilidades adecuadas en materia de seguridad informática de esos recursos.

6.6. La autoridad competente en materia de seguridad informática debería velar por que haya un adecuado reparto de responsabilidades entre el Estado y las autoridades competentes y los explotadores para garantizar que los riesgos derivados de las amenazas para la seguridad física nuclear con capacidades superiores se mantengan en un nivel aceptable.

6.7. La autoridad competente en materia de seguridad informática debería velar por que las autoridades competentes y los explotadores pertinentes planifiquen y aborden la seguridad informática a lo largo de la detección y la respuesta en caso de incidente relacionado con la seguridad informática.

RELACIONES ENTRE LAS AUTORIDADES COMPETENTES Y LOS EXPLOTADORES

6.8. La autoridad competente en materia de seguridad informática debería prever la coordinación de las responsabilidades en materia de seguridad informática entre las autoridades competentes y los explotadores dentro y fuera del régimen de seguridad física nuclear. Por ejemplo, puede haber autoridades nacionales responsables de la seguridad informática fuera del régimen de seguridad física nuclear, lo que hará necesaria la coordinación con las autoridades del régimen de seguridad física nuclear.

6.9. La autoridad competente en materia de seguridad informática debería establecer líneas claras de comunicación entre las autoridades competentes y los explotadores y, en su caso, el órgano o mecanismo de coordinación mencionado en el párrafo 3.11.

6.10. La autoridad competente en materia de seguridad informática debería garantizar la existencia de un mecanismo de cooperación, coordinación, intercambio de información y, en su caso, integración de las actividades de seguridad informática entre las autoridades competentes y los explotadores.

6.11. Al asignar responsabilidades en materia de seguridad informática a las autoridades competentes y a los explotadores, la autoridad competente en materia de seguridad informática debería equilibrar las exigencias contrapuestas de la necesidad de defensa en profundidad y el uso eficiente y eficaz de los recursos de que dispone el régimen de seguridad física nuclear del Estado, teniendo en cuenta las siguientes consideraciones:

a) La independencia contribuye a la defensa en profundidad porque las opciones de diseño y funcionamiento independientes tienen menos posibilidades de permitir fallos de causa común o de modo común. La independencia incluye la independencia funcional y financiera de las organizaciones reguladas y de cualquier otro órgano que se ocupe de la utilización de materiales nucleares u otros materiales radiactivos. La autoridad competente en materia de seguridad informática debería velar por que las autoridades competentes y los explotadores dispongan de competencias y niveles de capacidad suficientes para respaldar la independencia en su toma de decisiones en materia de seguridad informática.
b) El intercambio de capacidades puede aumentar la eficiencia y la eficacia en la utilización de los recursos. Por ejemplo, una autoridad competente o un explotador pueden confiar en otra autoridad competente en esferas especializadas de la seguridad informática forense porque esa competencia se necesita con poca frecuencia. En tal caso, un acuerdo entre las entidades pertinentes debería especificar el tiempo de respuesta pactado para proporcionar asistencia cuando se solicite. La autoridad competente en materia de seguridad informática debería velar por que se establezcan disposiciones adecuadas para garantizar la eficacia y la rapidez de la asistencia en los casos en que las autoridades competentes y los explotadores necesiten la asistencia de otras autoridades competentes.

6.12. Al considerar el equilibrio entre la independencia y la interdependencia de las autoridades competentes y los explotadores, la autoridad competente en

materia de seguridad informática debería tener en cuenta los recursos necesarios para protegerse de los ataques combinados y responder ante ellos, lo que puede implicar la combinación de medidas de seguridad informática con otras medidas de seguridad física nuclear (por ejemplo, fuerzas de respuesta de protección física), que podrían ser facilitadas por otras autoridades competentes.

6.13. La asignación de responsabilidades y competencias y de niveles de capacidad puede determinar la necesidad de crear nuevas organizaciones o de modificar las existentes.

COMPETENCIAS Y CAPACIDADES EN MATERIA DE SEGURIDAD INFORMÁTICA

6.14. La autoridad competente en materia de seguridad informática debería exigir a las autoridades competentes y a los explotadores que realicen un análisis de sus objetivos de seguridad informática para obtener una lista completa de las competencias necesarias para sus organizaciones. La autoridad competente en materia de seguridad informática puede optar por realizar ese análisis por su cuenta, sobre todo cuando la autoridad competente o el explotador aplican mayoritariamente las medidas de seguridad informática prescritas por la autoridad competente en materia de seguridad informática.

6.15. La autoridad competente en materia de seguridad informática debería exigir a las autoridades competentes y a los explotadores que demuestren que poseen las competencias necesarias en los niveles de capacidad adecuados para cumplir con las responsabilidades de seguridad informática que se les han asignado. En el anexo III se ilustra la asignación típica de responsabilidades a las autoridades competentes y en el anexo IV figura un ejemplo de marco de competencias y niveles de capacidad.

6.16. La autoridad competente en materia de seguridad informática debería exigir a las autoridades competentes y a los explotadores que demuestren que todas las personas con responsabilidades en materia de seguridad informática son dignas de confianza, tienen la capacitación adecuada y poseen las destrezas y la competencia suficientes en sus funciones laborales, así como con la sensibilidad adecuada sobre la amenaza de los ciberataques.

6.17. La autoridad competente en materia de seguridad informática debería exigir a las autoridades competentes y a los explotadores que apliquen programas de

capacitación continua a fin de crear y mantener las competencias necesarias para cumplir con sus responsabilidades en materia de seguridad informática.

6.18. La autoridad competente en materia de seguridad informática debería alentar a las autoridades competentes y a los explotadores a evaluar sus propios niveles de capacidad en las competencias pertinentes por lo que se refiere a sus responsabilidades, a fin de respaldar la creación y la evolución de sus competencias.

6.19. La autoridad competente en materia de seguridad informática debería llevar a cabo actividades de garantía para evaluar la capacitación y las destrezas en seguridad informática de las autoridades competentes y de los explotadores. La autoridad competente en materia de seguridad informática debería exigir a cada autoridad competente y a cada explotador que demuestren el mantenimiento continuo de sus competencias designadas y de sus niveles de capacidad en materia de seguridad informática, en consonancia con las responsabilidades de seguridad informática que se les han asignado.

RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA

6.20. La autoridad competente en materia de seguridad informática debería exigir a las autoridades competentes y a los explotadores que elaboren, apliquen y lleven a cabo procedimientos de seguridad informática para prevenir y detectar incidentes de seguridad informática y responder ante ellos.

6.21. La autoridad competente en materia de seguridad informática debería orientar a las autoridades competentes y a los explotadores sobre la constatación de incidentes que podrían ser incidentes de seguridad informática. Los incidentes de seguridad informática también pueden ser sucesos relacionados con la seguridad física nuclear, por ejemplo, el robo de información de carácter estratégico o la interrupción de las funciones de seguridad física nuclear o de seguridad tecnológica nuclear. Además, los ciberataques pueden formar parte de ataques combinados. La detección exitosa de ciberataques sutiles o encubiertos puede proporcionar indicadores anticipados de las posibles intenciones del adversario.

6.22. La autoridad competente en materia de seguridad informática debería garantizar que las autoridades competentes y los explotadores y las organizaciones de respuesta pertinentes dispongan de las capacidades de respuesta adecuadas para hacer frente a los incidentes de seguridad informática, y que esas organizaciones definan las circunstancias en las que se activarían esas capacidades en sus programas de seguridad informática.

6.23. La autoridad competente en materia de seguridad informática debería definir los requisitos para la notificación oportuna de los incidentes de seguridad informática al órgano regulador de la seguridad física nuclear o a otras autoridades competentes pertinentes.

6.24. La autoridad competente en materia de seguridad informática debería garantizar que una autoridad competente o explotador con capacidades que sean lo suficientemente avanzadas (por ejemplo, con competencia en materia de seguridad informática forense) realice la caracterización técnica de los incidentes de seguridad informática que afecten a los recursos digitales de carácter estratégico.

SIMULACROS

6.25. La autoridad competente en materia de seguridad informática debería garantizar que se realicen simulacros de seguridad física nuclear con un componente de seguridad informática para evaluar la capacidad del Estado de responder a incidentes de seguridad informática, incluidos los ataques combinados.

6.26. La autoridad competente en materia de seguridad informática debería garantizar que las autoridades competentes y los explotadores realicen periódicamente simulacros de seguridad informática para formar a los participantes y validar sus programas de seguridad informática, incluidos los planes de contingencia. En su caso, esos simulacros deberían integrarse con otros simulacros de seguridad física nuclear, y periódicamente deberían realizarse de forma conjunta con simulacros de emergencia.

ACTIVIDADES DE GARANTÍA

6.27. La autoridad competente en materia de seguridad informática debería llevar a cabo actividades de garantía para velar por la aplicación efectiva de la seguridad informática en todo el régimen de seguridad física nuclear del Estado y verificar que las medidas de seguridad informática aplicadas proporcionan un nivel de protección acorde con la evaluación de las amenazas y la determinación del riesgo aceptable por parte del Estado.

6.28. La autoridad competente en materia de seguridad informática debería garantizar de manera formal y asidua al Estado que existen suficientes competencias y niveles de capacidad en materia de seguridad informática en todas las autoridades competentes y explotadores.

Cualificación de la seguridad de las piezas y los servicios

6.29. Las autoridades competentes, los explotadores y sus respectivos proveedores, contratistas y suministradores deberían tener la garantía de que los equipos, las piezas y los servicios adquiridos cuentan con medidas de seguridad informática para evitar la introducción de factores de vulnerabilidad, incluida la introducción directa de programas informáticos maliciosos o vías de ciberataque.

6.30. Las autoridades competentes y los explotadores deberían asegurarse de que sus proveedores, contratistas y suministradores que contribuyen a los recursos digitales de carácter estratégico de los que son responsables apliquen los requisitos de seguridad informática pertinentes (por ejemplo, el desarrollo de *software* seguro) con el objetivo de minimizar los factores de vulnerabilidad de los recursos digitales de carácter estratégico y evitar el uso de la cadena de suministro como vía para los ciberataques. Esta labor comprende la revisión de las metodologías, los procesos y los equipos de los proveedores, contratistas y suministradores.

6.31. La autoridad competente en materia de seguridad informática podrá designar normas nacionales o internacionales para que las autoridades competentes, los explotadores, los proveedores, los contratistas y los suministradores las utilicen en los pliegos de condiciones para la adquisición de recursos digitales de carácter estratégico y servicios conexos. Esas normas deberían aplicarse a todas las fases del ciclo de vida de un recurso digital de carácter estratégico.

6.32. La autoridad competente en materia de seguridad informática podrá designar a una autoridad de certificación para que lleve a cabo actividades que garanticen que los proveedores, los contratistas y los suministradores que diseñan y suministran recursos digitales de carácter estratégico y prestan asistencia conexa siguen las prácticas de seguridad informática exigidas.

6.33. Se alienta a las autoridades competentes y a los explotadores, según proceda, a realizar otros controles de garantía a los proveedores, contratistas y suministradores, como pruebas de aceptación en fábrica e inspecciones o auditorías de seguridad informática (basadas en los requisitos contractuales).

