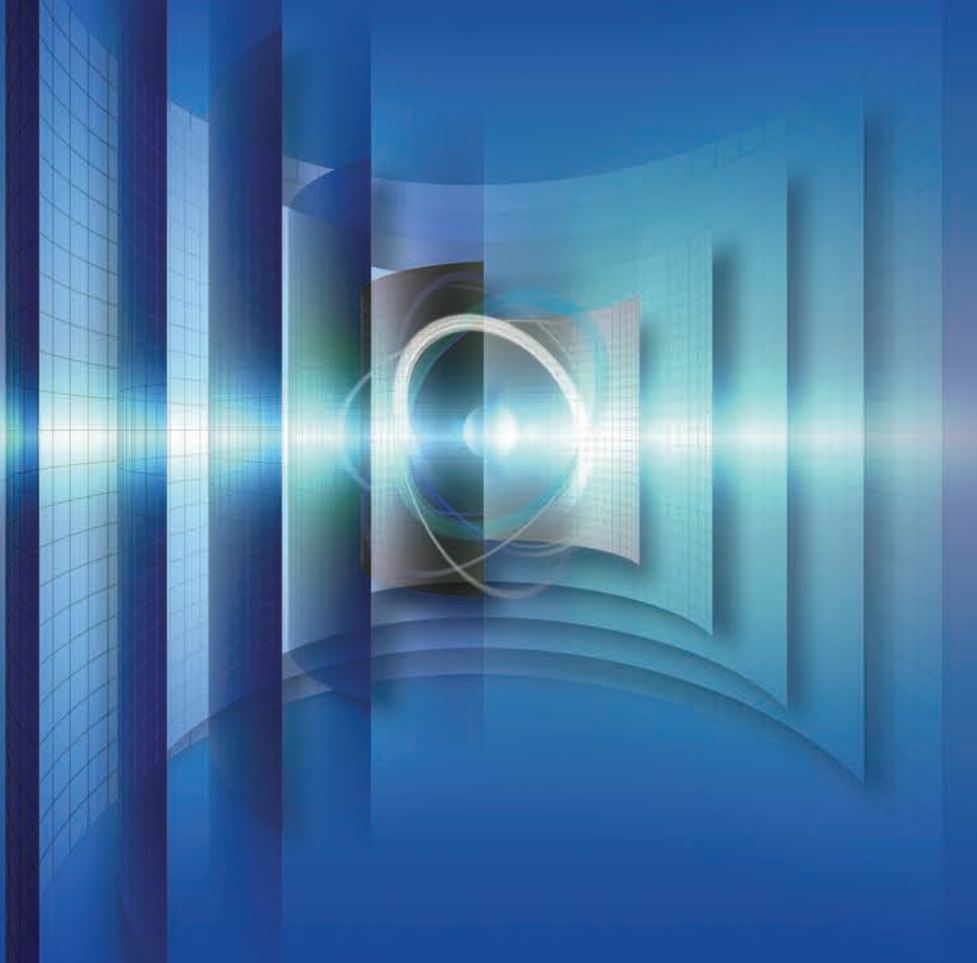
Colección de Seguridad Física Nuclear del OIEA N° 17T (Rev. 1)

Orientaciones técnicas

Técnicas de seguridad informática para instalaciones nucleares



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.

TÉCNICAS DE SEGURIDAD INFORMÁTICA PARA INSTALACIONES NUCLEARES

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
GUINEA
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, REINO DE LOS
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
Nº 17-T (Rev. 1)

TÉCNICAS DE SEGURIDAD INFORMÁTICA PARA INSTALACIONES NUCLEARES

ORIENTACIONES TÉCNICAS

ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA
VIENA, 2024

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
Abril de 2024
STI/PUB/1921

TÉCNICAS DE SEGURIDAD INFORMÁTICA PARA INSTALACIONES NUCLEARES
OIEA, VIENA, 2024
STI/PUB/1921
ISBN 978-92-0-310123-3 (papel) | ISBN 978-92-0-309723-9 (pdf) | ISBN 978-92-0-309823-6 (epub)
ISSN 2521-1803

PREFACIO

Rafael Mariano Grossi
Director General

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

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

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

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

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

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

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

NOTA EDITORIAL

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

Las orientaciones publicadas en la Colección de Seguridad Física Nuclear del OIEA no son vinculantes para los Estados, pero estos pueden ayudarse de ellas para cumplir las obligaciones que les incumben en virtud de instrumentos jurídicos internacionales y para asumir sus responsabilidades en materia de seguridad física nuclear dentro de su territorio. Las orientaciones en las que se usan formas verbales condicionales tienen por fin presentar buenas prácticas internacionales y señalar la existencia de 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 en cuestión 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, que se utilizan para dar ejemplos prácticos o facilitar información o explicaciones adicionales, no son parte integrante del texto principal.

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

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

INFORMACIÓN GENERAL

1.1. La seguridad física nuclear procura prevenir y detectar actos delictivos o intencionales no autorizados que estén relacionados con materiales nucleares y otros materiales radiactivos y con instalaciones y actividades conexas, o que vayan dirigidos contra estos, así como responder a tales actos. La seguridad física de los materiales y las instalaciones nucleares incluye la protección física, la seguridad física relacionada con el personal (por ejemplo, la determinación de la probidad y medidas contra las amenazas internas) y la seguridad física de la información.

1.2. Los grupos o personas que planifiquen o cometan actos dolosos relacionados con material nuclear o una instalación nuclear podrían beneficiarse del acceso a información de carácter estratégico y a recursos de información de carácter estratégico relacionados con el material, la instalación o las medidas de seguridad física existentes.

1.3. Las Nociones Fundamentales de Seguridad Física Nuclear [1] y las tres publicaciones relativas a las recomendaciones de seguridad física nuclear [2 a 4] hacen hincapié en la importancia de proteger la información de carácter estratégico. La *Colección de Seguridad Física Nuclear del OIEA* Nº 23-G, *Seguridad física de la información nuclear* [5], proporciona orientación sobre la adopción de medidas adecuadas para determinar, clasificar y proteger la información de carácter estratégico con el fin de lograr la seguridad física efectiva de la información en el marco del régimen de seguridad física nuclear de un Estado.

1.4. Los ciberataques en instalaciones nucleares pueden contribuir a causar daños físicos en la instalación y/o a desactivar sus sistemas de seguridad física o tecnológica (es decir, sabotaje), a obtener un acceso no autorizado a información nuclear de carácter estratégico, o a lograr la retirada no autorizada de materiales nucleares. Por tanto, la seguridad informática es fundamental en las instalaciones nucleares para proteger tanto la seguridad física como la seguridad tecnológica.

1.5. La protección de los activos digitales de carácter estratégico (SDA)[1] se recomienda en el párrafo 4.10 de la referencia [2], que afirma 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*".

En la referencia [6] se reconoce la necesidad específica de proteger los sistemas informáticos contra las amenazas de agentes internos.

1.6. En la *Colección de Seguridad Física Nuclear del OIEA* Nº 42-G, *Computer Security for Nuclear Security* [7], se presenta orientación general sobre seguridad informática para la seguridad física nuclear, y en la *Colección de Seguridad Física Nuclear del OIEA* Nº 33-T, *Computer Security of Instrumentation and Control Systems at Nuclear Facilities* [8], se presenta orientación más específica sobre la seguridad informática de los sistemas de instrumentación y control en instalaciones nucleares. La presente publicación tiene por objeto complementar esta orientación presentando información detallada sobre técnicas de seguridad informática para otros sistemas de las instalaciones nucleares.

OBJETIVO

1.7. El objetivo de la presente publicación es ayudar a los Estados Miembros a implantar la seguridad informática en las instalaciones nucleares con el fin de prevenir la retirada no autorizada de materiales nucleares, el sabotaje de instalaciones nucleares y el acceso no autorizado a información nuclear de carácter estratégico, así como de proteger contra tales actos. La presente publicación aborda la seguridad informática en relación con las actividades y organizaciones de apoyo como proveedores, contratistas y suministradores. Si bien la presente publicación centra su atención en la seguridad física de las instalaciones nucleares, la aplicación de esta orientación también puede beneficiar a la seguridad tecnológica de las instalaciones y su rendimiento operacional.

1.8. La presente publicación aborda el uso de enfoques basados en el conocimiento de los riesgos para establecer y perfeccionar las políticas, programas y medidas

[1] Los activos digitales de carácter estratégico son recursos de información de carácter estratégico que consisten en sistemas informáticos o que forman parte de estos.

de seguridad informática con el fin de proteger los SDA y otros activos digitales. Las instalaciones nucleares dependen de los SDA y otros activos digitales para garantizar su seguridad tecnológica y física. La presente publicación describe la integración de la seguridad informática en el sistema de gestión de una instalación u organización, e incluye orientación relativa a la definición de políticas y requisitos y a actividades para elaborar, aplicar, sostener, mantener, evaluar y mejorar de forma continua las medidas de seguridad informática que protegen la instalación frente a ciberataques, de conformidad con la evaluación de la amenaza o la amenaza base de diseño (ABD) [9].

1.9. La presente publicación también ofrece orientación técnica relativa a la protección de otros activos digitales en instalaciones nucleares.

1.10. La presente publicación va dirigida a los órganos reguladores y otras autoridades competentes y a los explotadores de instalaciones nucleares y sus proveedores, contratistas y suministradores.

ALCANCE

1.11. La orientación incluida en la presente publicación concierne a la implantación y gestión de la seguridad informática para velar por la seguridad física nuclear en las instalaciones nucleares. La presente publicación es aplicable a todas las etapas del período de vida de una instalación nuclear [10].

1.12. La seguridad informática en las instalaciones nucleares tiene por objeto proteger diversos sistemas que contribuyen a distintos aspectos de la seguridad física nuclear, como la protección física y los sistemas de contabilidad y control de materiales nucleares. La presente publicación no se ocupa del diseño o funcionamiento de dichos sistemas, salvo cuando el diseño o funcionamiento estén relacionados con la protección de estos sistemas a través de medidas de seguridad informática.

1.13. La presente publicación se ocupa de todos los activos digitales relacionados con una instalación nuclear, incluidos los sistemas de instrumentación y control de la instalación (I&C). En la referencia [8] se ofrece orientación adicional sobre consideraciones específicas de seguridad informática para los sistemas de instrumentación y control de la instalación que proporcionan seguridad tecnológica, seguridad física o funciones auxiliares.

ESTRUCTURA

1.14. Después de esta introducción, en la sección 2 se presentan la terminología clave, los conceptos básicos y las relaciones. En la sección 3 se describen las consideraciones generales de seguridad informática en instalaciones nucleares. En las secciones 4 y 5 se presenta orientación sobre la gestión de riesgos de seguridad informática (CSRM) a nivel de la instalación y sistemas, respectivamente. En la sección 6 se presenta orientación sobre consideraciones para la CSRM a nivel de la instalación y sistemas con respecto a las diferentes etapas del período de vida de la instalación. En la sección 7 se presenta la síntesis de un programa de seguridad informática (CSP). En la sección 8 se presenta un ejemplo ilustrativo de la implantación de una arquitectura defensiva de seguridad informática (DCSA) y medidas de seguridad informática conexas.

1.15. El apéndice proporciona orientación específica sobre algunos elementos de un CSP. El anexo I proporciona ejemplos de escenarios de ataque que pueden servir para evaluar la seguridad informática en instalaciones nucleares. El anexo II proporciona un ejemplo de la asignación de niveles de seguridad informática para una central nuclear. El anexo III proporciona un ejemplo de la aplicación de niveles y zonas de seguridad informática.

2. RELACIONES Y CONCEPTOS BÁSICOS

2.1. Esta sección aclara el significado de términos importantes que se utilizan en la presente publicación.

SEGURIDAD FÍSICA NUCLEAR Y SEGURIDAD INFORMÁTICA

2.2. Las Nociones Fundamentales de Seguridad Física Nuclear [1] establecen que los blancos con respecto a la seguridad física nuclear son los siguientes:

> "*Materiales nucleares, otros materiales radiactivos, instalaciones conexas, actividades conexas,* u otros lugares u objetos a los que podría dirigirse una *amenaza para la seguridad física nuclear*, comprendidos los *eventos públicos importantes*, los *lugares estratégicos*, la *información de carácter estratégico* y los *recursos de información de carácter estratégico*".

Además de la información almacenada sobre SDA, la información de carácter estratégico incluye *software* relativo a dichos activos, lo cual incluye *software* del tiempo de ejecución, soporte lógico inalterable integrado, herramientas de desarrollo, herramientas de prueba, *software* de herramientas de mantenimiento y sistemas operativos.

2.3. La referencia [1] afirma que un sistema de seguridad física nuclear es "un conjunto integrado de *medidas de seguridad física nuclear*". Las medidas de seguridad física nuclear se definen del siguiente modo:

> "Medidas encaminadas a impedir que una *amenaza para la seguridad física nuclear* culmine en actos delictivos o actos intencionales no autorizados que estén relacionados con *materiales nucleares*, *otros materiales radiactivos*, *instalaciones conexas* o *actividades conexas*, o que vayan dirigidos contra ellos, o a detectar *sucesos relacionados con la seguridad física nuclear* o responder a ellos" [1].

2.4. La orientación general sobre seguridad informática [7] afirma que el Estado debería formular y mantener una estrategia nacional de seguridad informática como parte de su régimen de seguridad física nuclear. Puesto que las instalaciones nucleares entran dentro del régimen de seguridad física nuclear, la seguridad informática en estas instalaciones ha de incluirse en la estrategia nacional de seguridad informática correspondiente. Las funciones de una instalación que apoyan la seguridad tecnológica y física han de protegerse frente a los adversarios. Cuando estas funciones de una instalación utilizan tecnologías digitales, dependen de estas o están respaldadas por estas, es necesaria la seguridad informática para proteger dichas funciones.

2.5. La seguridad informática está relacionada con los sistemas informáticos, sobre todo con los sistemas que realizan o apoyan funciones de una instalación que son importantes para la seguridad física nuclear y la seguridad tecnológica nuclear, o que están relacionadas con ellas (a saber, activos digitales). La seguridad informática proporciona técnicas y herramientas para hacer frente a los ciberataques y a actuaciones u omisiones humanas que puedan afectar a la seguridad.

Funciones de una instalación, niveles de seguridad informática y zonas de seguridad informática

2.6. Un enfoque estándar para proteger sistemas de forma estructurada con arreglo a un enfoque graduado es utilizar los conceptos de niveles de seguridad

informática y zonas de seguridad informática. El nivel de seguridad informática asignado a una zona de seguridad informática se basa en el grado más alto de protección de seguridad que necesita cualquier función de una instalación desempeñada por un sistema en esa zona. Se asigna el mismo nivel de seguridad informática a todos los sistemas de esa zona. Por lo general, un modelo de zonas de una instalación nuclear consta de muchas zonas distintas, y varias zonas pueden tener asignado el mismo nivel de seguridad informática.

2.7. La función de una instalación es un conjunto coordinado de acciones y procesos que es necesario realizar en una instalación nuclear. Las funciones de una instalación incluyen funciones que son importantes para la seguridad física nuclear, o que están relacionadas con esta, y funciones que son importantes para la seguridad tecnológica nuclear, o que están relacionadas con esta (a saber, funciones de seguridad tecnológica)[2]. Las funciones de una instalación se asignan a sistemas[3], cada uno de los cuales realiza una o más de esas funciones.

2.8. Un nivel de seguridad informática es una designación que indica el grado de protección de seguridad necesario para una función de una instalación y, por consiguiente, para el sistema que realiza dicha función. Cada nivel de seguridad informática está asociado a un conjunto de requisitos impuestos por el explotador para que se proporcione el nivel adecuado de protección a los activos digitales asignados a ese nivel mediante el uso de un enfoque graduado. Cada nivel de seguridad informática necesitará distintos conjuntos de medidas de seguridad informática para satisfacer los requisitos de seguridad informática correspondientes a dicho nivel.

2.9. Una zona de seguridad informática es una agrupación lógica y/o física de activos digitales a los que se asigna el mismo nivel de seguridad informática y que comparten requisitos comunes de seguridad informática debido a propiedades intrínsecas de los sistemas o a sus conexiones con otros sistemas (y, según convenga, criterios adicionales). El uso de zonas de seguridad informática pretende simplificar la administración, comunicación y aplicación de las medidas de seguridad informática[4].

---

[2] Las funciones de una instalación también incluyen funciones operacionales y administrativas (u organizativas).

[3] Los sistemas pueden estar dentro o fuera del emplazamiento o en la nube.

[4] El concepto de zonas de seguridad informática puede aplicarse a instalaciones existentes y antiguas, así como a nuevos diseños.

2.10. Otros criterios para definir las zonas de seguridad informática pueden ser los siguientes:

a) las responsabilidades organizativas, por ejemplo, diferentes zonas de seguridad informática para sistemas que son responsabilidad de diferentes departamentos;
b) la necesidad de mantener la separación, por ejemplo, diferentes zonas de seguridad informática para sistemas redundantes en el mismo nivel de seguridad informática que realizan la misma función en una instalación;
c) zonas ya definidas para otros fines, por ejemplo, una zona de seguridad informática se define, en aras de la simplicidad, igual que una zona ya establecida para fines administrativos o de comunicación.

2.11. En la figura 1 se ilustran las relaciones idealizadas entre los conceptos relativos a las funciones de una instalación, los niveles de seguridad informática, los sistemas y las zonas de seguridad informática.

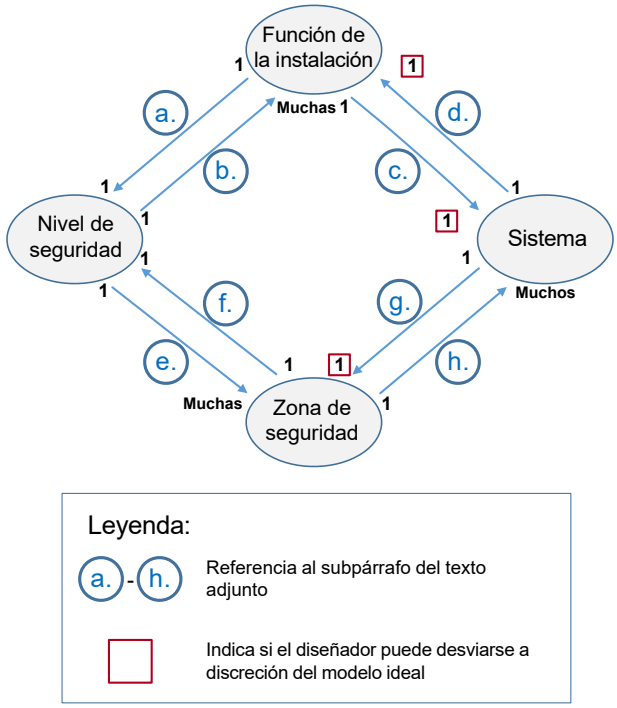


Figura 1. Relaciones idealizadas entre función de una instalación, nivel de seguridad informática, sistema y zona de seguridad informática.

2.12. En la figura 1 se etiquetan las distintas relaciones idealizadas, que se describen a continuación:

a) Cada función de la instalación se asigna a un único nivel de seguridad informática.
b) Cada nivel de seguridad informática puede aplicarse a una o varias funciones de la instalación.
c) Idealmente, cada función de la instalación se asigna a un sistema, siempre que sea posible[5].
d) Idealmente, cada sistema realiza una función de la instalación, siempre que sea posible[6].
e) Cada nivel de seguridad informática puede aplicarse a una o varias zonas de seguridad.
f) A cada zona de seguridad informática se le asigna un único nivel de seguridad informática.
g) Cada sistema se sitúa dentro de una única zona de seguridad informática, siempre que sea posible[7].
h) Cada zona de seguridad informática puede constar de uno o varios sistemas.

Gestión de riesgos de seguridad informática

2.13. La CSRM de la instalación (véase la sección 4) aborda las funciones de la instalación y determina la asignación de estas funciones a niveles de seguridad informática y a uno o más sistemas. Los sistemas heredan los niveles de seguridad informática de las funciones que tienen asignadas.

2.14. La CSRM a nivel de sistemas (véase la sección 5) forma parte de la CSRM de la instalación y se ocupa de los sistemas y determina a) los límites de las

---

[5] Por ejemplo, una función puede asignarse a dos sistemas de parada independientes distintos.

[6] Por ejemplo, una interfaz persona-máquina. Idealmente, desde el punto de vista de la seguridad física, un único sistema realizaría una única función de la instalación, pero los diseñadores pueden asignar más de una función de la instalación a un sistema si lo consideran necesario para apoyar el rendimiento humano, operacional o de seguridad tecnológica.

[7] Idealmente, desde el punto de vista de la seguridad física, cada función de la instalación sería realizada por un único sistema que está dentro de una única zona de seguridad informática y, por tanto, tiene asignado un único nivel de seguridad, pero los diseñadores pueden desviarse de ese ideal debido a otras consideraciones, por ejemplo, sistemas de protección contra incendios o de protección física que abarcan toda la instalación (o una parte considerable de esta) y, por tanto, pueden atravesar áreas físicas que contienen zonas asignadas a distintos niveles de seguridad.

zonas de seguridad informática con arreglo a las funciones de la instalación que se realizan y la conectividad de los sistemas, y b) las medidas de seguridad informática que han de aplicarse para cumplir los requisitos del nivel de seguridad informática de la zona.

2.15. Los productos de los procesos de gestión de riesgos suelen basarse en el desarrollo de escenarios, el análisis y, en algunos casos, el rendimiento para aumentar la confianza en las evaluaciones cualitativas. Hay dos clases de escenarios: funcionales y técnicos. Por lo general, los escenarios funcionales se utilizan en el proceso de CSRM de la instalación, mientras que los escenarios técnicos se utilizan en el proceso de CSRM a nivel de sistemas.

Exigencias contrapuestas de simplicidad, eficiencia y seguridad informática

2.16. Es necesario equilibrar las exigencias contrapuestas de simplicidad, eficiencia y seguridad informática a la hora de considerar lo siguiente:

a) la determinación y enumeración de las funciones de una instalación;
b) la asignación de las funciones de una instalación a sistemas;
c) el desarrollo de sistemas;
d) la especificación de requisitos de seguridad informática para distintos niveles de seguridad informática sobre la base de un enfoque graduado;
e) el establecimiento de límites lógicos y/o físicos para las zonas de seguridad informática.

2.17. Las consideraciones relativas a la simplicidad podrían fomentar la preferencia por asignar una única función a un único sistema. Esto podría dar lugar a una DCSA que permita establecer medidas de seguridad informática eficientes dentro de cada zona para cada función de la instalación (presuponiendo una relación unívoca entre sistemas y funciones). Sin embargo, los sistemas necesitarían interconexiones para poder integrar funciones separadas de la instalación y, por tanto, el sistema de niveles de seguridad informática y zonas de seguridad informática podría volverse más complejo debido al mayor número de zonas de seguridad informática y de interconexiones entre estas zonas.

2.18. Sin embargo, las consideraciones relativas a la eficiencia en la realización de las funciones de una instalación por parte de los sistemas podrían fomentar la preferencia por asignar múltiples funciones a un único sistema integrado. Aunque esto podría dar lugar a un menor número de zonas de seguridad informática, la complejidad del sistema podría aumentar, dificultando la aplicación de medidas de seguridad informática eficaces en todas estas zonas. Además, asignar a la zona

de seguridad informática un nivel de seguridad informática apropiado para la función más importante del sistema podría reducir aún más la eficiencia, ya que podría aplicarse un nivel de protección superior al necesario a funciones menos importantes que se hayan integrado en el sistema.

2.19. El equilibrio entre eficiencia y simplicidad también puede incluir equilibrar la realización de funciones de la instalación a través de sistemas, con la asignación de sistemas a zonas de seguridad informática y niveles de seguridad informática. Por lo tanto, la CSRM normalmente implicará una serie de iteraciones para definir las zonas de seguridad informática y las medidas de seguridad informática conexas con el fin de encontrar el equilibrio óptimo entre simplicidad y eficiencia. Las iteraciones tendrán que demostrar que las modificaciones propuestas de las definiciones de las zonas de seguridad informática no comprometerán las funciones de la instalación de tal modo que den lugar a consecuencias más graves.

Modelo conceptual de zonas de una instalación nuclear

2.20. En la figura 2 se muestra un ejemplo de modelo conceptual de zonas de una instalación nuclear, que incluye las siguientes características:

a) La instalación que sirve de ejemplo está asociada a graves consecuencias en caso de retirada no autorizada de material o sabotaje.
b) El número de niveles de seguridad informática se limita a cinco, siendo el nivel 1 el que presenta las exigencias de protección más estrictas y el nivel 5 el que presenta las menos estrictas.
c) Cada sistema se sitúa dentro de una zona de seguridad informática.
d) A cada zona (incluidos sus sistemas) se le asigna un nivel de seguridad informática.
e) Una o varias zonas pueden tener asignado el mismo nivel de seguridad informática.

2.21. La figura 2 ilustra una aplicación conceptual de sistemas, niveles de seguridad informática y zonas de seguridad informática. El nivel de seguridad informática asignado tiene el siguiente efecto en los requisitos para las funciones de la instalación, sistemas y zonas de seguridad informática:

a) Los niveles de seguridad informática más altos (más estrictos) suelen exigirse para menos funciones (y, por tanto, se aplican a menos sistemas) que los niveles de seguridad más bajos. En la figura 2, el nivel de seguridad 1 se aplicaría a un conjunto mínimo de funciones esenciales, cada una de las cuales estaría asignada idealmente a un único sistema, mientras que el nivel

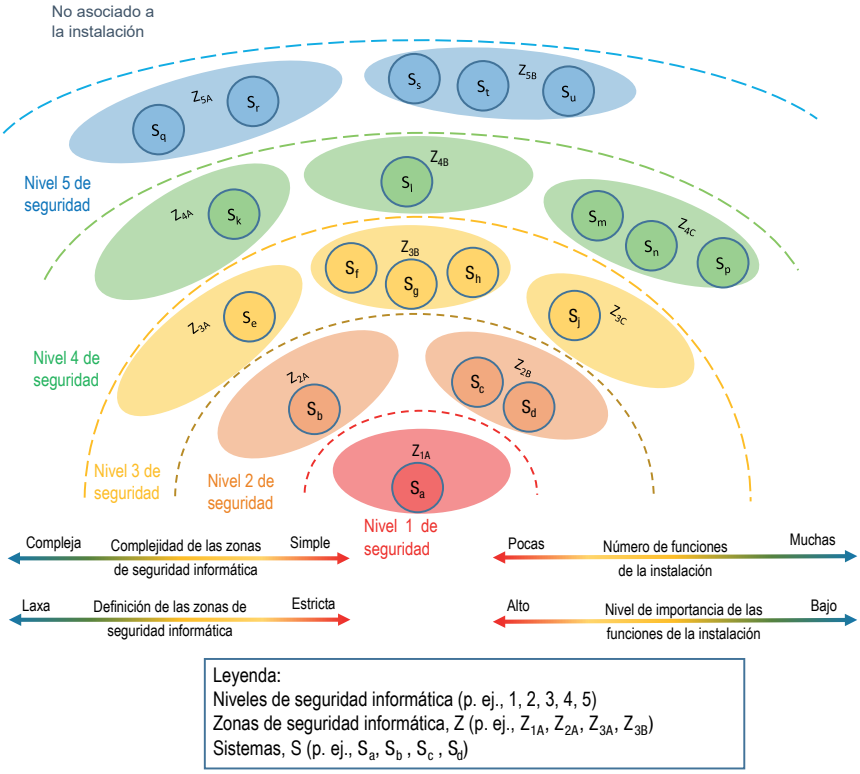


Figura 2. Modelo conceptual de niveles y zonas de seguridad informática.

de seguridad 5 permitiría que un único sistema tuviera muchas funciones asignadas.

b) Los niveles de seguridad informática más altos (más estrictos) suelen ser más sencillos (es decir, menos complejos) que los más bajos. En la figura 2, la zona Z_{1A} contiene un único sistema determinista cuyas interacciones lógicas y físicas con otras zonas (y sistemas) se minimizan en la medida de lo posible, mientras que la zona Z_{5B} tiene muy pocas restricciones con respecto a las interacciones con otras zonas (y sistemas).

c) La complejidad de las zonas suele estar correlacionada con su tamaño físico y lógico. Por ejemplo, en la zona Z_{1A}, es probable que las ubicaciones físicas de los SDA se limiten a una zona vital, mientras que en la zona Z_{3C}, cualquier activo digital podría estar en cualquier lugar de la zona protegida. El aumento del área física de zona vital (Z_{1A}) a zona protegida (Z_{3C}) incrementa potencialmente tanto el número de puntos de acceso como el número

de personal autorizado que requiere acceso físico y que, por tanto, puede interactuar con los activos digitales.

d) El tamaño lógico de una zona puede expresarse como el número de activos digitales direccionables instalados dentro de un sistema. Por ejemplo, el alcance lógico de la zona Z_{3A} podría tener un menor número de direcciones asignables para una capacidad limitada de activos digitales, mientras que la zona Z_{5A} podría tener un alcance más amplio con más direcciones lógicas disponibles para activos digitales actuales y futuros.

e) En estos ejemplos, el número de posibles activos digitales direccionables aumenta de forma similar al ejemplo del tamaño de la zona física del párrafo 2.21 c). No obstante, la instalación de activos digitales adicionales afecta de forma considerable al tamaño de la zona lógica, pero no al tamaño de la zona física[8]. Esto significa que el número de interacciones lógicas potenciales aumenta solamente cuando se instalan activos digitales adicionales dentro de una zona, lo cual aumenta el número y la complejidad de estas interacciones dentro de la zona y su límite.

2.22. El rigor con el que se definen las zonas de seguridad informática puede depender de los niveles de seguridad asignados a dichas zonas. Por ejemplo, para la zona Z_{1A}, tanto los límites físicos como los lógicos se definen de manera estricta, mientras que la zona Z_{5A} podría necesitar solamente una definición estricta del límite lógico, y el límite físico podría definirse de forma más laxa (por ejemplo, dentro de un centro de datos, servicio en la nube u oficina corporativa).

2.23. Los límites de los sistemas (lógicos y físicos) pueden ser útiles a la hora de definir los límites de las zonas de seguridad informática. En la práctica, una zona puede comprender uno o más sistemas, cada uno de los cuales comprende uno o más activos digitales, o se apoya en ellos, para realizar o apoyar la función asignada de la instalación[9].

2.24. Los límites de las zonas de seguridad informática suelen tener mecanismos de control del acceso físico (por ejemplo, armarios cerrados con llave, barreras, bloqueadores de puertos) y mecanismos de desacoplamiento para el flujo de datos

---

[8] Por lo general, el tamaño físico de una zona vital será varias veces mayor que el de los activos digitales ubicados dentro de sus límites y, por tanto, no supone una limitación para el número de activos digitales que podrían estar ubicados en ella.

[9] Tal vez sea necesario asignar algunos sistemas analógicos que realizan funciones de la instalación (véase el párrafo 3.2) a un nivel de seguridad informática y colocarlos en una zona de seguridad informática. Se supone que los sistemas analógicos se apoyan en activos digitales, por ejemplo, una herramienta digital para calibrar un sistema analógico.

(por ejemplo, filtros de paquetes, cortafuegos, diodos de datos) con el fin de prevenir ciberataques u otras formas de acceso no autorizado y de evitar que los errores se propaguen de una zona a otra (especialmente de una zona con requisitos de protección menos estrictos a otra con requisitos más estrictos).

2.25. El modelo de zonas establece un enfoque graduado y una defensa en profundidad. Un ciberataque que se origine fuera de la instalación tendría que superar o eludir varias capas de medidas de seguridad informática antes de poder comprometer un sistema con nivel de seguridad informática 1, 2 o 3. Las medidas para los niveles de seguridad informática 4 y 5 también pueden contribuir a proteger los niveles de mayor protección[10]. Por ejemplo, proporcionar una capacidad de detección temprana dentro de las zonas asignadas a los niveles de seguridad 4 o 5 ofrecería la posibilidad de contener y mitigar el ciberataque antes de que este pueda afectar a los SDA de nivel 1, 2 o 3.

MEDIDAS DE SEGURIDAD INFORMÁTICA

2.26. En un enfoque graduado, la solidez de las medidas de seguridad informática establecidas para proteger una función de la instalación es directamente proporcional a las consecuencias que puedan producirse en el peor de los casos si la función de la instalación se ve comprometida.

2.27. Las medidas de seguridad informática se utilizan para los siguientes fines:

a) prevenir, detectar y retrasar actos delictivos u otros actos intencionales no autorizados, y responder a ellos;
b) mitigar las consecuencias de tales actos, y
c) recuperarse de las consecuencias de tales actos.

2.28. Las medidas de seguridad informática también pueden utilizarse para los siguientes fines:

a) reducir la susceptibilidad de los activos digitales a actos dolosos;
b) impedir que actos no dolosos degraden la seguridad física nuclear.

---

[10] Algunas zonas de la figura 2 pueden estar aisladas, sin una conexión de red permanente. No obstante, las zonas de este tipo con activos digitales siempre tendrán alguna forma de dependencia de información intermitente — por ejemplo, actualizaciones mediante CD-ROM o USB — lo cual constituye una oportunidad para el adversario.

2.29. Las medidas de seguridad informática pueden asignarse a una de estas tres categorías: medidas de control técnico, medidas de control físico o medidas de control administrativo (véase la referencia [7]).

2.30. Las medidas de seguridad informática también pueden contribuir a otras medidas destinadas a la protección física, la seguridad física relacionada con el personal y la seguridad física de la información, o apoyarse en ellas. La sección 8 ofrece un ejemplo de la aplicación de medidas de seguridad informática en el marco de una DCSA que consta de cinco niveles.

SISTEMAS INFORMÁTICOS Y ACTIVOS DIGITALES (INCLUIDOS LOS SDA)

2.31. Los sistemas informáticos utilizan tecnologías digitales, dependen de dichas tecnologías o se apoyan en ellas. Estos sistemas desempeñan un papel cada vez más amplio en la realización de funciones importantes en instalaciones nucleares y operaciones conexas. Cada vez más, los sistemas informáticos se integran en nuevos diseños y pueden introducirse en instalaciones existentes durante su modernización o para aumentar la productividad o fiabilidad.

2.32. Los sistemas informáticos son tecnologías que crean, computan, comunican o almacenan información digital, o proporcionan acceso a ella, o que realizan, prestan o controlan servicios relacionados con dicha información. Estos sistemas, que pueden ser físicos o virtuales, incluyen computadoras de mesa, computadoras portátiles, tabletas, otras computadoras personales, teléfonos inteligentes, unidades centrales, servidores, 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. Algunos sistemas informáticos son programables, lo que permite modificar los pasos de procesamiento sin cambiar el *hardware*. Los sistemas informáticos son susceptibles a los ciberataques.

2.33. En el contexto de la presente publicación, el término “activo digital” se refiere a un sistema informático asociado a una instalación nuclear. Todo activo digital que desempeñe un papel importante en la seguridad tecnológica o física de una instalación nuclear se considerará un SDA[11].

[11] Algunos Estados Miembros utilizan denominaciones similares a la de SDA, como “activos digitales fundamentales” o “ciberactivos esenciales”. Estos términos podrían no ser directamente equivalentes a los SDA.