COOPERACIÓN Y ASISTENCIA INTERNACIONALES

6.34. La autoridad competente en materia de seguridad informática debería velar por que existan las relaciones necesarias con las autoridades homólogas de otros Estados y con los organismos internacionales para poder utilizar eficazmente

la cooperación y la asistencia internacionales, cuando proceda, a los fines de respaldar la seguridad informática relacionada con los regímenes de seguridad física nuclear. La autoridad competente en materia de seguridad informática debería considerar esas relaciones a la luz de las responsabilidades, las capacidades y las competencias de todas las organizaciones pertinentes.

7. ELABORACIÓN DE UN PROGRAMA DE SEGURIDAD INFORMÁTICA

7.1. En la presente sección se describen los componentes y las medidas recomendadas del programa de seguridad informática para cada organización. En la figura 8 se ilustra un ejemplo de marco para el programa de seguridad informática que incluye documentos de apoyo y subsidiarios.

7.2. El programa de seguridad informática de cada autoridad competente y explotador define el papel de esa organización en la aplicación de la estrategia, en la forma de funciones, responsabilidades y procedimientos organizativos. En el programa de seguridad informática también se especifican los medios con que la autoridad competente o el explotador pretende alcanzar los objetivos de seguridad informática o aplicar las medidas de seguridad informática especificadas por la legislación, la reglamentación, las normas y las orientaciones de su órgano regulador y de la autoridad competente en materia de seguridad informática.

7.3. La autoridad competente en materia de seguridad informática debería garantizar que cada autoridad competente u explotador elabore y mantenga su programa de seguridad informática según lo establecido en la presente sección. El programa de seguridad informática debería establecerse en el marco del plan general de seguridad del emplazamiento y dentro del sistema de gestión de cada organización.

7.4. La autoridad competente en materia de seguridad informática debería velar por que la seguridad informática se promueva como un componente esencial de la cultura de la seguridad física nuclear y debería fomentar un empeño de mejora continua mediante el compromiso explícito del personal directivo superior de cada autoridad competente u explotador.

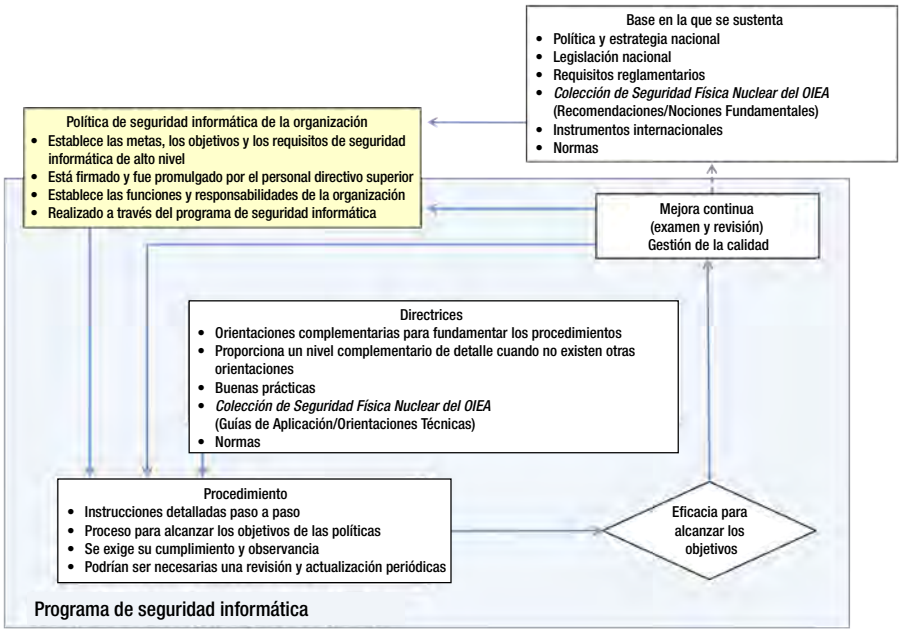


Fig. 8. Panorama general de un programa de seguridad informática.

CONTENIDO DE UN PROGRAMA DE SEGURIDAD INFORMÁTICA

7.5. El programa de seguridad informática debería describir la seguridad informática en la organización, desde el punto de vista de la susceptibilidad a los factores de vulnerabilidad, las medidas de protección, el análisis de consecuencias y las medidas de mitigación, a fin de determinar y mantener el nivel aceptable de riesgo derivado de los ciberataques y facilitar la recuperación a unas condiciones operacionales seguras.

7.6. El contenido de un programa de seguridad informática debería incluir, como mínimo, los siguientes aspectos:

a) Organización y responsabilidades:
   i) organigramas;
   ii) personas responsables y responsabilidades jerárquicas;
   iii) sanciones y medidas correctivas;
   iv) proceso de revisión y aprobación periódica, e
   v) interfaces con otros programas.

b) Gestión de recursos digitales:
   i) lista de todos los sistemas computerizados;
   ii) lista de todas las aplicaciones de los sistemas computerizados;
   iii) diagramas de flujo de datos y de red, incluidas todas las conexiones con sistemas computerizados externos;
   iv) gestión de la configuración (*hardware*, *firmware*, aplicaciones de *software*, estado de los equipos y configuraciones conexas), y
   v) clasificación de los recursos digitales y definición de los recursos digitales de carácter estratégico, incluida la clasificación de la importancia (es decir, la contribución a la seguridad física nuclear, la seguridad tecnológica nuclear y las funciones de contabilidad y control de los materiales nucleares).

c) Evaluación de riesgos, factores de vulnerabilidad y cumplimiento:
   i) periodicidad de la revisión y reevaluación del programa de seguridad informática;
   ii) autoevaluación (incluidos los procedimientos para la realización de pruebas de carácter activo y pasivo);
   iii) reevaluación periódica y reactiva de los riesgos y metodología conexa;
   iv) procedimientos de auditoría y seguimiento y corrección de deficiencias, y
   v) revisión del cumplimiento de la legislación y la normativa.

d) Diseño de la seguridad del sistema:
   i) principios fundamentales de arquitectura y diseño;
   ii) enfoques fundamentales de diseño de seguridad (por ejemplo, niveles y zonas de seguridad);
   iii) formalización de los requisitos de seguridad informática para proveedores, contratistas y suministradores, y
   iv) seguridad a lo largo del ciclo de vida.

e) Procedimientos operacionales de seguridad:
   i) control de acceso;
   ii) seguridad de los datos;
   iii) seguridad de las comunicaciones;
   iv) seguridad de plataformas y aplicaciones (por ejemplo, endurecimiento, gestión de parches, protección contra los programas maliciosos);
   v) monitorización del sistema (incluida la gestión de registros);
   vi) mantenimiento de la seguridad informática;
   vii) manejo de incidentes;
   viii) continuidad de las actividades y recuperación en casos de desastre, y
   ix) copia de seguridad del sistema.

f) Gestión de personal:
   i) controles de confianza (investigación de personal);

ii) sensibilización y capacitación;
iii) cualificación del personal, y
iv) cese de empleo o traslado de personal.

7.7. El programa de seguridad informática debería ser una parte integrada y coordinada del sistema de gestión de la organización. El programa de seguridad informática puede estar dividido en partes que tengan diferentes niveles de clasificación de seguridad, para facilitar el uso del plan de manera eficiente y coherente con la regla de "necesidad de saber" y los requisitos de confidencialidad.

7.8. El programa de seguridad informática debería revisarse periódicamente y actualizarse para reflejar los nuevos conocimientos pertinentes, tanto los pertenecientes al régimen de seguridad física nuclear como los ajenos a este, incluidos los siguientes:

a) nuevas tecnologías que se podrían utilizar en los ciberataques o para su empleo como protección contra estos;
b) nuevas características de las ciberamenazas, incluidos los cambios detectados en las tácticas, las técnicas y los procedimientos, y
c) nuevos tipos de incidentes de seguridad informática o de sucesos relacionados con la seguridad física nuclear.

7.9. El programa de seguridad informática debería prever simulacros periódicos para formar a los participantes y validar el programa de seguridad informática, incluidos los planes de contingencia. En su caso, esos simulacros deberían integrarse con otros simulacros de seguridad, y periódicamente deberían realizarse de forma conjunta con simulacros de emergencia.

EVALUACIÓN DE RIESGOS A NIVEL INSTITUCIONAL

7.10. Dependiendo de las capacidades de las autoridades competentes o de los explotadores y del potencial impacto adverso de los ciberataques en los recursos digitales de carácter estratégico de los que son responsables, el programa de seguridad informática puede incluir una metodología para que las organizaciones lleven a cabo evaluaciones de riesgo locales de sus sistemas computerizados en las que se tenga en cuenta el entorno local de amenazas.

7.11. El objetivo de esa evaluación es llevar a cabo las siguientes tareas:

a) determinar y comprender el riesgo, así como los factores que contribuyen a ese riesgo;
b) servir de base para indicar los sistemas computerizados y los recursos digitales de carácter estratégico;
c) establecer valores de referencia para apoyar los análisis de los cambios en los recursos digitales de carácter estratégico y otros recursos digitales, la amenaza y el impacto potencial en la seguridad informática y el impacto resultante en la seguridad física nuclear, y
d) ayudar a validar los requisitos de nivel superior.

7.12. La organización puede realizar evaluaciones de riesgo tanto a nivel institucional como de sistema.

7.13. En esas evaluaciones de riesgo se debería utilizar como base la declaración nacional de amenazas o la amenaza base de diseño y se deberían considerar otras fuentes de información disponibles sobre ciberamenazas para fundamentar el proceso de evaluación.

7.14. En el proceso de evaluación de riesgos deberían considerarse las consecuencias adversas para la seguridad física nuclear o la seguridad tecnológica nuclear derivadas de que cada sistema computerizado se viera comprometido o funcionara incorrectamente, como base para determinar cuáles son los recursos digitales de carácter estratégico.

7.15. Si los resultados de la evaluación de riesgos se desvían significativamente de lo que ha dado por sentado la autoridad competente en materia de seguridad informática, las autoridades competentes o los explotadores deberían resolver esa cuestión de manera oportuna. Esas desviaciones pueden ser, por ejemplo, el resultado de cambios en el entorno local de las amenazas o cambios en los equipos que introducen nuevos factores de vulnerabilidad.

7.16. En la evaluación de riesgos deberían abordarse de forma colectiva todos los aspectos de la seguridad física nuclear, incluidas, por ejemplo, la protección física y la protección contra las amenazas que plantean los agentes internos, así como la seguridad informática, con el fin de evaluar el riesgo de ataques combinados. Por ello, la evaluación de riesgos debería realizarse con las aportaciones de expertos en cada una de esas esferas.

MEDIDAS DE SEGURIDAD INFORMÁTICA

7.17. En el programa de seguridad informática se especificarán las medidas de seguridad informática que proporcionan funciones de prevención, detección, retraso, respuesta y mitigación, y las que garantizan que los actos no dolosos no den lugar a una degradación de la seguridad informática que se traduzca en una mayor susceptibilidad a los ciberataques.

7.18. Se pueden asignar medidas específicas de seguridad informática de los siguientes tres tipos:

a) Medidas de control técnico: soluciones de *hardware* o *software* para la protección, detección, mitigación y recuperación en caso de intrusiones u otros actos dolosos dirigidos contra los recursos digitales de carácter estratégico. A la hora de evaluar la eficacia de los distintos tipos de medidas, deberían tenerse en cuenta las ventajas de las medidas técnicas de control, en particular la realización de acciones de protección continuas y automáticas.
b) Medidas de control físico: barreras físicas para la protección de los recursos digitales de carácter estratégico contra los daños físicos y el acceso físico no autorizado. Las medidas de control físico incluyen guardias y barreras como cerraduras, vallas, puertas, encajonamientos, dispositivos de indicación de manipulación ilícita y salas de aislamiento.
c) Medidas de control administrativo: políticas, procedimientos y prácticas diseñadas para proteger los recursos digitales de carácter estratégico mediante el control de las acciones y comportamientos del personal. Las medidas de control administrativo incluyen medidas operacionales y de gestión, suelen ser de carácter directivo y especifican lo que los empleados y el personal de terceros deberían y no deberían hacer, pero también incluyen medidas susceptibles de ejercer influencia, como la promoción de una sólida cultura de la seguridad física.

UN ENFOQUE GRADUADO PARA DETERMINAR LAS MEDIDAS DE SEGURIDAD INFORMÁTICA

7.19. Las medidas de seguridad informática dentro del programa de seguridad informática deberían basarse en un enfoque graduado, en el que las medidas de seguridad se apliquen proporcionalmente al impacto potencial de un ciberataque. Una aplicación práctica del enfoque graduado consiste en asignar los sistemas computerizados de seguridad física nuclear por zonas y aplicar medidas de seguridad informática graduadas para cada zona. Un enfoque común para la

aplicación de las medidas de seguridad informática graduadas es la designación de niveles de seguridad informática (véanse los párrafos 2.41 a 2.46).

7.20. El programa de seguridad informática debería incluir un método documentado, como el descrito en la sección 2, a fin de determinar el nivel de seguridad informática adecuado para cada recurso digital, incluidos los recursos digitales de carácter estratégico, si así lo exige la autoridad competente en materia de seguridad informática. Por ejemplo, se puede exigir a algunas autoridades competentes u explotadores que apliquen medidas de seguridad informática prescriptivas, en lugar de determinar por sí mismos los requisitos de nivel de seguridad de los sistemas computerizados, los recursos digitales y los recursos digitales de carácter estratégico.

7.21. La autoridad competente en materia de seguridad informática debería aprobar el método utilizado para determinar los niveles de seguridad informática.

DISEÑO DE MEDIDAS DE SEGURIDAD INFORMÁTICA

7.22. El programa de seguridad informática debería promover la incorporación de medidas de seguridad informática, en la mayor medida posible, en el diseño de los sistemas computerizados. Las medidas de seguridad informática suelen ser mucho más fáciles de aplicar y más eficaces cuando se incorporan como parte del diseño y no cuando se añaden *a posteriori*.

7.23. A la hora de diseñar sistemas computerizados, deberían tenerse en cuenta tanto los requisitos de seguridad física nuclear como los de seguridad tecnológica nuclear.

DEFENSA EN PROFUNDIDAD PARA LAS MEDIDAS DE SEGURIDAD INFORMÁTICA

7.24. El concepto de defensa en profundidad es fundamental para la seguridad física nuclear. El programa de seguridad informática debería establecer cómo se aplica la defensa en profundidad a las medidas de seguridad informática. Ese objetivo puede lograrse de diferentes maneras, entre ellas las siguientes:

a) Utilizar medidas de seguridad informática diversas e independientes, y exigir independencia en su diseño, funcionamiento y mantenimiento. De ese modo, por ejemplo, se garantizará que una sola vulnerabilidad de seguridad

informática no proporcione a un adversario la oportunidad de saltarse sistemáticamente varias capas de defensa en profundidad.

b) Separación de funciones del personal o los equipos que tienen acceso privilegiado a los recursos digitales de carácter estratégico. En ese ámbito debería tenerse en cuenta la separación de funciones en el diseño, la aplicación y la administración de las medidas de seguridad informática de las operaciones de la instalación o actividad.

GESTIÓN DE PROVEEDORES, CONTRATISTAS Y SUMINISTRADORES

7.25. Las autoridades competentes o explotadores pueden recurrir a proveedores, contratistas o suministradores para obtener bienes o servicios que necesariamente implican que los proveedores, contratistas o suministradores accedan a información de carácter estratégico y a recursos digitales de carácter estratégico. En esos casos, un acuerdo jurídico, como una licencia o el contrato de suministro de los bienes o servicios, debería incluir los requisitos adecuados relativos a la seguridad informática.

7.26. A la hora de redactar esas licencias o contratos, las autoridades competentes y los explotadores deberían considerar la posibilidad de incluir disposiciones que tengan en cuenta el hecho de que los proveedores, los contratistas y los suministradores podrían poseer información exclusiva y de ámbito privado sobre sus productos o servicios (por ejemplo, sobre los factores de vulnerabilidad a los ciberataques que podrían ponerse de manifiesto una vez finalizado el contrato original) y que se les podría exigir que compartieran esta información con las autoridades competentes y los explotadores.

7.27. Las autoridades competentes y los explotadores deberían definir en sus programas de seguridad informática requisitos específicos de seguridad informática para los proveedores, contratistas y suministradores. Esos requisitos pueden incluir requisitos relacionados con el trabajo en el emplazamiento y fuera de él.

7.28. Las autoridades competentes y los explotadores deberían garantizar que los proveedores, contratistas y suministradores apliquen medidas de seguridad informática en el desarrollo y la entrega de los productos y servicios que proporcionan.

7.29. Las autoridades competentes y los explotadores pueden definir requisitos específicos de seguridad informática en el marco de los acuerdos contractuales. Esos requisitos pueden ser, entre otros, los siguientes:

a) requisitos de no divulgar información de carácter estratégico y otra información especificada;
b) requisitos de protección de la información de carácter estratégico, incluidos los requisitos de conservación o destrucción de esa información;
c) limitaciones del acceso permitido y de las actividades que se realizarán en los sistemas computerizados;
d) actividades prohibidas;
e) sanciones por incumplimiento de los requisitos de seguridad informática establecidos;
f) restricciones para el acceso a distancia, y
g) requisitos de las pruebas para los servicios y productos suministrados en el marco del contrato.

7.30. Las autoridades competentes y los explotadores pueden considerar la posibilidad de exigir a los proveedores, contratistas y suministradores que demuestren el cumplimiento de los requisitos contractuales de seguridad informática.

7.31. Las autoridades competentes y los explotadores deberían exigir que los proveedores, los contratistas y los suministradores informaran oportunamente de los incidentes de seguridad informática, incluida la constatación de posibles amenazas y factores de vulnerabilidad que pudieran afectar a la seguridad física nuclear. Las obligaciones y los protocolos de presentación de información deberían formar parte del contrato.

7.32. La utilización de proveedores, contratistas y suministradores puede dar lugar a la transferencia o el reparto de riesgos. Esa transferencia o reparto de riesgos también puede exigir la aprobación del órgano regulador de la seguridad física nuclear o de la autoridad competente en materia de seguridad informática. Sin embargo, la responsabilidad de la seguridad física nuclear, incluida la seguridad informática, no puede transferirse a los proveedores, contratistas y suministradores.

8. MANTENIMIENTO DE LA SEGURIDAD INFORMÁTICA

8.1. En la presente sección se describen los elementos y medidas recomendados para mantener la seguridad informática como parte de un régimen de seguridad física nuclear. Esos elementos y medidas deberían estar documentados en el programa de seguridad informática.

8.2. Las autoridades competentes y los explotadores deberían contar con programas adecuados de desarrollo de los recursos humanos a fin de garantizar que mantengan las competencias y el nivel de capacidad necesarios para desempeñar las responsabilidades que se les asignan en materia de seguridad informática.

8.3. Las autoridades competentes y los explotadores deberían disponer de procesos para aprovechar las mejores prácticas y las enseñanzas extraídas de la experiencia [1], en particular de los incidentes de seguridad informática y, cuando sea posible, de otras autoridades competentes y explotadores, otros sectores pertinentes y organizaciones equivalentes en otros Estados.

8.4. Las autoridades competentes y los explotadores deberían incluir la seguridad informática en sus programas de sostenibilidad y respaldarla con recursos suficientes. Los programas de sostenibilidad deberían abarcar los aspectos pertinentes de las competencias y los niveles de capacidad necesarios en el desarrollo, la aplicación, el mantenimiento y la desactivación o la retirada de los recursos digitales de carácter estratégico y otros recursos digitales.

CULTURA DE LA SEGURIDAD FÍSICA NUCLEAR

8.5. El establecimiento, el fomento y el mantenimiento de una sólida cultura de la seguridad física nuclear es un elemento esencial de cualquier régimen de seguridad física nuclear [1]. En el ámbito de la seguridad informática, las personas y los procesos suelen ser el factor clave para asegurar los sistemas computerizados, y el error humano es una de las principales causas de los incidentes de seguridad informática. La cultura de la seguridad física nuclear debería ayudar a los empleados a reconocer comportamientos inusuales de los sistemas computerizados, o de las personas que los utilizan, y a informar al respecto, así como a informar sobre errores humanos que podrían afectar negativamente a la seguridad informática.

8.6. La seguridad informática debería promoverse como un componente esencial de la cultura de la seguridad física nuclear mediante el compromiso explícito del personal directivo superior y a través de la sensibilización y la capacitación. El programa de seguridad informática debería incluir actividades que refuercen la cultura de la seguridad física nuclear.

8.7. Como parte de una cultura de la seguridad física nuclear eficaz, todas las organizaciones deberían asegurarse de que sus empleados y contratistas comprendan plenamente sus responsabilidades en materia de seguridad informática y la importancia de estas, en particular con respecto a la seguridad nuclear física y tecnológica. Los empleados y contratistas deberían recibir enseñanza y capacitación en materia de seguridad informática acorde con sus funciones y responsabilidades.

CAPACITACIÓN

8.8. Las autoridades competentes y los explotadores deberían establecer programas de capacitación sobre seguridad informática para todos los empleados y contratistas, en los que se dé cuenta de la estrategia y que tengan como objetivo crear y mantener sus competencias y niveles de capacidad designados.

8.9. Los programas de capacitación deberían incluir actividades de sensibilización y desarrollo de competencias y destrezas.

8.10. Entre los temas recomendados para la sensibilización y la capacitación en materia de seguridad informática se encuentran los siguientes:

a) conocimiento de los tipos de ciberamenazas y de las técnicas de ataque conexas;
b) sensibilidad y orientación para contrarrestar la ingeniería social;
c) reconocimiento de un ciberataque y respuesta ante él;
d) responsabilidades de los individuos en materia de seguridad informática y sanciones por incumplimiento;
e) impacto potencial de los ciberataques en la seguridad nuclear física y tecnológica;
f) buenas prácticas de seguridad informática;
g) uso de dispositivos portátiles y soportes extraíbles;
h) uso de las redes sociales, y
i) cambios en el nivel o la naturaleza de la ciberamenaza o el riesgo.