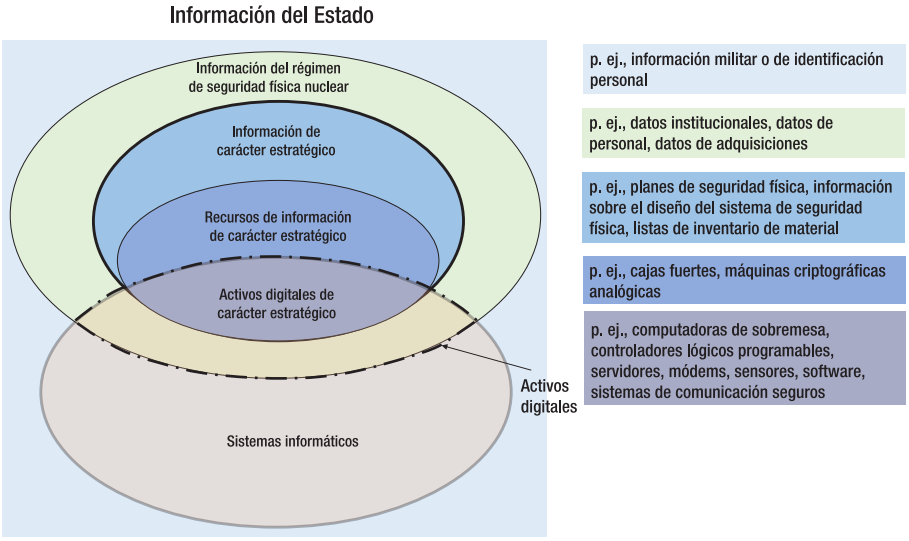


Figura 3. Sistemas de información e informáticos de un Estado y en el régimen de seguridad física nuclear.

2.34. La seguridad informática se ocupa de la protección de los sistemas informáticos para evitar que se vean comprometidos[12]. La seguridad informática es un subconjunto de la seguridad física de la información (tal y como se define, por ejemplo, en la norma ISO/IEC 27000 [11]) y comparte muchos de sus objetivos, metodologías y terminología.

2.35. En la figura 3 se muestra la relación entre seguridad física de la información, información de carácter estratégico, recursos de información de carácter estratégico, activos digitales y SDA.

CIBERATAQUE

2.36. Un ciberataque es un acto doloso realizado con la intención de robar, alterar o destruir un blanco específico, o de privar de acceso a él, accediendo sin autorización a un sistema vulnerable (o actuando en su interior) [8]. Un ciberataque puede ser llevado a cabo por personas u organizaciones y puede tener como

[12] Términos como “seguridad de la tecnología de la información” y “ciberseguridad” se consideran sinónimos de “seguridad informática” y no se utilizan en la presente publicación.

objetivo información de carácter estratégico o recursos de información de carácter estratégico. Los ciberataques presentan las siguientes características especiales:

a) Se pueden ocultar.
b) Su ejecución puede retrasarse, basarse en condiciones determinadas o iniciarse a distancia.
c) El personal (por ejemplo, ingenieros, guardias, personal de operaciones y mantenimiento, contratistas) puede ser engañado para que apoye el ataque sin darse cuenta.

2.37. Toda situación que comprometa los activos digitales podría ofrecer vías de acceso para los ciberataques dirigidos contra los SDA, facilitarlos o contribuir a ellos, lo cual repercutiría negativamente en la seguridad física nuclear y la seguridad tecnológica nuclear. Por lo tanto, es necesario proporcionar una protección adecuada — basada en un enfoque graduado y la defensa en profundidad — a todos los activos digitales asociados con la instalación de modo que no puedan utilizarse para comprometer los SDA. Toda situación que comprometa un SDA degrada la seguridad física nuclear y podría dar lugar a un suceso relacionado con la seguridad física nuclear[13] cuyas consecuencias serían las siguientes (del mejor al peor de los casos):

a) sin consecuencias;
b) consecuencias insignificantes;
c) consecuencias limitadas (incluidas consecuencias para la seguridad tecnológica, como un incidente operacional previsto, y efectos operacionales, como el rendimiento de la central);
d) consecuencias moderadas (por ejemplo, degradación de la capacidad para prevenir y detectar sucesos relacionados con la seguridad física nuclear, y para responder a ellos);
e) consecuencias importantes (por ejemplo, divulgación no autorizada o pérdida de información de carácter estratégico), o
f) consecuencias graves (por ejemplo, consecuencias radiológicas inaceptables debidas a un sabotaje o retirada no autorizada de material nuclear u otros materiales radiactivos).

2.38. Las capacidades de los posibles adversarios podrían incluir el uso eficaz de ciberataques. Por consiguiente, los SDA son blancos tanto por su efecto sobre las funciones de la instalación como por ser un medio que pueden utilizar

[13] Los sucesos relacionados con la seguridad física nuclear pueden tener consecuencias que afecten a la seguridad física nuclear, a la seguridad tecnológica nuclear o a ambas.

los adversarios para facilitar y lograr sus objetivos, y podrían ser objeto de ataques específicos.

INTERRELACIÓN CON LA SEGURIDAD TECNOLÓGICA

2.39. Una función de seguridad tecnológica es "un cometido específico que hay que llevar a cabo con fines de *seguridad tecnológica"* [12]. Las funciones de seguridad tecnológica son necesarias "en una *instalación* o *actividad* para prevenir o mitigar toda consecuencia radiológica en situación de *funcionamiento normal*, en caso de *incidente operacional previsto* y en *condiciones de accidente*" [12].

2.40. Por ejemplo, las funciones fundamentales de seguridad tecnológica que son necesarias para todos los estados de una central (requisito 4 de la Colección de Normas de Seguridad del OIEA Nº SSR-2/1 (Rev. 1), *Seguridad de las centrales nucleares: Diseño* [13]) son las siguientes:

a) el control de la reactividad;
b) la eliminación del calor del reactor y del almacén de combustible;
c) el confinamiento del material radiactivo, el blindaje contra la radiación y el control de las emisiones radiactivas previstas, así como la limitación de las emisiones radiactivas accidentales.

2.41. El párrafo 3.46 de la referencia [2] señala que las funciones de protección física son la detección, la dilación y la respuesta. Dichas funciones utilizan la defensa en profundidad y aplican un enfoque graduado para proporcionar una protección eficaz adecuada.

2.42. Las funciones de protección física y las funciones de seguridad tecnológica no están necesariamente relacionadas entre sí de manera intrínseca, lo que dificulta el tratamiento coherente de ambos tipos de funciones en las metodologías de evaluación de riesgos. Por lo tanto, describir y designar las funciones de una instalación que sean importantes para la seguridad física, o que estén relacionadas con ella, de manera similar a las funciones de una instalación que sean importantes para la seguridad tecnológica, o que estén relacionadas con ella (es decir, funciones de seguridad tecnológica), simplificará la determinación de la importancia de las funciones de una instalación y permitirá tratar por igual las funciones de seguridad tecnológica y las funciones de seguridad física de

importancia equivalente. A continuación figuran algunos ejemplos de funciones de una instalación que son importantes para la seguridad física:

a) la detección de intromisiones (incluida la evaluación) en un punto crítico de detección;
b) el control del acceso de personas y equipos al material de categoría I o a zonas vitales, y
c) las comunicaciones para coordinar las fuerzas de respuesta durante un suceso relacionado con la seguridad física nuclear.

3. CONSIDERACIONES GENERALES RELATIVAS A LA SEGURIDAD INFORMÁTICA

DETERMINACIÓN DE LAS FUNCIONES DE LA INSTALACIÓN

3.1. La referencia [7] afirma lo siguiente:

> "El primer paso de un proceso sistemático [para aplicar medidas de seguridad informática en el marco de la seguridad física nuclear] 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 informáticos y los activos informáticos digitales que los integran [es decir, activos digitales] en apoyo de esas funciones."

En el caso de una instalación nuclear, estos activos digitales son los sistemas informáticos que es necesario proteger para que no se vean comprometidos, como se recomienda en el párrafo 4.10 de la referencia [2], y corresponden a los SDA de que se ocupa la presente publicación.

3.2. El explotador debería determinar y enumerar las funciones de toda la instalación de forma sistemática para que el conjunto de funciones de la instalación que se haya determinado pueda evaluarse de forma integral. El explotador debería proporcionar la lista de funciones de la instalación que se hayan determinado a la

autoridad competente[14] con arreglo a la reglamentación nacional. Deberían tenerse en cuenta los requisitos de seguridad informática[15] relativos a estas funciones de la instalación, sea cual sea el medio para realizarlas (por ejemplo, la tecnología específica empleada, ya sea analógica o digital).

3.3. La realización de las funciones de la instalación se basará o se apoyará en la información de carácter estratégico y los recursos de información de carácter estratégico pertinentes y en otros activos digitales conexos.

PROTECCIÓN DE LA INFORMACIÓN DE CARÁCTER ESTRATÉGICO Y LOS ACTIVOS DIGITALES

3.4. El explotador debería aplicar medidas de seguridad informática para garantizar la protección adecuada (incluida la trazabilidad) de la información de carácter estratégico, los recursos de información de carácter estratégico y los SDA. La seguridad informática se garantiza a través de medidas que aseguran la confidencialidad, la integridad y la disponibilidad, además de cumplir cualquier otro requisito especificado por la autoridad competente.

3.5. El explotador debería determinar cuál es la información de carácter estratégico, teniendo en cuenta las consecuencias de que se vea comprometida y los requisitos del Estado con respecto a la seguridad física de dicha información. La referencia [5] proporciona orientación detallada sobre la formulación de los requisitos de un Estado en materia de información de carácter estratégico.

3.6. La información de carácter estratégico puede determinarse directamente teniendo en cuenta las posibles consecuencias asociadas a su divulgación no autorizada (como se indica en la referencia [5]), por ejemplo, la información sobre arreglos de seguridad física, que un adversario podría utilizar para planificar un acto doloso. Para este tipo de información, la confidencialidad suele ser el atributo que requiere un mayor grado de protección. La información de carácter estratégico también puede determinarse de forma menos directa teniendo en cuenta su

[14] En la presente publicación, por "autoridad competente" se entiende la autoridad a la que el Estado asigna la responsabilidad de la seguridad informática en el contexto de la seguridad física nuclear. Puede tratarse de la autoridad competente en materia de seguridad física nuclear o de la autoridad competente en materia de seguridad informática.

[15] En la presente publicación, los requisitos de seguridad informática incluyen requisitos específicos por escrito impuestos por la autoridad competente pertinente o por el explotador para satisfacer los requisitos de seguridad informática definidos por la autoridad competente o los requisitos reglamentarios.

importancia funcional (es decir, su importancia para la facilitación o realización de una función de la instalación), por ejemplo, datos exactos y oportunos sobre la presión de la caldera, los cuales es más probable que sean explotados por un adversario mediante su modificación o destrucción. Para este tipo de información, la integridad y disponibilidad de la información pueden ser, como mínimo, tan importantes como la confidencialidad.

3.7. La información del plan de seguridad física del emplazamiento puede clasificarse como información de carácter estratégico y pueden aplicarse medidas para proteger su confidencialidad durante un período prolongado de tiempo, ya que la información seguirá siendo de carácter estratégico durante todo el período de validez del plan.

3.8. Con respecto a un sistema de instrumentación y control y sus datos de procesos, un explotador podría dar prioridad a las medidas que garanticen la disponibilidad e integridad del sistema frente a las que garanticen la confidencialidad. En ese caso, los datos de procesos son importantes para la correcta realización y disponibilidad de la función y solo tienen carácter estratégico durante los intervalos muy limitados en los que el sistema de instrumentación y control realiza una acción de control basada en los datos. Sin embargo, una vez que los datos de procesos dejan de ser importantes para la realización y disponibilidad de la función (es decir, ya no pueden constituir la base de una acción de control), los datos históricos de procesos tienen valor solamente en función de su carácter estratégico. Por lo tanto, el beneficio para la seguridad física derivado de una mayor garantía de la confidencialidad (para proteger el carácter estratégico de la información) ha de sopesarse frente al derivado de proteger la integridad y disponibilidad.

3.9. Si bien es posible que la protección de la confidencialidad de los datos de procesos de estos sistemas no requiera medidas estrictas, la pérdida de confidencialidad de otros datos relacionados con los sistemas, como las contraseñas de administración, el código fuente y otros datos clave, proporcionaría al adversario una ventaja considerable en la planificación y ejecución de ciberataques dirigidos contra el sistema y podría hacer necesario el fortalecimiento de las medidas. Además, podría ser necesario clasificar los datos históricos de procesos (por ejemplo, registros) para limitar su distribución (por ejemplo, aplicación de un control administrativo) con el fin de reducir el riesgo de divulgación no autorizada a un nivel aceptable.

ENFOQUE BASADO EN EL CONOCIMIENTO DE LOS RIESGOS

3.10. La seguridad informática debería aplicarse siguiendo un enfoque basado en el conocimiento de los riesgos. La figura 4 de la referencia [7] ofrece una visión general de un enfoque de este tipo para las medidas de seguridad informática.

3.11. El riesgo, en el contexto de la seguridad informática, corresponde al riesgo asociado a que un adversario explote las vulnerabilidades de un activo digital o grupo de activos digitales para cometer o facilitar un acto doloso. Este riesgo se expresa como una combinación de la probabilidad de que el ataque tenga éxito y la gravedad de sus consecuencias si se produce.

EVALUACIÓN Y GESTIÓN DE RIESGOS

3.12. El explotador debería establecer y aplicar un proceso de CSRM (a menos que el proceso de gestión corra a cargo de la autoridad competente). La autoridad competente puede especificar los requisitos normativos que han de seguirse y puede exigir que se utilice una metodología específica de evaluación de riesgos, o puede convenir en que se utilice la metodología de un explotador [7]. El proceso de evaluación para una instalación puede seguir el ejemplo de la evaluación de riesgos para la seguridad informática a nivel organizativo que se describe en los párrafos 7.10 a 7.16 de la referencia [7].

3.13. El proceso de CSRM debería incluir un proceso cíclico de mejora continua[16] en la gestión de los riesgos asociados a ciberataques dirigidos contra la instalación.

3.14. Las evaluaciones de riesgos periódicas e iterativas sirven para apoyar la toma de decisiones en el marco de un proceso de gestión de riesgos. Las evaluaciones de riesgos para la seguridad informática suelen ser cualitativas, con la inclusión de parámetros relativos (por ejemplo, alto, medio, bajo), pero podrían ser cuantitativas si se dispusiera de datos que fueran lo suficientemente fiables[17]. Los resultados de las evaluaciones de riesgos ayudarán a determinar los requisitos de seguridad informática adecuados.

---

[16] Un ejemplo de proceso cíclico de mejora continua es el ciclo de planificación, realización, comprobación y actuación.

[17] En el momento de publicación, no existen metodologías aceptadas internacionalmente que apliquen valores cuantitativos a las evaluaciones de riesgos para la seguridad física.

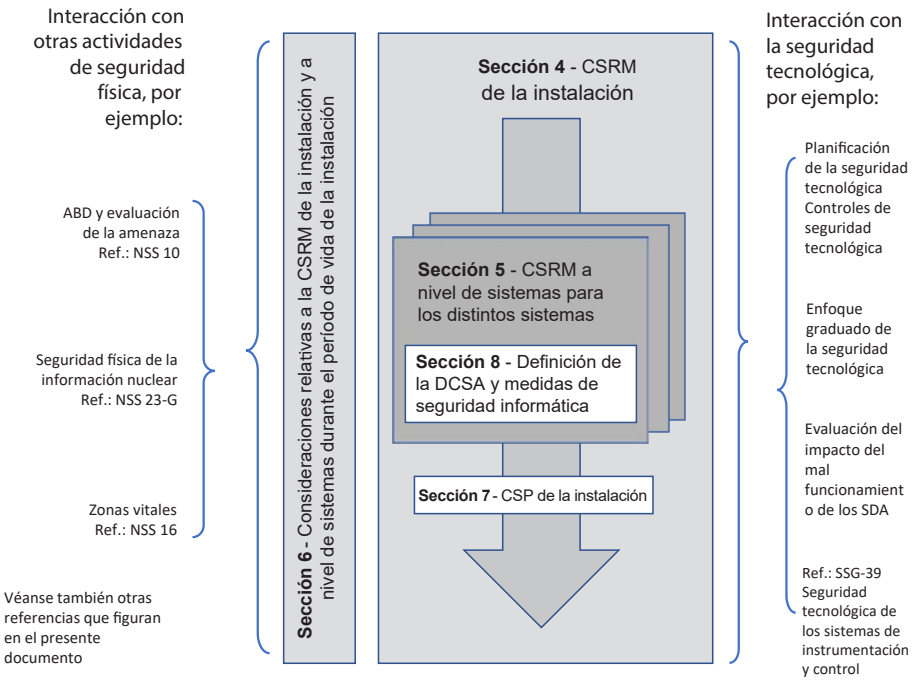


Figura 4. Estructura general de las orientaciones sobre la gestión de riesgos de seguridad informática (CSRM) en la presente publicación. CSP: programa de seguridad informática; ABD: amenaza base de diseño; DCSA: arquitectura defensiva de seguridad informática; NSS: Colección de Seguridad Física Nuclear; SDA: activo digital de carácter estratégico; SSG: Guía de Seguridad Específica.

3.15. El explotador debería realizar la CSRM de la instalación para cumplir los requisitos reglamentarios. La referencia [7] indica que esto puede incluir dos evaluaciones complementarias, una a nivel de organización y otra a nivel de sistemas, y dicho enfoque debería adoptarse para instalaciones complejas con un nivel de peligro elevado, como las instalaciones nucleares. Por tanto, en las orientaciones de la presente publicación se presupone que la CSRM de una instalación nuclear (CSRM de la instalación) incluye una fase específica de evaluación y gestión de riesgos a nivel de sistemas (CSRM a nivel de sistemas) (véase la figura 4). Esto implica dos etapas:

a) Evaluar y gestionar los riesgos agregados de seguridad informática para las funciones de la instalación en su conjunto. Esto garantizará que el explotador realice una evaluación completa de la instalación y proporcionará a la autoridad competente el medio principal para evaluar la eficacia global de la

CSRM en la instalación. La sección 4 ofrece orientación sobre cómo llevar a cabo la CSRM de la instalación.

b) Evaluar y gestionar los riesgos asociados a cada sistema que realiza o apoya esas funciones de la instalación. Esto garantizará que el explotador lleve a cabo una evaluación detallada de cada sistema que realiza o apoya una función de la instalación. La autoridad competente puede solicitar las evaluaciones detalladas como medio para examinar la eficacia de casos específicos de CSRM en la instalación. La sección 5 ofrece orientación sobre cómo llevar a cabo la CSRM a nivel de sistemas.

3.16. El explotador debería garantizar la independencia entre los equipos responsables de llevar a cabo la CSRM general para establecer los requisitos de seguridad informática de la instalación, los que aplican los requisitos y los que validan que se hayan cumplido los requisitos.

3.17. La gestión de riesgos es pertinente en todas las etapas del período de vida de la instalación y a lo largo de los ciclos de vida de los sistemas para fundamentar el desarrollo, la aplicación y el mantenimiento de las medidas de seguridad informática. La sección 6 determina las actividades relativas a la gestión de riesgos a lo largo del período de vida de una instalación.

3.18. Se debería realizar un examen de la evaluación de riesgos, y proceder a su actualización según convenga, en los siguientes casos:

a) Cuando aparece nueva información o conclusiones importantes que podrían invalidar las hipótesis establecidas en la política de seguridad informática, el CSP, la DCSA o la evaluación de la amenaza específica del emplazamiento vigentes.
b) Cuando se descubre una vulnerabilidad que invalida las medidas de seguridad informática o las hipótesis formuladas en una evaluación de riesgos de los sistemas.
c) Cuando se produce un incidente de seguridad informática en la instalación.
d) Cuando se modifica la declaración nacional de amenazas o la ABD (y las modificaciones son relevantes para los adversarios que emplean ciberataques o ataques combinados). Esto podría reflejar nuevas amenazas o mayores capacidades o recursos del adversario que podrían aumentar la probabilidad de éxito de los ciberataques.
e) Cuando hay un cambio en una función de la instalación, sistema, SDA o medida de seguridad informática. Ello debería incluir la introducción de nuevos equipos, *software* o procedimientos, o cualquier cambio importante en las competencias del personal de operación. El nivel de esfuerzo para

actualizar la evaluación de riesgos puede basarse en el nivel de protección asignado al SDA (por ejemplo, el nivel de seguridad informática).

f) Cuando cambian los requisitos reglamentarios.

g) Cuando ha de realizarse un examen periódico con arreglo al proceso de mejora continua para que la evaluación siga siendo válida.

3.19. Las actividades de reglamentación relacionadas con la seguridad física de la instalación, como la concesión de licencias, la inspección y la acción coercitiva, deberían tener debidamente en cuenta la seguridad informática. Los registros del proceso de gestión de riesgos y las decisiones y medidas resultantes deberían ponerse a disposición de la autoridad competente, previa solicitud, para que pueda examinarlos y evaluar si se cumplen los requisitos reglamentarios.

3.20. La estructura y el enfoque generales del proceso de gestión de riesgos deberían incluir lo siguiente:

a) CSRM de la instalación:
   i) la definición del ámbito de aplicación de la CSRM;
   ii) la caracterización de la instalación;
   iii) la caracterización de las amenazas;
   iv) la especificación de los requisitos;
   v) la verificación y validación, y
   vi) la aceptación por la autoridad competente.

b) CSRM a nivel de sistemas:
   i) la definición de los límites de los sistemas;
   ii) la determinación de los activos digitales (incluidos los SDA);
   iii) los requisitos de seguridad informática de los sistemas, y
   iv) la verificación.

3.21. Existen muchos métodos para llevar a cabo la evaluación de riesgos (véase, por ejemplo, ISO/IEC 27005 [14]). Las organizaciones han de elegir un método y adaptarlo a su entorno y objetivos institucionales específicos, teniendo en cuenta la necesidad de separar la gestión de riesgos a nivel de instalación y de sistemas.

NIVELES DE SEGURIDAD INFORMÁTICA BASADOS EN UN ENFOQUE GRADUADO

3.22. Los requisitos de seguridad informática y el diseño y aplicación de medidas para cumplir dichos requisitos deberían basarse en un enfoque graduado, en el que las medidas de seguridad informática se apliquen de manera directamente

Figura 5. Ilustración del enfoque graduado mediante el concepto de niveles de seguridad informática.

proporcional a las posibles consecuencias en caso de que se comprometa la función de la instalación. Como se indica en la sección 2, una forma práctica de aplicar un enfoque graduado es asignar funciones de la instalación a niveles de seguridad informática, donde cada nivel de seguridad informática se caracteriza mediante requisitos de seguridad informática graduados, y pueden seleccionarse medidas de seguridad preventivas y protectoras para cumplir los requisitos del nivel correspondiente. La figura 5 ilustra el enfoque graduado mediante niveles de seguridad informática.

3.23. Mientras que los requisitos (por ejemplo, restricciones explícitas a la comunicación entre SDA asignados a distintos niveles) son fijados por los niveles de seguridad informática, las medidas de seguridad (por ejemplo, el tipo específico de cortafuegos utilizado para restringir dichas comunicaciones) para proteger los activos digitales (incluidos los SDA) pueden elegirse en función de la estructura del nivel de seguridad informática y de la tecnología de los activos digitales específicos (incluidos los SDA).

3.24. En el enfoque de niveles de seguridad informática, es necesario definir los requisitos de seguridad informática para cada nivel teniendo en cuenta lo siguiente:

a) Los requisitos genéricos deberían aplicarse ampliamente en toda la instalación y entidad explotadora y pueden aplicarse a todos los activos digitales. Dichos requisitos contribuyen a mejorar la cultura de la seguridad física nuclear mediante una mayor concienciación sobre la seguridad informática. También mejoran la resiliencia de la seguridad informática y pueden proporcionar una defensa en profundidad adicional. No puede

considerarse que los requisitos genéricos aporten beneficios a un nivel o sistema de seguridad informática específico porque las medidas genéricas suelen aplicarse a una amplia gama de activos digitales y no puede garantizarse que se utilicen de forma sistemática y eficaz.

b) Se asignan niveles de seguridad informática, que van del nivel 5 (la menor protección necesaria) al nivel 1 (la mayor protección necesaria) (véase la figura 5). En este enfoque, los sistemas que contienen SDA estarían en los niveles de seguridad informática 1 a 3, mientras que los sistemas en los niveles 4 y 5 contienen otros activos digitales.

c) Los requisitos de seguridad informática se especifican y aplican en función de los niveles de seguridad informática asignados, con arreglo a un enfoque graduado. Dichos requisitos deberían basarse en la defensa en profundidad, según la cual los activos digitales asignados a niveles de seguridad que ofrecen una mayor protección no dependen únicamente de activos digitales o medidas de seguridad informática de niveles de seguridad con menor protección, ni confían en ellos sin reservas.

d) Las medidas de seguridad informática aplicadas en cumplimiento de los requisitos de cada nivel de seguridad informática deberían tener en cuenta la independencia y diversidad de las medidas, con el fin de reducir vulnerabilidades comunes que podrían permitir que se eludan o superen múltiples capas de defensa en profundidad. No obstante, puede ser necesario que algunas medidas de seguridad informática aplicadas en un nivel de seguridad informática se repitan en otros niveles de seguridad informática.

e) Gracias a la aplicación de un enfoque por capas y una defensa en profundidad, las medidas de seguridad informática en los niveles inferiores pueden ayudar a proteger los niveles superiores, especialmente en lo que respecta a la detección temprana de ciberataques.

f) Los sistemas informáticos que están fuera del control del CSP no están asignados, por lo que ningún activo digital en ningún nivel de seguridad informática debería confiar en ellos.

3.25. La sección 8 ofrece orientación sobre los requisitos de seguridad informática para un enfoque graduado mediante el ejemplo de cinco niveles de seguridad informática y requisitos genéricos de seguridad informática.

4. GESTIÓN DE RIESGOS DE SEGURIDAD INFORMÁTICA DE LA INSTALACIÓN

4.1. La CSRM de la instalación es un proceso complejo que debería ser llevado a cabo por un equipo multidisciplinario de personas con aptitudes y competencias en seguridad física nuclear, seguridad tecnológica nuclear, operaciones, mantenimiento, seguridad informática e ingeniería[18]. Este equipo podría tener una composición similar a la propuesta para las evaluaciones de la protección física (véase la referencia [15]).

4.2. La CSRM de la instalación es un proceso iterativo que se realiza por fases. Podría ser necesario examinar y modificar las hipótesis, determinaciones o resultados de una fase anterior en función de los resultados de una fase posterior. Está previsto que las actividades de verificación se realicen entre fases.

OBJETIVO DE LA GESTIÓN DE RIESGOS DE SEGURIDAD INFORMÁTICA DE LA INSTALACIÓN

4.3. El objetivo de la CSRM de la instalación es evaluar y gestionar los riesgos asociados a ciberataques que puedan degradar la seguridad física nuclear o la seguridad tecnológica nuclear de la instalación.

4.4. La CSRM de la instalación debería velar por que se cumplan los requisitos reglamentarios en materia de seguridad informática.

4.5. La CSRM de la instalación debería tener en cuenta una evaluación de los adversarios que se haya determinado que podrían atacar la instalación y sus objetivos (por ejemplo, el sabotaje, la retirada no autorizada de material nuclear o material radiactivo, el acceso no autorizado a información de carácter estratégico), incluida una evaluación del atractivo que los blancos[19] de la instalación representan

[18] Algunos Estados Miembros tal vez utilicen denominaciones como “equipo de ciberseguridad” para nombrar al personal necesario en materia de seguridad informática.

[19] El atractivo de los blancos puede abordarse en la evaluación de la amenaza o la ABD y puede complementarse con la información facilitada por el Estado a través de sus autoridades competentes.

para estos adversarios. La evaluación de las amenazas por parte del Estado podría proceder de la declaración nacional de amenazas o de la ABD[20].

4.6. La CSRM de la instalación debería incluir una determinación de la importancia de cada función de la instalación con arreglo a la importancia que dicha función tiene para los objetivos del explotador. Estas determinaciones pueden permitir la elaboración de una lista jerárquica[21] de posibles sucesos relacionados con la seguridad física nuclear (desde los más graves hasta los que no tienen consecuencias) en caso de que se vea comprometida una función de la instalación[22]. La figura 7 de la referencia [7] puede utilizarse en la elaboración de dicha lista jerárquica.

4.7. La CSRM de la instalación debería tener en cuenta las funciones de la instalación, pero no su implantación técnica en sistemas y activos digitales, lo cual se aborda en la CSRM a nivel de sistemas (véase la sección 5).

4.8. La adopción de un enfoque sistemático para la CSRM de la instalación en todas las instalaciones de un Estado puede ayudar a las autoridades competentes a supervisar de manera eficaz la aplicación de la seguridad informática en las instalaciones nucleares.

[20] La ABD se deriva de la evaluación vigente por parte del Estado de una amenaza y sirve de base para la formulación de medidas de seguridad física nuclear. El explotador es el principal responsable de proporcionar medidas de seguridad física nuclear para hacer frente a la capacidad de la amenaza descrita en la ABD. Algunos Estados Miembros presentan una declaración nacional de amenazas en lugar de una ABD.

[21] Lista ordenada que coloca las funciones de la instalación en grupos de consecuencias más o menos similares.

[22] El explotador también puede incluir otras funciones que se haya determinado que revisten importancia para la instalación aparte de las relativas a la seguridad tecnológica o la seguridad física.

DESCRIPCIÓN GENERAL DE LA GESTIÓN DE RIESGOS DE SEGURIDAD INFORMÁTICA DE LA INSTALACIÓN

Aportaciones a la gestión de riesgos de seguridad informática de la instalación

4.9. El explotador debería utilizar los siguientes elementos como aportaciones a la CSRM de la instalación:

a) La declaración nacional de amenazas o la ABD, y el análisis conexo si está disponible.
b) Los requisitos reglamentarios aplicables y otros documentos. Entre ellos pueden figurar los requisitos de clasificación de la información del Estado.
c) El análisis de la seguridad de los sistemas informáticos de la instalación. Este análisis de la seguridad puede servir para definir los requisitos de seguridad informática, pero resulta insuficiente para este fin, ya que no aborda todas las situaciones de mal funcionamiento, especialmente las causadas por actos dolosos.
d) El plan de seguridad física del emplazamiento [15]. El plan de seguridad física del emplazamiento puede servir para determinar las funciones de la instalación que son importantes para la seguridad física, o que están relacionadas con ella, y la importancia que estas tienen para alcanzar los objetivos del explotador. Dicho plan puede incorporar el CSP de la instalación o aspectos de este.
e) La política de seguridad informática de la instalación.
f) Documentos del CSP actual de la instalación y de programas anteriores, incluida información relativa a la asignación de funciones de la instalación a sistemas y la evaluación de la amenaza específica de la instalación.

Fases de la gestión de riesgos de seguridad informática de la instalación

4.10. A continuación se describen las fases de la CSRM de la instalación:

a) Definición del alcance: Definir el alcance de la evaluación de riesgos teniendo en cuenta los objetivos del explotador para la instalación (por ejemplo, la seguridad tecnológica, la seguridad física, las operaciones, la preparación para emergencias), los límites físicos y lógicos, y la etapa del período de vida de la instalación. En esta fase deberían determinarse los requisitos previos para la evaluación y las aportaciones a esta.
b) Caracterización de la instalación: Determinar las funciones de la instalación y sus interacciones e interdependencias, determinar la información de carácter

estratégico que podría servir para planificar un ataque contra la instalación, y determinar los blancos sobre la base de las funciones de la instalación y la información de carácter estratégico que se hayan determinado.

c) Caracterización de las amenazas: Analizar la declaración nacional de amenazas o la ABD y cualquier otra información pertinente o análisis de amenazas para determinar tácticas, técnicas y procedimientos específicos, así como habilidades de los adversarios, que podrían utilizarse en ciberataques (incluidos los ataques combinados) dirigidos contra blancos de la instalación nuclear. La caracterización de las amenazas es un modelo, desarrollado mediante el análisis de los aspectos aplicables de la información sobre la amenaza, para generar una representación de los adversarios que plantean el mayor riesgo. Esta fase de caracterización de las amenazas delimita la gama de escenarios de ataque creíbles.

d) Especificación de los requisitos de seguridad informática: Generar requisitos de seguridad informática con respecto a la instalación. La fase de especificación incluye lo siguiente:
   i) elaborar y documentar un CSP;
   ii) recomendar las modificaciones necesarias de la política de seguridad informática;
   iii) asignar las funciones de la instalación que se hayan determinado a niveles de seguridad informática, y
   iv) crear o modificar requisitos para la DCSA.

   Esta fase puede incluir la aplicación de técnicas de análisis (por ejemplo, la evaluación de la vulnerabilidad, la evaluación de la amenaza) y métodos de evaluación (véase el párrafo 4.98) para formular requisitos a partir de las fases de caracterización de la instalación y de caracterización de las amenazas, y de los requisitos reglamentarios.

e) CSRM a nivel de sistemas: El CSP y la DCSA se aplican a cada sistema. La CSRM a nivel de sistemas se describe con mayor detalle en la sección 5. Podría ser necesario introducir cambios en el CSP y la DCSA a la luz de la experiencia derivada de la aplicación del programa y de la arquitectura en cada sistema.

f) Implantación de sistemas y su integración en la instalación: Esta fase no se aborda en mayor profundidad en la presente publicación. Tal vez sea necesario introducir cambios en la DCSA y el CSP a la luz de la experiencia de ingeniería práctica derivada de la implantación e integración de sistemas.

g) Actividades de garantía: No se trata estrictamente de una fase de la CSRM de la instalación, sino más bien de un conjunto de actividades continuas que

también se realizan en cada proceso de la CSRM a nivel de sistemas. Se utilizan tres tipos de actividad de garantía:

i) la evaluación del cumplimiento de los requisitos de seguridad informática;

ii) la verificación de cada fase de la CSRM, y

iii) la validación de la seguridad informática de la instalación.

Los escenarios son una parte fundamental de las actividades de evaluación, verificación y validación.

h) Productos de la CSRM de la instalación: Estos productos comprenden el CSP (revisado), la DCSA, la evaluación de la amenaza específica del emplazamiento y el informe de cumplimiento de la CSRM de la instalación. Parte o la totalidad de estos documentos se someterá al examen y aceptación de la autoridad competente. Los productos de la CSRM pueden contribuir al perfeccionamiento continuo por parte del Estado de sus requisitos reglamentarios.

4.11. Las fases de la CSRM de la instalación se muestran en la figura 6, que ofrece una visión general del proceso de CSRM de la instalación. Estas fases se describen más detalladamente en el resto de la presente sección.

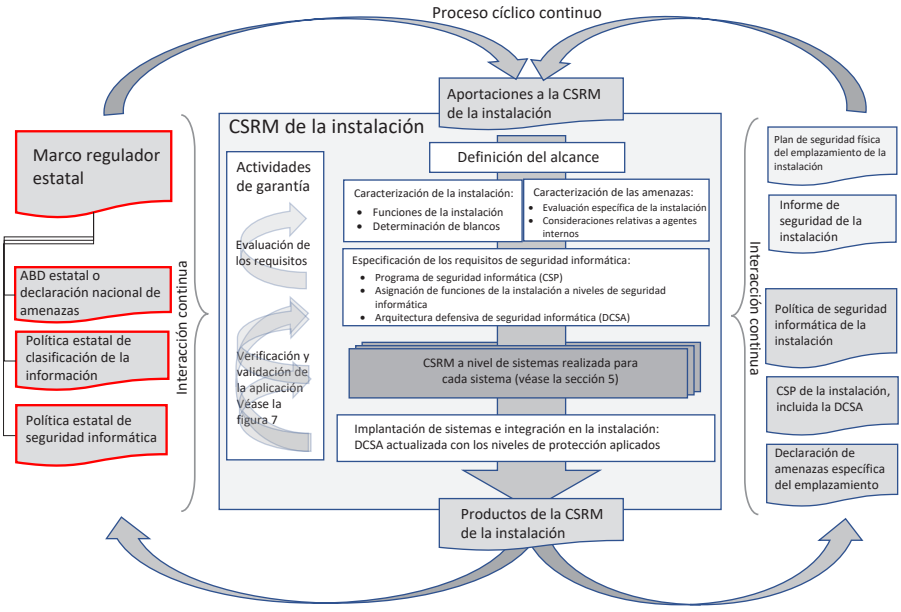


Figura 6. Visión general del proceso de gestión de riesgos de seguridad informática de la instalación. ABD: amenaza base de diseño.