8.11. El personal de mantenimiento, operaciones e ingeniería responsable de los sistemas nucleares debería tener conocimiento de los riesgos, tanto para la seguridad física nuclear como para la seguridad tecnológica nuclear, asociados a posibles ciberataques que afecten a las funciones de instrumentación y control.

8.12. El personal de mantenimiento, operaciones e ingeniería responsable de los sistemas de protección física debería reconocer los posibles efectos de los ciberataques en las funciones de los sistemas de protección física.

8.13. Los cambios en las normas y los procedimientos de seguridad deberían comunicarse a todos los empleados y contratistas pertinentes tan pronto como sea posible.

8.14. Debería impartirse capacitación especializada, adecuada a sus funciones laborales específicas, a los empleados y contratistas con responsabilidades administrativas y técnicas relacionadas con la seguridad informática (por ejemplo, el personal de apoyo a las tecnologías de la información, el personal de instrumentación y control, los administradores de sistemas de seguridad, el personal de mantenimiento de equipos técnicos).

8.15. En los programas de capacitación deberían especificarse los requisitos de capacitación para los proveedores, contratistas y suministradores, tanto para el trabajo en el emplazamiento como fuera de él.

8.16. El personal directivo superior debería recibir capacitación periódica y sesiones informativas de sensibilización sobre las ciberamenazas y la gestión de riesgos.

8.17. Las autoridades competentes y los explotadores deberían revisar y actualizar con frecuencia sus programas de capacitación para tener en cuenta el carácter dinámico de la seguridad informática, incluidos los cambios en la ciberamenaza y en las técnicas de ciberataque.

8.18. Las autoridades competentes y los explotadores deberían asignar la responsabilidad y los recursos adecuados para apoyar y mantener los programas de capacitación.

8.19. Deberían mantenerse registros de la capacitación formal que han cursado todos los empleados y contratistas.

8.20. Las actividades de capacitación y sensibilización sobre la seguridad de la información y la seguridad informática suelen impartirse conjuntamente. En el anexo III de la referencia [8] figura un ejemplo de programa de sensibilización sobre la seguridad de la información, que puede adaptarse para incluir la seguridad informática.

PLANES DE CONTINGENCIA Y RESPUESTA

8.21. En el programa de seguridad informática deberían documentarse las medidas de seguridad informática para la detección de las consecuencias de los incidentes de seguridad informática, la respuesta ante ellas y su mitigación.

8.22. En el programa de seguridad informática deberían especificarse las acciones de análisis y respuesta adecuadas para caracterizar la causa, los efectos inmediatos y el impacto potencial del incidente de seguridad informática. Es posible que esos elementos no sean evidentes, pero deberían determinarse lo antes posible.

8.23. El análisis del incidente de seguridad informática debería incluir la consideración de la posibilidad de que ese incidente podría ser un ataque inicial o una actividad de reconocimiento para un futuro ataque.

8.24. El programa de seguridad informática debería incluir planes de contingencia para responder a los ciberataques. En esos planes debería tenerse en cuenta la posibilidad de que se produzcan ataques de agentes internos y combinados. En el plan de contingencia deberían señalarse varios tipos específicos de incidentes de seguridad informática y la respuesta que exigen.

8.25. Cuando un incidente de seguridad informática constituye asimismo un suceso relacionado con la seguridad física nuclear, debería activarse el plan de contingencia correspondiente. En el programa de seguridad informática y los planes de contingencia conexos se deberían especificar las acciones inmediatas que se adoptarán siempre que la seguridad tecnológica nuclear esté en peligro (en esos casos, también pueden activarse los planes de emergencia, pero estos quedan fuera del alcance de la presente publicación).

8.26. El programa de seguridad informática debería incluir los criterios para la participación de recursos adicionales y su papel en la respuesta a los incidentes de seguridad informática.

8.27. El análisis de los incidentes de seguridad informática puede entrañar la participación de un equipo transversal para analizar el impacto tanto en la seguridad física nuclear como en la seguridad tecnológica nuclear.

ACTIVIDADES DE GARANTÍA DE LA SEGURIDAD INFORMÁTICA

8.28. Las autoridades competentes y los explotadores deberían velar por que sus sistemas de gestión incluyan medios eficaces para garantizar el cumplimiento de los requisitos de seguridad informática, también en la cadena de suministro.

8.29. Las autoridades competentes y los explotadores (excepto los que solo aplican las medidas de seguridad informática prescritas por el órgano regulador o la autoridad competente en materia de seguridad informática) deberían garantizar a la autoridad competente en materia de seguridad informática que los recursos asignados a la seguridad informática sean adecuados y proporcionados al nivel de amenaza definido en la evaluación de las amenazas.

8.30. Las autoridades competentes y los explotadores deberían garantizar que las inspecciones o evaluaciones para verificar el cumplimiento de los requisitos de seguridad física nuclear incluyan la evaluación de las medidas de seguridad informática.

Apéndice

CONSIDERACIONES DE LA INTERFAZ DE SEGURIDAD TECNOLÓGICA NUCLEAR PARA LA SEGURIDAD INFORMÁTICA DE LAS INSTALACIONES

A.1. El sabotaje de una instalación podría comprometer su seguridad tecnológica nuclear o su disponibilidad en el caso de un ciberataque a los sistemas importantes para la seguridad tecnológica de la instalación que utilizan sistemas computerizados, dependen de ellos o se sustentan en ellos. Esos ataques pueden provocar fallos o un mal funcionamiento de esos sistemas importantes para la seguridad tecnológica de una manera que no se produciría si los sistemas estuvieran en sus condiciones operacionales o en los estados de fallo previstos.

A.2. Los actos dolosos pueden afectar a un solo sistema (o elemento) o ser la causa común de un comportamiento indeseable de varios sistemas (o elementos). En el diseño de la instalación debería garantizarse que los actos dolosos no puedan provocar el fallo o eludir los diferentes niveles de la defensa en profundidad de la seguridad tecnológica.

A.3. La seguridad informática pretende reducir la posibilidad de que los adversarios cometan actos de sabotaje a través de ciberataques que podrían comprometer la seguridad física, la seguridad tecnológica o la disponibilidad de la instalación. La seguridad informática contribuye a todos los niveles de defensa en profundidad de la seguridad tecnológica, como se describe en la referencia [12], por lo que debería aplicarse a las funciones, los sistemas y los equipos de todos los niveles.

A.4. La interfaz seguridad tecnológica-seguridad física en la seguridad informática comprende una serie de elementos importantes para la seguridad física nuclear y la seguridad tecnológica nuclear. Esos elementos comprenden sistemas, procedimientos y personal. Las medidas de seguridad tecnológica nuclear suelen ofrecer también funciones valiosas para la seguridad física nuclear (y viceversa), por lo que al desarrollar medidas de seguridad informática deberían tenerse en cuenta las oportunidades de aprovechar esas funciones complementarias.

A.5. Un ejemplo de una medida de seguridad tecnológica que también puede reportar beneficios para la seguridad física es una característica que proporciona la comprobación automática de la validez, la autenticidad y la integridad de los datos recibidos antes de su uso dentro de una función de seguridad tecnológica.

El mantenimiento o la modificación de la característica puede degradar las funciones de seguridad tecnológica o seguridad física si quienes realizan esas actividades no son conscientes de las distintas funciones (interdependencias). Por lo tanto, tanto las funciones de seguridad tecnológica como las de seguridad física que realizan estas características deberían describirse en la documentación del sistema y de los componentes.

A.6. La estrategia de seguridad tecnológica también puede influir negativamente en la seguridad física (o viceversa). Por ejemplo, el diseño de la seguridad tecnológica suele implicar la asignación de funciones a diferentes elementos o sistemas para aislar los efectos de los fallos, y la adopción de sistemas redundantes y diversos para que los fallos aislados no comprometan las funciones importantes. Esa estrategia puede dar lugar a un aumento del número de elementos del sistema importantes para la seguridad tecnológica, lo que incrementaría su complejidad y puede aumentar el número de posibles objetivos de un ciberataque. Por lo tanto, siempre hay que tener en cuenta tanto las medidas de seguridad física como las de seguridad tecnológica para detectar y resolver cualquier conflicto.

A.7. La idoneidad de una determinada medida de seguridad informática dependerá tanto de las consideraciones de seguridad física como de las de seguridad tecnológica, por lo que para diseñar esas medidas son necesarios conocimientos en ambas esferas. Las medidas de seguridad informática incluirán medidas técnicas, físicas y administrativas, y todas ellas han de funcionar conjuntamente. Este enfoque puede requerir, por ejemplo, que ciertas funciones de seguridad física (por ejemplo, la recopilación de registros de auditoría, la generación de alarmas de seguridad) sean ejecutadas por sistemas que puedan monitorizar los sistemas de instrumentación y control pero que no puedan influir en su desempeño, o que las exploraciones activas de seguridad física se realicen solo cuando los sistemas de instrumentación y control estén fuera de línea. Pueden permitirse excepciones a este enfoque, pero habría que analizarlas y justificarlas en función de cada caso.

A.8. Es probable que el riesgo aceptable para una instalación sea el mismo tanto si la causa inicial es un suceso relacionado con la seguridad tecnológica o con la seguridad física. Los enfoques habituales para lograr este objetivo pueden resumirse en los siguientes términos:

a) Tanto en la seguridad tecnológica como en la seguridad física se aplica el concepto de defensa en profundidad (es decir, el empleo de varias capas de protección).

b) Se tiene en cuenta la prevención de un suceso iniciador, la detección temprana de cualquier situación anormal y la respuesta rápida para evitar que la situación se agrave.
c) La mitigación de las consecuencias está prevista en el diseño, en caso de que fallen los pasos anteriores.
d) Existe una amplia planificación de emergencias para hacer frente a las situaciones en las que fallan la prevención, la detección y la mitigación.

A.9. La relación entre la seguridad informática y la seguridad tecnológica necesita una coordinación eficaz, por ejemplo, en la clasificación y la gestión de los recursos según distintas consideraciones de seguridad física y seguridad tecnológica. Esa relación puede complicarse por la creciente dependencia del *software* y las redes que tienen los sistemas computerizados y la consiguiente rapidez con la que estos cambian, lo que conlleva que el diseño y el funcionamiento de las medidas de seguridad informática también cambien rápidamente. Ese hecho constituye un reto cuando los análisis de la seguridad se basan en predicciones precisas del comportamiento determinista futuro. Ese análisis puede complicarse aún más por la incertidumbre sobre la eficacia de las medidas de seguridad informática, lo que significa que tal vez el análisis no proporcione predicciones precisas sobre el comportamiento futuro del sistema en respuesta a los sucesos iniciadores (por ejemplo, cuando son objeto de ciberataques).

A.10. Es probable que para aplicar medidas de seguridad informática a los sistemas existentes sea necesario revisar el análisis de la seguridad existente. En general, las medidas de seguridad informática integradas tienen la capacidad potencial de limitar o alterar de otro modo el comportamiento del sistema importante para la seguridad tecnológica, a diferencia de las medidas aisladas o independientes.

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] *Convención sobre la Protección Física de los Materiales Nucleares*, INFCIRC/274/Rev.1, OIEA, Viena, 1980; *Enmienda de la Convención sobre la Protección Física de los Materiales Nucleares*, INFCIRC/274/Rev.1/Mod.1, OIEA, Viena, 2016.

[3] 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.

[4] 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.

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

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Facilities, IAEA Nuclear Security Series No. 17-T (Rev. 1), IAEA, Vienna (in preparation).

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

[9] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Information Technology — Security Techniques — Information Security Risk Management, ISO/IEC 27005:208, ISO, Geneva (2018).

[10] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Evaluación nacional de amenazas para la seguridad física nuclear, amenazas base de diseño y declaraciones de amenazas representativas, Colección de Seguridad Física Nuclear del OIEA* Nº 10-G (Rev. 1), OIEA, Viena, 2022.

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

[12] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Seguridad de las centrales nucleares: Diseño*, *Colección de Normas de Seguridad del OIEA* Nº SSR-2/1 (Rev. 1), OIEA, Viena, 2017.

Anexo I

PROPUESTA DE ORIENTACIONES DE LA CATEGORÍA "RECOMENDACIONES" SOBRE SEGURIDAD INFORMÁTICA PARA UN RÉGIMEN NACIONAL DE SEGURIDAD FÍSICA NUCLEAR

I-1. Los "ELEMENTOS DEL RÉGIMEN DE SEGURIDAD FÍSICA NUCLEAR DE UN ESTADO PARA LA SEGURIDAD INFORMÁTICA" del presente anexo fueron elaborados por expertos de más de 20 Estados Miembros para complementar las publicaciones de Recomendaciones existentes en la *Colección de Seguridad Física Nuclear del OIEA* [I-1 a I-3], y son orientaciones de la categoría "Recomendaciones" sobre el diseño, la aplicación y el mantenimiento de la seguridad informática en el régimen de seguridad física nuclear de un Estado. Los Estados pueden optar por tratar el texto como orientaciones de la categoría "Recomendaciones". Las orientaciones de aplicación que figuran en el texto principal de la presente publicación son coherentes con las orientaciones de la categoría "Recomendaciones" que se proponen en el presente anexo.

ANTECEDENTES

I-2. El objetivo de las publicaciones de Recomendaciones de la *Colección de Seguridad Física Nuclear del OIEA* [I-1 a I-3] es brindar orientación a los Estados y a sus autoridades competentes sobre cómo desarrollar o mejorar, aplicar y mantener un régimen nacional de seguridad física nuclear eficaz para garantizar la seguridad física, respectivamente, de los materiales nucleares y las instalaciones nucleares, los materiales radiactivos y las instalaciones conexas y los materiales nucleares y otros materiales radiactivos no sometidos a control reglamentario.

I-3. En las publicaciones de Recomendaciones se exponen las buenas prácticas que deberían adoptar los Estados Miembros al aplicar las Nociones Fundamentales de Seguridad Física Nuclear [I-4]. En las Nociones Fundamentales se precisa la responsabilidad de los Estados de garantizar que la información de carácter estratégico y los recursos de información de carácter estratégico estén protegidos de las amenazas a la seguridad física nuclear.

I-4. La seguridad física nuclear puede tener como objetivo la información de carácter estratégico o los recursos de información de carácter estratégico para socavar el desempeño de las funciones del sistema de seguridad física nuclear o de seguridad tecnológica nuclear. El ataque podría ser un acto solitario de

sabotaje o podría formar parte de un ataque combinado contra una instalación, que incluya elementos tanto de un ciberataque como de un ataque físico, o contra una organización a fin de obtener acceso no autorizado a material. Por lo tanto, la seguridad informática es intrínseca al régimen de seguridad física nuclear del Estado y es necesaria para alcanzar sus objetivos.

I-5. Los recursos digitales de carácter estratégico son los recursos de información de carácter estratégico que son sistemas computerizados que si se vieran comprometidos podrían dar lugar a impactos adversos en la seguridad física nuclear. Por lo tanto, los recursos digitales de carácter estratégico exigen la aplicación de medidas de seguridad informática.

I-6. Las medidas de seguridad informática tienen como objetivo mantener la confidencialidad, la integridad y la disponibilidad de la información de carácter estratégico de los recursos digitales de carácter estratégico y dentro de ellos mismos.

I-7. Las publicaciones de Recomendaciones existentes carecen de orientaciones suficientes sobre las medidas de seguridad informática para la protección de los recursos digitales de carácter estratégico.

OBJETIVO

I-8. En el presente anexo figuran orientaciones sobre seguridad informática para la aplicación de los elementos esenciales de las Nociones Fundamentales de Seguridad Física Nuclear [I-4] cuando no se abordan con suficiente detalle en las Recomendaciones [I-1 a I-3]. Las presentes orientaciones no pretenden modificar en absoluto las Recomendaciones existentes.

I-9. El presente anexo se dirige a los Estados, las autoridades competentes, los explotadores[1], los suministradores, los proveedores, los contratistas, los profesionales de la seguridad física nuclear y los profesionales de la seguridad tecnológica nuclear.

[1] En este contexto, se entiende por “explotadores” los titulares de licencias, los remitentes y los transportistas.

ALCANCE

I-10. Las presentes orientaciones se aplican a los aspectos de seguridad informática de la seguridad física nuclear.

I-11. En las orientaciones se abordan aspectos generales de la seguridad informática aplicables a todos los ámbitos de la seguridad física nuclear, incluida la seguridad física de los materiales nucleares y las instalaciones nucleares [I-1], de los materiales radiactivos y las instalaciones conexas [I-2] y de los materiales nucleares y otros materiales radiactivos no sometidos a control reglamentario [I-3]. Estas orientaciones deberían aplicarse con un enfoque graduado.

ELEMENTOS DEL RÉGIMEN DE SEGURIDAD FÍSICA NUCLEAR DE UN ESTADO PARA LA SEGURIDAD INFORMÁTICA

Responsabilidad del Estado

I-12. El Estado debería formular una estrategia de seguridad informática[2] que respalde su régimen de seguridad física nuclear.

Asignación de responsabilidades en materia de seguridad informática

I-13. El Estado debería nombrar a las autoridades competentes y dotarlas de responsabilidades para formular y aplicar el marco legislativo y reglamentario de la seguridad informática que respalde el régimen de seguridad física nuclear. La autoridad competente en materia de seguridad informática puede ser diferente de la autoridad competente (o de las autoridades competentes) en otros aspectos de la seguridad física nuclear.

I-14. El Estado debería garantizar que las funciones, los roles y otras disposiciones relativas a la seguridad informática se definan y coordinen estrechamente entre todas las autoridades competentes que participen en la seguridad física nuclear y dentro de ellas.

---

[2] Esa estrategia puede ser específica para los regímenes de seguridad física nuclear o puede ser más general, como una estrategia aplicable a la protección de infraestructuras críticas. Algunos Estados pueden utilizar el término “política” en este contexto.

Marco legislativo y reglamentario

I-15. El Estado debería garantizar que el marco legislativo y reglamentario incluyera requisitos de seguridad física nuclear para prevenir y detectar actos no autorizados contra los sistemas computerizados que podrían afectar negativamente a la seguridad física nuclear y responder ante ellos. Esos requisitos deberían utilizarse a la hora de llevar a cabo la evaluación de las amenazas del Estado.

I-16. El Estado debería establecer un proceso de inspección y aplicación para verificar el cumplimiento de los requisitos de seguridad informática de su marco legislativo y reglamentario.

I-17. El Estado debería garantizar que las sanciones por actos no autorizados contra los sistemas computerizados que podrían afectar negativamente a la seguridad física nuclear formaran parte de su marco legislativo y reglamentario.

Autoridades competentes

I-18. Las autoridades competentes deberían velar por que los explotadores formulen y apliquen una política de seguridad informática y los correspondientes programas de seguridad informática en consonancia con los requisitos nacionales de seguridad física nuclear.

I-19. Las autoridades competentes deberían garantizar que la seguridad informática forme parte de la evaluación y la concesión de licencias u otros procedimientos para conceder la autorización.

I-20. Las autoridades competentes deberían verificar el cumplimiento continuado de los requisitos de seguridad informática por parte del explotador mediante inspecciones periódicas y, cuando sea necesario, recurrir a acciones coercitivas para garantizar que se adopten medidas correctivas.

Responsabilidad de los explotadores

I-21. Los explotadores deberían determinar cuáles son los recursos digitales de carácter estratégico y describirlos en función de sus consecuencias potenciales para la seguridad física nuclear si se vieran comprometidos.

I-22. Los explotadores deberían definir las medidas de seguridad informática adecuadas[3] y garantizar que esas medidas se apliquen para proteger los recursos digitales de carácter estratégico de cualquier peligro a lo largo de su ciclo de vida (en la mayor medida posible), de acuerdo con los conceptos de enfoque graduado y defensa en profundidad.

I-23. Los explotadores deberían aplicar la seguridad informática como un principio de diseño para los recursos digitales de carácter estratégico y su utilización, incluida la protección contra el acceso no autorizado (de personas, procesos o equipos) y contra los programas maliciosos.

I-24. Los explotadores deberían evaluar y gestionar las medidas de seguridad informática de manera que no influyan negativamente en la protección física, la seguridad tecnológica nuclear y las actividades de contabilidad y control de materiales nucleares.

I-25. Los explotadores deberían realizar actividades con fines de garantía para verificar que sus medidas de seguridad informática cumplen con los requisitos de seguridad informática.

I-26. Los explotadores deberían garantizar que las medidas de seguridad informática se integren en sus disposiciones de gestión de la cadena de suministro nuclear con el objetivo de minimizar los factores de vulnerabilidad de los sistemas computerizados y evitar el uso de la cadena de suministro como vía para los ciberataques.

I-27. Las organizaciones estatales, incluidas las autoridades competentes, deberían seguir las recomendaciones de los párrafos I-21 a I-26 a la hora de proteger los recursos digitales de carácter estratégico de los que son responsables.

Cooperación y asistencia internacionales

I-28. La cooperación y la asistencia internacionales deberían incluir consideraciones de seguridad informática pertinentes para la seguridad física nuclear.

---

[3] Las medidas de seguridad pueden consistir en medidas de control físico, técnico y administrativo.

Determinación y evaluación de las amenazas

I-29. En la evaluación de las amenazas por parte del Estado[4] (y la amenaza base de diseño, si procede) se debería tener en cuenta a los posibles adversarios que utilicen capacidades informáticas, incluida la capacidad potencial de las actividades de los agentes internos y de los ataques combinados. La evaluación de las amenazas debería revisarse y actualizarse para reflejar los cambios en las ciberamenazas, y debería comunicarse oportunamente.

I-30. Cuando la amenaza base de diseño o la evaluación de las amenazas relativas a ciberataques es independiente de la amenaza base de diseño o de la evaluación de las amenazas relativas a un ataque físico, el Estado debería garantizar que las evaluaciones de las amenazas (y la amenaza base de diseño, si procede) se lleven a cabo de forma coordinada.

Interfaz entre la seguridad tecnológica y la seguridad física

I-31. La interfaz entre la seguridad tecnológica y la seguridad física, incluida la seguridad informática, debería gestionarse de manera que se garantice que no se perjudiquen entre sí y que, en la medida de lo posible, se apoyen mutuamente.

Mantenimiento de la seguridad informática

I-32. La seguridad informática debería abordarse de forma integrada y coordinada dentro del sistema de gestión de cada autoridad competente y explotador.