4.12. Hay un proceso de CSRM de la instalación por instalación, dentro del cual hay un proceso de CSRM a nivel de sistemas separado para cada sistema. En el caso de un emplazamiento que contenga múltiples instalaciones o de una organización que explote múltiples instalaciones, puede haber un proceso para todo el emplazamiento o toda la organización, dando lugar a uno o más conjuntos de productos de CSRM de la instalación. En este caso, el explotador puede decidir cuántos conjuntos de productos se generan, pero debería velar por que el proceso se aplique de forma exhaustiva a cada instalación.

DEFINICIÓN DEL ALCANCE

4.13. El explotador debería determinar el alcance de la CSRM de la instalación, que corresponderá a la extensión física o lógica de las funciones de la instalación y los sistemas conexos que atañen a la seguridad física nuclear. Entre las consideraciones que cabría tener en cuenta a la hora de definir el alcance figuran el perímetro físico de la instalación; la ubicación de los proveedores, contratistas y suministradores autorizados; las oficinas corporativas de la entidad explotadora; los centros de datos fuera del emplazamiento, y cualquier otro lugar estratégico. El alcance de la evaluación también puede variar en función de la etapa del período de vida de la instalación o de la capacidad y madurez de la entidad explotadora (véanse los párrafos 5.26 a 5.29 de la referencia [7]).

CARACTERIZACIÓN DE LA INSTALACIÓN

Determinación de las funciones de la instalación

4.14. El explotador debería determinar todas las funciones de la instalación sin tener en cuenta cómo se realizan dichas funciones. La presencia y el uso de activos digitales en toda la instalación y a lo largo de su período de vida hacen probable que los activos digitales se utilicen para realizar o apoyar la mayoría de las tareas y actividades clave relacionadas con las funciones de la instalación.

4.15. A la hora de caracterizar la instalación y determinar las funciones de la misma, debería tenerse en cuenta la etapa del período de vida en que esta se encuentra [10]. Las diferentes funciones de la instalación serán pertinentes en diferentes etapas del período de vida, y su importancia relativa podría cambiar.

4.16. Las funciones de la instalación se caracterizan por los siguientes elementos:

a) Importancia intrínseca: La importancia de la función de la instalación para la seguridad física nuclear y la seguridad tecnológica nuclear y las posibles consecuencias para la instalación si la función no se realiza de manera correcta[23]. Esta es la característica principal.
b) Posibles efectos en caso de que el sistema se vea comprometido: Las distintas formas en que la función de la instalación podría no realizarse correctamente.
c) Interdependencias entre funciones: La importancia de una función de la instalación puede derivarse de otras funciones que dependen de ella.
d) La puntualidad y exactitud con que ha de realizarse la función de la instalación.

Importancia intrínseca de las funciones de la instalación

4.17. Debería compararse la importancia de todas las funciones de la instalación con el fin de agrupar las que tengan una importancia similar, utilizando si es posible una escala común que incluya consideraciones tanto de seguridad física como de seguridad tecnológica.

4.18. Con respecto a las funciones de la instalación que sean importantes para la seguridad física nuclear, o estén relacionadas con ella, debería utilizarse un sistema de clasificación basado en las consecuencias para la seguridad física nuclear, como el que aparece en la figura 7 de la referencia [7], con el fin de determinar la importancia de la función.

4.19. Con respecto a las funciones de la instalación que sean importantes para la seguridad tecnológica nuclear, o estén relacionadas con ella, puede utilizarse un sistema de clasificación de la seguridad tecnológica consolidado para determinar la importancia de la función. Sin embargo, las consideraciones de seguridad física

[23] La importancia de la función para la seguridad física nuclear puede asociarse a menudo con las consecuencias de que la función no se realice correctamente. En lo que respecta a las instalaciones nucleares, las consecuencias que se consideran más graves corresponden a casos en que la retirada no autorizada de material nuclear y el sabotaje dan lugar a consecuencias radiológicas inaceptables. Podrían considerarse otras consecuencias, como la divulgación no autorizada de información de carácter estratégico. Otras posibles consecuencias podrían estar asociadas a otros objetivos institucionales, por ejemplo, mantener la reputación o seguir cumpliendo otros reglamentos ambientales. En la norma ISO 27005:2018 [14] puede encontrarse una lista de posibles consecuencias.

pueden requerir la asignación de una importancia superior a la indicada por la clasificación de seguridad tecnológica de una función.

4.20. La determinación de la importancia de las funciones de la instalación debería tener en cuenta que la realización de las funciones de seguridad tecnológica (por parte de los sistemas) puede contribuir a la seguridad física y que la realización de las funciones de seguridad física puede contribuir a la seguridad tecnológica. Por consiguiente, la importancia asignada a una función de seguridad tecnológica para la seguridad informática puede diferir de la clase de seguridad tecnológica a la que pertenece.

4.21. Por ejemplo, un sistema con una función de la instalación que detecte la radiación con el fin de proteger al personal (objetivo de seguridad tecnológica) también puede servir para detectar la retirada no autorizada de material nuclear (objetivo de seguridad física nuclear). Si bien el fallo de la función de protección radiológica desde el punto de vista de la seguridad tecnológica podría tener consecuencias limitadas, las consecuencias del fallo para la seguridad física nuclear podrían ser más graves. Por lo tanto, a las funciones de la instalación proporcionadas por el sistema en este ejemplo se les asignaría un valor de importancia en función de su importancia para los objetivos de seguridad física nuclear. (Como alternativa, el explotador podría optar por implantar sistemas independientes para separar las funciones que apoyan la seguridad tecnológica nuclear y la seguridad física nuclear, y en este ejemplo podría asignarse una importancia menor a la función que apoya la seguridad tecnológica nuclear.)

Posibles efectos en la función de la instalación en caso de que un sistema se vea comprometido

4.22. Además de considerar la importancia intrínseca de la función de la instalación, el explotador debería considerar los efectos en la función de la instalación en caso de que el sistema destinado a realizarla se vea comprometido. Los efectos son los siguientes (ordenados de mayor a menor gravedad):

a) El comportamiento de la función de la instalación es indeterminado. Esto significa que la función puede alterarse de cualquier manera sin haberse detectado que el sistema había quedado comprometido previamente.
b) El comportamiento de la función de la instalación cambia de forma imprevista (y pueden realizarse otras acciones), pero estas anomalías son observables por parte del explotador.
c) El comportamiento de la función de la instalación falla.

d) El comportamiento de la función de la instalación es el previsto, es decir, la función de la instalación no se ve perjudicada por el hecho de que el sistema se haya comprometido (es decir, el sistema tolera fallos).

4.23. Un sistema que sirve para realizar una función de la instalación puede funcionar mal de diferentes maneras al verse comprometido, y los efectos de este mal funcionamiento dependen de las circunstancias y del entorno en el momento en que se ve comprometido, de la naturaleza del ciberataque que crea esa situación, y de la importancia de la función de la instalación. Por ejemplo, un sistema que realice una función menos importante de la instalación podría, a través de interdependencias e interacciones entre las funciones, ser utilizado para atacar un sistema que realice una función más importante.

4.24. Con respecto a cada sistema y cada tipo de efecto al verse comprometido (es decir, mal funcionamiento), las consecuencias para la instalación serán distintas. Estas consecuencias deberían evaluarse, y la importancia asignada a las funciones de la instalación debería basarse en estas posibles consecuencias. Al evaluar las consecuencias, debería tenerse en cuenta la pérdida de confidencialidad, integridad o disponibilidad de la información de carácter estratégico, así como las consecuencias relacionadas con la retirada no autorizada de material o el sabotaje de la instalación.

4.25. La importancia asignada a una función de la instalación debería tener en cuenta si la función puede definirse de tal manera que sea válida para todas las condiciones o modos posibles de los que esta pueda depender. Si la función de la instalación no puede delimitarse de este modo, la lista de consecuencias podría estar incompleta y tal vez convenga realizar un análisis adicional o asignar un valor de mayor importancia (utilizando un enfoque conservador).

Interdependencias entre funciones de la instalación

4.26. La determinación de la importancia de una función de la instalación también debería tener en cuenta las posibles consecuencias de que un sistema se vea comprometido (o funcione mal) para otras funciones de la instalación que dependen de ella. Los siguientes son ejemplos de ese tipo de dependencias funcionales:

a) Dependencia de la información: una función de la instalación proporciona información a otra función de la instalación. A continuación figuran ejemplos de mal funcionamiento:
   i) interrupción de las instrucciones de control automatizadas de un proceso de la instalación;

ii) situación en que las alarmas proporcionadas a los oficiales de seguridad se ven comprometidas;
iii) visualización de información incorrecta sobre la monitorización de la central para el personal de operación;
iv) no facilitar información a los encargados de la respuesta a emergencias o a los oficiales de seguridad física nuclear;
v) pérdida o manipulación de procedimientos o instrucciones, o de registros que documenten los resultados de estos procedimientos.

b) Dependencia de recursos físicos o de ingeniería: una función de la instalación proporciona un recurso físico a otra función de la instalación. Esto incluye los recursos necesarios para mantener la otra función de la instalación directamente y los recursos necesarios para mantener esos recursos. A continuación figuran ejemplos de mal funcionamiento:
i) interrupción del suministro de agua o electricidad;
ii) condiciones ambientales imprevistas;
iii) no programación de las tareas de mantenimiento preventivo;
iv) fallo de los sistemas de protección física (por ejemplo, controles del acceso, detección de intromisiones).

c) Dependencia de las políticas o los procedimientos: un cambio en una función de la instalación requiere un cambio en otra función de la instalación. Por ejemplo, si la política exige que se proporcionen funciones de sumidero de calor primario y secundario cuando un reactor esté en estado crítico, si uno de esos sumideros de calor deja de estar disponible, el reactor tiene que pasar a un estado subcrítico.

d) Efectos de proximidad: los efectos en una función de la instalación por un mal funcionamiento o fallo físico de otros sistemas que se encuentran físicamente cerca de los que realizan dicha función.

4.27. El análisis de las interacciones e interdependencias entre las funciones de la instalación podría revelar que en el alcance de la evaluación se ha omitido una función importante de la instalación. Las dependencias pueden extenderse más allá de la instalación, por ejemplo, el suministro de agua o electricidad a la instalación. En el análisis de las dependencias entre las funciones de la instalación tal vez sea necesario tener en cuenta algunas funciones proporcionadas por organizaciones externas. En este caso, puede ser necesario revisar el alcance de la evaluación para incluir esas dependencias o realizar cambios en la instalación que eliminen las dependencias.

4.28. La segregación de los sistemas que realizan funciones de la instalación para limitar las interacciones e interdependencias entre estas podría simplificar

la especificación de los niveles y requisitos de seguridad informática y podría mejorar la eficacia y eficiencia de las medidas de seguridad informática.

Puntualidad y exactitud necesarias para las interdependencias entre las funciones de la instalación

4.29. La determinación de la importancia de las funciones de la instalación también puede tener en cuenta la puntualidad y exactitud con las que una función de la instalación ha de responder a otra función de la instalación. La puntualidad puede entenderse desde el punto de vista de los requisitos relativos a la disponibilidad de información de carácter estratégico, y la exactitud puede entenderse desde el punto de vista de los requisitos relativos a la integridad de dicha información:

a) La disponibilidad de la información implica que, por ejemplo, las alertas proporcionadas por una función de la instalación se notifiquen con prontitud para que puedan realizarse otras funciones de la instalación, como la evaluación de la alerta y la respuesta a la misma.
b) La integridad de la información implica que, por ejemplo, una función de la instalación proporcione datos exactos sobre variables ambientales (por ejemplo, temperatura, presión, frecuencia, nivel) de las que dependen otras funciones de la instalación.

Determinación del blanco

4.30. En la referencia [1], la definición de blanco es la siguiente:

> "*Materiales nucleares, otros materiales radiactivos, instalaciones conexas, actividades conexas*, u otros lugares u objetos a los que podría dirigirse una *amenaza para la seguridad física nuclear*, comprendidos los *eventos públicos importantes*, los *lugares estratégicos*, la *información de carácter estratégico* y los *recursos de información de carácter estratégico*".

4.31. Algunos sistemas que realizan funciones de la instalación serán blancos y deberían determinarse a partir de la lista de funciones de la instalación elaborada durante la CSRM de la instalación, utilizando las definiciones de zonas vitales [16] e información de carácter estratégico [5]. El hecho de que un sistema de este tipo se considere un blanco no cambia la importancia de la función de la instalación, pero supone una consideración adicional a la hora de determinar los requisitos de seguridad informática.

4.32. Los blancos asociados a funciones importantes de seguridad tecnológica y seguridad física de la instalación deberían definirse como SDA mediante el proceso descrito en los párrafos 3.6 a 3.9. Estos SDA también deberían analizarse para determinar el valor que pueda tener toda información de carácter estratégico conexa. Esto garantizará que los SDA y su información conexa se tengan en cuenta en el programa de seguridad física de la información y el CSP de la instalación y reciban el nivel de protección adecuado.

Documentación de las funciones de la instalación

4.33. El explotador debería documentar todas las funciones de la instalación que se hayan determinado y evaluado durante la CSRM de la instalación.

4.34. La determinación de todas las funciones de la instalación depende de la disponibilidad de registros completos y exactos que describan las interacciones e interdependencias entre las funciones. Estos registros permitirán evaluar aquellas funciones que podrían repercutir negativamente en otras si no se realizan correctamente.

4.35. Las interacciones e interdependencias de una función de la instalación pueden ser internas o externas, así como permanentes o temporales. Por ejemplo, durante el desarrollo de sistemas, puede ser necesaria la interacción entre los entornos de desarrollo y operacional mediante el transporte físico de nuevos programas informáticos, datos o dispositivos, pero estas interacciones podrían eliminarse cuando los sistemas estén en funcionamiento.

4.36. Al analizar las consecuencias de un ataque dirigido contra una función de la instalación, el explotador debería considerar la posibilidad de que este forme parte de un ataque que afecte a varias funciones de la instalación o de un ataque combinado (es decir, un ciberataque combinado con un ataque físico).

4.37. Es posible que en el análisis sea necesario incluir una evaluación iterativa de cada función de la instalación, de modo que se realice una evaluación para determinar la importancia intrínseca de la función y otra para determinar la importancia sobre la base de las interacciones e interdependencias con otras funciones de la instalación. Debería utilizarse el mayor de los dos niveles de importancia obtenidos a partir de estas evaluaciones.

4.38. Debería asignarse la mayor importancia a las funciones de la instalación que tienen una relación directa entre la función que no se realiza correctamente y las consecuencias más graves (por ejemplo, las funciones de la instalación

relacionadas estrechamente con las tres funciones principales de seguridad, a saber, control de la criticidad, eliminación de calor y contención del material [12])[24]. En estos casos, la asignación de importancia no debería tener en cuenta otros parámetros o factores.

CARACTERIZACIÓN DE LAS AMENAZAS

4.39. La caracterización de las amenazas depende de dos procesos continuos distintos, los cuales están interrelacionados:

a) la evaluación de amenazas por parte del Estado y la elaboración y el mantenimiento de la declaración nacional de amenazas o la ABD utilizando fuentes de inteligencia, y
b) la evaluación de la amenaza específica de la instalación, teniendo en cuenta el análisis de la información específica de la instalación y la información sobre adversarios específicos.

Fuentes de la información sobre amenazas

4.40. El párrafo 3.34 de la referencia [2] dice lo siguiente:

> "Las autoridades estatales competentes, utilizando diversas fuentes de información creíble, deberían definir la *amenaza* y las capacidades conexas en forma de una *evaluación de amenazas* y, si procede, una *amenaza base de diseño*. La *amenaza base de diseño* se elabora a partir de una evaluación por el Estado de la amenaza de *retirada no autorizada* y *sabotaje*".

En la referencia [9] puede consultarse información adicional sobre la ABD.

4.41. El explotador debería establecer medidas encaminadas a determinar, conservar y gestionar información específica[25] relacionada con posibles ciberataques y adversarios (por ejemplo, correos electrónicos de suplantación de identidad, muestras de programas maliciosos) para poder realizar un análisis de

[24] Véase también el cuadro 1 de la referencia [17] para las relaciones entre las funciones que figuran en el análisis de los sucesos iniciadores postulados y las categorías de seguridad.

[25] Esta información específica puede ser facilitada por el explotador, una autoridad competente u otra organización estatal. Puede tratarse de información clasificada, por lo que es necesario que cumpla los requisitos estatales relativos a la determinación y tratamiento de la información de carácter estratégico.

seguimiento en apoyo de la caracterización de las amenazas. El explotador debería velar por que estas medidas se apliquen de tal forma que no afecten negativamente a la seguridad nuclear física o tecnológica.

4.42. La caracterización de las amenazas por parte del explotador puede incluir elementos de evaluaciones de amenazas realizadas por otras organizaciones (por ejemplo, las propias evaluaciones del explotador, informes de fuentes de libre acceso).

4.43. Se alienta a la autoridad competente pertinente a que presente un análisis de la información específica recopilada por el explotador de forma oportuna y cooperativa y a que apoye el intercambio de este análisis y de otra información importante, en consonancia con los requisitos del Estado en materia de información de carácter estratégico [5]. La notificación periódica de incidentes a la autoridad competente pertinente por parte del explotador puede ser valiosa como análisis de amenazas, y la caracterización es una actividad continua que requiere información actualizada.

4.44. Durante la elaboración de la declaración nacional de amenazas o la ABD, la autoridad competente y otras autoridades estatales pertinentes deberían tener (o deberían tener acceso a) competencias técnicas y conocimientos sobre posibles incidentes de seguridad informática (por ejemplo, ciberataques) contra instalaciones nucleares.

4.45. La referencia [7] proporciona orientación sobre la evaluación de las ciberamenazas para un régimen de seguridad física nuclear, así como descripciones detalladas de las posibles procedencias de los ataques y los mecanismos de ataque conexos pertinentes para las instalaciones nucleares, y de las metodologías utilizadas para evaluar y detectar amenazas.

Caracterización de las amenazas específicas de la instalación

4.46. El explotador debería elaborar y mantener una caracterización de las amenazas específicas de la instalación en apoyo de la evaluación del riesgo de seguridad informática para la instalación. Ello debería incluir un análisis de la declaración nacional de amenazas o la ABD para caracterizar las amenazas específicas para la seguridad física nuclear de la instalación que contribuyan al riesgo para la seguridad informática. El análisis debería describir los posibles objetivos, capacidades, tácticas y técnicas de las amenazas pertinentes, lo cual serviría de base para formular la política de seguridad informática y el CSP de la instalación, o para validar su eficacia.

4.47. El explotador debería realizar la caracterización de las amenazas en los siguientes casos:

a) Cuando el explotador realiza una evaluación de riesgos para la seguridad informática de la instalación. A veces puede tratarse de un análisis menos profundo para comprobar el análisis y las hipótesis anteriores.
b) Cuando la autoridad competente presenta una nueva ABD o declaración nacional de amenazas.
c) Cuando el explotador recibe información que pueda invalidar hipótesis formuladas en el análisis vigente.

4.48. La caracterización de las amenazas realizada por el explotador debería describir los conocimientos, capacidades y financiación, así como las posibles campañas, blancos, tácticas, técnicas y procedimientos de los posibles adversarios que se hayan determinado, y cualquier atributo adicional de especial relevancia. El párrafo 5.19 de la referencia [9] ofrece una lista de posibles atributos adicionales para la caracterización de las amenazas.

4.49. La caracterización de las amenazas realizada por el explotador debería determinar posibles combinaciones de tácticas y técnicas que podrían utilizarse en un ataque, como acciones remotas y locales coordinadas, el uso de agentes internos y adversarios externos, o ataques que combinen ciberataques con ataques físicos. La caracterización de las amenazas debería incluir la posibilidad de que se produzcan ciberataques secuenciales o paralelos con consecuencias acumulativas, en los que participen uno o varios adversarios, así como casos en los que no haya indicios de connivencia entre diferentes adversarios (ataques no colaborativos).

4.50. La caracterización de las amenazas realizada por el explotador debería permitir enumerar y evaluar los tipos de ataque creíbles. Esta lista constituirá la base de los requisitos y especificaciones de seguridad informática de la DCSA.

4.51. La caracterización de las amenazas debería indicar si el adversario tiene la capacidad para llevar a cabo un tipo de ataque concreto y si el adversario puede comprometer un sistema que realiza una función de la instalación de tal manera que su comportamiento sea indeterminado (es decir, se sitúe fuera de su base de diseño).

Consideraciones adicionales respecto a las amenazas de agentes internos

4.52. La caracterización de las amenazas debería tener en cuenta las amenazas de agentes internos. En la referencia [6] se proporciona orientación específica.

Con respecto a la seguridad informática, las amenazas de agentes internos pueden clasificarse de la siguiente manera:

a) Agente interno pasivo: agente interno con la motivación para facilitar actos dolosos, pero no para iniciarlos. Las medidas de seguridad informática para hacer frente a un agente interno pasivo podrían basarse en medidas preventivas, entre ellas tener una cultura sólida de la seguridad física. Por lo general, un agente interno pasivo no se verá disuadido por las medidas de detección, porque su acceso a la información y a los sistemas es legítimo, pero tratará de evitar que se detecte que actúa de forma dolosa.
b) Agente interno activo: agente interno con la motivación para iniciar actos dolosos. Es probable que haya menos agentes internos activos que pasivos. Los controles de seguridad informática para hacer frente a un agente interno activo han de ser más exhaustivos que los destinados a hacer frente a un agente interno pasivo y deberían incluir medidas de protección como la segregación de tareas y la compartimentación de la información, el acceso físico o los privilegios del sistema.
c) Agente interno involuntario: agente interno sin la motivación para cometer un acto doloso y que no es consciente de que está siendo utilizado por un adversario. Por ejemplo, en un ciberataque, un agente interno involuntario podría no ser consciente de que ciertas acciones pueden proporcionar información o acceso autenticado a un adversario, como al hacer clic en un enlace doloso de un correo electrónico que aparenta proceder de una fuente de confianza.

4.53. Las rutas de los adversarios y los plazos conexos en relación con las amenazas de agentes internos difieren de otras amenazas debido al acceso autorizado de dichos agentes. Este acceso permite a los agentes internos, por ejemplo, utilizar una serie no continua de tareas que se realizan durante un largo período de tiempo. Por ejemplo, la recopilación de credenciales administrativas (ya sea mediante ingeniería social o comprometiendo los sistemas) para anular medidas como los controles del acceso o la segregación de tareas podría tener lugar a lo largo de varias semanas, meses o años.

ESPECIFICACIÓN DE LOS REQUISITOS DE SEGURIDAD INFORMÁTICA

Política de seguridad informática y programa de seguridad informática

4.54. La política de seguridad informática[26] del explotador especifica los objetivos y requisitos generales para la seguridad informática de la instalación, aplicando un enfoque graduado y la defensa en profundidad. Estos requisitos generales son especificados por el explotador, de conformidad con los requisitos reglamentarios aplicables, y se aplican sin excepciones. La política de seguridad informática contribuye a la CSRM de la instalación, la cual puede ampliar y perfeccionar la política de seguridad informática de la instalación.

4.55. El explotador debería elaborar y documentar su CSP[27] como parte de la CSRM de la instalación. El CSP es un marco para la aplicación de la política de seguridad informática de la instalación que se utilizará a lo largo del período de vida de esa instalación. El contenido de un CSP típico se describe en la sección 7 e incluye el conjunto de requisitos específicos de seguridad informática de la instalación, además de los requisitos que se hayan determinado mediante un enfoque basado en el conocimiento de los riesgos.

4.56. El explotador debería definir requisitos de seguridad informática en el CSP para los siguientes ámbitos, que se describen con más detalle en la sección 7:

a) las funciones y responsabilidades organizativas;
b) la evaluación de los riesgos, la vulnerabilidad y el cumplimiento;
c) los procedimientos de seguridad de la organización;
d) el diseño y la gestión de la seguridad de los sistemas;
e) la gestión de activos y de la configuración, y
f) la gestión del personal.

4.57. El explotador debería especificar en el CSP las medidas de seguridad informática de referencia que sean obligatorias para cada nivel de seguridad informática. Estas medidas probablemente consistan en requisitos que representan políticas y procesos organizativos y se traducirán en procedimientos.

---

[26] Algunas organizaciones pueden referirse a la política de seguridad informática como estrategia de seguridad informática.

[27] Algunas organizaciones pueden referirse al CSP como plan de seguridad informática.

4.58. Deberían determinarse y definirse requisitos relativos a la solidez de las medidas de seguridad informática para cada nivel de seguridad informática, con arreglo a los requisitos reglamentarios (si procede). Se desaconsejan vehementemente las excepciones a la aplicación de una medida específica dentro de un nivel de seguridad informática, y toda excepción de este tipo debería justificarse y documentarse en la CSRM de la instalación.

4.59. Los principales productos de la fase de especificación de la CSRM de la instalación son la documentación del CSP (o CSP revisado) y un informe de cumplimiento para la autoridad competente en el que se indique cómo la aplicación del CSP garantizará que se cumplan los requisitos reglamentarios. La documentación del CSP puede ser un único documento o una colección de documentos distintos, pero debería incluir lo siguiente:

a) Una declaración que indique el nivel de protección de seguridad informática que ha de proporcionarse para cada nivel de seguridad informática. Esta declaración puede ser cualitativa o cuantitativa, pero debería ser verificable.
b) El requisito de realizar y documentar exámenes y evaluaciones de riesgos de la seguridad informática de manera periódica en cada etapa del período de vida de la instalación.
c) Una definición de las funciones y responsabilidades necesarias para apoyar la seguridad informática.
d) Una especificación para la DCSA, que combine los requisitos de seguridad informática derivados de la aplicación por parte del explotador de un enfoque basado en el conocimiento de los riesgos y cualquier requisito de este tipo impuesto a la instalación en virtud de la legislación o los reglamentos nacionales. Las especificaciones de la DCSA deberían incluir lo siguiente:
    i) los requisitos para aplicar un enfoque graduado (por ejemplo, el número de niveles de seguridad informática);
    ii) los requisitos para la defensa en profundidad;
    iii) cualquier requisito adicional (por ejemplo, de autenticidad, no repudio y trazabilidad) necesario para cumplir el nivel de protección correspondiente a cada nivel de seguridad informática;
    iv) requisitos que proporcionen y mantengan la capacidad de prevenir, detectar y retrasar ciberataques, mitigar sus efectos y recuperarse tras estos, y
    v) los requisitos específicos relativos a las medidas de seguridad informática para cada nivel de seguridad informática que han de aplicarse a las respectivas zonas de seguridad informática.
e) Un registro de los escenarios funcionales u otros métodos de evaluación utilizados en el análisis para elaborar requisitos. Es importante que se

desarrollen otros escenarios de forma independiente para ofrecer una mayor garantía respecto a los requisitos (es decir, un mayor nivel de confianza). El uso de escenarios para aumentar el nivel de confianza en el producto de la fase de especificación se describe con más detalle en los párrafos 4.116 a 4.122.

4.60. El explotador debería presentar la documentación del CSP pertinente para someterla al examen de la autoridad competente, junto con el informe de cumplimiento.

Asignación de sistemas que realizan funciones de la instalación a niveles de seguridad informática

4.61. La CSRM de la instalación debería incluir o utilizar una lista priorizada de funciones de la instalación, ordenadas según la importancia de la función de la instalación, como base para la aplicación de un enfoque graduado con el fin de proporcionar el mayor nivel de garantía de protección a aquellas funciones que tengan mayor posibilidad de provocar las consecuencias más graves.

4.62. El objetivo del enfoque por niveles de seguridad informática es simplificar la aplicación de un enfoque graduado. Los niveles de seguridad informática determinan qué conjunto de requisitos de seguridad informática se aplican para proporcionar el nivel adecuado de protección al sistema que realiza una función de la instalación.

4.63. El explotador debería determinar el número de niveles de seguridad informática que se utilizarán, teniendo en cuenta los requisitos reglamentarios aplicables. Por ejemplo, un explotador podría optar por aplicar un nivel de seguridad informática diferente para cada función de la instalación. Sin embargo, la complejidad de la aplicación del enfoque aumenta cuanto mayor es el número de niveles de seguridad informática. Limitar el número de niveles de seguridad informática permite aplicar enfoques y métodos comunes a distintos sistemas. Por lo tanto, la instalación puede optar por utilizar un número menor de niveles. El beneficio de la simplicidad al reducir el número de niveles debería sopesarse frente al costo en recursos y eficiencia que supone aplicar medidas más estrictas a las funciones de la instalación de lo absolutamente necesario en todos los casos.

4.64. El explotador debería asegurarse de que cada función de la instalación se asigna a un único nivel de seguridad informática.

4.65. En algunos casos, las funciones de la instalación que son importantes para la seguridad física, o que están relacionadas con esta, podrían no estar lo suficientemente delimitadas como para poder distinguirlas claramente de otras funciones. La imposibilidad de distinguir las funciones de la instalación entre sí aumenta la complejidad a la hora de asignar el nivel de importancia de dichas funciones. Por lo tanto, las funciones de la instalación deberían ser distintas e independientes entre sí en la medida de lo posible. El explotador puede estudiar la posibilidad de modificar las funciones de la instalación con el fin de simplificar la aplicación del enfoque graduado, lo que a su vez también podría ser beneficioso a la hora de aplicar la defensa en profundidad.

4.66. El explotador debería incluir lo siguiente en la documentación del CSP:

a) el número de niveles de seguridad informática y los requisitos correspondientes a las medidas de seguridad informática conexas, y
b) la lista ordenada de funciones de la instalación, indicando cómo estas han sido asignadas a los niveles de seguridad informática.

Especificación de la arquitectura defensiva de seguridad informática

4.67. El explotador debería diseñar e implantar una DCSA en la que todos los sistemas que realizan funciones de la instalación se asignen a un nivel de seguridad informática y se protejan con arreglo a los requisitos de seguridad informática especificados para dicho nivel.

4.68. El explotador debería especificar las medidas de seguridad informática de referencia que sean obligatorias para cada nivel de seguridad informática en el marco de la DCSA. Estas medidas de referencia pueden incluir medidas de control técnico, administrativo y físico.

4.69. La DCSA debería tener por objeto eliminar o limitar las posibles rutas de ciberataque (señaladas en la caracterización de las amenazas) que un adversario podría utilizar para comprometer los sistemas que realizan funciones de la instalación. En la referencia [16]se detallan procesos similares para reducir las rutas físicas de que dispone el adversario.

4.70. Deberían establecerse límites de seguridad informática[28] entre los sistemas que realizan funciones de la instalación que tienen diferentes niveles de seguridad informática.

Requisitos de la especificación de la DCSA para aplicar un enfoque graduado

4.71. La especificación de la DCSA debería expresar los requisitos generales (incluido el número de niveles de seguridad informática) e incluir la robustez de las medidas para cada nivel de seguridad informática, la robustez de las medidas entre los distintos niveles de seguridad informática y las normas para la comunicación entre zonas con distintos niveles de seguridad informática.

4.72. La especificación de la DCSA debería garantizar que las funciones de la instalación con mayor importancia se asignen al nivel de seguridad informática más estricto. Deberían definirse los requisitos para las comunicaciones entre sistemas asignados a diferentes funciones de la instalación. Debería controlarse el flujo de datos entre funciones de la instalación con diferentes niveles de seguridad informática, con arreglo a un enfoque basado en el conocimiento de los riesgos.

4.73. La especificación de la DCSA debería garantizar que la complejidad del diseño de los sistemas se reduzca cuando sea posible para simplificar la aplicación de las medidas de seguridad informática. Disminuir la complejidad de las medidas de seguridad informática puede aumentar tanto el rendimiento como la fiabilidad.

Requisitos de la especificación de la DCSA para aplicar la defensa en profundidad

4.74. La especificación de la DCSA debería exigir la aplicación de la defensa en profundidad a través de capas sucesivas[29] de medidas de seguridad informática que un adversario ha de superar o eludir para comprometer los sistemas que realizan funciones de la instalación.

---

[28] En la presente publicación, los límites de seguridad informática se definen como los límites lógicos y físicos de un sistema o de un conjunto de sistemas con el mismo nivel de seguridad que, por tanto, pueden protegerse mediante la aplicación de medidas de seguridad comunes (por ejemplo, zonas de seguridad informática).

[29] En la presente publicación, el término “capas” se refiere a capas de defensa en profundidad. En el caso de la seguridad informática, esto suele conseguirse mediante el establecimiento de zonas de seguridad informática (incluidas las medidas de seguridad informática) con arreglo a los requisitos relativos a los niveles de seguridad informática y la DCSA.

4.75. La especificación de la DCSA debería exigir una combinación determinada de medidas de control técnico, físico y administrativo para proporcionar una defensa en profundidad.

4.76. La especificación de la DCSA debería exigir un diseño que garantice que no se produzcan consecuencias inaceptables en caso de que se vea comprometida o falle una única medida de seguridad informática.

4.77. La especificación de la DCSA debería exigir el uso de medidas independientes y diversas para garantizar que una vulnerabilidad común no permita a un adversario comprometer o eludir varias capas de defensa en profundidad con una sola táctica.

4.78. La especificación de la DCSA debería exigir la aplicación de la defensa en profundidad entre capas y dentro de cada capa. Las capas de defensa pueden utilizar una combinación de medidas aplicables a distintos niveles de seguridad informática y aplicarlas a distintas zonas de seguridad informática. Con respecto a las consecuencias más graves (es decir, consecuencias radiológicas importantes debidas al sabotaje o a la retirada no autorizada de material nuclear de la categoría I), deberían aplicarse medidas de seguridad informática en múltiples capas independientes con el fin de proporcionar un comportamiento determinista y a prueba de fallos[30] de los sistemas en caso de ciberataque.

4.79. La especificación de la DCSA debería apoyarse en un informe de análisis para determinar las medidas de seguridad informática que sean a prueba de fallos y deterministas en el marco de la aplicación de la defensa en profundidad. La autoridad competente podrá solicitar la presentación de este informe para someterlo a examen.

Defensa en profundidad entre capas

4.80. La especificación de la DCSA debería exigir que cada capa de defensa en profundidad esté protegida frente a ciberataques que se originen en capas adyacentes. Las capas y sus medidas de seguridad informática conexas deberían impedir o retrasar el avance de los ataques.

4.81. La especificación de la DCSA debería exigir que las medidas de seguridad informática utilizadas en una capa se seleccionen y funcionen de manera distinta e independiente con respecto a las medidas de seguridad informática utilizadas

[30] El término “a prueba de fallos” significa que el fallo de una medida da lugar a una condición que mantiene la seguridad de la función que la medida tiene por objeto proteger.

en una capa adyacente, con el fin de mitigar los fallos de causa común de los mecanismos de protección utilizados para el aislamiento entre capas. Con arreglo al principio de enfoque graduado, estos requisitos deberían ser más estrictos para las capas que requieran la protección más estricta (es decir, los niveles 1 y 2 de seguridad informática).

Defensa en profundidad dentro de una capa

4.82. La especificación de la DCSA debería exigir que se emplee una combinación de medidas de seguridad informática dentro de cada capa para reducir al mínimo la posibilidad de que se superen o eludan múltiples medidas si una de ellas se ve comprometida. Con arreglo al principio de enfoque graduado, estos requisitos deberían ser mayores para las capas que requieran la protección más estricta (es decir, los niveles 1 y 2 de seguridad informática, siendo el nivel 1 el de mayor nivel de protección).