I-33. La seguridad informática debería promoverse como un componente esencial de la cultura de la seguridad física nuclear.

I-34. La seguridad informática debería formar parte de los programas de sostenibilidad de las autoridades competentes y de los explotadores, con el apoyo de los recursos adecuados.

Planificación y preparación y respuesta para incidentes de seguridad informática

I-35. El Estado debería garantizar la existencia de planes de contingencia y las capacidades de las autoridades competentes, los explotadores y otras partes

[4] Puede denominarse “evaluación nacional de las amenazas”.

pertinentes para hacer frente adecuadamente a los incidentes de seguridad informática que podrían afectar negativamente a la seguridad física nuclear.

I-36. El Estado debería garantizar que las autoridades competentes, los explotadores y otras partes pertinentes realicen simulacros con asiduidad para evaluar y validar los aspectos de seguridad informática de los planes de respuesta.

I-37. El régimen de seguridad física nuclear del Estado debería incluir requisitos para la notificación oportuna de incidentes de seguridad informática a la autoridad o autoridades competentes.

REFERENCIAS DEL ANEXO I

[I–1] 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.

[I–2] 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.

[I–3] INSTITUTO INTERREGIONAL DE LAS NACIONES UNIDAS PARA INVESTIGACIONES SOBRE LA DELINCUENCIA Y LA JUSTICIA, OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO, OFICINA EUROPEA DE POLICÍA, ORGANISMO INTERNACIONAL DE ENERGIA ATÓMICA, ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL, ORGANIZACIÓN INTERNACIONAL DE POLICÍA CRIMINAL-INTERPOL, ORGANIZACIÓN MUNDIAL DE ADUANAS, *Recomendaciones de seguridad física nuclear sobre materiales nucleares y otros materiales radiactivos no sometidos a control reglamentario, Colección de Seguridad Física Nuclear del OIEA* Nº 15, OIEA, Viena, 2012.

[I–4] 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.

Anexo II

PERFILES DE LAS CIBERAMENAZAS

II-1. Comprender la ciberamenaza es importante para elaborar y aplicar medidas de protección. La amenaza cibernética es diferente de la amenaza física para los materiales nucleares y otros materiales radiactivos y sus instalaciones y operaciones conexas. La ciberamenaza no está limitada por la proximidad del lugar, por el número de atacantes o por los límites de la instalación objetivo. La comprensión de las características de la ciberamenaza, así como de los posibles escenarios de ataque, proporciona una valiosa perspectiva de las medidas de prevención y respuesta. Los adversarios y sus herramientas, tácticas y objetivos son elementos dinámicos, y es necesario mantener la diligencia en la evaluación de las amenazas actuales.

II-2. Las tendencias predominantes son las siguientes [II-1, II-2]:

a) un número creciente de adversarios con capacidad para realizar ciberataques;
b) un número creciente de personas o grupos que ofrecen "ciberdelincuencia como servicio", lo que reduce las barreras de entrada para los adversarios que antes carecían de las destrezas necesarias;
c) aumento de la sofisticación de las técnicas utilizadas para los ciberataques, lo que dificulta la detección y la respuesta;
d) uso continuado de la ingeniería social en los ciberataques, incluidos las técnicas de suplantación de identidad por correo electrónico y los ataques de abrevadero;
e) los adversarios se centran cada vez más en encontrar y explotar los factores de vulnerabilidad de los sistemas de control industrial;
f) proliferación del *ransomware*, y
g) dificultad constante para asegurar la cadena de suministro contra los ciberataques.

II-3. Como mínimo, la autoridad competente para la evaluación de las ciberamenazas, la autoridad competente en materia de seguridad informática y los explotadores que participen en el proceso de evaluación de las amenazas tienen que tener en cuenta los atributos y las características que se describen en la siguiente sección para cada amenaza interna y externa que se defina. La caracterización de la ciberamenaza es difícil debido a que entraña identificar a los atacantes y a que se puede producir un ataque anónimo. Sin embargo, puede ser útil elaborar perfiles de amenaza.

ATRIBUTOS Y CARACTERÍSTICAS DE LAS CIBERAMENAZAS

II-4. Los siguientes atributos y características de las ciberamenazas pueden ser útiles para elaborar perfiles de amenazas:

a) Motivaciones: políticas, económicas, ideológicas o personales.
b) Intenciones: sabotear materiales radiactivos o una instalación radiológica, robar materiales radiactivos o nucleares, causar pánico entre la población y perturbación social, instigar la inestabilidad política, causar lesiones y víctimas en cifras elevadas, robar información de carácter estratégico.
c) Destrezas pertinentes (capacidades): destrezas en el uso de sistemas computerizados y automatizados de control en apoyo directo de los ataques físicos, para la recopilación de información, para los ataques informáticos, para la obtención de dinero.
d) Conocimientos: objetivos, planos y procedimientos del emplazamiento, medidas de seguridad física, medidas de seguridad tecnológica y procedimientos de protección contra la radiación, operaciones, utilización potencial de materiales nucleares u otros materiales radiactivos.
e) Financiación: fuente, suma y disponibilidad.
f) Tácticas: uso de la ocultación, el engaño o la fuerza.

DESCRIPCIÓN BÁSICA DE LA CIBERAMENAZA

II-5. Las amenazas pueden clasificarse de muchas maneras. Las siguientes categorías se presentan a modo de ejemplo (algunas categorías pueden solaparse).

II-6. Amenaza de agentes internos: uno de los ataques más difíciles de defender es la amenaza de agentes internos. Un “agente interno” es una persona autorizada para acceder a instalaciones o actividades conexas, a información de carácter estratégico o a recursos de información de carácter estratégico, que podría cometer o facilitar la comisión de actos delictivos o actos intencionales no autorizados relacionados con materiales nucleares, otros materiales radiactivos, instalaciones conexas o actividades conexas, o dirigidos contra ellos, u otros actos que el Estado determine que tienen un impacto negativo en la seguridad física nuclear [II-3]. El agente interno es alguien de confianza y que ha sido capacitado en los sistemas internos y que, por cualquier razón, utiliza ese acceso y esos conocimientos de manera que los compromete de forma potencialmente dolosa. Los motivos específicos de las actividades de los agentes internos varían mucho, y en esta categoría hay personas que van desde empleados descontentos hasta agentes secretos. El agente interno involuntario es un caso especial. Un

agente interno involuntario es un agente interno sin la intención ni la motivación de cometer un acto doloso que es explotado por un adversario sin que dicho agente interno involuntario sea consciente de ello [II-3].

II-7. Extremistas: el extremismo se refiere a los grupos que van más allá de la norma en la expresión política o social (es decir, el activismo que ha superado los comportamientos aceptados). Los extremistas pueden llevar a cabo un acto en solitario o pueden coordinarse libremente con individuos de mentalidad similar en un ciberataque contra un objetivo designado. Esos colectivos pueden no estar estrechamente controlados por una figura central y pueden no estar trabajando de acuerdo con reglas de enfrentamiento específicas.

II-8. Piratas informáticos por placer: entre los piratas informáticos por placer hay personas o grupos motivados por la fama o la notoriedad más que por el deseo de infligir daños o por el beneficio económico. El daño causado por los piratas informáticos por placer puede no ser selectivo (es decir, la instalación nuclear no era el objetivo específico); en cambio, puede ser el resultado de un entorno hostil. Un ejemplo sería el sistema de control de una instalación nuclear infectado con un virus común debido a la gestión insegura de los dispositivos portátiles y los soportes extraíbles.

II-9. Delincuencia organizada: la delincuencia organizada ha desarrollado ciberataques muy sofisticados y selectivos contra distintos sectores de la industria. El objetivo es el beneficio monetario, que puede proceder directamente del robo de dinero o indirectamente de la venta de datos robados o de la venta de información sobre una pista para otras amenazas.

II-10. Estado nación: Los Estados nación suelen representar una amenaza persistente y con muchos medios. Las motivaciones y los objetivos de estos ataques se limitan normalmente a la recopilación de información, y a menudo se rigen por reglas de enfrentamiento estructuradas.

II-11. Terroristas: en el pasado, los ciberataques atribuidos a los terroristas consistían en gran medida en esfuerzos poco sofisticados, como el “bombardeo de correos electrónicos” de enemigos ideológicos, los ataques de denegación de servicio o la desfiguración de sitios web, pero los terroristas pueden estar adquiriendo una competencia técnica cada vez mayor para realizar ataques basados en la red. Esa competencia técnica puede provenir de conocimientos internos o del empleo de piratas informáticos [I-4]. Los terroristas pueden tener como objetivo infraestructuras críticas como las centrales nucleares e intentar

sabotearlas, pero su objetivo también puede ser la adquisición de materiales nucleares y otros materiales radiactivos.

CARACTERÍSTICAS DE LOS ATAQUES

II-12. También es importante entender las características de los ataques para poder crear medidas de disuasión, prevención, detección, mitigación y respuesta. En las secciones siguientes se describen varios tipos de ataques (las categorías no se excluyen entre sí).

Ataque no selectivo

II-13. Es probable que muchas de las amenazas descritas anteriormente lleven a cabo ataques selectivos contra objetivos específicos de seguridad física nuclear. Sin embargo, también pueden producirse ataques no selectivos, por ejemplo, se pueden introducir inadvertidamente códigos maliciosos no dirigidos en las redes y sistemas computerizados, lo que afectaría negativamente a la seguridad física nuclear. Un ejemplo sería el sistema de control de una instalación nuclear infectado con un virus común debido a la gestión insegura de los soportes móviles.

Ataques persistentes

II-14. Un ciberataque puede tener como objetivo un impacto inmediato o puede formar parte de una campaña continuada contra una instalación u organización. Un ataque persistente puede comenzar con un sistema computerizado comprometido y, a continuación, una campaña prolongada de recogida de información. El resultado puede ser un suceso impactante, o el ataque puede tener como objetivo simplemente establecer una presencia para futuras actividades.

Ataques combinados

II-15. Los ataques combinados son actos coordinados que consisten en un ciberataque asociado a un acto físico. Por ejemplo, un sistema de control de acceso físico podría verse comprometido por un ciberataque para permitir la entrada física de personas no autorizadas.

CUADROS DE PERFILES DE AMENAZAS

II-16. Los cuadros II-1 y II-2 ilustran un posible conjunto de perfiles de atacantes. El cuadro II-1 se centra en las amenazas de agentes internos (véase también la referencia [II-3]), mientras que en el cuadro II-2 se precisan las posibles amenazas externas. En los cuadros se asocian los tipos generales de atacantes con sus recursos, la duración del ataque, las herramientas que probablemente se utilicen y las motivaciones del atacante. Los perfiles tienen que adaptarse a las distintas situaciones.

REFERENCIAS DEL ANEXO II

[II–1] AUSTRALIAN CYBER SECURITY CENTRE, ACSC 2015 Threat Report (2015), www.cyber.gov.au/sites/default/files/2020-04/ACSC_Threat_Report_2015.pdf

[II–2] GEORGIA INSTITUTE OF TECHNOLOGY, Emerging Cyber Threats Report 2016 (2015), https://iisp.gatech.edu/sites/default/files/documents/threats_report_2016.pdf

[II–3] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Medidas de prevención y de protección contra las amenazas de agentes internos*, *Colección de Seguridad Física Nuclear del OIEA* N° 8-G (Rev. 1), OIEA, Viena, 2022.