Modelo de confianza

4.83. La aplicación de un enfoque graduado y de la defensa en profundidad debería ser compatible con un modelo de confianza aplicable. Entre los modelos de confianza que pueden aplicarse figuran los siguientes:

a) probidad del personal (es decir, protección contra amenazas de agentes internos) [6];
b) protección de información de carácter estratégico (es decir, clasificada) (por ejemplo, Bell-LaPadula[31]), y
c) protección de la integridad (por ejemplo, Biba, Clark-Wilson[32]).

[31] El modelo Bell-LaPadula vela por el cumplimiento de la confidencialidad: para que una persona o un proceso acceda a la información, estos deberían tener una clara necesidad de conocerla y deberían estar autorizados para tener acceso al menos a la categoría de la información de carácter estratégico.

[32] Los modelos Biba y Clark-Wilson protegen la integridad de la información: el modelo Biba impide la modificación de datos por partes no autorizadas, pero no impide la modificación no autorizada por partes autorizadas (es decir, agentes internos), mientras que el modelo Clark-Wilson impide ambas cosas.

RELACIÓN CON LA GESTIÓN DE RIESGOS DE SEGURIDAD INFORMÁTICA A NIVEL DE SISTEMAS — REALIZADA PARA CADA SISTEMA

4.84. Una vez especificados los requisitos de seguridad informática, la aplicación de dichos requisitos se realiza tal como se ilustra en la figura 6 (véase también la figura 7). La aplicación de los requisitos exige comprender los modos en que los activos digitales realizan las funciones de la instalación.

4.85. Los procesos de gestión de riesgos en la CSRM de la instalación y a nivel de sistemas tienen interacciones importantes (véanse las figuras 6 y 7). La CSRM de la instalación incluye la asignación de una o más funciones de la instalación a distintos sistemas y, por tanto, establece el alcance de la CSRM de cada sistema, pero la CSRM de la instalación también podría verse afectada por los productos de la CSRM a nivel de sistemas en un proceso iterativo. Por ejemplo, en los sistemas de protección física, pueden asignarse múltiples funciones de la instalación a un único sistema debido a que no se dispone de sistemas con funciones segregadas. Esto restringe la capacidad de dividir el sistema en zonas separadas, lo cual limita el modelo de zonas a un límite físico o a un límite lógico.

4.86. En el caso de las instalaciones o sistemas antiguos, algunas estructuras, sistemas y componentes tal vez no sean modificables o alterables. Esto podría implicar, en la fase de la CSRM a nivel de sistemas, que no puedan cumplirse algunos requisitos definidos en la CSRM de la instalación, y el explotador tal vez tenga que revisar la CSRM de la instalación para determinar una especificación adecuada del CSP y de la DCSA que cumpla los requisitos de seguridad.

4.87. Las CSRM de la instalación y a nivel de sistemas deberían examinarse, y tal vez sea necesaria su revisión, en los siguientes casos:

a) Al revisarse la CSRM de la instalación o el análisis de la seguridad tecnológica de la instalación.
b) Cuando el sistema no puede cumplir plenamente los requisitos señalados en el producto de la CSRM de la instalación.
c) Al realizarse modificaciones en el sistema que puedan afectar a la CSRM de la instalación.
d) Al producirse sucesos o incidentes de seguridad física importantes.
e) Al detectarse nuevas amenazas o vulnerabilidades o cambios en estas.

4.88. El examen de los procesos de CSRM de la instalación y a nivel de sistemas ha de incluirse en el proceso de gestión del cambio de la instalación para

garantizar que concuerden entre sí y se mantengan actualizados. Estos análisis también contribuyen a establecer los requisitos (por ejemplo, definir los niveles de seguridad informática) para nuevos sistemas o aplicaciones.

4.89. Las tendencias de las sucesivas iteraciones correspondientes a la CSRM de la instalación y a nivel de sistemas deberían evaluarse periódicamente para detectar los siguientes tipos de patrones adversos:

a) Un riesgo que muestre un patrón claro de aumento hacia el umbral de riesgo inaceptable o más allá de este. En este caso, deberían estudiarse formas de evitar que se supere el umbral de riesgo.
b) Un riesgo que alcance o supere el umbral. En este caso, será necesario tomar las medidas adecuadas (por ejemplo, informar a la autoridad competente, aplicar medidas compensatorias acordes con la urgencia que se haya determinado a partir de los datos relativos a la tendencia del riesgo).

4.90. Deberían analizarse las tendencias asociadas a los distintos sistemas para garantizar que la tendencia no invalide el producto de la CSRM de la instalación. Por ejemplo, las evaluaciones de la vigilancia de los sistemas pueden realizarse continuamente, mientras que los informes de monitorización del funcionamiento de los sistemas pueden aprobarse periódicamente. Los productos de la CSRM de los sistemas que corresponda deberían examinarse en el proceso de la CSRM de la instalación para garantizar que no haya cambios en el riesgo global de la instalación.

ACTIVIDADES DE GARANTÍA

4.91. Hay tres tipos de actividades de garantía:

a) La evaluación, que proporciona confianza en los productos de las fases en que no es posible la verificación (por ejemplo, las fases de caracterización de las amenazas y de especificación de requisitos de seguridad informática). Debido a la naturaleza de la información respecto a la cual se formulan los requisitos de seguridad informática (por ejemplo, estimaciones de la amenaza, hipótesis sobre los modos de fallo de las funciones de la instalación en caso de que los sistemas se vean comprometidos), el explotador no puede estar seguro de que los requisitos sean correctos. Por lo tanto, la evaluación es necesaria para que el explotador tenga confianza en los productos de la fase de especificación de los requisitos de seguridad informática, es decir, el CSP y la DCSA.

b) La verificación, que permite confirmar que los resultados de una fase cumplen los objetivos y requisitos definidos para esa fase. En la medida de lo posible, las actividades de verificación tienen lugar entre fases sucesivas de la CSRM de la instalación y a nivel de sistemas. Esto puede conllevar una serie de métodos o análisis basados en el rendimiento para verificar los productos de cada fase antes de contribuir con ellos a una fase posterior.
c) La validación, que corresponde al proceso de determinar si la seguridad informática de la instalación proporciona una protección adecuada contra la amenaza (tal como se define en la caracterización de las amenazas) y cumple los requisitos reglamentarios.

Evaluación

4.92. El explotador debería evaluar el CSP y la DCSA con el fin de verificar que su implantación será eficaz para reducir la posibilidad de que los adversarios comprometan los sistemas que realizan funciones de la instalación, concretamente por los siguientes medios:

a) la determinación y asignación de funciones a niveles de seguridad informática;
b) la asignación de medidas de seguridad informática a esos niveles, y
c) especificaciones relativas a las medidas de seguridad informática.

4.93. La evaluación del CSP y de la DCSA debería incluir pruebas funcionales y de rendimiento en cumplimiento de los requisitos reglamentarios. La evaluación debería tener en cuenta, según convenga, la CSRM tanto de la instalación como a nivel de sistemas y todo el período de vida de la instalación.

4.94. El explotador debería considerar la posibilidad de recurrir a expertos independientes para examinar su CSP y DCSA.

4.95. El explotador debería justificar todas las hipótesis relativas a la probabilidad de que se produzcan ataques o de que estos prosperen (por ejemplo, la vulnerabilidad, la exposición, la oportunidad) que se utilicen en la evaluación. Debería suponerse que la probabilidad es 1 para los escenarios propuestos que puedan dar lugar a consecuencias radiológicas inaceptables[33] o a la retirada no autorizada de material nuclear (es decir, situaciones en que los SDA se vean comprometidos).

[33] En la referencia [8] se ofrece orientación sobre la definición de consecuencias radiológicas inaceptables.

4.96. La declaración nacional de amenazas o la ABD y la evaluación de las amenazas específica de la instalación sirven de base para que el explotador pueda realizar un análisis que confirme las hipótesis formuladas durante la asignación de funciones de la instalación al nivel de seguridad informática adecuado. El uso de escenarios funcionales creíbles (párrafo 4.120 a)) puede ofrecer un mayor nivel de garantía respecto a la calidad de la evaluación (véase el anexo I para ejemplos de escenarios).

4.97. Las medidas de seguridad informática basadas en el CSP y la DCSA proporcionan funciones de detección, dilación y respuesta a través de medidas de control físico (p. ej., instalación), técnico (p. ej., cortafuegos) y administrativo (p. ej., personal, procedimientos). La interacción de estas medidas de seguridad informática con las funciones de la instalación que son importantes para la seguridad tecnológica y la seguridad física, y los sistemas que tienen asignados, plantea dificultades a la hora de evaluar la eficacia del CSP.

4.98. Existen diversos métodos de evaluación, entre ellos los siguientes:

a) El análisis por árboles de ataque (también denominado "análisis por vectores de ataque" y "análisis por grafos de ataque"). Consiste en proponer un conjunto de diversas rutas posibles del adversario para determinar si existe un alto nivel de garantía de que cada ataque fracase (es decir, que pueda impedirse que el adversario continúe por la ruta) o sea detectado y se responda a este antes de que el adversario alcance el objetivo. El análisis por árboles de ataque puede servir, con la caracterización de las amenazas, para evaluar si las medidas basadas en el CSP y la DCSA son eficaces a la hora de eliminar o reducir al mínimo la posibilidad de que los ataques del adversario planteados prosperen.
b) La simulación. Esto incluye simulaciones informáticas de elementos del CSP (incluida la DCSA) y ejercicios de escritorio que permiten considerar los planes de seguridad física y contingencia, así como la toma de decisiones por parte del adversario y de los responsables de la respuesta a incidentes de seguridad informática. Estas herramientas sirven para evaluar el funcionamiento global del CSP, teniendo en cuenta todas las medidas. Por ejemplo, los ejercicios de escritorio podrían ayudar a determinar las oportunidades de que dispone un adversario en función de sus capacidades y características (por ejemplo, si son agentes internos), o las vulnerabilidades de la función.
c) Ejercicios. Pueden incluir pruebas de funcionamiento tanto a nivel de la instalación como a nivel de sistemas (por ejemplo, pruebas de penetración), así como simulacros de ataque por personal designado (por ejemplo, para

ataques combinados), ya sea sobre el terreno o en condiciones de prueba. Estos ejercicios pueden abordar la eficacia del CSP a la hora de proporcionar protección a toda la instalación, a partes de ella o a conjuntos específicos de sistemas o medidas frente al ataque simulado de un adversario. En esta actividad de evaluación, se recogen datos relativos al funcionamiento de las medidas de seguridad informática, que se utilizan para evaluar la eficacia global del CSP.

4.99. La simulación y los ejercicios suelen realizarse como parte del análisis basado en escenarios, en el que los ataques planteados (escenarios) se especifican en detalle y se simulan o se utilizan como base para los ejercicios. El análisis basado en escenarios suele complementar el análisis por árboles de ataque examinando tácticas y técnicas específicas que utiliza el adversario para superar las medidas de seguridad informática.

4.100. La eficacia del CSP, de la DCSA o de las distintas medidas de seguridad informática puede evaluarse cuantitativa o cualitativamente, o de ambas formas. La autoridad competente puede prescribir los métodos de evaluación determinista que han de utilizarse para los distintos tipos de blanco, amenaza y escenario. Se propone que la eficacia global del CSP y de la DCSA se defina de forma prudente como el nivel mínimo de eficacia que sigue cumpliendo los objetivos reglamentarios una vez que se han considerado todas las tácticas y técnicas del adversario y escenarios creíbles.

Verificación

4.101. El objetivo de la verificación en este contexto es evaluar la calidad de los productos de una fase con respecto a las especificaciones antes de que estos se utilicen en una fase posterior.

4.102. En la medida de lo posible, la verificación debería tener lugar entre fases sucesivas de la CSRM de la instalación o a nivel de sistemas.

4.103. Los resultados de la verificación pueden dar lugar a la adopción de las siguientes medidas por parte del explotador:

a) subsanar toda deficiencia en el diseño o la aplicación de las medidas de seguridad informática para cumplir los requisitos, y
b) determinar, analizar y aplicar las actualizaciones que puedan ser necesarias para subsanar las deficiencias detectadas y mejorar el rendimiento.

4.104. Estas actividades de verificación pueden incluir métodos de evaluación, como ejercicios, pruebas de rendimiento, simulaciones o análisis (por ejemplo, la evaluación de la vulnerabilidad) (véase el párrafo 4.98).

4.105. Por ejemplo, la evaluación de los productos basada en el análisis por árboles de ataque tiene en cuenta el flujo de información entre sistemas, dispositivos, redes y ubicaciones. El intercambio de información entre sistemas puede permitir que los adversarios exploten estas rutas, lo que podría comprometer los sistemas y, por consiguiente, las funciones de la instalación. El análisis por árboles de ataque en esta etapa tiene en cuenta las rutas genéricas con el objetivo de reducir al mínimo o eliminar la posibilidad de que un adversario consiga acceder a ellas.

4.106. El explotador debería utilizar un enfoque graduado a la hora de determinar el nivel de esfuerzo que corresponda aplicar a la verificación y validación. El mayor nivel de esfuerzo debería aplicarse a las funciones o sistemas que se hayan asignado a los niveles de seguridad informática más estrictos (es decir, los que requieran el mayor nivel de protección).

4.107. La verificación debería repetirse de forma periódica (por ejemplo, anualmente) o según convenga para tener en cuenta cualquier cambio en los blancos o en los requisitos del programa de seguridad física nuclear.

Validación

4.108. El explotador debería validar que los sistemas, una vez integrados, tengan el nivel de protección adecuado para cumplir los requisitos de seguridad informática que se especifican en el CSP y la DCSA. La figura 7 ilustra las actividades de verificación y validación en el marco del proceso de la CSRM, el CSP y la DCSA.

4.109. El explotador debería validar que los sistemas, tal y como están instalados en la instalación, tengan el nivel adecuado de protección de seguridad informática para realizar las correspondientes funciones de la instalación de modo que cumplan los requisitos relativos a la seguridad física de la instalación.

4.110. El explotador debería validar que el nivel de protección de seguridad informática sea suficiente para garantizar que la explotación de la instalación cumpla los requisitos reglamentarios o los requisitos del explotador que se especifican en los requisitos de seguridad física de la instalación.

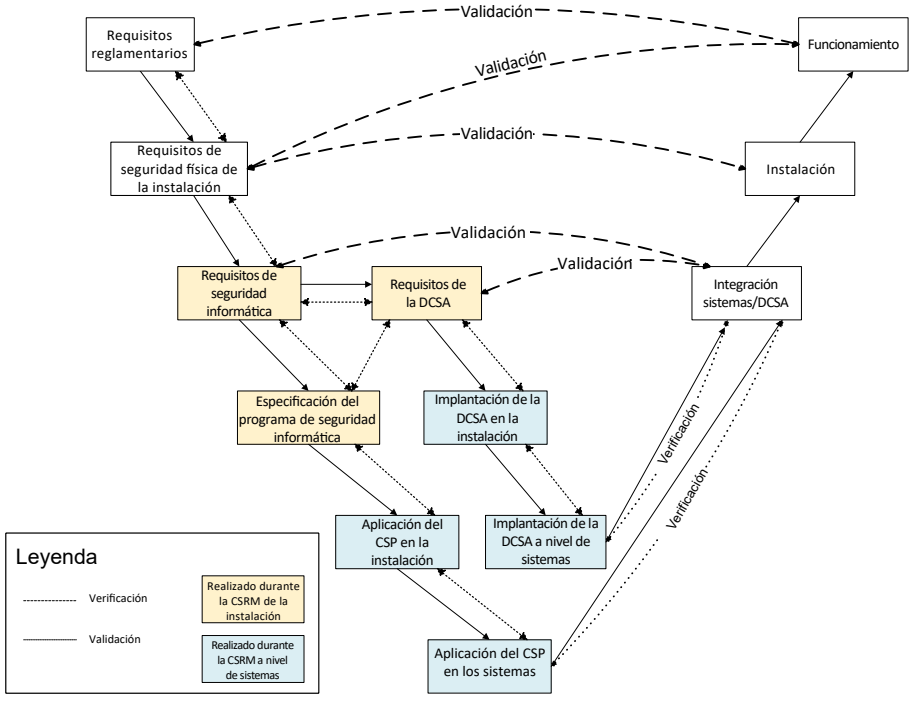


Figura 7. Visión general de las actividades de verificación y validación en el marco del proceso de gestión de riesgos de seguridad informática (CSRM). CSP: programa de seguridad informática; DCSA: arquitectura defensiva de seguridad informática.

4.111. En caso de que la validación indique que el nivel de protección no es suficiente, el explotador debería revisar su CSP y DCSA para aumentar la protección. El explotador no puede reducir el nivel de protección sin la conformidad de la autoridad competente.

4.112. El explotador debería validar los productos de los procesos de la CSRM de la instalación y a nivel de sistemas. Los productos de la CSRM de la instalación deberían validarse con respecto a los requisitos reglamentarios y del explotador. Los productos de la CSRM a nivel de sistemas deberían cumplir los requisitos del CSP y la DCSA.

4.113. El explotador debería tener en cuenta el nivel de riesgo agregado de la instalación, incluida la referencia a los requisitos reglamentarios y de diseño aplicables. Ello también debería incluir el nivel de riesgo a nivel de sistemas para cada sistema que contenga un SDA.

4.114. El explotador debería validar las evaluaciones de riesgos a nivel de instalación y sistemas con respecto a la declaración nacional de amenazas o la ABD utilizando escenarios que impliquen ataques que afecten a múltiples sistemas y a la arquitectura global. Estos escenarios difieren de los utilizados en la CSRM a nivel de sistemas (párrafo 5.5 j)) y los especificados en la declaración nacional de amenazas o la ABD. Pueden incluir ataques combinados que comprometan diversos sistemas independientes con el objetivo de detectar vulnerabilidades en algún punto de la instalación.

4.115. La validación completa de los resultados tanto de la CSRM de la instalación como de la CSRM a nivel de sistemas debería tener en cuenta los escenarios técnicos y funcionales que se describen a continuación.

Determinación y elaboración de escenarios

4.116. El explotador debería determinar y elaborar escenarios basados en la evaluación de las amenazas por parte del Estado con arreglo a lo dispuesto en la declaración nacional de amenazas o la ABD y, según convenga, la evaluación de amenazas específica de la instalación. Se recomienda encarecidamente a los explotadores que incluyan a expertos en ciberataques y capacidades de amenaza conexas en la elaboración de estos escenarios. Esta pericia puede encontrarse en las autoridades competentes, los servicios de inteligencia y las fuerzas del orden. Podría exigirse al explotador que presente estos escenarios detallados a la autoridad competente para someterlos a examen y aceptación.

4.117. El análisis de escenarios podría aportar una mejor comprensión de los puntos más vulnerables de la instalación, los procesos, las arquitecturas de sistemas y los procedimientos. Podría ser necesario realizar un análisis más detallado para determinar las medidas de seguridad informática ya implantadas o las que sea necesario añadir con el fin de hacer frente a las vulnerabilidades detectadas.

4.118. Los escenarios deberían servir para verificar los resultados de la evaluación de riesgos para la seguridad informática de la instalación, incluidos el análisis de las posibles tácticas de los adversarios, la probabilidad de ataque y las posibles consecuencias.

4.119. Los escenarios deberían reevaluarse periódicamente de modo que sigan siendo adecuados para cumplir los objetivos de seguridad frente a cambios en las amenazas.

4.120. Hay dos categorías de escenarios:

a) Escenarios funcionales, que son escenarios basados en las evaluaciones de amenazas y que reflejan los posibles efectos sobre las funciones de la instalación en caso de que se vean comprometidos los sistemas que realizan dichas funciones. Estos escenarios incluyen los que implican sabotajes que dan lugar a consecuencias radiológicas inaceptables y la retirada no autorizada de material nuclear. Los escenarios funcionales también pueden servir para determinar dependencias fundamentales entre funciones o sistemas.
b) Escenarios técnicos, que son escenarios basados en la implantación técnica específica de medidas de seguridad informática y que incluyen información detallada sobre la implantación real o potencial de activos digitales. Estos escenarios pueden evaluarse mediante ejercicios de escritorio o basados en el funcionamiento, lo cual suele formar parte de la verificación y validación de los productos de la CSRM de la instalación y a nivel de sistemas.

4.121. Estos escenarios se elaboran y analizan entre las fases de la CSRM de la instalación y la CSRM a nivel de sistemas, y dentro de los elementos de la CSRM de la instalación, según convenga, para su análisis. Estos escenarios son necesarios para aumentar la confianza en los productos de la fase de especificación de requisitos, pero también pueden servir para formular dichos requisitos. El conjunto de escenarios utilizados en el análisis para formular los requisitos no puede ser idéntico al conjunto de escenarios utilizados en las actividades de garantía.

4.122. Los escenarios en cuestión deberían incluir múltiples rutas de ataque (por ejemplo, a través de diferentes redes y sistemas locales), ataques en que participen agentes internos y ataques combinados. También deberían incluir la posibilidad de que se produzcan ciberataques secuenciales que multipliquen las consecuencias pero que no muestren indicios de connivencia entre diferentes adversarios (ataques no colaborativos).

4.123. Los escenarios pueden incluir lo siguiente:

a) ataques independientes por parte de un único adversario;
b) ataques coordinados por un grupo de adversarios que trabajan juntos;
c) ataques oportunistas, en los que adversarios independientes logran crear un ataque combinado. Por ejemplo, un adversario revela públicamente una vulnerabilidad, lo que permite a otros adversarios dirigir su ataque contra los sistemas y equipos de la instalación;
d) capacidades específicas de la amenaza [9], y

e) ataques combinados con elementos cibernéticos y físicos coordinados.

El análisis por árboles de ataque puede ayudar a determinar escenarios de amenazas, así como a determinar estrategias de protección.

4.124. Los escenarios deberían examinarse y actualizarse de forma periódica en los siguientes casos:

a) cuando se actualice la declaración nacional de amenazas o la ABD;
b) cuando se lleve a cabo una modificación importante de la instalación;
c) cuando se introduzcan cambios en los procesos de seguridad física, las contramedidas fundamentales y las arquitecturas;
d) cuando se detecten nuevas rutas de ataque creíbles;
e) cuando se introduzcan nuevos requisitos reglamentarios;
f) cuando se tenga conocimiento de nuevas vulnerabilidades críticas[34], especialmente las que afecten a medidas importantes de seguridad informática, y
g) cuando cambie la caracterización de las amenazas.

4.125. Con respecto a los escenarios más relevantes, deberían determinarse vectores y componentes de ataque específicos y documentarse sus riesgos.

PRODUCTO DE LA GESTIÓN DE RIESGOS DE SEGURIDAD INFORMÁTICA EN LA INSTALACIÓN

4.126. La documentación del CSP de la instalación debería describir las medidas de seguridad informática necesarias para mantener la protección contra los adversarios que se han analizado durante la evaluación.

4.127. El producto de la CSRM de la instalación debería comprender la documentación del CSP de la instalación y una determinación del riesgo agregado de la instalación basada en una evaluación de la eficacia de las medidas que, según el CSP, ofrecen protección contra los adversarios descritos en la declaración nacional de amenazas o la ABD.

[34] Por ejemplo, el Sistema Común de Puntuación de Vulnerabilidades, versión 3.0, señala como "críticas" (es decir, con una puntuación de 9,0 a 10) aquellas vulnerabilidades que son explotables en red, que tienen una complejidad de ataque baja, y que comprometen por completo la confidencialidad, la integridad y la disponibilidad.

4.128. El informe de la CSRM de la instalación debería incluir un examen y análisis generales del diseño del sistema de seguridad física y de la gestión de la configuración, con arreglo a lo dispuesto en el CSP. Durante la CSRM a nivel de sistemas debería realizarse un análisis más detallado.

4.129. Las funciones de la instalación y sus correspondientes sistemas en el producto de la CSRM de la instalación deberían abordarse en evaluaciones de riesgos exhaustivas a nivel de sistemas, tal como se describe en la sección 5.

4.130. Debería facilitarse a la autoridad competente la evaluación por parte del explotador del riesgo asociado a las diferentes funciones y del riesgo agregado de la instalación.

5. GESTIÓN DE RIESGOS DE SEGURIDAD INFORMÁTICA A NIVEL DE SISTEMAS

CONSIDERACIONES GENERALES

5.1. El explotador debería establecer un proceso sistemático y sometido a examen periódico que gestione el riesgo de seguridad informática para los activos digitales, incluidos los SDA, dentro de los sistemas que realizan las funciones de la instalación que se han determinado en el proceso de CSRM de la instalación[35]. En caso de que se comprometan los SDA, las consecuencias suelen tener distintos niveles de gravedad (como se describe en la referencia [7]). La CSRM de la instalación debería incluir la CSRM a nivel de sistemas para cada sistema, como se describe en la presente sección. La CSRM a nivel de sistemas debería tener en cuenta todos los activos digitales del sistema, incluidos los SDA.

5.2. La CSRM a nivel de sistemas debería ser realizada por un equipo multidisciplinario parecido al de la CSRM de la instalación. No obstante, la composición del equipo de CSRM a nivel de sistemas puede adaptarse para atender consideraciones específicas asociadas a cada sistema.

[35] Podría estar justificado ampliar este análisis con el fin de incluir otros sistemas excluidos del alcance de la evaluación de riesgos para la seguridad informática de la instalación que no estén relacionados directamente con los objetivos de la seguridad física nuclear.

5.3. El explotador debería utilizar un enfoque graduado a la hora de determinar el nivel de esfuerzo que ha de aplicarse a la gestión de riesgos para cada sistema. El mayor nivel de esfuerzo debería aplicarse a los sistemas que realicen o apoyen las funciones de la instalación asignadas a los niveles de seguridad informática más estrictos (es decir, que requieren el mayor nivel de protección), con arreglo a lo dispuesto en el proceso de CSRM de la instalación.

VISIÓN GENERAL

5.4. El objetivo principal de la CSRM a nivel de sistemas es evaluar y gestionar las medidas de seguridad informática para garantizar que estas proporcionen el nivel de protección adecuado al sistema específico (es decir, el necesario para su nivel de seguridad informática), con arreglo a los requisitos definidos en el producto de la CSRM de la instalación.

5.5. Para cumplir este objetivo, la CSRM a nivel de sistemas incluye los siguientes pasos:

a) Evaluar cada función de la instalación, los sistemas asignados para realizar la función y el nivel de seguridad informática aplicado a dichos sistemas — teniendo en cuenta otras funciones de la instalación para las que se hayan determinado interacciones e interdependencias en la fase de caracterización de la instalación de la CSRM de la instalación — con el fin de definir los límites funcionales de los sistemas.
b) Determinar el alcance de cada sistema, incluidos los sistemas que apoyan otras funciones de la instalación que interactúan con la función realizada por el sistema y dependen de ella. Esto puede incluir el análisis de la arquitectura general de sistemas para determinar las ubicaciones, los límites, las interfaces y las vías de comunicación de los sistemas que contienen activos digitales, incluidos los SDA.
c) Determinar los activos digitales dentro de esos sistemas (y crear el correspondiente inventario).
d) Definir y establecer zonas de seguridad informática sobre la base de los requisitos que se hayan determinado en el CSP de la instalación y la DCSA.
e) Determinar los SDA y otros activos digitales dentro de los límites de zona mediante el análisis de activos, que consiste en una evaluación de los activos digitales para determinar si son esenciales para realizar la función de la instalación.

f) Asignar activos digitales, incluidos los SDA, al nivel de seguridad informática que se haya asignado en el producto de la CSRM de la instalación a la función de seguridad física o tecnológica que realizan en la instalación.
g) Aplicar a toda la zona el nivel de seguridad informática más estricto asignado a cualesquiera de las funciones que proporcionan los activos digitales dentro de la zona, y asignar todos los activos digitales dentro de la zona a ese nivel.
h) Aplicar medidas de seguridad informática de referencia (véanse los párrafos 4.58 y 4.68) y medidas adicionales de seguridad informática a los SDA y otros activos digitales (incluso en los límites de zona), teniendo en cuenta las especificidades de los sistemas que se hayan determinado para cumplir los requisitos de los niveles de seguridad informática asignados.
i) Facilitar un proceso para determinar las medidas de control técnico, las medidas de control administrativo o las medidas de control físico que pueden aplicarse para cumplir las medidas de seguridad informática de referencia.
j) Analizar rutas de ataque, escenarios y vulnerabilidades específicos para verificar la eficacia de las medidas de seguridad informática aplicadas.
k) Si el análisis muestra que un sistema no está suficientemente protegido por las medidas de seguridad informática de referencia, aplicar medidas adicionales o compensatorias para reducir el riesgo a un nivel aceptable.
l) Elaborar un informe de la CSRM a nivel de sistemas para el sistema que se haya determinado.

5.6. Este proceso puede dar lugar a la determinación de otros activos digitales que no formaban parte de los sistemas asignados a funciones de la instalación durante la CSRM de la instalación, o respecto a los cuales se determinó que estaban fuera del límite de un sistema o zona durante la CSRM a nivel de sistemas. En tales casos, debería realizarse un análisis adicional para garantizar la inclusión de todos los activos digitales conexos en la evaluación y el CSP.

5.7. Los productos de la CSRM a nivel de sistemas deberían incluir la priorización de riesgos dentro del sistema para determinar la aplicación adecuada de medidas de seguridad informática. El proceso debería tener en cuenta la ubicación de los componentes que integran el sistema, las vulnerabilidades y los niveles y zonas de seguridad informática, si están definidos, así como la importancia de los SDA y otros activos digitales dentro del sistema que se evalúa.

PROCESO DE LA GESTIÓN DE RIESGOS DE SEGURIDAD INFORMÁTICA A NIVEL DE SISTEMAS

5.8. El explotador debería realizar la CSRM a nivel de sistemas en los siguientes casos:

a) cuando se construya una instalación por primera vez (para cada sistema);
b) cuando se modifique una instalación (para cada sistema);
c) cuando se implante un nuevo sistema o activo digital (para cada sistema afectado);
d) cuando se modifique un sistema o activo digital (para cada sistema afectado), y
e) cuando se revise el proceso de CSRM de la instalación (para cada sistema).

5.9. Deberían determinarse las siguientes aportaciones y se debería facilitar su uso durante la CSRM a nivel de sistemas:

a) los productos de la CSRM de la instalación (por ejemplo, las especificaciones del CSP y la DCSA);
b) el informe de análisis de la seguridad;
c) el plan de seguridad física del emplazamiento, y
d) la política de seguridad informática.

Requisitos generales de la arquitectura defensiva de seguridad informática para la seguridad informática

5.10. El explotador debería utilizar los requisitos correspondientes a la DCSA establecidos durante la CSRM de la instalación para elaborar, aplicar y mantener medidas de seguridad informática destinadas a los sistemas y activos digitales con el fin de prevenir, detectar y retrasar los ciberataques, mitigar sus efectos y recuperarse tras estos.

5.11. Las medidas de seguridad informática deberían ser eficaces durante todo el período de vida de la instalación, por ejemplo, durante los períodos de mantenimiento y clausura, cuando pueden introducirse cambios importantes en la configuración. Las actividades de vigilancia, mantenimiento y recuperación no deberían proporcionar medios que permitan a un adversario eludir las medidas de seguridad informática, por ejemplo, eludiendo la protección de las vías de comunicación entre funciones de la instalación que tienen diferentes niveles de seguridad informática.

5.12. Deberían aplicarse límites de seguridad informática[36] entre zonas de seguridad informática, los cuales deberían protegerse utilizando diferentes medidas de seguridad informática.

5.13. Debería controlarse el flujo de datos entre zonas de diferentes niveles de seguridad informática y entre zonas del mismo nivel de seguridad informática, utilizando un enfoque basado en el conocimiento de los riesgos, para garantizar que la DCSA siga siendo eficaz.

Definición de los límites de sistemas

5.14. El límite de sistemas define el alcance de la CSRM de cada sistema y abarca los sistemas respecto a los cuales se haya determinado que proporcionan una función concreta de la instalación sobre la base de la caracterización de la instalación. Ello debería tener en cuenta las interdependencias entre las funciones de la instalación y los sistemas correspondientes.

5.15. La CSRM a nivel de sistemas debería incluir la determinación y documentación de los límites de sistemas. Ello incluye todos los componentes, subcomponentes, interfaces y entornos del sistema en cuestión durante todas las etapas del período de vida de la instalación, así como aquellos otros sistemas que proporcionan funciones auxiliares o de apoyo.

5.16. Pueden utilizarse los siguientes pasos para definir los límites del sistema que se evalúa:

a) Determinar todas las interfaces del sistema.
b) Determinar todos los puntos en que los datos entran y salen del sistema (puntos en que es probable que un adversario intente introducir un código malicioso). En la evaluación de riesgos de seguridad del sistema debería tenerse en cuenta cualquier medio que pueda utilizarse para introducir un código malicioso en el sistema. Por ejemplo, podría introducirse un código malicioso a través de conexiones de comunicación, productos y servicios suministrados, o dispositivos portátiles que estén conectados temporalmente al equipo objeto de ataque.

[36] En la presente publicación, los "límites de seguridad informática" se definen como los límites lógicos y físicos de un sistema o un conjunto de sistemas con el mismo nivel de seguridad que, por tanto, pueden protegerse mediante la aplicación de medidas comunes de control de la seguridad física (es decir, zonas de seguridad informática).

c) Determinar los procedimientos que conllevan una interacción con el sistema durante el funcionamiento normal y en circunstancias específicas (por ejemplo, la aplicación de parches).
d) Determinar qué vías de datos (de haberlas) no son utilizadas por ningún procedimiento durante el funcionamiento y mantenimiento del sistema. Las vías de datos no utilizadas representan una vulnerabilidad importante.
e) Determinar el nivel de seguridad informática asignado al sistema (a partir del producto de la CSRM de la instalación).
f) Enumerar las medidas de seguridad informática aplicadas al sistema o a su entorno.

Definición y establecimiento de zonas de seguridad informática

5.17. Las especificaciones del CSP y la DCSA elaboradas durante la CSRM de la instalación imponen requisitos de seguridad informática con respecto a la aplicación del modelo de zonas. El CSP también incluirá una lista de las funciones de la instalación y los sistemas asignados a las mismas.

5.18. El explotador debería aplicar medidas de seguridad informática que cumplan los requisitos establecidos en la especificación de la DCSA. Al hacerlo, también debería tenerse en cuenta el cumplimiento de los siguientes criterios [8]:

a) Los sistemas que pertenecen a la misma zona forman un área de confianza para las comunicaciones internas entre esos sistemas, y el nivel de seguridad informática aplicado a toda una zona que cuenta con un área de confianza de ese tipo es el más estricto de los asignados a los sistemas implicados.
b) Se mantienen los requisitos de la arquitectura de seguridad tecnológica (por ejemplo, redundancia, diversidad, separación física y eléctrica, criterio del fallo único).
c) La defensa en profundidad se aplica tanto dentro de cada zona de seguridad informática (utilizando medidas diversas, independientes y superpuestas de control administrativo, físico y técnico), como entre zonas de seguridad informática.
d) Las medidas de control técnico que proporcionan medidas preventivas o protectoras continuas o automáticas (es decir, que no requieren intervención humana) complementan las medidas de control físico o administrativo (es decir, que requieren intervención humana), según convenga.
e) Todas las conexiones entre zonas disponen de mecanismos de desacoplamiento para el flujo de datos, que funcionan con arreglo a normas sujetas a zonas para impedir el acceso no autorizado e interacciones no

deseadas entre las zonas. Ello incluye las conexiones de red continuas y las conexiones intermitentes, por ejemplo, mediante soportes extraíbles.

f) El nivel de desacoplamiento entre zonas depende de los niveles de seguridad informática de ambas zonas. Las medidas de desacoplamiento incluyen medidas de control técnico, como filtros de paquetes, cortafuegos y diodos de datos, en los límites de zona para restringir el flujo de datos y la comunicación entre diferentes zonas.

g) Las comunicaciones permitidas entre zonas de diferentes niveles de seguridad siguen los requisitos especificados para los niveles implicados en el CSP. La formulación de requisitos para las comunicaciones permitidas puede tener en cuenta los modelos de confianza (véase el párrafo 4.83).

h) Si los requisitos del CSP permiten que los SDA de zonas asignadas a distintos niveles de seguridad se comuniquen, la conexión puede ser iniciada solamente por el SDA asignado al nivel de seguridad informática más alto (más estricto). Los SDA que realizan funciones de gestión de la información de carácter estratégico no suelen permitir la comunicación desde un nivel superior a uno inferior (es decir, la información fluye en sentido contrario), con arreglo al modelo de confianza de Bell-LaPadula (véase el párrafo 4.83).

i) Si la comunicación iniciada por el SDA que está sujeto al nivel inferior de seguridad informática[37] es inevitable e incumple el correspondiente modelo de confianza, se utilizan mecanismos de desacoplamiento excepcionalmente estrictos.

j) El acceso lógico o físico a los activos digitales de una zona mediante dispositivos móviles u otros equipos temporales autorizados se trata como una forma de conexión intermitente a dicha zona y está sujeto a las medidas de seguridad informática correspondientes tanto a la zona establecida como a los dispositivos conectados temporalmente. Dichos dispositivos están sujetos a medidas de seguridad informática adicionales si se conectan a más de una zona.

k) Las zonas pueden dividirse en subzonas para mejorar la configuración y evitar interacciones no deseadas con otros sistemas.