[II–4] CONGRESSIONAL RESEARCH SERVICE, Terrorist Use of the Internet: Information Operations in Cyberspace (2011), www.hsdl.org/?view&did=8233

CUADRO II-1. AMENAZAS INTERNAS

Amenaza	Recursos (destrezas, conocimientos, acceso, financiación)	Dedicación horaria y otros aspectos relacionados con el tiempo	Tácticas	Motivaciones	Intenciones
Agente secreto	Facilitación de la ingeniería social Acceso al sistema a cierto nivel Dispone de documentación del sistema y de conocimientos	Variada, pero generalmente no puede dedicar muchas horas fuera de las funciones habituales de su trabajo	Acceso existente, conocimientos de programación y arquitectura de sistemas Posible conocimiento de las contraseñas Posibilidad de instalar puertas traseras o troyanos específicamente diseñados Posible apoyo de expertos externos Podría estar bajo las órdenes de una persona externa	Políticas, económicas, ideológicas	Robar información institucional, secretos tecnológicos, información personal Sabotaje

CUADRO II-1. AMENAZAS INTERNAS (cont.)

Amenaza	Recursos (destrezas, conocimientos, acceso, financiación)	Dedicación horaria y otros aspectos relacionados con el tiempo	Tácticas	Motivaciones	Intenciones
Agente interno coaccionado	Acceso al sistema a cierto nivel Dispone de documentación del sistema y de conocimientos	Variada, pero generalmente no puede dedicar muchas horas fuera de las funciones habituales de su trabajo	Acceso existente, conocimientos de programación y arquitectura de sistemas Posible conocimiento de las contraseñas Posibilidad de instalar puertas traseras o troyanos específicamente diseñados Posible apoyo de expertos externos Bajo las órdenes de una persona externa	Personales	Robar información institucional, secretos tecnológicos, información personal Sabotaje
Agente interno involuntario	Acceso al sistema asociado a las funciones normales de trabajo		Proporciona involuntariamente acceso interno a un adversario	No son necesarias	

CUADRO II-1. AMENAZAS INTERNAS (cont.)

Amenaza	Recursos (destrezas, conocimientos, acceso, financiación)	Dedicación horaria y otros aspectos relacionados con el tiempo	Tácticas	Motivaciones	Intenciones
Empleado o usuario del sistema descontento (varios tipos)					
Empleados: usuarios no técnicos de computadoras	Recursos medios/ sólidos Acceso al sistema a cierto nivel Dispone de documentación del sistema y de conocimientos sobre sistemas institucionales y operativos específicos	Variada, pero generalmente no puede dedicar muchas horas (tal vez no sea así en todos los casos)	Acceso existente, conocimientos de programación y arquitectura de sistemas Posible conocimiento de las contraseñas Capacidad para insertar herramientas o códigos sencillos (con la posibilidad de que sean más complejos si tienen conocimientos informáticos específicos)	Económicas de índole personal	Venganza, estragos, caos Robar información institucional Avergonzar al empleador o a otro empleado Degradar la imagen pública o la confianza

CUADRO II-1. AMENAZAS INTERNAS (cont.)

Amenaza	Recursos (destrezas, conocimientos, acceso, financiación)	Dedicación horaria y otros aspectos relacionados con el tiempo	Tácticas	Motivaciones	Intenciones
Empleados: usuarios técnicos de ordenadores, administradores, desarrolladores, etc.	Alto nivel de acceso y autoridad informáticos Posible acceso a distancia	Puede dedicar mucho tiempo		Económicas de índole personal	
Contratados actualmente: terceras partes	Acceso local o remoto posiblemente asociado a la función de asistencia actual	Variada	Infiltración de elementos de la cadena de suministro con componentes que están comprometidos Infiltración a través de soportes móviles o conexión a distancia	Económicas de índole personal	

CUADRO II-1. AMENAZAS INTERNAS (cont.)

Amenaza	Recursos (destrezas, conocimientos, acceso, financiación)	Dedicación horaria y otros aspectos relacionados con el tiempo	Tácticas	Motivaciones	Intenciones
Empleado/usuario descontento (antiguo empleado)	Recursos limitados si no trabaja con un grupo mayor de personas Podría poseer aún la documentación del sistema Podría utilizar el antiguo acceso si ha quedado activado Posibles vínculos con el personal de las instalaciones	Variada, según el grupo de personas conexo	Posible conocimiento de las contraseñas Podría utilizar el antiguo acceso si ha quedado activado Podría haber creado puertas traseras en el sistema mientras era empleado Ingeniería social	Personales	Venganza, estragos, caos Robar información institucional Avergonzar al empleador o a otro empleado Degradar la imagen pública o la confianza

CUADRO II-2. AMENAZAS EXTERNAS

Amenaza	Recursos (destrezas, conocimientos, acceso, financiación)	Dedicación horaria y otros aspectos relacionados con el tiempo	Tácticas	Motivaciones	Intenciones
Ataque no selectivo	Destrezas variadas	Variada	No hay objetivos específicos, generalmente se basan en los procesos normales de la tecnología de la información y en los factores de vulnerabilidad, incluida la ingeniería social	Personales: diversión, estatus	Fama, atención de los medios de comunicación Comprometer el objetivo de oportunidad
Extremistas	Destrezas variadas, pero generalmente limitadas Escaso conocimiento del sistema, limitado a la información pública	Amenaza potencialmente sensible al momento cronológico, dado que las actividades pueden centrarse en sucesos actuales o recientes	Actividades de pirateo informático individuales o en pequeños grupos Distribución de herramientas a un colectivo mayor	Intención relacionada con efectos políticos	Atención de los medios de comunicación Humillación pública

CUADRO II-2. AMENAZAS EXTERNAS (cont.)

Amenaza	Recursos (destrezas, conocimientos, acceso, financiación)	Dedicación horaria y otros aspectos relacionados con el tiempo	Tácticas	Motivaciones	Intenciones
Pirata informático por placer	Destrezas variadas, pero generalmente limitadas Escaso conocimiento del sistema, limitado a la información pública	Puede dedicar mucho tiempo, tiene escasa paciencia	Códigos y herramientas generalmente disponibles Posible desarrollo de algunas herramientas	Personales: diversión, estatus	Comprometer el objetivo de oportunidad Explotar los objetivos más sencillos
Delincuencia organizada	Recursos sólidos Empleo de conocimientos especializados	Variada, pero sobre todo a corto plazo	Códigos, herramientas caseras Podría contratar a un pirata informático Podría contratar a un empleado antiguo o actual Ingeniería social	Chantaje Extorsión (beneficio económico) Jugar con los temores financieros y de percepción de las empresas Información para la venta (técnica, comercial o personal)	Robar material Robar información de carácter estratégico Vender información o acceso

CUADRO II-2. AMENAZAS EXTERNAS (cont.)

Amenaza	Recursos (destrezas, conocimientos, acceso, financiación)	Dedicación horaria y otros aspectos relacionados con el tiempo	Tácticas	Motivaciones	Intenciones
Estado nación	Recursos y conocimientos sólidos Actividades de recopilación de información Posible capacitación/ experiencia operativa en el sistema Equipos de expertos capacitados	Variada, pero capaz de soportar ataques sostenidos	Herramientas sofisticadas Podría contratar a un empleado antiguo o actual Ingeniería social	Política Recogida de información Establecer puntos de acceso para acciones posteriores	Robar tecnología Actividades de reconocimiento para futuros ataques Sabotaje

CUADRO II-2. AMENAZAS EXTERNAS (cont.)

Amenaza	Recursos (destrezas, conocimientos, acceso, financiación)	Dedicación horaria y otros aspectos relacionados con el tiempo	Tácticas	Motivaciones	Intenciones
Terroristas	Destrezas variadas Posible capacitación/ experiencia operativa en el sistema Posible infiltración con agente secreto Capacidad potencial para estar adecuadamente financiados Destrezas crecientes	Puede dedicar mucho tiempo, tiene mucha paciencia	Códigos, herramientas caseras Podría contratar a un pirata informático Podría contratar a un empleado antiguo o actual Ingeniería social	Recogida de información Establecer puntos de acceso para acciones posteriores Caos Venganza Influir en la opinión pública (miedo)	Apoyar los ataques combinados Actividades de reconocimiento para futuros ataques Sabotaje Robar material

Anexo III

ASIGNACIÓN DE RESPONSABILIDADES DE SEGURIDAD INFORMÁTICA

III-1. En el cuadro III-1 se describe una asignación típica de responsabilidades a las autoridades competentes. Podría ser beneficioso elaborar un cuadro de responsabilidades habituales de seguridad informática que se correspondan con estas responsabilidades habituales de seguridad física nuclear.

CUADRO III-1. RESPONSABILIDADES HABITUALES DE SEGURIDAD INFORMÁTICA EN UN RÉGIMEN DE SEGURIDAD FÍSICA NUCLEAR

Tipo de entidad	Responsabilidades en materia de seguridad física nuclear

CUADRO III-1. RESPONSABILIDADES HABITUALES DE SEGURIDAD INFORMÁTICA EN UN RÉGIMEN DE SEGURIDAD FÍSICA NUCLEAR (cont.)

Tipo de entidad	Responsabilidades en materia de seguridad física nuclear
Órgano regulador	Establecer un sistema de control reglamentario de los materiales radiactivos y las instalaciones y actividades conexas que atribuya la responsabilidad primaria en materia de seguridad física nuclear a las personas autorizadas Establecer un sistema de clasificación basada en la seguridad física Desarrollar y mantener un registro nacional de materiales radiactivos Participar en la evaluación nacional de las amenazas Formular y aplicar la amenaza base de diseño, la declaración de amenaza alternativa u otra amenaza definida a efectos de la reglamentación en materia de seguridad física Implantar el proceso de autorización (concesión de licencias), incluida la revisión y actualización de los sistemas de seguridad física y de las medidas de gestión de la seguridad física Establecer los requisitos reglamentarios y proporcionar directrices de seguridad física, incluidos los requisitos en materia de protección de la información Gestionar la interfaz entre la seguridad tecnológica y la seguridad física. Realizar inspecciones de seguridad física Emprender acciones coercitivas en caso de incumplimiento Tener presencia en las bases de datos regionales e internacionales y en otras actividades cooperativas Fomentar y promover una cultura de la seguridad física nuclear robusta Participar en la planificación y preparación y respuesta para sucesos relacionados con la seguridad física nuclear, incluida la participación en los simulacros Administrar los procedimientos de autorización y control de la importación y exportación de materiales radiactivos Notificar a los explotadores de una amenaza específica o del aumento de una amenaza Examinar y evaluar el diseño del sistema de seguridad física (en el proceso de autorización)

CUADRO III-1. RESPONSABILIDADES HABITUALES DE SEGURIDAD INFORMÁTICA EN UN RÉGIMEN DE SEGURIDAD FÍSICA NUCLEAR (cont.)