[37] Algunos Estados Miembros no permiten que la dirección de las comunicaciones vaya desde los niveles inferiores a los niveles superiores en el caso de instalaciones en que puedan producirse consecuencias graves o muy graves. En otros tipos de instalaciones (por ejemplo, instalaciones del ciclo del combustible nuclear, reactores modulares pequeños), la autoridad competente puede dejar a discreción del explotador la aplicación de rutas bidireccionales.

5.19. Debería considerarse la posibilidad de separar los activos digitales en distintas zonas cuando se cumpla alguna de las siguientes condiciones:

a) Los activos digitales pertenecen a sistemas que realizan distintas funciones de la instalación.
b) Los sistemas que contribuyen a la misma función de la instalación tienen asignados diferentes niveles de seguridad informática.
c) Los sistemas que contribuyen a la misma función de la instalación y tienen asignado el mismo nivel de seguridad informática son gestionados por dependencias institucionales diferentes.
d) Los servidores se comunican con múltiples clientes (por ejemplo, los utilizados con sistemas de control distribuido y controladores lógicos programables). La zona que requiera la protección más estricta debería contener el menor número posible de activos singulares.
e) Los sistemas necesitan comunicarse con componentes de infraestructura comunes utilizados por varios sistemas (por ejemplo, directorios, servidores de hora, recopiladores de registros de seguridad), pero no entre sí. Es necesario supervisar y controlar la comunicación entre las zonas que contengan estos tipos de sistemas y las zonas que contengan los componentes de infraestructura comunes.
f) Los sistemas son sistemas de administración (especialmente cuando se utilizan los mismos sistemas para administrar varios sistemas funcionales).
g) Los reglamentos exigen zonas diferenciadas.

5.20. Se podrá considerar la posibilidad de asignar activos digitales a zonas diferentes, a pesar de tener asignado el mismo nivel de seguridad informática, en los siguientes casos:

a) Los activos digitales están en sistemas que realizan distintas funciones de la instalación. En tales casos, la asignación de activos digitales a diferentes zonas puede mejorar la separación de las zonas y sistemas que contribuyen a una función de la instalación.
b) Diferentes dependencias institucionales se encargan de diferentes activos digitales.
c) Hay activos digitales aislados, o varios activos digitales del mismo sistema funcional están alojados en una red aislada.
d) Es necesario asignar a distintas zonas los sistemas redundantes independientes que realizan la misma función de la instalación.
e) Los reglamentos exigen la separación de los activos digitales.

5.21. Las conexiones de red y los intercambios locales (por ejemplo, a través de soportes extraíbles o dispositivos móviles) de datos entre sistemas de distintas zonas deberían limitarse únicamente a aquellos que sean esenciales. Cuando las conexiones de red a través de las fronteras de zona sean esenciales, estas deberían establecerse desde la zona con el nivel de seguridad informática más alto a la zona con el nivel de seguridad informática más bajo. Pueden aplicarse restricciones mediante el uso de medidas de control técnico (por ejemplo, dispositivos de filtrado) o medidas de control administrativo (por ejemplo, normas para el uso de soportes extraíbles en un sistema específico). Deberían documentarse las conexiones de red y los métodos que estén permitidos para el intercambio de datos en modo desconectado.

5.22. Una zona específica solo puede incluir sistemas (y activos digitales) del mismo nivel de seguridad informática. A la zona se le asigna el nivel de seguridad informática de los sistemas que están dentro de esta. Un determinado nivel de seguridad informática puede y debería aplicarse a diferentes zonas. Sin embargo, en algunos casos concretos puede resultar difícil separar en zonas diferentes los sistemas asignados a distintos niveles de seguridad informática. En tales casos, algunos sistemas podrían formar parte de una zona que tenga asignado un nivel de seguridad informática más estricto del que necesitan.

5.23. Solo deberían permitirse comunicaciones entre zonas del mismo nivel de seguridad informática o niveles adyacentes. Las comunicaciones entre zonas con diferentes niveles de seguridad informática deberían limitarse a puntos de entrada de zona específicos (por ejemplo, un punto de entrada que filtre las conexiones entre zonas con nivel 2 de seguridad informática y zonas con nivel 3 de seguridad informática). Las medidas de seguridad relativas a todos los puntos de entrada deberían definirse de manera eficiente y sistemática para lograr que la arquitectura general sea segura. Deberían aplicarse controles específicos en un punto de entrada de zona, por ejemplo, con respecto al contenido de los datos (por ejemplo, rangos aceptables de valores de parámetros) que entran o salen, o la firma digital de los datos. Los puntos de entrada de zona también deberían tener un control específico de registro de incidentes.

Determinación de los activos digitales

5.24. A la hora de determinar los activos digitales de un sistema deberían consultarse los siguientes registros:

a) la base de datos de activos del sistema (de todos los componentes digitales);
b) el inventario de *software* y soporte lógico inalterable;

c) listas de información de carácter estratégico relacionada con el sistema [5];
d) diagramas de la red y la arquitectura del sistema;
e) documentos relativos al diseño de la instalación, como el informe de análisis de la seguridad o los informes de pruebas;
f) diagramas del flujo de datos;
g) la lista de cuentas y privilegios de usuarios y del sistema, y
h) procedimientos relacionados con el sistema señalado.

5.25. La lista de activos digitales puede incluir sus identificadores, datos y especificaciones técnicas clave, descripciones de sus interfaces, referencias a evaluaciones de riesgos a nivel de instalación y sistemas, y los propietarios a los que se han asignado.

5.26. La lista de activos digitales debería mantenerse durante el período de vida de la instalación y someterse a un examen periódico. La lista también debería examinarse y actualizarse, según convenga, cada vez que se realice una evaluación de riesgos a nivel de sistemas.

5.27. Los activos digitales que también sean recursos de información de carácter estratégico deberían denominarse SDA. Los activos digitales que puedan facilitar un efecto adverso sobre la función de los SDA, o contribuir a este, también deberían señalarse y considerarse en el análisis de activos digitales para determinar, en consonancia con el CSP, si deberían denominarse SDA.

5.28. La lista de SDA debería clasificarse y protegerse como información de carácter estratégico.

Arquitectura de seguridad informática de los sistemas, incluido el análisis de los activos digitales

5.29. El explotador debería determinar las tareas y actividades clave que sean necesarias para proporcionar seguridad informática a la instalación. Estas tareas y actividades deberían asociarse a niveles de seguridad informática y a las correspondientes medidas de seguridad informática. El explotador debería velar por que se disponga de las capacidades y los recursos necesarios para realizar dichas tareas y actividades.

5.30. El proceso de CSRM a nivel de sistemas debería determinar todos los SDA. También puede ser necesario incluir los activos digitales que no son SDA en el análisis de amenazas específicas o tipos de ataque si el hecho de que se vean comprometidos podría afectar negativamente a un SDA. Debería calificarse el

nivel de esfuerzo asociado a la evaluación de riesgos a nivel de sistemas para garantizar que los sistemas a los que se asigne el nivel más alto de seguridad informática también se sometan a la evaluación más rigurosa.

5.31. Por lo general, debería asignarse el mismo nivel de seguridad informática a los sistemas que realizan la misma función de la instalación, incluidos los sistemas independientes, diferentes y redundantes. Se desaconseja vehementemente la asignación de un nivel de seguridad informática menos estricto a cualesquiera de estos sistemas, pudiendo considerarse solamente caso por caso si está respaldada por una justificación específica y un análisis de riesgos de seguridad.

5.32. El análisis de los SDA debería tener en cuenta información sobre el *hardware*, el soporte lógico inalterable y el *software* de dichos activos, lo cual puede contribuir a un análisis de vulnerabilidades. El análisis de vulnerabilidades puede dar lugar a la recomendación de llevar a cabo procedimientos para determinar, desactivar o eliminar servicios, puertos o interfaces innecesarios en el sistema (o la red) del SDA con el fin de reducir la superficie de ataque (es decir, fortalecimiento del sistema; véase el párrafo A.64).

5.33. Las interfaces de cada sistema (incluidos sus activos digitales) deberían analizarse y clasificarse con respecto al límite de zona. Pueden utilizarse las siguientes categorías:

a) Comunicaciones internas de confianza: Esta categoría incluiría las comunicaciones dentro de los sistemas y entre estos, o dentro de una zona o entre activos digitales dentro de un sistema, incluidas las vías internas para dispositivos en el límite de zona (por ejemplo, cortafuegos, diodos de datos). No existen medidas de seguridad informática que puedan controlar o proteger eficazmente las vías de comunicación interna de confianza frente a los ciberataques.
b) Comunicaciones externas autorizadas: Esta categoría incluiría las conexiones entre zonas a través de vías permitidas y dispositivos en el límite de zona autorizados. Dichas comunicaciones se establecen normalmente entre distintos sistemas que realizan diferentes funciones de la instalación. Las medidas de seguridad informática en forma de dispositivos en el límite de zona garantizan la monitorización continua de todas las vías de comunicación, ya sean digitales o analógicas, y que solo puedan utilizarse las que se hayan autorizado.
c) Posibles comunicaciones no autorizadas: Esta categoría incluiría la capacidad de realizar conexiones no autorizadas entre zonas, por ejemplo, utilizando cables de red, conexiones inalámbricas o soportes extraíbles. Dichas vías

de comunicación no autorizadas podrían realizarse entre sistemas o activos digitales que se encuentren en zonas diferentes, pero en proximidad física o lógica, por ejemplo, sistemas que se encuentren físicamente en la misma área sin que haya barreras físicas que controlen el acceso entre ellos.

5.34. Todos los activos digitales con vías de comunicación internas de confianza dentro de una zona deberían asignarse al mismo nivel de seguridad informática, es decir, el de la zona.

5.35. Los dispositivos en el límite de zona deberían asignarse a un nivel de seguridad informática equivalente al nivel más alto (más estricto) aplicado al equipo para el que han de ofrecer protección. Por ejemplo, un cortafuegos entre dos zonas de diferentes niveles de seguridad informática puede tener una vía de comunicación interna de confianza con la zona que tenga asignado el nivel de seguridad informática más alto, pero solo una vía de comunicación externa autorizada con la otra zona.

5.36. Otro ejemplo de dispositivo en el límite de zona puede ser un puesto de detección de programas maliciosos, o escáner antivirus, que sirve para analizar soportes extraíbles y dispositivos móviles antes de que entren y salgan de una zona. Este puesto tendría asignado el nivel de seguridad informática más alto aplicado a cualquier elemento de la zona para el que ha de ofrecer protección[38]. En este caso, el explotador ha de asegurarse de que el puesto no proporciona una ruta común que comprometa diferentes sistemas en diferentes zonas (por ejemplo, proporcionando una vulnerabilidad común que pueda ser explotada para comprometer diferentes sistemas).

5.37. Todos los activos digitales, incluidos los SDA, que estén conectados a través de una vía de comunicación interna de confianza deberían cumplir los requisitos generales de la DCSA. Las comunicaciones externas permitidas requieren medidas de seguridad informática adicionales (véase el párrafo 5.33 b)).

5.38. Puede permitirse que los SDA estén próximos (lógica o físicamente) a otros SDA siempre que existan medidas de seguridad informática que garanticen que estos sistemas no puedan interactuar a través de posibles vías de comunicación no autorizadas. Estas medidas podrían ser únicamente medidas de control

[38] Dichos puestos pueden resultar inadecuados para proteger los sistemas de nivel 1 o 2 debido a la dificultad de aplicar los requisitos de seguridad informática a un puesto autónomo. Además, los puestos que utilizan la detección de programas maliciosos basándose únicamente en "listas negras" o firmas no pueden proporcionar un alto nivel de protección.

administrativo. Normalmente, los SDA se asignan a los niveles de seguridad informática más altos (por ejemplo, niveles 1 a 3).

5.39. No debería permitirse que los activos digitales que no tengan autorización para comunicarse con SDA se encuentren en proximidad lógica o física con dichos activos cuando exista la posibilidad de que haya vías de comunicación no autorizadas. La DCSA debería prever la elaboración y el mantenimiento de medidas sólidas de seguridad informática para eliminar dichas vías o crear medidas compensatorias para reducir la posibilidad de que se utilicen.

5.40. Los activos digitales no asignados (es decir, los que no se han asignado a un nivel de seguridad informática) nunca deberían estar cerca de los SDA. Por ejemplo, los dispositivos móviles personales o el equipo de un proveedor que no hayan sido evaluados y asignados a un nivel concreto deberían tratarse como dispositivos potencialmente maliciosos para los SDA y no debería permitirse que estén cerca, lógica o físicamente, de los SDA de la instalación.

5.41. El análisis de activos debería incluir la evaluación de los efectos de escenarios creíbles de ciberataque en el sistema y el riesgo para la instalación. La evaluación debería tener en cuenta la posibilidad de que se produzcan ciberataques durante cualquier etapa del período de vida de la instalación o cualquier fase del ciclo de vida del sistema.

5.42. Los ciberataques podrían afectar a un solo sistema o a múltiples sistemas y podrían combinarse con otras formas de actos dolosos que provoquen daños físicos. Estas posibles interacciones específicas a nivel de componente deberían enumerarse en el informe de evaluación y evaluarse.

5.43. La evaluación debería tener en cuenta actos dolosos que puedan cambiar las señales de procesos, los datos de configuración de los equipos o el *software*.

5.44. El análisis de activos debería incluir la determinación de los lugares donde se almacena la información y las vías por las que esta fluye dentro del sistema (incluidos sus activos digitales). El análisis también debería determinar y justificar las medidas que se hayan aplicado para proteger las comunicaciones y flujos de datos necesarios y para detectar cualquier posible vulnerabilidad que aún exista. El análisis podría apoyarse en las siguientes acciones:

a) analizar o comprobar la eficacia de las medidas de seguridad física;
b) documentar el estado de las medidas, incluida la definición de posibles mejoras, y

c) respecto a los sistemas que se hayan determinado, garantizar que el *software* se haya sometido a una evaluación de la vulnerabilidad.

5.45. Por ejemplo, consideremos el intercambio de *software* (por ejemplo, código fuente, código objeto) entre un entorno de desarrollo y un sistema de seguridad física. Si no existen medidas de seguridad informática, el compilador (*hardware* y *software*) se asignará a la misma zona (y nivel de seguridad informática) que el propio sistema de seguridad física, al no existir ningún límite. Sin embargo, si se aplican medidas de seguridad física en el límite entre el compilador y el sistema, por ejemplo, para comprobar la integridad de los datos y detectar cualquier vulnerabilidad en el código procedente del compilador, el compilador podría situarse en una zona distinta y asignarse a un nivel de seguridad informática diferente del del propio sistema. Las medidas aplicadas al producto del compilador tienen por objeto proteger el sistema, por lo que se les asignaría el mismo nivel que el del sistema al que proporcionan protección.

5.46. El análisis de los activos digitales debería presentar una lista y una descripción de las medidas específicas de seguridad informática que se aplican a cada sistema. Las medidas deberían ser una combinación de medidas de control técnico, administrativo y físico.

5.47. El análisis de los activos digitales debería proporcionar un valor cualitativo o cuantitativo del umbral de riesgo aceptable.

Verificación de la evaluación de riesgos para la seguridad informática de los sistemas

5.48. El explotador debería verificar y validar la evaluación de riesgos para la seguridad informática de los sistemas para cada sistema con arreglo al alcance de la evaluación. Para la verificación de los productos de la CSRM a nivel de sistemas pueden utilizarse los métodos de evaluación descritos en el párrafo 4.98 relativos a la CSRM de la instalación.

Determinación y elaboración de escenarios para sistemas

5.49. La declaración nacional de amenazas o la ABD sirve de base para la generación de escenarios creíbles basados en la motivación, las capacidades, las intenciones y la oportunidad de los posibles adversarios (incluidos los adversarios que utilizan técnicas cibernéticas).

5.50. El explotador debería elaborar escenarios creíbles para cada sistema a partir de la caracterización de las amenazas como base para la validación de las medidas de seguridad informática que proporcionan protección al sistema. Los escenarios creíbles deberían incluir las posibles secuencias de las acciones de los adversarios que puedan comprometer los SDA.

5.51. Los escenarios deberían incluir rutas y técnicas de ataque comunes, entre las que pueden figurar las siguientes:

a) la ingeniería social, incluidos los ataques de suplantación de identidad;
b) los correos electrónicos maliciosos;
c) los sitios web maliciosos;
d) los dispositivos móviles infectados;
e) los equipos de mantenimiento e inspección comprometidos;
f) el acceso remoto;
g) los agentes internos (voluntarios e involuntarios), y
h) acciones que comprometan la cadena de suministro.

5.52. Deberían elaborarse escenarios coherentes con la declaración nacional de amenazas o la ABD que sea aplicable a la instalación para determinar los SDA que podrían estar expuestos a tales ataques. Puede ser beneficioso empezar la elaboración de escenarios considerando los casos más probables o con mayores consecuencias.

5.53. La elaboración de escenarios debería tener los siguientes objetivos (por orden de importancia):

a) determinar los escenarios con mayores consecuencias que afecten a los SDA, y
b) determinar los escenarios más probables que afecten a los activos digitales, incluidos los SDA.

5.54. Los métodos de evaluación (párrafo 4.98) deberían utilizar escenarios creíbles (párrafos 4.116 a 4.125) para verificar la eficacia de las medidas de seguridad informática aplicadas.

5.55. El explotador debería verificar que los activos digitales, incluidos los SDA, están debidamente protegidos contra los adversarios que se hayan determinado en la declaración nacional de amenazas o la ABD que sea aplicable a la instalación.

Informe sobre la gestión de riesgos de seguridad informática de los sistemas

5.56. El producto de la CSRM a nivel de sistemas debería documentarse en un informe que incluya lo siguiente:

a) La determinación de todos los SDA, incluidos (en la medida de lo posible) todos los componentes de *hardware* y *software* de cada SDA.
b) La determinación de los activos digitales que son componentes de los SDA, interactúan con ellos, los apoyan o podrían acceder a las vías de comunicación conectadas a dichos activos. Pueden incluir componentes de sistemas a los que se haya asignado un nivel de seguridad informática.
c) La determinación de vulnerabilidades, deficiencias o puntos débiles conocidos en los sistemas o componentes, por ejemplo, posibles problemas relativos a las adquisiciones (por ejemplo, el suministro de piezas falsificadas o de calidad inferior), o acciones u omisiones humanas que puedan afectar a la seguridad física.
d) La determinación de medidas de control técnico, administrativo y físico.
e) Recomendaciones para la aplicación de contramedidas.
f) Recomendaciones para mejorar las contramedidas (es decir, medidas adicionales de control técnico, administrativo o físico).
g) La detección de deficiencias en la documentación o los registros de la instalación.
h) La clasificación de la información de carácter estratégico.
i) Listas de control del acceso para el personal y servicios.
j) Medidas correctivas, cuando aparezcan condiciones adversas.
k) La evaluación del riesgo residual a nivel de sistemas.
l) La determinación y descripción de otros indicadores que ayuden a evaluar la seguridad informática (por ejemplo, tiempo medio entre fallos, tiempo medio de reparación, tiempo medio de detección, tiempo medio de recuperación, métrica de calidad de la seguridad física).

5.57. El informe relativo a la CSRM a nivel de sistemas debería clasificarse como información de carácter estratégico y protegerse debidamente.

6. CONSIDERACIONES SOBRE LA GESTIÓN DE RIESGOS DE SEGURIDAD INFORMÁTICA DE LA INSTALACIÓN Y LOS SISTEMAS DURANTE ETAPAS ESPECÍFICAS DEL PERÍODO DE VIDA DE UNA INSTALACIÓN

6.1. La presente sección ofrece orientación específica con respecto a las distintas etapas del período de vida de una instalación.

PLANIFICACIÓN

6.2. El explotador debería contrastar sus planes para la instalación con el reglamento de la autoridad competente y determinar las cuestiones que sea necesario abordar para cumplir los requisitos reglamentarios.

6.3. El explotador debería asegurarse de que dispone de una metodología formalizada para llevar a cabo un proceso detallado de CSRM de la instalación.

6.4. El explotador debería desarrollar el proceso de CSRM de la instalación con arreglo a lo dispuesto en la sección 4.

6.5. El explotador debería verificar que, siempre que pueda cumplirse la especificación de la DCSA, el riesgo residual no supere los niveles aceptables.

6.6. El explotador debería planificar el desarrollo de las competencias necesarias para apoyar la seguridad informática durante todas las etapas del período de vida de la instalación.

6.7. La etapa de planificación puede incluir actividades en lugares alejados del emplazamiento previsto de la instalación. El explotador debería aplicar medidas de seguridad informática a la información utilizada en estas actividades, y a otras aportaciones al ciclo de vida de la planificación y productos derivados de este, que sean de carácter estratégico o hagan uso de recursos de información de carácter estratégico.

SELECCIÓN DEL EMPLAZAMIENTO

6.8. El explotador debería incluir consideraciones de seguridad informática en la etapa de selección del emplazamiento de la instalación, ya que algunas actividades de apoyo a la seguridad informática solo pueden realizarse en el contexto del emplazamiento específico, y no a distancia o de forma genérica (por ejemplo, el establecimiento de redes aisladas, el acceso para equipos de respuesta a incidentes informáticos, la determinación de la disponibilidad de expertos en seguridad informática entre el personal local).

6.9. En sus planes de selección del emplazamiento de los principales equipos, el explotador debería tener en cuenta la necesidad de que puedan aplicarse las medidas de control físico que serán necesarias para complementar las medidas de seguridad informática.

6.10. A la hora de seleccionar el emplazamiento, el explotador debería tener en cuenta la disponibilidad de infraestructura local en apoyo de las medidas de seguridad informática (por ejemplo, redes de comunicaciones de emergencia).

DISEÑO

6.11. El explotador debería utilizar el producto de la labor de CSRM de la instalación realizada durante la etapa de planificación para garantizar que el proceso de diseño de la instalación contemple el cumplimiento de los requisitos de seguridad informática relativos a las funciones de la instalación (expresados en la DCSA y el CSP) como parte integrante de las actividades de ingeniería de sistemas de la instalación. Ello es aplicable al diseño de una nueva instalación o a la modificación del diseño para renovar o modificar la instalación durante la etapa de explotación.

6.12. El proceso de diseño debería tener en cuenta los requisitos de seguridad informática que surjan debido a las dependencias entre funciones de la instalación que se hayan determinado durante el proceso de CSRM de la instalación.

6.13. Los requisitos de seguridad informática deberían ser lo suficientemente detallados para poder tomar decisiones relativas al diseño, proceder a su verificación y evaluar los cambios que se hayan introducido en este.

6.14. El explotador debería realizar la CSRM a nivel de sistemas para cada sistema, incluida la verificación en cada paso del diseño de las medidas de seguridad informática.

6.15. La accesibilidad física y remota de los SDA dentro de zonas vitales por parte de un agente interno debería tenerse en cuenta en la etapa de diseño.

6.16. El explotador debería elaborar criterios de validación de la seguridad informática para la etapa de puesta en servicio. Los sistemas que realizan funciones de la instalación que tengan asignados los niveles más altos de seguridad informática deberían validarse de forma independiente.

6.17. En el proceso de diseño debería participar personal con conocimientos de seguridad informática de distintas partes de la entidad explotadora para garantizar lo siguiente:

a) que se incluyan los requisitos de seguridad informática adecuados;
b) que los cambios en el diseño mejoren la seguridad informática y no la degraden;
c) que los cambios, tal y como se aplican, cumplan los requisitos de seguridad informática que se hayan definido, y
d) que el examen de la eficacia incluya la seguridad informática.

6.18. El diseño debería incluir las indicaciones necesarias para la aplicación de los requisitos de seguridad informática. Debería conservarse la información relativa al diseño, como los informes de análisis, de modo que esté disponible en el futuro para los usuarios autorizados del diseño.

6.19. Dado que los documentos de diseño pueden contener información de carácter estratégico relacionada con la seguridad informática, todos los documentos de diseño deberían clasificarse con arreglo al sistema de clasificación de la información y protegerse debidamente.

6.20. El explotador debería asegurarse de que todo requisito de seguridad informática que hayan de cumplir los proveedores, contratistas y suministradores se especifique en sus contratos[39] [19]. Debería exigirse a los proveedores, contratistas y suministradores que dispongan de sistemas de gestión de la seguridad

[39] La norma de "criterios comunes" ISO/IEC 15408 de la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional [18] es uno de los instrumentos que puede servir de base para posibles requisitos de seguridad física.

informática y entornos de ingeniería seguros y que apliquen la seguridad física desde el diseño a los SDA que produzcan o suministren.

CONSTRUCCIÓN

6.21. El explotador debería asegurarse de que se establecen medidas de control físico, administrativo y técnico durante el proceso de construcción para mantener las medidas de prevención y protección exigidas por el CSP y la DCSA. Por ejemplo, si van a instalarse puertas con cerradura en un recinto, las cerraduras deberían instalarse y someterse a medidas de control antes de instalar los SDA dentro del recinto, o bien deberían establecerse las medidas compensatorias adecuadas.

6.22. El explotador debería asegurarse de que se apliquen las siguientes medidas de seguridad informática exigidas por el CSP y la DCSA durante la etapa de construcción:

a) actividades de garantía (es decir, pruebas, evaluaciones, auditorías);
b) el uso de espacios de almacenamiento temporal, con controles de procesos y seguridad física para verificar que los SDA no han sido manipulados ilícitamente;
c) la gestión del personal y la verificación de los productos de proveedores, contratistas y suministradores (tanto *in situ* como trabajando a distancia), desde la fabricación hasta la instalación, y
d) la evaluación y gestión de la cadena de suministro, garantizando que el proceso verificado de adquisiciones se sigue de forma sistemática y no se altera ilícitamente.

PUESTA EN SERVICIO

6.23. El explotador debería incluir la comprobación de las medidas de seguridad informática en sus pruebas de aceptación para la entrega de sistemas a la instalación por parte del proveedor de sistemas.

6.24. El explotador debería realizar actividades de configuración y pruebas durante la integración de sistemas y la DCSA (véase la figura 7) para cumplir

los requisitos de seguridad informática. Por ejemplo, deberían realizarse las siguientes actividades:

a) Las contraseñas y los métodos de autenticación secundaria para los activos digitales deberían cambiarse con arreglo a los procedimientos aprobados.
b) Deberían eliminarse las cuentas de desarrollo y construcción de los activos digitales y habilitarse medidas de control técnico.
c) Las herramientas de soporte de sistemas (*software* y *hardware*) deberían someterse a pruebas y evaluación utilizando las medidas de seguridad informática adecuadas.

6.25. El explotador debería realizar pruebas de validación de las medidas de seguridad informática. La validación de las medidas de seguridad informática y de las medidas de protección física debería realizarse de forma conjunta para garantizar una integración adecuada.

6.26. En el caso de que haya un conflicto entre las medidas de seguridad tecnológica y las medidas de seguridad física, deberían mantenerse las medidas que garanticen la seguridad tecnológica y el explotador debería encontrar una solución que también satisfaga los requisitos de seguridad informática. Hasta que se establezca una solución de ese tipo, deberían aplicarse medidas compensatorias de seguridad informática para reducir el riesgo a un nivel aceptable, las cuales deberían estar respaldadas por una justificación y un análisis de riesgos de seguridad física integrales. Las medidas compensatorias no deberían depender únicamente de medidas de control administrativo durante un período prolongado. Nunca debería aceptarse la ausencia de una solución de seguridad física.

6.27. El examen y aprobación de los documentos del CSP y materiales de apoyo aplicables (necesarios para el funcionamiento de los sistemas) deberían finalizar antes de la entrada en funcionamiento.

EXPLOTACIÓN

6.28. El explotador debería asignar la responsabilidad permanente de los cambios en el diseño, la gestión, el mantenimiento y las operaciones de todo el CSP a una persona (con el apoyo, según convenga, de otras personas que posean las aptitudes y los conocimientos adecuados).

6.29. El explotador debería conservar la documentación que describa cómo se aplican las medidas de seguridad informática, con arreglo al CSP, la DCSA y cualquier requisito impuesto externamente.

6.30. El explotador debería asegurarse de que los requisitos operacionales concuerden con el nivel de seguridad informática de los sistemas y activos digitales. Por ejemplo, podría ser necesario tener en cuenta lo siguiente:

a) Las restricciones de acceso, el control del acceso y la vigilancia pueden ser diferentes para los equipos asignados a distintos niveles de seguridad informática.
b) Es posible que se requieran distintos niveles de control de probidad para el personal que trabaja en distintos sistemas, en función del nivel de seguridad informática que tengan asignado.
c) Las funciones pueden estar separadas.

6.31. Las medidas aplicadas a los sistemas en el marco de una evaluación de la vulnerabilidad podrían provocar la inestabilidad de la central o de los procesos, por lo que solo deberían contemplarse mediante el uso de bancos de pruebas o sistemas de respaldo, durante las pruebas de aceptación en fábrica o durante paradas programadas de larga duración.

Mantenimiento

6.32. La presente sección es aplicable a las actividades de mantenimiento de corta duración que se realizan de forma habitual durante la etapa de explotación. El mantenimiento prolongado (por ejemplo, renovación, sustitución de sistemas, reparaciones) se aborda en las etapas de diseño, construcción y cese de la explotación.

6.33. El explotador debería garantizar que las actividades de mantenimiento se realicen de conformidad con el nivel de seguridad informática del sistema o activo digital objeto de mantenimiento. Por ejemplo, además de las consideraciones generales durante la explotación que se enumeran en el párrafo 6.30, deberían adoptarse las siguientes medidas:

a) Deberían especificarse las actividades de mantenimiento permitidas.
b) Debería determinarse y controlarse el acceso necesario para el mantenimiento.
c) Podrá limitarse el uso de los equipos de mantenimiento de modo que se utilicen solamente dentro de una zona de seguridad informática específica

(o para un sistema o activo digital específico) o únicamente para sistemas en un nivel de seguridad informática específico.

d) Podrán ser necesarios entornos de mantenimiento seguros para algunos sistemas o activos digitales.

6.34. Los sistemas pueden correr un mayor riesgo durante el mantenimiento, cuando es posible que se retiren o desactiven las medidas de seguridad informática. Además, es posible que haya rutas de acceso adicionales durante el mantenimiento, por ejemplo, derivadas de la necesidad de habilitar interfaces de mantenimiento a distancia o del uso de soportes extraíbles para configurar o actualizar el *software*.

6.35. El explotador debería establecer medidas compensatorias adecuadas cuando se retiren o desactiven las medidas normales de seguridad informática. Se incluyen los siguientes ejemplos:

a) Las medidas compensatorias deberían proporcionar protección física cuando el equipo no esté bajo llave.

b) Debería determinarse (y justificarse) de antemano la necesidad de utilizar interfaces remotas para el mantenimiento, y deberían aplicarse medidas adecuadas de seguridad informática a dichas interfaces con arreglo al CSP.

c) Debería controlarse y monitorizarse el uso de herramientas informáticas (por ejemplo, equipos de medición, ensayo y calibración) para garantizar que estas no se vean comprometidas por un ciberataque o proporcionen una vía que comprometa los sistemas en que se utilizan. Los equipos informáticos que puedan estar conectados temporalmente al sistema — como los equipos de prueba o configuración — deberían protegerse contra el *software* malicioso y las transferencias de datos no autorizadas. Debería reducirse al mínimo el uso de equipos externos para tales fines. Debería inspeccionarse cualquier equipo de ese tipo antes de introducirlo en la instalación.

d) Debería revisarse el *softwar*e para confirmar que esté libre de *software* malicioso antes de cargarlo en el sistema. Ello puede incluir la verificación de que el *software* no se ha alterado ilícitamente y es auténtico, por ejemplo, mediante la firma con funciones criptográficas *hash*.

e) También pueden utilizarse medidas de seguridad tecnológica (por ejemplo, la verificación concurrente por una segunda parte) para fines de seguridad física.

CESE DE LA EXPLOTACIÓN

6.36. Durante la etapa de cese de la explotación, es posible que se realicen modificaciones a gran escala en paralelo que afecten a múltiples sistemas.

6.37. El explotador debería considerar la posibilidad de aplicar medidas compensatorias para hacer frente a cualquier riesgo derivado de modificaciones o de la degradación de los sistemas de seguridad resultantes de cambios ambientales o estructurales. Ello puede incluir depender en mayor grado de las medidas de control administrativo y de los proveedores, contratistas y suministradores para aplicar dichas medidas.

6.38. A continuación figuran algunos ejemplos de cambios a los que pueden aplicarse medidas compensatorias:

a) La modificación o desactivación de las arquitecturas y medidas de seguridad informática para que puedan llevarse a cabo los trabajos de modificación.
b) Fluctuaciones en la dotación de personal, lo cual puede incluir la incorporación de nuevo personal *in situ* para realizar actividades relacionadas con los activos digitales, incluidos los SDA. Puede ser necesario establecer controles de la probidad adicionales u otras medidas para hacer frente a la amenaza de agentes internos.
c) La sustitución de un conjunto considerable de componentes, lo cual requiere la creación de un entorno de instalación seguro, un almacenamiento seguro y medidas adicionales para la manipulación y para el saneamiento en condiciones de seguridad de los SDA que se hayan sustituido.

RETIRADA DEL SERVICIO

6.39. Cuando se retiran del servicio activos digitales, debería evaluarse y documentarse el efecto de esta retirada (incluida cualquier pérdida de integración con otros activos digitales fuera de la instalación) en la seguridad informática. Si la retirada del servicio de un sistema o activo digital reduce la eficacia de las medidas de seguridad informática, el explotador debería establecer medidas compensatorias.

6.40. A medida que cambia el conjunto de funciones de la instalación, los activos digitales que apoyan estas funciones pueden reasignarse a un nivel de seguridad informática diferente o no asignarse a ningún nivel. Ello podría hacer necesario modificar las medidas de seguridad informática relativas a esos activos digitales.

6.41. El explotador debería garantizar la destrucción en condiciones de seguridad de los activos digitales que contengan información de carácter estratégico que no pueda desclasificarse de forma segura cuando se retiren del servicio.

7. ELEMENTOS DEL PROGRAMA DE SEGURIDAD INFORMÁTICA

REQUISITOS DE SEGURIDAD INFORMÁTICA

7.1. La política y el programa de seguridad informática deberían servir de base para los requisitos de seguridad informática definidos con arreglo a los resultados de la CSRM de la instalación y a nivel de sistemas (secciones 4 y 5, respectivamente) y teniendo en cuenta las etapas específicas del período de vida de la instalación (sección 6).