Tipo de entidad	Responsabilidades en materia de seguridad física nuclear
Fuerzas del orden	Responder para interrumpir actos dolosos (acceso no autorizado, retirada no autorizada, sabotaje) Participar en la planificación y preparación y respuesta para sucesos relacionados con la seguridad física nuclear, incluida la participación en los simulacros Participar en la evaluación nacional de las amenazas Señalar amenazas específicas o en aumento Hacer comprobaciones de antecedentes para verificar la probidad Detectar e investigar los sucesos relacionados con la seguridad física nuclear
Controles aduaneros y fronterizos	Participar en la evaluación nacional de las amenazas Señalar amenazas específicas o en aumento Controlar y detectar el incumplimiento con respecto a las importaciones o exportaciones Establecer comunicación con el órgano regulador con respecto al inventario nacional de materiales radiactivos
Servicios de inteligencia y seguridad	Dirigir la evaluación nacional de las amenazas Señalar amenazas específicas o en aumento
Organismos nacionales de respuesta a emergencias	Coordinar la planificación y preparación y respuesta para sucesos relacionados con la seguridad física nuclear
Organismos de defensa civil, sanidad y medio ambiente	Participar en la planificación y preparación y respuesta para sucesos relacionados con la seguridad física nuclear
Ministerio de justicia y autoridades judiciales	Imponer sanciones a los autores de actos dolosos
Ministerio de relaciones exteriores	Implicarse en la cooperación regional e internacional

Anexo IV

EJEMPLO DE MARCO DE COMPETENCIAS Y DE NIVELES DE CAPACIDAD EN MATERIA DE SEGURIDAD INFORMÁTICA

IV-1. El establecimiento de un marco de competencias y de los niveles de capacidad contribuye de manera fundamental a garantizar que las organizaciones y las personas sean y sigan siendo competentes para desempeñar sus funciones y responsabilidades en materia de seguridad informática.

IV-2. En el presente anexo se ilustra lo que se entiende por marco de competencias y niveles de capacidad. No se pretende ofrecer una orientación suficiente para formular ese marco.

IV-3. En el marco se precisa la competencia necesaria de los ámbitos específicos de la seguridad informática de cada organización o persona. Una lista de ejemplos de esos ámbitos es la siguiente:

a) gestión (capacidad, estrategia, gestión de crisis, gobernanza, organización);
b) respuesta a incidentes (informática forense, defensa de la red);
c) marco legislativo y reglamentario (derecho penal, reglamentación);
d) seguridad y gestión de la información (criptografía, cifrado, almacenamiento);
e) adquisiciones (contratos, cadena de suministro);
f) actividades de garantía (pruebas, certificación, gestión de la configuración);
g) arquitectura de la seguridad informática, y
h) coordinación y asistencia internacionales.

Como alternativa, en las normas internacionales ISO 27002 [IV-1] (para los sistemas de gestión de la seguridad de la información) e IEC 63096 [IV-2] (ISO 27002 aplicada a las centrales nucleares) figuran listas de esferas de control que se pueden adaptar como ámbitos de competencia.

IV-4. En el marco se precisan las destrezas y los conocimientos específicos de seguridad informática necesarios para cada competencia, fundamentados mediante la evaluación de las amenazas de ciberataque, el conocimiento de la naturaleza de los sistemas computerizados disponibles para el régimen de seguridad física nuclear y el conocimiento de los factores de vulnerabilidad de esos sistemas computerizados.

IV-5. Las organizaciones y las personas muestran diferentes niveles de madurez en las competencias de seguridad informática. El marco categoriza el nivel de capacidad de cada competencia mediante una escala de al menos tres niveles diferentes. De esa forma se puede aplicar un enfoque graduado. Un ejemplo de esa clasificación, de menor a mayor madurez, es el siguiente:

a) Fundamental (principiante): Muestra un comportamiento automático, basado en reglas, muy restringido e inflexible.
b) Intermedio: Actúa conscientemente para cumplir los objetivos y planes a largo plazo en el marco de la política establecida.
c) Avanzado (experto): Comprende intuitivamente la situación, es capaz de centrarse inmediatamente en los aspectos fundamentales.

IV-6. Se necesitan niveles más altos de capacidad para garantizar la protección contra amenazas de alta capacidad o para evitar consecuencias radiológicas graves. Por ejemplo, se considera que las autoridades competentes y los explotadores que almacenan, transportan o utilizan materiales nucleares de las categorías I o II, o que explotan instalaciones o realizan actividades que pueden tener consecuencias radiológicas graves, gestionan consecuencias muy graves o graves.

IV-7. El marco garantiza que las organizaciones y las personas responsables del diseño de las medidas de seguridad informática demuestren un alto nivel de las competencias pertinentes.

IV-8. Algunas organizaciones exigen que esas capacidades estén continuamente disponibles en el emplazamiento, mientras que otras dependen de la asistencia de otras organizaciones.

IV-9. En el marco se especifica detalladamente el perfil típico de las actividades que se podría permitir realizar a una autoridad competente, a un explotador o a un tercero. Por ejemplo, una autoridad competente o un explotador con las competencias necesarias de nivel avanzado puede desempeñar un papel de liderazgo en las actividades de evaluación nacional de las amenazas relacionadas con la seguridad informática. Una autoridad competente o un explotador con competencias de nivel fundamental solo puede desempeñar un papel de apoyo en la evaluación nacional de las amenaza. Así se ilustra en el cuadro IV-1.

CUADRO IV-1. CATEGORIZACIÓN DE LAS ACTIVIDADES SEGÚN EL NIVEL DE COMPETENCIA

Tipo de actividad	Partes interesadas fundamentales	Partes interesadas intermedias (se suman a las fundamentales)	Partes interesadas avanzadas (se suman a las intermedias)
Actividades relacionadas con el conocimiento del entorno de la amenaza	Mantener un conocimiento básico de los comportamientos de las amenazas (por ejemplo, los ataques de *phishing*)	Comprender las consecuencias de las amenazas a la seguridad informática en el propio entorno	Supervisar de forma constante y proactiva las amenazas a la seguridad informática en rápida evolución
Actividades relacionadas con la evaluación de las amenazas y la creación de escenarios	Contribuir cuando se les solicite (por ejemplo, facilitar detalles prácticos sobre lo que realmente sucede en el lugar de trabajo)	Participación en la evaluación nacional de las amenazas Creación de escenarios específicos para elaborar la evaluación de las amenazas cuando el impacto potencial sea medio, bajo o muy bajo	Papel principal en las actividades de evaluación nacional de las amenazas Creación de escenarios específicos en los que el impacto potencial sea muy alto o alto Evaluación de los escenarios a partir de los escenarios intermedios

REFERENCIAS DEL ANEXO IV

[IV–1] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Information Technology — Security Techniques — Code of Practice for Information Security Controls, ISO/IEC 27002:2013, ISO, Geneva (2013).

[IV–2] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation, Control and Electrical Power Systems — Security Controls, IEC 63096:2020, IEC, Geneva (2020).

GLOSARIO

ataque combinado. Acto doloso que implica el uso coordinado de un ciberataque y un ataque físico.

ciberataque. Acto doloso con la intención de robar, alterar o destruir un objetivo específico, o impedir el acceso a este, mediante el acceso no autorizado a un sistema computerizado susceptible (o mediante acciones dentro de él).

incidente de seguridad informática. Suceso que pone en peligro real o potencialmente la confidencialidad, integridad o disponibilidad de un sistema computerizado (incluida la información), o que constituye una violación o un riesgo inminente de violación de las políticas de seguridad.

información de carácter estratégico. Información, sea cual sea su forma, comprendidos los programas informáticos, cuya revelación, modificación, alteración o destrucción no autorizadas o la denegación de uso podría comprometer la seguridad física nuclear.

medidas de seguridad informática. Medidas destinadas a prevenir, detectar o retrasar las consecuencias de actos dolosos u otros actos que podrían comprometer la seguridad informática, responder ante ellas y mitigarlas.

nivel de seguridad informática. La robustez de la protección necesaria para cumplir con los requisitos de seguridad informática de una función relacionada con la seguridad física nuclear, la seguridad tecnológica nuclear, la contabilidad y el control de materiales nucleares o la gestión de información de carácter estratégico.

programa de seguridad informática. Plan para la aplicación de la estrategia de seguridad informática en el que se especifican las funciones, las responsabilidades y los procedimientos organizativos. En el programa, que forma parte del plan general de seguridad (o está vinculado a él), se especifican y detallan los medios para alcanzar los objetivos de seguridad informática.

recursos de información de carácter estratégico. Cualquier equipo o componente utilizado para almacenar, procesar, controlar o transmitir información de carácter estratégico. Por ejemplo, los recursos de información de carácter estratégico incluyen los sistemas de control, las redes, los sistemas de información y cualquier otro soporte electrónico o físico.

recursos digitales de carácter estratégico. Recursos de información de carácter estratégico que son sistemas computerizados o forman parte de ellos.

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

seguridad informática. Aspecto particular de la seguridad de la información que se ocupa de la protección de los sistemas computerizados para evitar que se vean comprometidos.

sistemas computerizados. Tecnologías que crean, procesan, computan, comunican o almacenan información digital, proporcionan acceso a ella o realizan, prestan o controlan servicios relacionados con dicha información.

ⓘ Estos sistemas pueden ser físicos o virtuales. Pueden incluir computadoras de sobremesa, computadoras portátiles, tabletas y otras computadoras personales, teléfonos inteligentes, computadoras centrales, servidores, computadoras virtuales, aplicaciones de *software*, bases de datos, soportes extraíbles, dispositivos de instrumentación y control digitales, controladores lógicos programables, impresoras, dispositivos de red y componentes y dispositivos integrados.

zona de seguridad informática. Grupo de sistemas con límites físicos o lógicos comunes —y, si es necesario, ordenados con criterios adicionales— al que se asigna un nivel de seguridad informática común para simplificar la administración, la comunicación y la aplicación de las medidas de seguridad informática.

PEDIDOS DE PUBLICACIONES

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

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

AMÉRICA DEL NORTE

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

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

RESTO DEL MUNDO

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

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

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

Pedidos individuales:
www.eurospanbookstore.com/iaea

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

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

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

La presente publicación brinda orientaciones sobre el desarrollo y la aplicación de la seguridad informática en cuanto componente clave de la seguridad física nuclear. Se refiere a los aspectos de la seguridad informática de la seguridad física nuclear y sus interfaces con la seguridad tecnológica nuclear y con otros elementos del régimen de seguridad física nuclear de un Estado, incluida la seguridad física de los materiales nucleares y las instalaciones nucleares, de los materiales radiactivos y las instalaciones conexas y de los materiales nucleares y otros materiales radiactivos no sometidos a control reglamentario. El alcance de la publicación incluye los sistemas computerizados que podrían afectar negativamente a la seguridad física nuclear o a la seguridad tecnológica nuclear si se vieran comprometidos; las funciones y responsabilidades del Estado y de las entidades pertinentes en relación con la seguridad informática en el régimen de seguridad física nuclear; las actividades que desempeña el Estado en cuanto al establecimiento y la aplicación de una estrategia de seguridad informática al servicio de la seguridad física nuclear; los elementos de los programas de seguridad informática, y las actividades para mantener la seguridad informática como parte del régimen de seguridad física nuclear.

ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA
VIENA