7.2. La seguridad informática en las instalaciones nucleares debería ser reconocida por el personal directivo superior y los directores como una disciplina transversal que requiere competencias, aptitudes y conocimientos especializados.

7.3. La responsabilidad general de la seguridad informática en una instalación nuclear recae en el personal directivo superior, el cual ha de conocer y comprender la amenaza cibernética y el posible efecto adverso de un ciberataque en la seguridad física nuclear.

7.4. El personal directivo superior debería velar por que todas las interacciones del explotador con terceros y todos los procesos internos se ajusten a los requisitos jurídicos y reglamentarios relacionados con la seguridad física de la información y la seguridad informática.

7.5. El personal directivo debería dar a conocer las creencias y valores de la cultura de la seguridad física nuclear en relación con la seguridad informática. Ello incluye promover el reconocimiento de que existe una amenaza creíble por parte de adversarios con competencias cibernéticas, y que esos adversarios (incluidas las amenazas de agentes internos) podrían llevar a cabo un ciberataque o un ataque combinado contra instalaciones nucleares.

Política de seguridad informática

7.6. La política de seguridad informática establece los objetivos generales de seguridad informática de una organización. La política de seguridad informática debería comenzar con una declaración clara de por qué se establece y debería definir la cuestión que se aborda, así como los objetivos y las consecuencias en caso de que no se siga la política. La política debería concordar con la política de seguridad informática del Estado y los requisitos reglamentarios pertinentes. La política debería ser aplicable y viable, y debería incluir indicadores que puedan medirse y auditarse.

7.7. La política de seguridad informática del explotador debería tener en cuenta los resultados de la CSRM de la instalación (véase la sección 4). La política de seguridad informática debería exigir la protección de los activos digitales, incluidos los SDA, para evitar que se vean comprometidos por los ciberataques. Las distintas cláusulas de la política deberían ser claras y concisas a la hora de determinar esos requisitos. La aplicación de los requisitos se aborda en detalle en el CSP.

7.8. La política de seguridad informática debería ser aprobada y aplicada por el personal directivo superior, y debería indicar la organización o persona responsable de la política y del CSP.

7.9. La política de seguridad informática debería formar parte de la política general de seguridad física de la instalación y debería coordinarse con otras responsabilidades de seguridad física pertinentes. Al establecer una política de seguridad informática, también hay que tener en cuenta su efecto sobre los aspectos jurídicos y los recursos humanos.

7.10. La política de seguridad informática puede determinar posibles sanciones y medidas disciplinarias contra el personal que no cumpla los requisitos de la política.

7.11. La política de seguridad informática debería reflejarse en el CSP y a través de otros elementos del CSP de nivel inferior que apoyen la aplicación de la seguridad informática.

7.12. Es necesario que la política establezca indicadores claros que se utilizarán para demostrar que se cumplen todos los aspectos de las políticas y que cada aspecto se realiza de forma satisfactoria.

Programa de seguridad informática

7.13. El CSP detalla cómo lograr los objetivos establecidos en la política de seguridad informática. El CSP establece las funciones, responsabilidades, procesos y procedimientos organizativos para aplicar la política de seguridad informática. Un CSP puede ser específico de una instalación (incluidos sus edificios y equipos conexos) o de una organización (incluidos todos sus emplazamientos y dependencias institucionales).

7.14. El CSP se debería formular, aplicar y mantener en el marco del plan de seguridad física global de la instalación.

7.15. El CSP debería tener en cuenta los resultados de la CSRM de la instalación (sección 4). La formulación del CSP puede incluir a personal de los ámbitos de la seguridad informática, la protección física, la seguridad tecnológica, las operaciones y la tecnología de la información (TI). El CSP se ilustra de manera esquemática en la figura 8.

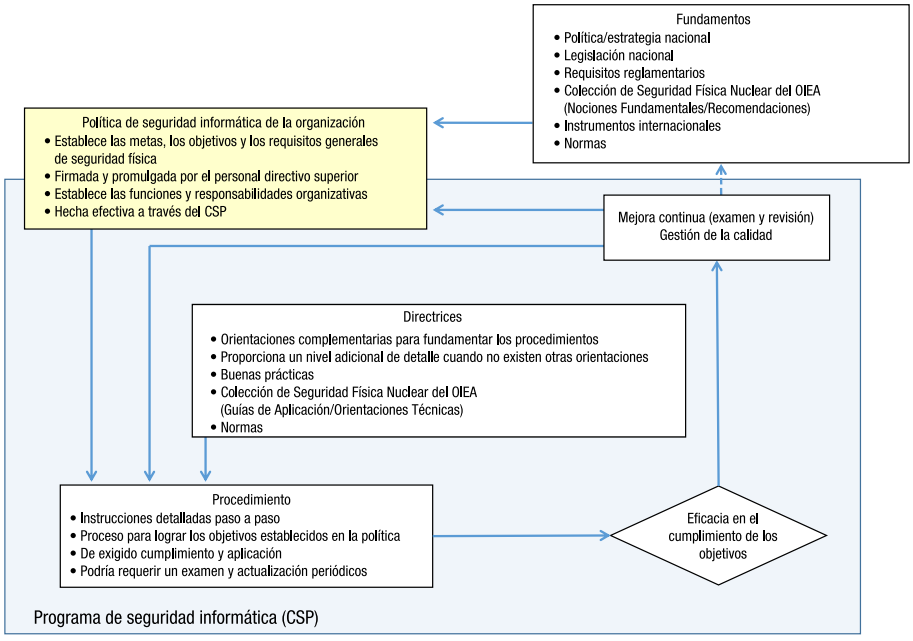


Figura 8. Sinopsis de un programa de seguridad informática típico.

7.16. El CSP debería examinarse y actualizarse a) de forma periódica para reflejar la evolución de la tecnología y las amenazas, y b) en caso de que se produzcan incidentes de seguridad informática u otros sucesos relacionados con la seguridad física nuclear.

Elementos del programa de seguridad informática

7.17. La referencia [7] describe los elementos de un CSP que son aplicables en general a organizaciones del régimen de seguridad física nuclear. Los párrafos 7.18 a 7.20 proporcionan información más detallada sobre los elementos de un CSP para instalaciones nucleares.

7.18. Los elementos del CSP deberían incluir medidas para subsanar las vulnerabilidades de los sistemas, la aplicación de medidas de seguridad informática, la realización de análisis de riesgos y la realización de actividades de garantía para lograr un nivel aceptable de riesgo de seguridad informática.

7.19. Los elementos del CSP deberían adaptarse y aplicarse a las distintas etapas del período de vida de una instalación y a las diferentes fases de los ciclos de vida de cada sistema. El CSP debería incluir información específica relativa a la implantación en estos distintos casos.

7.20. El explotador debería adaptar el CSP a su instalación, pero se sugiere que como mínimo se incluyan los siguientes ámbitos:

a) Organización y responsabilidades:
   i) organigramas;
   ii) personas responsables y responsabilidad de presentar informes (véanse los párrafos A.3 a A.13 del apéndice);
   iii) proceso de examen y aprobación periódico, e
   iv) interfaces con otros programas, como recursos humanos, seguridad física relacionada con el personal, protección física y capacitación (véanse los párrafos A.15 a A.38 del apéndice).
b) Gestión de los riesgos, la vulnerabilidad y el cumplimiento:
   i) proceso y productos de la CSRM de la instalación (véase la sección 4);
   ii) proceso y productos de la CSRM a nivel de sistemas (véase la sección 5), incluido el proceso de clasificación y determinación de activos digitales[40], incluidos los SDA;

[40] Los activos digitales incluyen medidas de control técnico que utilizan tecnologías digitales.

iii) frecuencia del examen y la reevaluación del plan de seguridad física;
iv) prácticas de autoevaluación;
v) procedimientos de auditoría y seguimiento y subsanación de deficiencias;
vi) método y ocasiones para iniciar o repetir la evaluación de riesgos y vulnerabilidades, y
vii) cumplimiento normativo y legislativo.

c) Diseño y gestión de la seguridad física:
i) arquitectura de seguridad física fundamental (es decir, DCSA);
ii) enfoques fundamentales de diseño de la seguridad física (es decir, niveles y zonas de seguridad informática);
iii) asignación de medidas de seguridad informática de referencia a cada nivel de seguridad informática;
iv) formalización de los requisitos de seguridad informática para contratistas, proveedores y suministradores, incluidos los contratos de mantenimiento, y
v) consideraciones de seguridad física para las etapas pertinentes del período de vida de la instalación (véase la sección 6).

d) Gestión de activos digitales:
i) atributos de los activos digitales (determinación, nivel de seguridad informática, zona, ubicación, consecuencias conexas);
ii) gestión de la configuración (*hardw*are, sistemas operativos, soporte lógico inalterable, aplicaciones de *software*, estado de los equipos, configuraciones conexas);
iii) diagramas de flujo de datos y de red que indiquen todas las conexiones externas con otros sistemas, e
iv) información de los suministradores sobre los activos.

e) Procedimientos de seguridad física:
i) gestión de incidentes de seguridad física;
ii) continuidad de las actividades;
iii) copia de seguridad, restablecimiento y recuperación de sistemas;
iv) cadena de suministro;
v) control del acceso;
vi) gestión de la información y las comunicaciones;
vii) seguridad física de plataformas y aplicaciones (por ejemplo, fortalecimiento de sistemas), y
viii) monitorización de sistemas, incluidos los registros.

f) Gestión del personal:
i) controles de probidad;
ii) sensibilización y capacitación;
iii) cualificación del personal;

iv) notificación de problemas de seguridad física, incluida la protección del personal que notifica estos problemas, y
v) rescisión del contrato o traslado.

7.21. En las normas internacionales [19 a 21] puede encontrarse más información sobre los elementos del CSP.

FUNCIONES Y RESPONSABILIDADES ORGANIZATIVAS

7.22. El explotador debería definir las funciones y responsabilidades relacionadas con la seguridad informática dentro de la organización.

7.23. El personal directivo debería velar por que todo el personal entienda quién es responsable dentro de la organización de dirigir el CSP en las esferas funcionales relacionadas con su trabajo. Es necesario que el personal con responsabilidades en materia de seguridad informática reciba capacitación sobre los elementos del CSP y los requisitos especificados en este.

7.24. La gestión de la seguridad informática debería integrarse en el sistema de gestión existente para la instalación (véanse los párrafos 7.30 a 7.34), en la medida que sea posible y factible. En el caso de instalaciones existentes, el sistema de gestión ya incluirá funciones y responsabilidades bien definidas, que deberían ajustarse para incorporar la seguridad informática.

7.25. El personal con responsabilidades importantes en materia de seguridad informática no debería tener conflictos de intereses con otras funciones de la organización o con otras responsabilidades. El personal directivo debería establecer políticas y procesos para evitar o mitigar cualquier posible conflicto.

7.26. El explotador debería velar por que las personas u organizaciones que realicen actividades clave de evaluación y verificación estén debidamente cualificadas y sean independientes.

7.27. La seguridad informática requiere la cooperación entre personal que desempeña distintas funciones y de distintas dependencias institucionales. El explotador debería establecer un marco formalizado con el fin de garantizar la cooperación interdisciplinaria.

7.28. El explotador ha de determinar las interrelaciones externas e internas que intervienen en el CSP. Ello incluye lo siguiente:

a) las interrelaciones habituales entre el explotador de la instalación y las autoridades competentes pertinentes (por ejemplo, órganos reguladores, fuerzas del orden, agencias de inteligencia, servicios de seguridad);
b) informar a las autoridades competentes e interactuar con las fuerzas de respuesta externas en caso de que se produzca un incidente de seguridad física;
c) la interrelación interna con el equipo de respuesta *in situ*;
d) las relaciones públicas, y
e) las relaciones con proveedores, contratistas y suministradores, incluida la cadena de suministro.

7.29. El explotador debería gestionar el riesgo mediante un proceso formalizado (es decir, CSRM de la instalación y a nivel de sistemas) que evalúe y gestione el riesgo y las vulnerabilidades de la instalación. El explotador debería utilizar los resultados de esos procesos en el marco de su sistema de gestión.

Sistema de gestión

7.30. El sistema de gestión debería integrar la seguridad informática, la protección física, la seguridad tecnológica, la salud, la calidad y elementos ambientales y financieros.

7.31. El sistema de gestión debería tener interfaces formales y consolidadas con la CSRM de la instalación y a nivel de sistemas.

7.32. Los objetivos de seguridad informática y de seguridad física de la información deberían definirse y gestionarse dentro del sistema de gestión de forma similar a otros objetivos operacionales.

7.33. El sistema de gestión debería examinarse para garantizar su completitud y conformidad con las políticas de seguridad física de la instalación. Debería examinarse y adaptarse a las condiciones cambiantes de la instalación y del entorno de forma periódica. La figura 3 de la referencia [22] ilustra el proceso de mejora continua de los sistemas de gestión.

7.34. Deberían examinarse los elementos del CSP (incluida la CSRM de la instalación y a nivel de sistemas), y las disposiciones necesarias en materia de seguridad informática deberían integrarse en el sistema de gestión.

Indicadores de seguridad informática

7.35. Los indicadores de seguridad informática pueden ser una herramienta eficaz para que los responsables de la seguridad física midan la madurez del sistema de gestión; el riesgo asociado a posibles ciberataques que afecten a los SDA; la eficacia de los distintos componentes de sus programas de seguridad física; la seguridad física de un sistema, producto o proceso concreto, y la capacidad del personal de la organización para ocuparse de las cuestiones de seguridad física de las que son responsables.

7.36. Los indicadores deberían servir de apoyo a las decisiones relacionadas con el nivel de riesgo aceptable y aportar datos para un registro de riesgos.

7.37. Debería realizarse un análisis para determinar parámetros y establecer indicadores que contribuyan a una gestión eficaz del CSP. Entre los indicadores que pueden ser de utilidad figuran el tiempo medio de recuperación (tras un ciberataque), el número de incidentes de seguridad informática, el número de restituciones de SDA (posibles reincidencias), y la información relativa a los retrasos en materia de seguridad física y al seguimiento de vulnerabilidades (por ejemplo, sistema común de puntuación, eficacia de la mitigación, tiempo de despliegue de controles, implantación de parches).

7.38. El uso de los indicadores debería integrarse en el sistema de gestión de la organización.

DISEÑO Y GESTIÓN DE LA SEGURIDAD FÍSICA

7.39. El diseño de la seguridad física de la instalación y los sistemas se especifica en la CSRM de la instalación y a nivel de sistemas (véanse las secciones 4 y 5, respectivamente). En la sección 8 se describe una aplicación práctica de estos productos, a saber, la DCSA y las medidas asignadas a los niveles de seguridad informática.

Requisitos de seguridad informática

7.40. Las modificaciones de la instalación o sistema deberían analizarse para determinar los posibles efectos sobre la seguridad física antes de introducir los cambios con el fin de poder gestionar los riesgos.

7.41. Debería tenerse en cuenta la seguridad informática a la hora de determinar las aportaciones de diseño, entre las que se incluyen las siguientes:

a) requisitos funcionales;
b) requisitos de interfaz;
c) requisitos operacionales;
d) ubicación del equipo;
e) consideraciones ambientales;
f) códigos y normas que han de utilizarse;
g) consideraciones contractuales;
h) consideraciones relativas a la cadena de suministro;
i) logística (por ejemplo, coordinación de operaciones complejas que afecten a muchas personas, instalaciones o suministros);
j) experiencia operacional anterior;
k) introducción de nuevas tecnologías;
l) consideraciones relativas al factor humano;
m) requisitos de diseño para cada disciplina de ingeniería (incluida la seguridad informática);
n) consideraciones relativas a la fabricación;
o) instalación;
p) puesta en servicio;
q) clausura, y
r) consideraciones financieras.

GESTIÓN DE ACTIVOS DIGITALES

7.42. Para cada activo digital, el explotador debería documentar los atributos que tengan importancia para la seguridad informática. Esos atributos pueden ser, entre otros, los siguientes:

a) el identificador y la ubicación del activo;
b) la configuración del activo;
c) las funciones y modalidades operacionales;
d) las interconexiones, incluidas las fuentes de alimentación;
e) el flujo de datos, incluidas las conexiones internas y externas;
f) los procedimientos que inician la comunicación, la frecuencia de la comunicación y los protocolos para dicha comunicación;
g) el análisis de los grupos de usuarios;
h) la propiedad (de los datos y sistemas informáticos), y

i) el nivel y la zona de seguridad informática, y la evaluación de las consecuencias de un fallo.

7.43. La gestión de activos digitales debería tener en cuenta el estado de las medidas de control técnico que utilizan tecnología digital en relación con los equipos. Las operaciones de seguridad informática y las operaciones de protección física pueden compartir la responsabilidad relativa a medidas, sistemas y procedimientos integrados de seguridad física. El control operacional conjunto puede incluir el control de los dispositivos físicos utilizados para proteger los equipos informáticos (por ejemplo, salas, puertas, llaves, cerraduras, cámaras, sensores de movimiento, indicadores de manipulación ilícita).

Gestión de la configuración

7.44. El objetivo de la gestión de la configuración es disponer de registros detallados y actualizados de los componentes de *software* y *hardware* instalados y de cómo estos se han configurado. La gestión de la configuración debería incluir la información necesaria para los siguientes fines:

a) determinar la necesidad de disponer de medidas de seguridad informática;
b) verificar que las medidas de seguridad informática se aplican y configuran de forma correcta;
c) gestionar los cambios a lo largo del ciclo de vida de los sistemas;
d) apoyar las evaluaciones de la seguridad informática, y
e) comprender los motivos de los cambios en las medidas de seguridad informática.

7.45. La gestión de la configuración incluye el proceso de gestión del cambio. La seguridad informática debería incluirse en este proceso, de modo que todos los cambios se evalúen desde el punto de vista de la seguridad informática antes de su aplicación. Por ejemplo, se realizan y documentan los exámenes pertinentes antes de llevar a cabo procedimientos que podrían eludir o modificar las medidas de seguridad informática implantadas, o reducir su eficacia. Los cambios de personal también pueden requerir cambios relacionados con la seguridad informática (por ejemplo, cancelación y gestión de credenciales).

PROCEDIMIENTOS DE SEGURIDAD FÍSICA

7.46. El explotador debería desarrollar procedimientos de seguridad física para apoyar el diseño y la gestión de la seguridad informática de la instalación y los

sistemas. Durante el desarrollo de estos procedimientos, el explotador debería considerar la regla de la actuación en pareja o la segregación de tareas, teniendo en cuenta el modelo de confianza adecuado y el nivel de seguridad asignado a la zona o zonas en que se aplica el procedimiento.

7.47. Los procedimientos que proporcionan instrucciones detalladas sobre cómo desactivar o eludir las medidas de seguridad informática deberían garantizar que dichas actividades queden debidamente registradas. El procedimiento también puede proporcionar instrucciones para la aplicación de medidas de seguridad informática alternativas o compensatorias cuando la medida de seguridad informática de referencia esté desactivada.

7.48. Estos procedimientos pueden ser nuevos procedimientos independientes o pueden integrarse en procedimientos existentes que cumplan uno o varios objetivos de seguridad tecnológica, seguridad física u organizativos.

GESTIÓN DE PERSONAL

7.49. La gestión de personal incluye las disposiciones necesarias para establecer un nivel adecuado de probidad, hacer cumplir los compromisos de confidencialidad, definir las competencias necesarias y, según convenga, imponer sanciones o rescindir un contrato.

7.50. Las actividades de seguridad informática y las actividades de seguridad física relacionadas con el personal deberían coordinarse para ofrecer protección contra las amenazas internas. En particular, puede ser necesario un mayor nivel de probidad para el personal con responsabilidades clave en materia de seguridad física (por ejemplo, administradores de sistemas, equipo de seguridad). En la referencia [6] se facilita más orientación con respecto a la protección frente a las amenazas de agentes internos.

7.51. El CSP debería incluir actividades de capacitación y concienciación para desarrollar y mantener las competencias y cualificaciones del personal y de la organización que sean necesarias para la seguridad informática.

8. EJEMPLO DE ARQUITECTURA DEFENSIVA DE SEGURIDAD INFORMÁTICA Y MEDIDAS DE SEGURIDAD INFORMÁTICA

8.1. A continuación se presenta un ejemplo de implantación de la DCSA con cinco niveles diferentes de seguridad informática en una central nuclear. Se trata de una de las posibles aplicaciones del enfoque graduado; la elección exacta de niveles, DCSA y medidas de seguridad informática, que debería adaptarse en función de la instalación y su entorno mediante la realización de un análisis específico.

EJEMPLO DE IMPLANTACIÓN DE UNA ARQUITECTURA DEFENSIVA DE SEGURIDAD INFORMÁTICA

8.2. Al implantar la DCSA, el explotador debería considerar la posibilidad de limitar los elementos dinámicos de las redes y los distintos sistemas para que su funcionamiento sea más predecible. Esta mayor predictibilidad podría contribuir a la aplicación de medidas eficaces de seguridad informática.

8.3. Las zonas que tengan asignado el nivel de seguridad informática más estricto solo deberían estar conectadas a zonas que tengan asignados niveles de seguridad inferiores mediante vías de comunicación de datos a prueba de fallos, deterministas y unidireccionales. La dirección de estas vías de datos debería ser desde la zona con el nivel de seguridad informática más estricto hacia la zona con el nivel de seguridad informática menos estricto[41]. Se recomienda encarecidamente no aplicar excepciones y estas solo pueden contemplarse de forma individualizada y estricta y cuando estén respaldadas por una justificación completa y un análisis de riesgos de seguridad física[42].

8.4. Los dispositivos digitales o las comunicaciones que se utilicen para la monitorización, el mantenimiento y la recuperación no deberían eludir las medidas

---

[41] Esto excluye las zonas que contienen funciones que se dedican solamente a la gestión de información de carácter estratégico, para las que la dirección se invierte. La información de carácter estratégico puede transmitirse a redes de datos restringidas, pero no al revés.

[42] Algunos Estados Miembros no permiten excepciones para las instalaciones en que puedan producirse consecuencias graves o muy graves. En otros tipos de instalaciones, la autoridad competente puede dejar a discreción del explotador la aplicación de vías bidireccionales.

de seguridad informática utilizadas para proteger las vías de comunicación entre dispositivos que tengan distintos niveles de seguridad informática.

8.5. Los sistemas que tengan asignado el nivel de seguridad informática más estricto deberían estar ubicados dentro de los límites de la zona más segura[43].

8.6. Las comunicaciones de datos entre los sistemas de la instalación y el centro de emergencia (situado en el emplazamiento o fuera de este) deberían estar protegidas por medidas de seguridad informática.

DESACOPLAMIENTO DE ZONAS DE SEGURIDAD INFORMÁTICA

8.7. Las medidas de seguridad informática que garantizan el desacoplamiento lógico y físico de las zonas se basan en los requisitos de los niveles de seguridad informática de estas. Para mantener la defensa en profundidad, no debería permitirse una vía directa que conecte varias zonas.

8.8. Las medidas de control técnico que proporcionan seguridad física en los límites de zonas deberían estar diseñadas para ser resilientes a los ciberataques y para proporcionar alertas en caso de una posible situación de riesgo o actividad dolosa.

CONECTIVIDAD EXTERNA

8.9. Cuando se proporcione conectividad externa, la seguridad física debería aplicarse mediante el uso del enfoque graduado. La prestación de servicios de conectividad externa debería cumplir los requisitos de protección de la confidencialidad, integridad y disponibilidad de la información de carácter estratégico correspondientes al nivel de seguridad informática asignado a la zona.

8.10. Deberían aplicarse las restricciones de acceso adecuadas (incluida la monitorización del acceso) para proporcionar una protección basada en el enfoque graduado, ya que estas conexiones externas pueden servir de vía para comprometer los sistemas de la instalación.

---

[43] Las funciones de las comunicaciones inalámbricas son problemáticas cuando se aplican en sistemas que tienen asignado el nivel de seguridad más estricto, ya que resulta difícil proporcionar un límite seguro para dichas comunicaciones.

8.11. Los siguientes son algunos ejemplos de los sistemas accesibles externamente:

a) los sistemas de vigilancia ambiental;
b) los sistemas de automatización de edificios;
c) los sistemas de protección contra incendios;
d) las comunicaciones con los centros de emergencia;
e) el acceso remoto para proveedores (cuando esté permitido);
f) los dispositivos de campo situados fuera del perímetro físico de seguridad, y
g) el control de visitantes.

8.12. La figura 9 presenta un ejemplo de implantación de una DCSA, en que se muestran niveles, zonas, sistemas y activos digitales. Ello se basa en la orientación proporcionada en la sección 3.

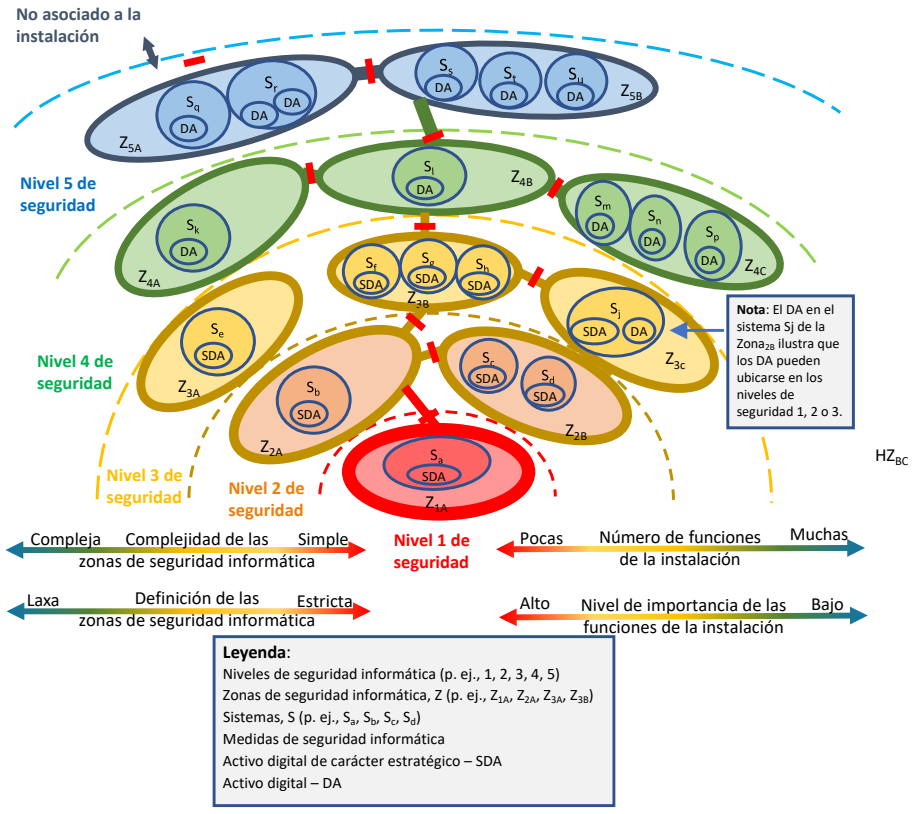


Figura 9. Ejemplo de implantación de una arquitectura defensiva de seguridad informática.

EJEMPLOS DE REQUISITOS

8.13. En los párrafos 8.16 a 8.21 se presentan ejemplos de requisitos de seguridad física aplicados dentro de cada nivel de seguridad informática. La elección exacta de niveles y los correspondientes requisitos de seguridad física deberían adaptarse en función de la instalación y su entorno mediante la realización de un análisis específico.

ACTIVOS DIGITALES NO ASIGNADOS

8.14. Puede haber dos tipos de activos digitales no asignados:

a) Equipos restringidos o proscritos, cuando las restricciones impuestas al explotador impiden evaluar la seguridad física de los activos digitales. Esto podría deberse a las condiciones de la licencia o a requisitos contractuales, reglamentarios o jurídicos que prohíben al explotador inspeccionar y modificar el equipo (por ejemplo, el equipo relacionado con las salvaguardias).
b) Equipos de los que no se haya informado, que pueden introducirse en la instalación sin que lo haya solicitado el explotador o sin su consentimiento previo. Estos equipos se consideran "de contrabando" hasta que pueda realizarse una evaluación de riesgos para la seguridad informática.

8.15. El explotador puede imponer restricciones a los activos no asignados hasta que estos puedan ser evaluados y asignados al nivel de seguridad informática adecuado y puedan aplicarse las medidas de seguridad informática correspondientes. Por ejemplo, los dispositivos que no estén asignados no deberían situarse cerca de sistemas que tengan niveles medios a muy altos de seguridad informática.

REQUISITOS GENÉRICOS

8.16. Se aplican los siguientes requisitos genéricos a los sistemas y niveles pertinentes:

a) Todas las medidas de seguridad técnicas, físicas, de personal y organizativas para sistemas y redes se diseñan y aplican de forma sistemática y con arreglo a procesos y procedimientos aprobados.
b) Se definen políticas y prácticas para cada nivel de seguridad informática.

c) Los usuarios están obligados a cumplir las políticas de seguridad física y los procedimientos operativos de seguridad física.
d) El personal al que se permite el acceso al sistema cuenta con la debida cualificación y experiencia y su probidad ha sido verificada, cuando sea necesario.
e) Los usuarios y administradores tienen acceso solamente a las funciones de los sistemas que necesitan para realizar su trabajo. Se evita la acumulación de derechos de acceso por parte de una sola persona.
f) La funcionalidad e interfaces del sistema se limitan en la medida de lo posible, con el objetivo de reducir la vulnerabilidad global del sistema.
g) Se han establecido medidas adecuadas de control del acceso y autenticación de usuarios.
h) Se han establecido medidas de protección contra las infecciones y la propagación de programas maliciosos.
i) Se realiza un registro y monitorización de la seguridad física, incluidos procedimientos para responder de forma adecuada.
j) Se monitorizan las vulnerabilidades de aplicaciones y sistemas, y se adoptan las medidas oportunas.
k) Se examina periódicamente la idoneidad y eficacia de las medidas.
l) Se realizan evaluaciones periódicas de la vulnerabilidad de los sistemas.
m) Los soportes extraíbles se controlan con arreglo a los procedimientos operativos de seguridad física. No se permite conectar dispositivos privados a sistemas y redes.
n) Los activos digitales y las medidas de seguridad informática conexas se mantienen de forma estricta utilizando los procedimientos de gestión del cambio aplicables.
o) Existen procedimientos adecuados de copia de seguridad y recuperación.
p) A un dispositivo de servicio se le asigna exactamente un nivel de seguridad informática.
q) El acceso físico a los componentes y sistemas, incluidos los dispositivos de servicio, está restringido con arreglo a sus funciones.
r) Existen medidas para impedir la introducción no autorizada de sistemas en las zonas de seguridad informática.
s) Solo los usuarios autorizados y cualificados pueden introducir modificaciones en los sistemas.

REQUISITOS DEL NIVEL 1 DE SEGURIDAD FÍSICA

8.17. Además de los requisitos genéricos, se utilizan requisitos relativos a las medidas preventivas y de protección para los sistemas que son fundamentales para

la instalación y que requieren el máximo nivel de seguridad física (por ejemplo, los sistemas de protección del reactor). Estos requisitos pueden ser, entre otros, los siguientes:

a) Los sistemas se diseñan y aplican de modo que puedan verificarse y probarse frente al posible ataque de un adversario.
b) Ningún flujo de datos en red de ningún tipo procedente de sistemas que tengan asignados niveles de seguridad informática menos estrictos puede entrar en los sistemas de nivel 1 cuando la integridad y la disponibilidad sean prioritarias. Solo es posible la comunicación hacia el exterior. Se recomienda encarecidamente no aplicar excepciones y estas solo pueden contemplarse de forma individualizada y estricta y cuando estén respaldadas por una justificación completa y un análisis de riesgos de seguridad física[44].
c) No se permite el acceso para el mantenimiento a distancia.
d) El acceso físico y lógico a los sistemas se controla, monitoriza y registra de forma estricta.
e) El número de miembros del personal que tienen acceso a los sistemas se limita a un mínimo absoluto.
f) La regla de la actuación en pareja se aplica para prevenir acciones no autorizadas por parte de una amenaza interna.
g) Se registran y monitorizan todas las actividades y posibles sucesos relacionados con la seguridad física.
h) La conexión de dispositivos de almacenamiento externos se aprueba y verifica caso por caso.
i) Se aplican procedimientos organizativos y administrativos estrictos a toda modificación, incluidos el mantenimiento de *hardware*, las actualizaciones de *software* y las modificaciones de *software*.

REQUISITOS DEL NIVEL 2 DE SEGURIDAD FÍSICA

8.18. Además de los requisitos genéricos, deberían utilizarse requisitos relativos a las medidas preventivas y de protección para sistemas, como los sistemas de control operacional, que requieran un alto nivel de seguridad física. Estos requisitos pueden ser, entre otros, los siguientes:

a) Solo se permite un flujo de datos en red unidireccional hacia el exterior desde los sistemas de nivel 2 hacia los de nivel 3. Solo pueden aceptarse los mensajes de acuse de recibo necesarios o los mensajes de señales

[44] Algunos Estados Miembros no permiten excepciones.

controlados en sentido contrario (entrante) (por ejemplo, para el TCP/IP (protocolo de control de transmisión/protocolo de Internet)).

b) No se permite el mantenimiento a distancia.

c) El número de miembros del personal que tiene acceso a los sistemas se mantiene al mínimo, estableciendo una clara distinción entre usuarios y personal administrativo.

d) El acceso físico y lógico a los sistemas se controla y documenta de forma estricta.

e) Se evita el acceso administrativo desde otros niveles de seguridad informática. De no ser posible, dicho acceso se controla de forma estricta (por ejemplo, adoptando la regla de la actuación en pareja y la autenticación de doble factor).

f) Se toman todas las medidas razonables para garantizar la integridad y disponibilidad de los sistemas.

REQUISITOS DEL NIVEL 3 DE SEGURIDAD FÍSICA

8.19. Además de los requisitos genéricos, deberían utilizarse requisitos relativos a las medidas preventivas y de protección para los sistemas en tiempo real que no sean necesarios para las operaciones (por ejemplo, los sistemas de supervisión de procesos en una sala de control), si todos estos sistemas tienen un nivel de gravedad medio para diversas ciberamenazas. Estos requisitos pueden ser, entre otros, los siguientes:

a) No se permite el acceso a Internet desde sistemas de nivel 3.

b) Se monitorizan los registros, incluidos los registros de sucesos, de los recursos clave.

c) Se aplican pasarelas de seguridad física para proteger este nivel frente a conexiones de datos no controladas procedentes de sistemas de nivel 4 y para permitir solamente actividades específicas y limitadas.

d) Se controlan las conexiones físicas a los sistemas.

e) Se controla y documenta el acceso físico y lógico a los sistemas.

f) Se permite el acceso para el mantenimiento a distancia caso por caso, siempre que se someta a un control riguroso; el usuario y computadora remotos siguen una política de seguridad física definida, que se especifica en el contrato.

g) Las funciones de sistemas que estén a disposición de los usuarios se controlan mediante mecanismos de control del acceso y se basan en la regla de la “necesidad de conocer”. Se estudia con detenimiento toda excepción

a esta regla y se garantiza la protección por otros medios (por ejemplo, el acceso físico).

h) Se evita el acceso administrativo desde otros niveles de seguridad informática siempre que sea posible. De no serlo, dicho acceso se controla de forma estricta (por ejemplo, mediante la autenticación de doble factor).

REQUISITOS DEL NIVEL 4 DE SEGURIDAD FÍSICA

8.20. Además de los requisitos genéricos, deberían aplicarse requisitos relativos a las medidas de seguridad informática a los sistemas de gestión de datos técnicos que se utilicen para la gestión de actividades de explotación o mantenimiento en relación con componentes o sistemas necesarios para las operaciones en virtud de la especificación técnica (por ejemplo, permiso de trabajo, orden de trabajo, etiquetado de advertencia, gestión de la documentación), si dichos sistemas requieren niveles medios de seguridad informática. Estos requisitos pueden ser, entre otros, los siguientes:

a) No se permite el acceso a Internet desde sistemas de nivel 4.

b) Se aplican pasarelas de seguridad física para proteger este nivel frente a comunicaciones de datos no autorizadas a través de redes de instalaciones o empresas externas de confianza y aprobadas, y para permitir actividades específicas que estén autorizadas.

c) Se controlan las conexiones físicas a los sistemas.

d) El acceso para el mantenimiento a distancia se permite bajo control; el usuario y la computadora remotos siguen una política de seguridad física definida, que se especifica en el contrato.

e) Las funciones de sistemas que estén a disposición de los usuarios se controlan mediante mecanismos de control del acceso. Se estudia con detenimiento toda excepción a esta regla y se garantiza la protección por otros medios.

f) Se permite el acceso externo remoto a determinados servicios y para usuarios autorizados, siempre que existan mecanismos adecuados de control del acceso.

REQUISITOS DEL NIVEL 5 DE SEGURIDAD FÍSICA

8.21. Deberían utilizarse requisitos que especifiquen medidas de seguridad informática para sistemas que no tengan una importancia directa con respecto al control técnico o los fines operacionales (por ejemplo, sistemas de ofimática), si

dichos sistemas requieren niveles bajos de seguridad informática. Estos requisitos pueden ser, entre otros, los siguientes:

a) El nivel de seguridad informática no se sitúa por debajo de un nivel de protección de referencia, definido con arreglo a la tecnología más avanzada.
b) Solo los usuarios autorizados y cualificados pueden introducir modificaciones en los sistemas.
c) Se permite el acceso a Internet desde sistemas de nivel 5, siempre que se apliquen las medidas preventivas y de protección adecuadas.
d) Se permite el acceso externo remoto para usuarios autorizados, siempre que existan las medidas adecuadas.
e) La conexión física de dispositivos de terceros a sistemas y redes se somete a control técnico. Las interfaces con sistemas de nivel superior se caracterizan y evalúan de forma independiente para garantizar el cumplimiento de las especificaciones de la arquitectura de seguridad informática.

Apéndice

ELEMENTOS CONCRETOS DE UN PROGRAMA DE SEGURIDAD INFORMÁTICA

A.1. El presente apéndice proporciona ejemplos de elementos concretos del CSP para su uso con el enfoque de seguridad informática basado en la ejecución. Es posible que el explotador tenga que modificar estos elementos para reflejar circunstancias organizativas concretas o específicas de la instalación, pero los ejemplos abarcan todos los tipos de información que el explotador necesita para formular e implantar un CSP eficaz.

A.2. El explotador precisaría estos elementos u otros parecidos para facilitar el entendimiento entre las dependencias institucionales, los proveedores, contratistas y suministradores, y las autoridades competentes. Tal vez convenga adaptar los elementos a las características específicas de la entidad explotadora y la instalación para mejorar el entendimiento.

ORGANIZACIÓN Y RESPONSABILIDADES DE LA INSTALACIÓN

Personal directivo

A.3. El personal directivo superior de una instalación establece una política de seguridad informática, así como procesos y mecanismos de apoyo para garantizar que esta se aplique. Para ello, el personal directivo superior debería adoptar las siguientes medidas:

a) Asumir la responsabilidad general de todos los aspectos de la seguridad informática.
b) Definir los objetivos de seguridad física de la instalación.
c) Velar por que se cumplan las leyes y los reglamentos pertinentes.
d) Mantenerse al corriente de la amenaza para la seguridad física nuclear vigente y las tendencias conexas.
e) Establecer el nivel de aceptación de riesgos para la instalación.
f) Asignar responsabilidades organizativas en materia de seguridad informática.
g) Garantizar una comunicación adecuada entre el personal responsable de los distintos aspectos de la seguridad física nuclear.
h) Velar por el cumplimiento de la política de seguridad informática.
i) Proporcionar los recursos adecuados para aplicar un CSP sostenible.

j) Velar por que se realicen exámenes y actualizaciones periódicos de la política y los procedimientos de seguridad informática.
k) Garantizar el apoyo a los programas de capacitación y sensibilización.

Especialista en seguridad informática

A.4. El explotador debería asignar la responsabilidad general de la seguridad informática de la instalación a una persona o grupo. En la presente publicación, el titular de esa función recibe el nombre de "especialista en seguridad informática"[45].

A.5. El especialista en seguridad informática debería colaborar estrechamente con las actividades de toda la instalación, pero de manera independiente. Además, debería tener una relación jerárquica clara, accesible y directa con el personal directivo superior, ya que la seguridad informática puede afectar a casi todas las actividades de la instalación.

A.6. Las responsabilidades en materia de seguridad informática en los diferentes departamentos de la organización deberían definirse y coordinarse de forma clara para evitar lagunas o conflictos y para garantizar que la seguridad informática se aplique de forma sistemática. Ello es especialmente necesario si el cargo de especialista en seguridad informática se asigna a un grupo en lugar de a una persona: el especialista en seguridad informática debería constituir una autoridad única dentro de la entidad explotadora, con la responsabilidad de atender los problemas que atañen a la organización en su conjunto y de resolver cualquier conflicto que pueda surgir.

A.7. El especialista en seguridad informática debería conocer a fondo la seguridad informática y conocer bien otros aspectos de la seguridad física en instalaciones nucleares, además de tener conocimientos sobre la seguridad tecnológica nuclear y la gestión de proyectos y la capacidad para integrar a personas de distintas disciplinas en un equipo eficaz.

A.8. El especialista en seguridad informática debería tener la facultad y responsabilidad de administrar el CSP.

---

[45] En otros casos, esta función puede denominarse "oficial de seguridad informática", "oficial jefe de seguridad de la información", "oficial de seguridad de la tecnología de la información" u "oficial de seguridad de la información", o puede asignarse a múltiples cargos.

A.9. Entre las responsabilidades específicas que suele tener un especialista en seguridad informática se incluyen las siguientes:

a) Asesorar al personal directivo superior en materia de seguridad informática.
b) Dirigir el equipo de seguridad informática.
c) Promover la seguridad informática dentro de la organización, incluidas las mejoras que sean necesarias.
d) Coordinar y controlar el desarrollo de las actividades de seguridad informática (por ejemplo, aplicar la política de seguridad informática, las directivas y directrices específicas, los procedimientos y, en última instancia, las medidas de seguridad informática).
e) Colaborar con el personal de protección física y otros miembros del personal encargado de la seguridad física y tecnológica para planificar y especificar las medidas de seguridad informática, incluidas las destinadas a responder a incidentes de seguridad informática.
f) Determinar los sistemas que resultan esenciales para la seguridad informática dentro de la instalación (es decir, aquellos que proporcionan medidas de seguridad informática de referencia). Debería informarse a los propietarios de los activos sobre el papel que desempeñan sus equipos en la seguridad informática.
g) Realizar evaluaciones periódicas de los riesgos para la seguridad informática, independientemente del personal de operaciones.
h) Realizar inspecciones, auditorías y exámenes periódicos de las medidas de seguridad informática de referencia y presentar informes de situación al personal directivo superior.
i) Desarrollar y organizar capacitación en seguridad informática y cualificación para el personal pertinente.
j) Prepararse frente a incidentes de seguridad informática y dirigir la correspondiente respuesta, incluida la coordinación con el personal interno y externo pertinente que participe en la respuesta.
k) Investigar incidentes de seguridad informática y desarrollar las medidas correctivas posteriores.
l) Participar en la evaluación de la seguridad física general de la instalación.
m) Participar en el análisis de los requisitos de los nuevos sistemas informáticos.

Equipo de seguridad informática

A.10. El explotador debería nombrar y asignar personal para el equipo de seguridad informática. Este equipo puede estar formado por un grupo fijo de personas o incluir a personas con conocimientos específicos, según convenga.

El equipo apoya al especialista en seguridad informática en el cumplimiento de sus obligaciones: el especialista en seguridad informática ha de tener acceso a conocimientos especializados en todas las disciplinas asociadas a la seguridad informática, incluidas la seguridad tecnológica de la instalación y las operaciones de la central, así como la protección física y la seguridad física relacionada con el personal.

A.11. Los miembros del equipo de seguridad informática deberían encargarse de promover la seguridad informática en sus respectivas dependencias institucionales.

A.12. Las actividades del equipo de seguridad informática incluyen la monitorización activa de los activos digitales, incluidos los SDA, para detectar cualquier indicio de un posible ciberataque, y la coordinación de la respuesta a los incidentes de seguridad informática. Ello podría incluir proveer de personal a un centro de operaciones de seguridad física para monitorizar y evaluar posibles incidentes de seguridad informática y para iniciar y apoyar las actividades de respuesta, lo cual también podría necesitar el apoyo de otras organizaciones.

Otras responsabilidades del personal directivo

A.13. El personal directivo de los distintos niveles de la organización debería velar por que se preste la debida atención a la seguridad informática dentro de sus ámbitos de competencia. Entre las responsabilidades que suele tener el personal directivo en sus respectivos ámbitos figuran las siguientes:

a) comprender la importancia y el papel de la seguridad informática en la seguridad física nuclear;
b) actuar en el marco de los requisitos y procesos definidos por el CSP;
c) proporcionar requisitos operacionales y comentarios al personal directivo superior relacionados con la seguridad informática, y solucionar cualquier conflicto que exista entre los requisitos operacionales, de seguridad física y de seguridad tecnológica;
d) avisar al personal directivo superior de cualquier situación que pueda provocar cambios en el nivel de seguridad informática, como cambios de personal, equipos o procesos;
e) velar por que el personal reciba la capacitación e información adecuada sobre las cuestiones de seguridad informática relacionadas con sus funciones;
f) velar por que los proveedores, contratistas y suministradores que trabajan para ellos actúen en el marco de los requisitos y procesos definidos por el CSP;

g) realizar un seguimiento y monitorización de los incidentes de seguridad informática, responder a estos y presentar los informes correspondientes, y
h) aplicar las medidas de seguridad informática.

Responsabilidades individuales

A.14. Cada persona dentro de una organización debería ser responsable de realizar sus propias tareas con arreglo al CSP. Entre las responsabilidades específicas figuran las siguientes:

a) comprender la importancia y el papel de la seguridad informática en la seguridad física nuclear;
b) comprender la política de la organización en materia de seguridad informática;
c) conocer los procedimientos de seguridad informática relativos a su trabajo;
d) actuar en el marco de las limitaciones derivadas de la política de seguridad informática;
e) notificar al personal directivo cualquier cambio que pueda afectar negativamente a la seguridad informática;
f) notificar a los puntos de contacto pertinentes y al personal directivo todo incidente o posible incidente que pueda comprometer la seguridad informática, y
g) asistir a la capacitación inicial sobre seguridad informática y a cursos de perfeccionamiento de forma periódica.

Responsabilidades interdepartamentales

A.15. La seguridad informática es una disciplina transversal que afecta a muchas actividades y dependencias institucionales diferentes que, a su vez, repercuten en ella. La seguridad informática requiere una estrecha coordinación y cooperación entre las distintas dependencias institucionales para ser eficaz. Los párrafos A.16 a A.38 describen algunas de las responsabilidades departamentales y cuestiones transversales.

Protección física

A.16. Tanto el plan de seguridad física del emplazamiento como el CSP son esenciales a la hora de formular un plan de seguridad física global para la instalación, por lo que han de complementarse mutuamente. Los SDA están

protegidos por requisitos de control del acceso físico y, de comprometerse los sistemas informáticos, puede producirse una degradación o pérdida de las funciones de protección física. Además, los adversarios podrían intentar atacar una instalación mediante la coordinación de un ciberataque y un ataque físico (es decir, un ataque combinado).

A.17. Si las dependencias institucionales responsables del plan de seguridad física del emplazamiento y del CSP son diferentes, deberían comunicarse entre sí y coordinar sus esfuerzos para garantizar la concordancia entre los planes durante el proceso de formulación y examen.

A.18. El explotador debería asignar al personal de protección física las funciones y responsabilidades pertinentes en la formulación, aplicación y mantenimiento del CSP. Entre ellas pueden figurar las siguientes:

a) garantizar que solo se permita el acceso autorizado a los SDA;
b) detectar los soportes extraíbles y dispositivos móviles no autorizados que entren en la instalación;
c) detectar la retirada no autorizada de información o activos de información de la instalación;
d) garantizar la aplicación de las políticas relativas a cualquier soporte extraíble y dispositivo móvil permitido en la instalación (por ejemplo, análisis para detectar *software* malicioso antes de la entrada en la instalación);
e) notificar incidentes de seguridad informática (por ejemplo, detección de *software* malicioso, retirada no autorizada de activos de información) con arreglo al procedimiento de respuesta correspondiente;
f) evaluar las prácticas de seguridad física de la información (por ejemplo, controles simulados, comprobación de salas y armarios cerrados bajo llave, establecimiento de normas para los dispositivos destinados a la protección física de los activos de información, control y monitorización del acceso), y
g) apoyar la respuesta a incidentes de seguridad informática relacionados con el sistema de protección física.

Tecnología de la información

A.19. El personal informático realiza tareas de apoyo, gestión y administración dentro de una instalación nuclear. Estas tareas pueden incluir actividades relacionadas con activos digitales utilizados para preparar y archivar procedimientos operacionales y de mantenimiento, instrucciones de trabajo, sistemas de gestión de la configuración, documentos de diseño y manuales de funcionamiento.

A.20. El CSP debería determinar de forma clara los activos digitales y las redes conexas que sean responsabilidad del personal informático. El personal informático debería monitorizar los activos digitales y redes conexas que se hayan determinado y notificar todo incidente de seguridad informática al personal directivo superior y al especialista en seguridad informática con arreglo al plan de respuesta a incidentes.

A.21. El personal informático debería tomar medidas para prevenir que los incidentes de seguridad informática relacionados con activos digitales (pero no con los SDA) y redes se propaguen de tal modo que afecten a los SDA.

Ingeniería

A.22. El personal de ingeniería debería disponer de procesos formales que garanticen la coordinación con otras dependencias institucionales pertinentes para asegurar que las medidas de seguridad física nuclear y seguridad tecnológica nuclear se diseñen y apliquen de forma integrada con arreglo a los requisitos establecidos en el CSP. El personal de ingeniería debería reconocer que la seguridad tecnológica, la protección física y la seguridad informática son disciplinas distintas que requieren el apoyo de expertos debidamente cualificados en dichas disciplinas.

A.23. El personal de ingeniería debería aportar pruebas de la eficacia de la arquitectura de seguridad informática (es decir, la DCSA) que puedan compararse con los resultados previstos sobre la base de la CSRM de la instalación y a nivel de sistemas.

A.24. El personal de ingeniería debería liderar o apoyar el proceso de CSRM a nivel de sistemas para los sistemas de la instalación de los que sean propietarios.

A.25. El personal de ingeniería debería proporcionar orientación a los proveedores, contratistas y suministradores sobre los requisitos de seguridad informática relativos a los sistemas de la instalación. El personal de ingeniería es responsable de examinar los diseños de los proveedores para garantizar que cumplen los requisitos de seguridad informática. El personal de ingeniería debería solicitar al proveedor que confirme que los productos suministrados a la instalación se han desarrollado en un entorno seguro. El personal de ingeniería debería establecer y seguir un procedimiento para examinar la documentación técnica de los productos, aceptar las remesas de productos *in situ* y probar los productos con el fin de garantizar que se cumplan los requisitos de seguridad informática.

A.26. El personal de ingeniería debería garantizar que existan actividades de monitorización del funcionamiento para confirmar que las medidas de seguridad informática sigan siendo eficaces.

Operaciones

A.27. El CSP debería determinar los sistemas y redes de la instalación que sean responsabilidad del personal de operaciones. Dicho personal es responsable de cumplir los requisitos establecidos en el CSP con respecto a estos sistemas.

A.28. El personal de operaciones debería velar por que la DCSA y las medidas de seguridad informática de las que sean responsables se mantengan y sigan siendo eficaces.

A.29. El personal de operaciones debería velar por que existan procedimientos para detectar incidentes de seguridad informática e iniciar una respuesta con respecto a los sistemas y redes que estén bajo su responsabilidad.

A.30. El personal de operaciones debería promover la conciencia situacional para velar por que solo se utilicen soportes extraíbles y dispositivos móviles autorizados dentro de la instalación.

Organización de las adquisiciones y la cadena de suministro

A.31. La adquisición de productos debería cumplir las especificaciones relativas al equipo, dispositivo o componente. Las especificaciones deberían incluir requisitos de seguridad informática adecuados.

A.32. Los procesos de adquisición deberían incluir controles para garantizar que los SDA desarrollados o suministrados por proveedores y suministradores incluyan medidas de seguridad informática acordes con el nivel de seguridad informática asignado a cada SDA.

A.33. El personal de adquisiciones debería comprender la importancia de requisitos específicos de seguridad informática en el ámbito de las adquisiciones. Estos requisitos deberían hacerse cumplir mediante acuerdos jurídicos con proveedores, contratistas y suministradores, como licencias o contratos.

A.34. Es posible que el personal de adquisiciones y de ingeniería no sepa que un dispositivo de uso general se clasificará como SDA si el explotador lo utiliza en una aplicación concreta. En tales casos, los dispositivos deberían adquirirse

teniendo en cuenta la posibilidad de que puedan utilizarse como SDA, y deberían aplicarse los requisitos de seguridad informática adecuados.

A.35. El personal de adquisiciones debería colaborar con el personal de ingeniería para que los requisitos de seguridad informática se especifiquen como requisitos contractuales con los proveedores, contratistas o suministradores y los diseños presentados por los proveedores, contratistas o suministradores cumplan los requisitos de seguridad informática. El personal de adquisiciones también debería informar al personal de ingeniería en caso de que los servicios de asistencia de un proveedor, contratista o suministrador para un SDA dejen de estar disponibles, o parezca probable que dejen de estarlo.

A.36. El personal de adquisiciones debería considerar la posibilidad de proceder a un examen de los proveedores, contratistas y suministradores antes de concertar un acuerdo contractual. Dicho examen puede incluir el análisis de los procesos utilizados por el proveedor, contratista o suministrador para diseñar, desarrollar, probar, implantar o apoyar los SDA o la evaluación de la capacitación y experiencia del proveedor, contratista o suministrador relativas al desarrollo de SDA con los niveles de seguridad informática necesarios. El examen también puede contribuir a a) determinar si los proveedores, contratistas o suministradores primarios disponen de medidas de seguridad para evaluar adecuadamente la probidad de los proveedores, contratistas o suministradores secundarios, y b) garantizar la procedencia de los SDA, los componentes de los SDA y el *software* y actualizaciones proporcionados al explotador.

A.37. El personal de adquisiciones debería velar por que todos los proveedores, contratistas y suministradores de SDA dispongan de procedimientos de notificación al explotador en caso de que se produzcan incidentes en la cadena de suministro que puedan afectar a los SDA (por ejemplo, incidentes que comprometan los componentes del SDA, la tecnología del SDA, los procesos de desarrollo o la información de carácter estratégico).

A.38. El personal de adquisiciones debería considerar la posibilidad de garantizar que los proveedores, contratistas y suministradores de SDA dispongan de una ruta de distribución de confianza para la entrega de SDA, componentes de SDA y *software* y actualizaciones al explotador.

GESTIÓN DE LOS RIESGOS, LA VULNERABILIDAD Y EL CUMPLIMIENTO

Interfaces y relaciones externas relativas a la gestión de riesgos

A.39. Los procesos de gestión de riesgos deberían incluir el análisis de las relaciones externas (es decir, proveedores, contratistas y suministradores). La responsabilidad y rendición de cuentas relativas al cumplimiento de los requisitos derivados del CSRM a nivel de sistemas deberían especificarse en los arreglos contractuales.

A.40. El explotador debería auditar e inspeccionar las actividades pertinentes de los proveedores, contratistas y suministradores para garantizar que se cumplan los requisitos de seguridad informática establecidos en el CSP. En los contratos concertados con proveedores, contratistas y suministradores se les debería exigir a estos que permitan al explotador realizar estas actividades.

A.41. Los procesos de gestión de riesgos del explotador deberían tener en cuenta los requisitos reglamentarios y otros requisitos externos que afecten a la seguridad informática. El explotador debería permitir que las autoridades competentes pertinentes mantengan la supervisión y realicen inspecciones con respecto a las medidas encaminadas a cumplir estos requisitos.

Garantía de la seguridad informática

A.42. Las actividades de garantía de la seguridad informática deberían llevarse a cabo a lo largo del período de vida de la instalación, como se describe en las secciones 4 y 5. Las actividades específicas de garantía variarán en función de la etapa del período de vida. La referencia [8] proporciona información detallada de las actividades de garantía aplicables a los sistemas de instrumentación y control.

A.43. Dichas actividades por parte de un explotador podrían incluir evaluaciones (incluidas auditorías), exámenes, ejercicios y pruebas[46].

A.44. El explotador debería verificar que el CSP concuerde con su política de seguridad informática (por ejemplo, puede utilizarse la evaluación de la seguridad informática para verificar el cumplimiento de los requisitos de seguridad informática que reflejan la política del explotador). Esto puede conllevar una

[46] Los ejercicios y pruebas también pueden utilizarse para otros elementos del CSP, como los procedimientos de seguridad física y la gestión del personal.

serie de evaluaciones complementarias para analizar distintos elementos del CSP y su aplicación. Los resultados de las evaluaciones incluirán la determinación de deficiencias y buenas prácticas, así como propuestas de mejoras.

A.45. Estas actividades deberían servir de base para la mejora continua del CSP. Para ello, las actividades de garantía deberían ser repetibles y fiables y deberían realizarse de forma periódica, así como cada vez que se produzca un incidente de seguridad informática o cambie la amenaza.

A.46. Las actividades de garantía deberían incluir la evaluación de la eficacia organizativa y las medidas adoptadas para garantizar la correcta aplicación y eficacia de la seguridad informática.

A.47. Las actividades de garantía pueden ser realizadas por grupos internos o externos: por ejemplo, la evaluación de la seguridad informática puede ser realizada por un equipo interno como actividad de autoevaluación. Si la evaluación es realizada por grupos externos, los resultados han de verificarse internamente.

A.48. Las actividades de garantía internas y externas deberían complementarse con evaluaciones independientes realizadas por partes externas. Será necesario que los evaluadores independientes tengan acceso al personal, la documentación y los equipos pertinentes. Los evaluadores independientes pueden ser miembros de la entidad explotadora o personas ajenas a esta, pero han de ser independientes respecto a quienes realizaron, verificaron y supervisaron la labor que se evalúa.

A.49. La probidad de los evaluadores independientes o externos debería determinarse antes de que se les permita tener acceso a la información o instalación, ya que es probable que las actividades de garantía estén relacionadas con información de seguridad informática de carácter estratégico. Para más información sobre las evaluaciones de la probidad, véase la referencia [6].

A.50. Los procedimientos de evaluación independiente deberían incluir restricciones adecuadas con respecto a la retirada, uso, almacenamiento y distribución de la información de carácter estratégico y deberían prever la destrucción de dicha información cuando ya no sea necesaria.

A.51. La capacidad para realizar actividades de garantía debería desarrollarse y mantenerse de tal modo que se adapte a los cambios en la tecnología y la amenaza cibernética. Esta capacidad es necesaria tanto para el personal que realiza las actividades de garantía como para la autoridad competente, que podría tener que examinar los resultados de estas actividades.

Alcance de la evaluación

A.52. El explotador debería determinar el alcance de la evaluación en lo que respecta a los ámbitos funcionales y de seguridad física.

A.53. El alcance debería adecuarse a la etapa del período de vida de la instalación. Por ejemplo, en algunas etapas puede ser necesaria una evaluación completa de la seguridad informática, mientras que en otras puede resultar más apropiada la evaluación de ámbitos funcionales o de seguridad física específicos. (La referencia [8] indica actividades de evaluación en diversos momentos del ciclo de vida del sistema de instrumentación y control.)

Técnicas de evaluación

A.54. El equipo de evaluación debería utilizar las siguientes técnicas, según proceda, a la hora de obtener la información que necesita para formular sus conclusiones y recomendaciones:

a) el examen de documentos y registros (por ejemplo, leyes, reglamentos, registros de la instalación);
b) entrevistas con el personal de las organizaciones pertinentes, como el personal de la autoridad competente, el personal de operación de la instalación y representantes de otras organizaciones, y
c) la observación directa de la organización, sus prácticas y sistemas, y la aplicación de medidas de seguridad informática.

Elaboración del informe de evaluación

A.55. El componente de recopilación de datos de la evaluación consiste en registrar observaciones y datos de interés a partir del examen de documentos y registros, entrevistas con el personal y observaciones directas. Las observaciones pueden ser significativas por separado, pero también pueden servir de indicador colectivo de tendencias en la instalación u organización que tal vez sea necesario abordar. Por lo tanto, el explotador debería indicar las observaciones que respalden conclusiones relativas a tendencias o problemas recurrentes.

A.56. Las observaciones deberían analizarse con respecto a requisitos tales como reglamentos nacionales, procedimientos organizativos o normas del sector, según proceda. Se señala una conclusión en caso de que no se cumpla un requisito regulatorio o un procedimiento interno. Los criterios aplicados para

señalar conclusiones han de definirse y acordase debidamente en la etapa de planificación de la evaluación.

A.57. Las observaciones no siempre dan lugar a conclusiones, y no todas las conclusiones son negativas: pueden incluir la determinación de buenas prácticas, prácticas organizativas o procedimientos que proporcionen un método eficaz, por lo general novedoso, para cumplir los objetivos de seguridad física. Se pueden determinar y notificar buenas prácticas para que otras organizaciones puedan adoptarlas con el fin de mejorar su propia seguridad informática.

A.58. Además de las conclusiones y buenas prácticas, el equipo de evaluación también puede presentar recomendaciones y sugerencias en el informe de evaluación en relación con las conclusiones.

A.59. Las recomendaciones ofrecen directrices para cumplir requisitos jurídicos y reglamentarios o normas internacionales (por ejemplo, obligaciones contraídas en virtud de convenciones), según convenga. Las recomendaciones no suelen incluir cómo corregir un problema, sino que solo indican que es necesario corregirlo.

A.60. Las sugerencias aportan un nivel adicional de información sobre una conclusión, lo cual incluye propuestas de medidas correctivas o de mitigación. Dicha información no procede necesariamente de la orientación normativa, sino más bien de normas técnicas y buenas prácticas del sector.

Ejemplo de método de evaluación

A.61. En la referencia [23] se describe un ejemplo de método de evaluación. Dicho ejemplo presenta una evaluación transversal de las operaciones funcionales de una instalación y su seguridad informática. Ello contribuye a garantizar la cobertura de los procesos y sistemas que realizan funciones de la instalación, incluidas las operaciones, la seguridad tecnológica, la seguridad física y la preparación y respuesta para casos de emergencia.

GESTIÓN DE ACTIVOS DIGITALES

Plan de gestión de la configuración

A.62. Las medidas de seguridad informática que protegen los SDA deberían gestionarse en el marco de un plan de gestión de la configuración. Dicho plan

debería ser desarrollado y aplicado por el explotador y debería incluir las siguientes medidas:

a) Asignar las funciones y responsabilidades pertinentes y definir los procesos y procedimientos de gestión de la configuración.
b) Detallar la configuración de los SDA y sus interacciones.
c) Determinar en qué momento del ciclo de vida de desarrollo de sistemas los SDA se someten a la gestión de la configuración.
d) Establecer los medios para determinar los SDA y un proceso de gestión de las medidas de seguridad informática para protegerlos.

Configuración de referencia

A.63. Debería mantenerse al día la configuración de referencia de los SDA en el marco del control de la configuración. La configuración de referencia debería actualizarse según convenga sobre la base de la monitorización del rendimiento de los sistemas y, por ejemplo, para reflejar el fortalecimiento de los sistemas o los efectos de las modificaciones en la seguridad informática.

Fortalecimiento de sistemas

A.64. El explotador debería considerar la posibilidad de establecer un proceso sistemático para el fortalecimiento de sistemas de los SDA. El fortalecimiento de sistemas consiste en la aplicación de un conjunto de medidas de control administrativo y técnico diseñadas para hacer que los componentes del sistema informático sean menos vulnerables a los ciberataques mediante la retirada o desactivación de componentes de *hardware* y *software* que no sean necesarios para el funcionamiento o mantenimiento del sistema. A continuación figuran tipos de *hardware* y *software* que suelen retirarse o desactivarse:

a) protocolos o interfaces de red que no se utilicen (incluida la desactivación del *software* del controlador);
b) periféricos que no se utilicen (incluida la desactivación del *software* del controlador);
c) apoyo para soportes extraíbles;
d) comunicaciones por cable e inalámbricas no autorizadas;
e) servicios de mensajería no relacionados con las funciones de la instalación que realice el sistema;
f) servicios y aplicaciones de medios sociales;
g) servidores o clientes para servicios que no se utilicen;

h) compiladores de *software* en estaciones de trabajo de los usuarios y servidores, excepto los utilizados para el desarrollo de sistemas;
i) compiladores de *software* para lenguajes que no se utilicen en el sistema de control;
j) protocolos de redes y comunicaciones que no se utilicen;
k) programas de optimización administrativa, diagnósticos y funciones gestión de red y de gestión de sistemas que no se utilicen;
l) copias de seguridad de archivos, bases de datos y programas utilizados durante el desarrollo de sistemas;
m) archivos de configuración y datos que no se utilicen;
n) ejemplos de programas y *scripts*;
o) programas de optimización del procesamiento de documentos que no se utilicen;
p) complementos innecesarios para aplicaciones (por ejemplo, navegadores), y
q) juegos.

A.65. El fortalecimiento de sistemas debería ser obligatorio para los SDA que utilicen componentes disponibles en el mercado, cuya funcionalidad debería reducirse a la necesaria para poder realizar las funciones relativas a la instalación (o las funciones relativas a los sistemas) del SDA.

A.66. El fortalecimiento de sistemas debería tener como objetivo reducir la cantidad de datos que hay que monitorizar y analizar para determinar la seguridad física del activo digital o sistema que se protege. El fortalecimiento de sistemas también puede ayudar al explotador a comprender mejor el funcionamiento normal y la funcionalidad del sistema.

A.67. El fortalecimiento de sistemas puede incluir el uso de tecnología para garantizar que solo las versiones aprobadas de los programas informáticos autorizados puedan ejecutarse en el SDA. Los registros del fortalecimiento de sistemas deberían incluir documentación sobre las bibliotecas que haya utilizado la tecnología.

A.68. El fortalecimiento de sistemas debería utilizar únicamente mecanismos de actualización seguros y de confianza. Estos mecanismos de actualización deberían evaluarse para garantizar que eliminen o reduzcan al mínimo la posibilidad de que la actualización se utilice como ruta para atacar el sistema que se esté actualizando, por ejemplo, garantizando que las actualizaciones del sistema se identifiquen mediante las firmas cifradas de los proveedores autorizados.

Consideraciones relativas a las actualizaciones de *software*

A.69. Los proveedores publican actualizaciones de seguridad informática, normalmente en forma de "parches", para subsanar las vulnerabilidades detectadas en sus sistemas. Dado que las modificaciones de los sistemas de seguridad han de seguir procedimientos que requieren un uso intensivo de recursos, la instalación inmediata de un parche tal vez no sea posible, poniendo en riesgo al sistema durante algún tiempo.

A.70. El explotador debería obtener del proveedor o elaborar él mismo una lista de los componentes de *software* utilizados en los sistemas y las actualizaciones de *software* aplicables (incluidos los parches de seguridad).

A.71. El explotador debería contar con un proceso formal para garantizar que se evalúen las actualizaciones de seguridad informática de los equipos y componentes con el fin de determinar su aplicabilidad y efecto y, en concreto, si su instalación inmediata es necesaria para mitigar la vulnerabilidad conexa. El explotador debería instalar la actualización o proporcionar medidas compensatorias eficaces que protejan de forma adecuada frente a la explotación de la vulnerabilidad.

A.72. El explotador debería determinar y aplicar medidas de seguridad informática que proporcionen una seguridad física robusta para poder evaluar las actualizaciones y las vulnerabilidades conexas sin que dichas vulnerabilidades sean explotadas durante el período de evaluación e instalación. Por ejemplo, el fortalecimiento de sistemas podría reducir el número de actualizaciones de seguridad que hayan de evaluarse e instalarse, al no ser necesario instalar actualizaciones que afecten solamente a la funcionalidad que se haya eliminado o desactivado.

PROCEDIMIENTOS DE SEGURIDAD FÍSICA

Monitorización de sistemas

A.73. Todos los sistemas abarcados por el CSP deberían tener asignado un propietario (por ejemplo, un ingeniero de sistemas) que se encargue de monitorizar el sistema.

A.74. La monitorización de sistemas debería incluir la monitorización del estado y eficacia de las medidas de seguridad informática.

A.75. El propietario del sistema debería velar por que los soportes de recuperación y la información de configuración estén actualizados y que los planes de recuperación del sistema se mantengan y puedan ejecutarse cuando sea necesario (por ejemplo, mediante simulacros periódicos del plan de recuperación).

Control de cambios en la configuración

A.76. Los cambios en la configuración de un SDA deberían controlarse teniendo en cuenta de forma explícita los análisis de las consecuencias para la seguridad física. El director o propietario del activo debería aprobar todo cambio en la configuración de un SDA antes de que este se aplique. Esta aprobación debería documentarse formalmente.

A.77. Las actividades asociadas al cambio en la configuración de un SDA deberían ser examinadas por el especialista en seguridad informática. Deberían prepararse, conservarse y examinarse los registros de los cambios realizados en la configuración de un SDA.

A.78. El especialista en seguridad informática debería tener la responsabilidad general de supervisar las actividades de control de los cambios de configuración que afecten a los SDA, pero puede delegar esta función en los propietarios de los activos. El especialista en seguridad informática debería establecer requisitos para garantizar que se realice y coordine una supervisión eficaz.

Ejercicios de seguridad informática (incluidos simulacros)

A.79. La monitorización continua de la eficacia de un CSP en la práctica debería incluir la evaluación de sus componentes mediante ejercicios.

A.80. Los ejercicios de seguridad física de la información y seguridad informática pueden combinar la evaluación con la capacitación. Los ejercicios también deberían incluir escenarios de ataques combinados que incorporen ciberataques y ataques físicos coordinados.

A.81. El sistema de gestión de la seguridad física de la información y la seguridad informática puede ponerse a prueba de forma graduada con respecto al personal que desempeña diferentes funciones y a diferentes niveles dentro de la organización. Los ejercicios ponen a prueba el grado de eficacia de los procesos de trabajo y las comunicaciones en la respuesta a un incidente de seguridad informática; también proporcionan capacitación al personal de todos los niveles que se ocupa de la gestión y respuesta.

A.82. El explotador debería considerar las ventajas que ofrecen las siguientes prácticas:

a) ejercicios relativos a los procedimientos de seguridad física para comprobar la eficacia de los procedimientos a la hora de cumplir los objetivos del CSP, y
b) simulacros para capacitar al personal en la ejecución de los procedimientos de seguridad física y, de ese modo, mejorar el conocimiento de los procedimientos, la justificación de las tareas del procedimiento y la respuesta a los incidentes de seguridad informática.

Pruebas intrusivas

A.83. El explotador debería estudiar la posibilidad de realizar pruebas intrusivas (simulando un ciberataque real en sistemas reales) como parte de la evaluación de la seguridad informática de un sistema o de un activo digital, teniendo en cuenta las consideraciones jurídicas, de seguridad tecnológica y de seguridad física, así como la capacidad del explotador para evitar o remediar cualquier efecto adverso causado al activo digital y al sistema. La referencia [8] indica las restricciones específicas relativas a las pruebas intrusivas de los sistemas de instrumentación y control.

A.84. Puesto que el método detallado de un ciberataque dependerá en gran medida de la configuración exacta de los sistemas atacados, el sistema sometido a prueba ha de ser lo más parecido posible al sistema real. Deberían existir procedimientos de copia de seguridad completa y restablecimiento para devolver el sistema a un estado estable conocido si una prueba de evaluación crea condiciones anormales.

A.85. El plan de pruebas debería especificar el calendario y presupuesto de las pruebas y determinar los objetivos de estas, los entregables previstos, el *hardware* y *software* que se utilizarán, los recursos necesarios, las reglas de intervención y un procedimiento de recuperación.

A.86. Entre las técnicas utilizadas en las pruebas pueden figurar las siguientes:

a) El "registro de la huella digital", que consiste en determinar y cuantificar todas las comunicaciones dentro de los componentes de un sistema, y entre estos, y en analizar los efectos de estas comunicaciones en los SDA a los que

se refieren las pruebas. El registro de la huella digital de una red proporciona la siguiente información:

i) valores de referencia de la red;
ii) un diagrama de red exacto;
iii) la detección de dispositivos maliciosos o comunicaciones de datos dolosas;
iv) la verificación de que los dispositivos de protección de límites funcionan debidamente, y
v) la determinación de oportunidades para mejorar el establecimiento de zonas y la protección del perímetro.

b) El "fuzzing", cuyo objetivo es encontrar errores o vulnerabilidades en un componente o sistema introduciendo una gran diversidad de datos de forma automatizada para detectar tipos de datos y puntos de entrada que podrían utilizarse con fines dolosos. Dicha técnica puede detectar puntos débiles en la codificación del *software* y proporcionar una indicación de la fortaleza del sistema.

A.87. Los indicadores de seguridad informática pueden servir de base común para evaluar las vulnerabilidades. La utilización de indicadores acertados y consensuados (por ejemplo, un sistema común de puntuación de vulnerabilidades) proporciona una base común para comparar vulnerabilidades entre distintos sistemas. El explotador debería evaluar las posibles formas en que podrían explotarse las vulnerabilidades detectadas y tomar medidas para evitar que ello suceda. El explotador debería considerar la posibilidad de notificar todas las vulnerabilidades para su inclusión en una base de datos nacional de vulnerabilidades.

Respuesta a incidentes de seguridad informática

A.88. El personal de seguridad informática debería ser responsable de notificar cualquier presunto incidente de seguridad informática con arreglo al plan de respuesta a incidentes. El explotador debería estudiar la posibilidad de impartir cursos especializados de sensibilización para el personal que desempeñe funciones clave que no estén directamente relacionadas con la seguridad informática, pero que podrían verse afectadas por fallos en esta.

A.89. El explotador debería contar con un plan de contingencia para detectar incidentes de seguridad informática que podrían afectar a los SDA, y para responder a ellos (y con respecto a cualquier otro suceso relacionado con la seguridad física nuclear que implique incidentes de seguridad informática). El plan debería prever procedimientos para determinar la ubicación y naturaleza

de la amenaza, prevenir o mitigar las consecuencias de cualquier acto doloso, notificar dicha información a las autoridades competentes pertinentes y recuperarse del suceso.

A.90. La respuesta a incidentes consiste en un conjunto de actividades (véase la figura 10), cada una de las cuales debería tenerse en cuenta.

A.91. Los incidentes de seguridad informática pueden comprometer la confidencialidad, integridad y/o disponibilidad de los datos procesados, almacenados o transmitidos por un sistema informático. Un incidente de seguridad informática también puede infringir una política de seguridad informática explícita o implícita, una política de uso aceptable o una práctica estándar de seguridad informática. Algunos sucesos adversos (por ejemplo, inundaciones, incendios, cortes de electricidad, calor excesivo) pueden provocar una parada del sistema, pero no son el resultado de actos dolosos y, por tanto, no se consideran incidentes de seguridad informática.

A.92. Un incidente de seguridad informática puede convertirse en un incidente o infracción de seguridad física de la información si compromete o se sospecha que compromete información de carácter estratégico. La referencia [5] proporciona ejemplos de información asociada a instalaciones nucleares que puede ser de carácter estratégico.

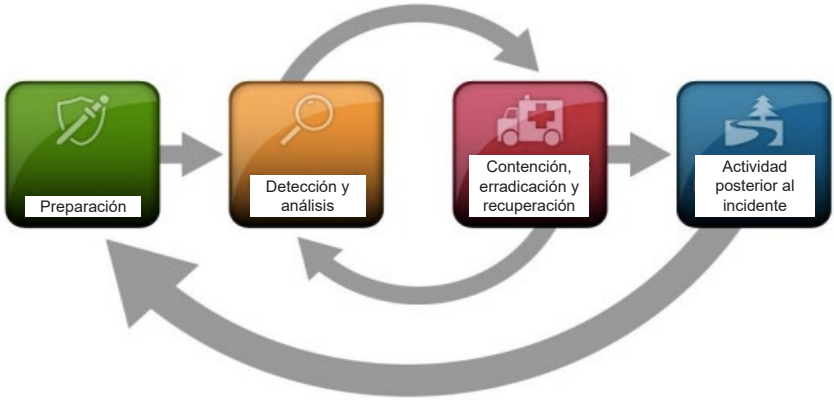


Figura 10. Respuesta a incidentes de seguridad informática (reproducido a partir de la referencia [24] por cortesía del Instituto Nacional de Estándares y Tecnologías, NIST).

A.93. El explotador debería crear un equipo local de respuesta a incidentes de seguridad informática, que sea responsable de responder a los incidentes de seguridad informática que se produzcan dentro de la organización. El tamaño, la composición y la capacidad del equipo de respuesta a incidentes de seguridad informática dependerán de la naturaleza de la organización y de su infraestructura informática, pero este debería incluir a expertos en seguridad física nuclear, seguridad tecnológica nuclear y preparación y respuesta para casos de emergencia, así como en seguridad informática. El equipo de respuesta a incidentes de seguridad informática puede tener los mismos miembros que el equipo de seguridad informática, o algunos miembros en común con este.

A.94. Un grupo de respuesta a emergencias informáticas es una autoridad técnica que proporciona asistencia y capacidad de respuesta cuando se produce un incidente de seguridad informática. El grupo de respuesta a emergencias informáticas puede existir a distintos niveles (por ejemplo, nacional, local, sector industrial). El grupo de respuesta a emergencias informáticas puede servir para complementar la capacidad interna de respuesta de seguridad informática de una entidad explotadora a la hora de responder a cualquier incidente de seguridad informática. La disponibilidad de este grupo para responder en momentos de crisis debería tenerse en cuenta al planificar las actividades de respuesta de la entidad explotadora.

A.95. El explotador debería garantizar la participación en los ejercicios por parte de los miembros del grupo de respuesta a emergencias informáticas que formarían parte de la respuesta, así como de los miembros del equipo de respuesta a incidentes de seguridad informática. Deberían tenerse en cuenta las interrelaciones entre el grupo de respuesta a emergencias informáticas y el equipo de respuesta a incidentes de seguridad informática, incluidas las actividades preparatorias (por ejemplo, la acreditación previa de los miembros del grupo de respuesta a emergencias informáticas para acceder a zonas señaladas de la instalación). Los ejercicios deberían diseñarse para poner a prueba los elementos clave de comunicación entre las autoridades competentes, el grupo de respuesta a emergencias informáticas, el equipo de respuesta a incidentes de seguridad informática y las operaciones en el emplazamiento, como se muestra en la figura 11.

Figura 11. Interrelaciones en la respuesta a incidentes de seguridad informática.

Fases de la respuesta a incidentes de seguridad informática

Preparación

A.96. Las medidas de planificación en la fase de preparación incluyen el establecimiento de una política que guíe los procesos operacionales de respuesta a incidentes de seguridad informática, la definición de las funciones y responsabilidades de todas las partes implicadas en la respuesta a incidentes, la redacción de procedimientos acordes con la política, y la determinación de los activos disponibles para dicha respuesta. Es necesario definir claramente los requisitos y criterios que se utilicen para responder a incidentes de seguridad informática. El plan de medidas de respuesta debería ser aprobado por el personal directivo superior.

Detección y análisis

A.97. Durante la fase de detección y análisis, el equipo de respuesta a incidentes de seguridad informática debería encargarse de la caracterización técnica del incidente. Las actividades de detección incluyen garantizar que exista una monitorización de datos adecuada para apoyar la detección mediante la recopilación y conservación de información relacionada con posibles incidentes. El equipo de respuesta a incidentes de seguridad informática puede utilizar un entorno de pruebas y evaluación especializado para analizar incidentes sin afectar a los sistemas operacionales ni alterar las posibles pruebas forenses.

A.98. Las actividades de análisis pueden ir más allá del equipo de respuesta a incidentes de seguridad informática y la caracterización técnica inicial del incidente, y algunos aspectos del análisis pueden requerir amplios recursos. Entre las prioridades de análisis habituales figuran las siguientes:

a) determinar los posibles efectos del incidente de seguridad informática en la seguridad física nuclear, la seguridad tecnológica nuclear y la preparación y respuesta para casos de emergencia, y determinar medidas para restablecer las condiciones de seguridad de la instalación;
b) determinar el alcance del incidente para establecer una respuesta adecuada;
c) determinar los daños que pueda causar el incidente de seguridad informática por lo que respecta a la pérdida de información, los daños físicos a la instalación y la percepción pública;
d) determinar la naturaleza del incidente de seguridad informática con respecto a la intención inmediata del adversario y posibles amenazas futuras, incluida la posibilidad de que un futuro ataque aproveche los efectos derivados de este incidente;
e) determinar la causa básica del incidente de seguridad informática y las medidas necesarias para prevenir futuros incidentes de naturaleza similar, o mitigar sus efectos, y
f) identificar al adversario y elaborar el perfil correspondiente, que incluya las técnicas y herramientas utilizadas y las vulnerabilidades explotadas por este.

Mitigación (contención, erradicación y recuperación)

A.99. Las medidas de mitigación tienen por objeto contener un incidente de seguridad informática; erradicar cualquier programa malicioso o corregir cualquier mal funcionamiento o configuración alterada de los sistemas afectados, y restablecer el funcionamiento de los sistemas y la integridad de los datos, utilizando medidas compensatorias según convenga. Incluso si los componentes o sistemas comprometidos no realizan una función esencial de seguridad tecnológica o seguridad física, han de ser revisados y aprobados para evitar que el ataque se propague a un componente o sistema que sí realice una función de ese tipo. Las actividades de mitigación continúan y se adaptan a medida que se recopila y analiza la información durante la fase de detección y análisis.

A.100. Al planificar la forma de contener los incidentes de seguridad informática, el explotador debería reconocer que, durante la investigación del incidente, pueda determinarse que una serie de componentes o sistemas se hayan visto comprometidos. Si alguno de los componentes o sistemas comprometidos

desempeña una función esencial de seguridad tecnológica o seguridad física — como contribuir a la protección de los SDA, al funcionamiento de la instalación en condiciones de seguridad o a la protección de material nuclear u otros materiales radiactivos — será necesario aplicar medidas compensatorias para desempeñar esa función hasta que el componente o sistema pueda volver a ponerse en funcionamiento.

A.101. Las medidas de recuperación pueden incluir la sustitución por un elemento equivalente (por ejemplo, un cortafuegos de seguridad); el aislamiento de las estructuras, sistemas y componentes de seguridad tecnológica respecto del componente o sistema comprometido, o medidas temporales, como un guardia que controle el acceso a la parte afectada de la instalación en sustitución de un sistema digital de control del acceso. Las medidas de recuperación han de reemplazar la función, y no necesariamente el componente o sistema comprometido.

Actividades posteriores al incidente

A.102. La última fase de la respuesta son las actividades posteriores al incidente para aplicar medidas que impidan la repetición de tipos similares de incidentes de seguridad informática en el futuro, permitan su rápida detección y/o reduzcan al mínimo sus consecuencias. Esta fase puede incluir el aprendizaje de lecciones dentro de la organización y el intercambio de inteligencia sobre amenazas y lecciones aprendidas, según convenga, con la comunidad más amplia de respuesta a incidentes de seguridad informática para ayudar a prevenir que un ataque parecido tenga éxito en otro lugar. Las conclusiones posteriores al incidente pueden permitir la formulación de nuevas medidas de seguridad física para prevenir la reinfección y proporcionar información para actualizar los perfiles de amenazas y vulnerabilidades. Otras actividades posteriores al incidente pueden incluir evaluar la eficacia del CSP y determinar la capacitación necesaria para subsanar cualquier deficiencia en la respuesta del personal, así como evaluar los recursos que fueron necesarios para hacer frente al incidente de seguridad informática como guía para la planificación de cara a futuros incidentes.

Notificación

A.103. Durante la respuesta a un incidente de seguridad informática puede haber situaciones en las que sea necesario o conveniente informar de ello a las autoridades competentes (u otras organizaciones). Las notificaciones permiten informar oportunamente a todas las personas que es necesario que estén al corriente de un incidente de seguridad informática. Dado que es probable que quienes respondan al incidente estén ocupados, el explotador ha de considerar

detenidamente la frecuencia de las notificaciones y el grado de detalle proporcionado. El explotador puede considerar la posibilidad de asignar a una persona específica como punto de contacto para la notificación de incidentes de seguridad informática y para atender las solicitudes de información de organizaciones externas.

Planificación de actividades

A.104. La planificación de actividades debería garantizar que se determinen y planifiquen los requisitos de seguridad informática relativos a la realización y verificación de las actividades.

A.105. Deberían determinarse las cualificaciones necesarias del personal y de los contratistas en materia de seguridad informática para las actividades que se realicen, lo cual debería tenerse en cuenta en la planificación. Cada organización responsable tiene la responsabilidad de notificar presuntos incidentes de seguridad informática con arreglo al plan de respuesta a incidentes.

A.106. A la hora de elaborar instrucciones de trabajo, hay que tener en cuenta los requisitos de seguridad informática. Estas podrían incluir instrucciones para lo siguiente:

a) la supresión de medidas de seguridad informática (para permitir el mantenimiento);
b) la adopción de medidas alternativas o compensatorias (mientras no estén disponibles las medidas normales);
c) la reactivación de las medidas de seguridad informática (tras el mantenimiento), y
d) confirmar que las medidas de seguridad informática se han restablecido de forma correcta.

A.107. Las instrucciones de mantenimiento deberían incluir instrucciones para configurar los ajustes de seguridad de los dispositivos.

A.108. Si el mantenimiento requiere la eliminación de equipos que ya no son necesarios, estos equipos deberían desinfectarse o destruirse de forma segura.

A.109. Los requisitos en materia de adquisiciones relacionados con la seguridad informática deberían determinarse y aplicarse en el plan de trabajo.

SENSIBILIZACIÓN Y CAPACITACIÓN

A.110. Aunque las computadoras se utilizan en muchos ámbitos de la vida laboral y personal, existe una falta general de conciencia y conocimientos sobre la tecnología, las ciberamenazas, las medidas de seguridad informática y los posibles efectos en caso de que esta se vea comprometida. La sensibilización y capacitación en materia de seguridad informática son necesarias para todo el personal y los contratistas de organizaciones que tengan responsabilidades relacionadas con la seguridad física nuclear.

A.111. Los errores humanos provocan incidentes de seguridad informática, o contribuyen negativamente a ellos. El personal de todos los niveles precisa una sensibilización y reafirmación continua en materia de seguridad informática.

A.112. La sensibilización sobre su importancia puede contribuir a la seguridad informática de la siguiente manera:

a) fomentando la comprensión de que la seguridad informática apoya no solo la seguridad física nuclear de la instalación, sino también su seguridad tecnológica;
b) asegurando una comprensión común de los aspectos clave de la seguridad informática dentro de la organización;
c) alentando la observación y el acompañamiento experto de los compañeros, la notificación de posibles incidentes de seguridad informática y seguridad física de la información, y la conciencia situacional;
d) fomentando la comprensión de que los ciberataques pueden afectar simultáneamente a múltiples medidas de seguridad física y/o seguridad tecnológica, reduciendo la defensa en profundidad;
e) aportando medios para poder solucionar los conflictos entre los objetivos de seguridad tecnológica y seguridad física;
f) reconociendo y fomentando las buenas prácticas en materia de seguridad informática, y
g) sensibilizando sobre la manera en que los seres humanos pueden contribuir sin darse cuenta a los incidentes de seguridad informática.

A.113. Los siguientes indicadores pueden utilizarse para evaluar la conciencia en materia de seguridad informática en una organización:

a) Los requisitos de seguridad informática se documentan de forma clara y el personal los entiende bien.

b) Existen protocolos y procedimientos claros y eficaces para utilizar los sistemas informáticos tanto dentro como fuera de la organización.
c) Los miembros del personal comprenden la importancia de las medidas de seguridad informática establecidas en el CSP, y son conscientes de ella.
d) Los sistemas informáticos se mantienen en condiciones de seguridad y funcionan con arreglo a los valores de referencia de seguridad informática y los procedimientos aprobados.
e) El incumplimiento de los procedimientos de seguridad informática es considerado grave e indeseable por parte de todos.
f) Los resultados de las observaciones, evaluaciones, pruebas y ejercicios son positivos (por ejemplo, las pruebas indican que el personal no responde a los correos electrónicos de suplantación de identidad).
g) El personal directivo está plenamente comprometido con las iniciativas de seguridad física, ya estén relacionadas con los sistemas cibernéticos o físicos, y las apoya.

A.114. El objetivo de un programa de capacitación en seguridad informática es garantizar que el personal y los contratistas tengan los conocimientos y la capacidad necesarios para realizar su trabajo con arreglo a los requisitos y procedimientos de seguridad informática de la instalación. La capacitación en seguridad informática debería incorporarse a un sistema de gestión de la capacitación ya existente.

A.115. El explotador debería contar con un programa de capacitación que incluya los siguientes elementos:

a) Un programa de capacitación en seguridad informática, cuya superación sea imprescindible para acceder a los sistemas informáticos. La capacitación debería concordar con los niveles de seguridad informática de los sistemas a los que tenga acceso quien la reciba.
b) Una capacitación y cualificación especializadas para quienes tengan responsabilidades clave en materia de seguridad física (por ejemplo, especialista en seguridad informática, equipo de seguridad informática, otros oficiales de seguridad física, directores de proyectos, administradores de tecnología de la información, ingenieros de sistemas, diseñadores, técnicos, personal de gestión de documentos, personal de proyectos, personal de adquisiciones, contratistas, personal directivo superior).
c) Material de capacitación que se actualice de forma periódica para incluir nuevos procedimientos y medidas con el fin de hacer frente a las amenazas emergentes.

d) Capacitación que se repita de forma periódica para garantizar que el personal esté familiarizado con los procedimientos y amenazas más recientes.
e) El requisito de que el personal reconozca que comprende sus responsabilidades en materia de seguridad informática.
f) Evaluaciones prácticas de la comprensión por parte del personal de sus responsabilidades en materia de seguridad informática.

A.116. Deberían utilizarse diversos enfoques de capacitación, como el aprendizaje electrónico, clases presenciales, ejercicios prácticos y foros de debate[47]. Las organizaciones externas, incluido el OIEA, pueden proporcionar material de apoyo a dichas actividades.

A.117. El programa de capacitación debería incluir a) indicadores para evaluar la conciencia en materia de seguridad informática y la eficacia de la capacitación, y b) procesos de mejora continua y capacitación periódica de repaso y actualización para el personal, según convenga.

EJEMPLO DE PROCESO DE PLANIFICACIÓN DE LA RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA

A.118. En la referencia [25] se incluye un ejemplo de proceso para planificar la respuesta a incidentes de seguridad informática.

[47] Los foros de debate pueden dar lugar a filtraciones de información que podrían ayudar al adversario; por lo tanto, se desaconseja la publicación de información en foros de debate abiertos y de acceso público.

REFERENCIAS

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

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

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

[4] INSTITUTO INTERREGIONAL DE LAS NACIONES UNIDAS PARA INVESTIGACIONES SOBRE LA DELINCUENCIA Y LA JUSTICIA, OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO, OFICINA EUROPEA DE POLICÍA, ORGANISMO INTERNACIONAL DE 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.

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

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

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

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

[9] 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.

[10] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Seguridad física durante el período de vida de una instalación nuclear*, *Colección de Seguridad Física Nuclear del OIEA* Nº 35-G, OIEA, Viena, 2022.

[11] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary, ISO/IEC 27000:2018, ISO, Geneva (2018).
[12] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Glosario de seguridad del OIEA: Terminología empleada en seguridad tecnológica nuclear y protección radiológica*, edición de 2018, OIEA, Viena, 2022.
[13] 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.
[14] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Information Security Risk Management, ISO/IEC 27005:2018, ISO, Geneva (2018).
[15] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Protección física de los materiales y las instalaciones nucleares (aplicación del documento INFCIRC/225/Rev. 5)*, *Colección de Seguridad Física Nuclear del OIEA* Nº 27-G, OIEA, Viena, 2019.
[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Identification of Vital Areas at Nuclear Facilities, IAEA Nuclear Security Series No. 16, IAEA, Vienna (2013).
[17] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Clasificación de las estructuras, los sistemas y los componentes de una central nuclear desde el punto de vista de la seguridad*, *Colección de Normas de Seguridad del OIEA* Nº SSG-30, OIEA, Viena, 2021.
[18] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Evaluation Criteria for IT Security, ISO/IEC 15408:2009, ISO, Geneva (2009).
[19] ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN, COMISIÓN ELECTROTÉCNICA INTERNACIONAL, *Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos*, ISO/IEC 27001:2013, ISO, Ginebra, 2013.
[20] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems — Requirements for Security Programmes for Computer-Based Systems, IEC 62645:2014, IEC, Geneva (2014).
[21] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Code of Practice for Information Security Controls, ISO/IEC 27002:2013, ISO, Geneva (2013).
[22] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Sistema de gestión de instalaciones nucleares*, *Colección de Normas de Seguridad del OIEA* Nº GS-G-3.5, OIEA, Viena, 2017.
[23] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Evaluación de la seguridad física informática en las instalaciones nucleares*, OIEA, Viena, 2018.

[24] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Computer Security Incident Handling Guide, NIST SP 800-61, Rev. 2, NIST, Gaithersburg (2012).
[25] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Planificación de la respuesta a incidentes de seguridad física informática en las instalaciones nucleares*, OIEA, Viena, 2018.

Anexo I

POSIBLES ESCENARIOS DE ATAQUE CONTRA SISTEMAS DE LAS INSTALACIONES NUCLEARES

I-1. El presente anexo proporciona algunos ejemplos de formas en que los adversarios podrían explotar las vulnerabilidades de los sistemas que realizan funciones esenciales de una instalación. No obstante, se trata solo de ejemplos, y los explotadores han de pensar de forma creativa sobre la seguridad informática para imaginar cómo podrían actuar los adversarios y cómo las medidas de seguridad informática podrían contrarrestar sus acciones.

I-2. Los ejemplos proceden de conversaciones con expertos de los Estados Miembros. No pretenden ofrecer una lista exhaustiva de posibilidades o una fórmula para atacar instalaciones nucleares, sino más bien un punto de partida para que los explotadores de instalaciones y los Estados Miembros formulen planes encaminados a hacer frente al entorno dinámico y en constante cambio de las ciberamenazas.

I-3. Un ciberataque coordinado puede constar de varias fases:

a) la determinación de uno o varios blancos;
b) la realización de actividades de reconocimiento;
c) la obtención de acceso a los sistemas pertinentes o la realización de acciones que los comprometan de otro modo;
d) la ejecución del ataque, y
e) la ocultación de pruebas sobre el ataque y el adversario.

I-4. Los adversarios emplearán la totalidad o parte de estas tácticas, y es necesario tenerlas en cuenta a la hora de crear perfiles de ciberamenazas específicos para los sistemas de instrumentación y control de las instalaciones nucleares y otros activos digitales de carácter estratégico (SDA). Los ejemplos de escenarios que figuran en el presente anexo incluyen el uso de estas tácticas e ilustran tipos comunes de ataque sugeridos por expertos en seguridad informática con experiencia en la industria nuclear.

I-5. Los tipos de amenaza se describen en la referencia [I-1].

ESCENARIO I: CIRCUNSTANCIAS EN QUE SE COMPROMETEN SERVICIOS DE APOYO QUE DAN ACCESO A SISTEMAS OPERACIONALES ESENCIALES

I-6. Objetivo del ataque: Obtener acceso a información nuclear y activos digitales explotando una ruta de confianza utilizada por los proveedores para prestar apoyo.

I-7. Descripción: El ataque se dirige inicialmente al portal de acceso remoto basado en Internet, a través del cual los proveedores tienen acceso a información de carácter estratégico y a los SDA de la instalación para prestar apoyo. El adversario compromete el portal y, a través del aumento de privilegios, obtiene el control administrativo de la base de datos y cambia la dirección de correo electrónico asociada a un proveedor específico. Este proveedor tiene acceso remoto a información operacional esencial sobre la instalación y algunos de los SDA. El adversario utiliza la función de "contraseña olvidada" del portal, que envía un enlace para actualizar la contraseña a la dirección de correo electrónico introducida por el adversario. El adversario utiliza este enlace para cambiar la contraseña del proveedor e inicia sesión en el portal con la identidad del proveedor autorizado. Una vez dentro, el adversario tiene acceso a toda la información del portal y a todos los SDA a los que el proveedor tiene acceso. A continuación, el adversario empieza a modificar los ajustes y parámetros operacionales de los SDA, lo que provoca inestabilidad operacional y, finalmente, la parada de la instalación.

ESCENARIO II: EXPLOTACIÓN DE LA CONFIANZA TRANSITIVA ENTRE LOS SERVIDORES DE INFORMES DE LA RED PERIMETRAL Y LOS SDA INTERNOS

I-8. Objetivo del ataque: Acceder a los sistemas y SDA internos.

I-9. Descripción:

1) Por medio de herramientas de código abierto y motores de búsqueda, el adversario localiza el servidor de la red perimetral[1] utilizado para comunicar información de producción relacionada con isótopos nucleares desde

[1] Las redes de este tipo se utilizan como "amortiguadores" entre los sistemas internos de confianza y los sistemas de acceso público que no son de confianza, como Internet. A veces se denominan "zonas desmilitarizadas".

sistemas internos de confianza a Internet. Este servidor se encuentra en la red perimetral, pero recibe datos de un servidor de la base de datos maestra en la misma red que el sistema de control de una instalación que produce isótopos nucleares. El servidor de la base de datos maestra recoge información del entorno de producción interno y envía esta información a la base de datos situada en la red perimetral. La red perimetral está separada de la red de producción por un cortafuegos, cuya configuración incluye una lista de control del acceso para garantizar que solo la base de datos del servidor de la red perimetral pueda comunicarse con la base de datos maestra.

2) El adversario explota una vulnerabilidad para obtener acceso administrativo al servidor de la red perimetral y toma el control del canal de comunicación entre ese servidor y el servidor de la base de datos maestra en la red del sistema de control. El cortafuegos está configurado para permitir las comunicaciones entre la red perimetral y la base de datos maestra (es decir, establece una "confianza transitiva" entre las redes), de modo que el adversario, que tiene el control del servidor en la red perimetral, puede conectarse directamente a la base de datos maestra en la red del sistema de control.
3) El adversario utiliza la conexión a la base de datos maestra para realizar un reconocimiento y enumeración de los activos del sistema de control que se encuentran en la misma red. Al no haber medidas de seguridad en la red del sistema de control, el adversario puede hacerse con el control de los SDA y comprometer la tecnología que controla el desarrollo, la gestión, el transporte, el almacenamiento y el inventario de isótopos.

ESCENARIO III: INFECCIÓN DE LOS SISTEMAS DE INSTRUMENTACIÓN Y CONTROL DE UNA CENTRAL NUCLEAR MEDIANTE PROGRAMAS MALICIOSOS

I-10. Objetivo del ataque: Forzar la parada de una central nuclear.

I-11. Descripción:

1) Un ingeniero de una central nuclear trabaja en casa con una computadora portátil que se utiliza para apoyar la ingeniería y optimización de la central, actualizar los programas de rendimiento y "afinar" el *software* de monitorización de la seguridad tecnológica.
2) Mientras está en casa, el ingeniero utiliza la computadora para acceder al sitio web de un proveedor y obtener una actualización de *software* para los sistemas de instrumentación y control que son fundamentales para apoyar

las operaciones de la central. Mientras la actualización se descarga, el ingeniero utiliza un banco en línea, visita el sitio web corporativo y utiliza los medios sociales, durante lo cual un *software* malicioso queda descargado en la computadora. Se trata de un programa malicioso nuevo que no es detectado por el *software* antivirus de la computadora.

3) Dado que la política corporativa prohíbe llevar la computadora a la central, el ingeniero copia la actualización que ha descargado del sistema de control en un dispositivo de almacenamiento USB, con la intención de utilizarlo para aplicar las actualizaciones de *software* a los activos de instrumentación y control. Sin embargo, el programa malicioso también se ha copiado a sí mismo en el dispositivo USB, y cuando el ingeniero lo utiliza para instalar la actualización a través de una estación de trabajo de ingeniería en la central, el programa malicioso se copia a sí mismo en el sistema de la central. El explotador de la central supone que las medidas implantadas de protección física impedirán que una computadora no autorizada se conecte a la red del sistema de control de la central, y no se ha tenido en cuenta la posibilidad de infección a través de soportes extraíbles.
4) Una vez que el programa malicioso infecta la estación de trabajo de ingeniería, se replica y se propaga a otros componentes conectados en red dentro de la central. Puesto que el explotador no ha implantado medidas de seguridad informática en la central y no hay ningún *software* antivirus en los sistemas esenciales de la central, el programa malicioso infecta los activos digitales esenciales de la red, provocando fallos y obligando a parar la central.

ESCENARIO IV: OBTENCIÓN DE INFORMACIÓN DE CARÁCTER ESTRATÉGICO SOBRE LAS OPERACIONES DE UNA CENTRAL NUCLEAR DIRECTAMENTE DE EQUIPOS RETIRADOS DEL SERVICIO DE FORMA INDEBIDA

I-12. Objetivo del ataque: Obtener información suficiente para planificar un ataque preciso contra las operaciones de una central.

I-13. Descripción:

1) Un adversario recoge información a partir de los medios sociales y la observación según la cual una instalación nuclear va a adquirir un sistema de control en forma de actualización de sistemas. Además, el explotador de la instalación tiene previsto vender equipos operacionales antiguos para ayudar a sufragar el nuevo sistema de control.

2) Dado que la instalación no cuenta con un procedimiento formal de retirada del servicio relativo a la seguridad física de la información, se vende un sistema que se utilizaba para realizar operaciones esenciales de instrumentación y control sin examinar ni eliminar la información almacenada en él. El adversario compra el sistema y descubre información actualizada relativa a archivos de proyectos, diagramas de red, nombres de usuario y contraseñas, y otros datos que permiten conocer de forma exhaustiva las operaciones de la instalación nuclear.
3) El adversario utiliza esta información con el fin de elaborar un plan para atacar SDA específicos utilizados en la instalación y crear correos electrónicos convincentes para utilizarlos en una campaña de suplantación de identidad. Finalmente, el adversario utiliza tanto la información obtenida del sistema adquirido como la proporcionada involuntariamente por las víctimas de la campaña de suplantación de identidad para lanzar un ataque combinado contra la instalación.

ESCENARIO V: INGENIERÍA SOCIAL ESTRATÉGICA DIRIGIDA AL OFICIAL DE SEGURIDAD FÍSICA DE UNA INSTALACIÓN

I-14. Objetivo del ataque: Obtener, mediante ingeniería social, información de un oficial de seguridad física de una instalación que pueda servir para promover un ataque.

I-15. Descripción:

1) Un adversario realiza una campaña de ingeniería social dirigida contra un oficial de seguridad física de una instalación mediante el uso de técnicas de suplantación de identidad, el reconocimiento físico e información pública disponible, incluida la procedente de la presencia del oficial en los medios sociales.
2) El adversario, bajo una identidad falsa, utiliza esta información para empezar a comunicarse directamente con el oficial de seguridad física, quien llega a confiar en él de forma gradual, creyendo que se trata de otra persona. A medida que la correspondencia continúa, el adversario empieza a adjuntar archivos creíbles a los correos electrónicos que, en realidad, contienen *software* malicioso que, al activarse, abre de forma encubierta una ruta de comunicación con la computadora del adversario y envía archivos específicos desde la computadora del oficial de seguridad física al adversario. Con esta información, el adversario es capaz de crear planes

precisos y detallados para atacar los sistemas de protección física de la central e interceptar materiales nucleares en tránsito.

REFERENCIA DEL ANEXO I

[I–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security for Nuclear Security, IAEA Nuclear Security Series No. 42-G, IAEA, Vienna (2021).

Anexo II

EJEMPLO DE ASIGNACIÓN DE NIVELES DE SEGURIDAD INFORMÁTICA PARA UNA CENTRAL NUCLEAR

II-1. La asignación de niveles de seguridad informática a sistemas (o a zonas que contienen sistemas) se basa en las consecuencias que pueda tener un ataque para cada sistema con respecto a la seguridad tecnológica, la seguridad física y el funcionamiento de la instalación: cuanto menos tolerables sean las consecuencias, más estricto será el nivel de seguridad informática.

II-2. Para evitar el análisis individual de cada sistema y posible consecuencia, pueden establecerse criterios que faciliten la asignación de los niveles de seguridad informática.

II-3. Una consideración fundamental es la clasificación del sistema desde el punto de vista de la seguridad tecnológica. Sin embargo, no hay una conexión automática entre los niveles de seguridad informática y las clases de seguridad tecnológica. Es necesario que un sistema que sea importante para la seguridad tecnológica tenga asignado un nivel de seguridad informática estricto, pero también puede ser necesario que los sistemas sin clasificación de seguridad tecnológica tengan asignado un nivel estricto si desempeñan un papel esencial en la prevención de posibles consecuencias graves para la seguridad física.

II-4. Un ejemplo de enfoque graduado de los niveles de seguridad informática utiliza los siguientes criterios generales:

1) El nivel 1 de seguridad informática se asigna a los sistemas digitales de la central respecto a los cuales el hecho de que su integridad o disponibilidad se vean comprometidas podría dar lugar a consecuencias radiológicas para la población situada fuera del emplazamiento. Ello corresponde al criterio para los sistemas con clasificación de seguridad tecnológica 1E/F1A (correspondientes a los sistemas que apoyan funciones de la categoría A en el sistema de seguridad tecnológica de la Comisión Electrotécnica Internacional [II-1]).
2) El nivel 2 de seguridad informática se asigna a los sistemas digitales de la central respecto a los cuales el hecho de que su integridad o disponibilidad se vean comprometidas podría degradar uno o varios de los siguientes aspectos:
    i) la gestión de una emergencia;

ii) la seguridad tecnológica de la central durante su funcionamiento normal;
iii) el funcionamiento del proceso nuclear principal, y
iv) la protección física de la central.

3) El nivel 3 de seguridad informática se asigna a los sistemas digitales de la central respecto a los cuales el hecho de que su integridad o disponibilidad se vean comprometidas no tiene consecuencias radiológicas ni efectos adversos para la seguridad tecnológica o la protección física, pero podría tener otros efectos importantes. Tales sistemas podrían incluir, en particular, activos digitales que contribuyan al funcionamiento o mantenimiento de la central, o sistemas que podrían afectar la generación de energía.
4) El nivel 4 de seguridad informática se asigna a los sistemas digitales de una central respecto a los cuales el hecho de que su integridad o disponibilidad se vean comprometidas no tiene un efecto a corto plazo en el rendimiento de la central, pero puede tener un efecto de ese tipo a más largo plazo.
5) El nivel 5 de seguridad informática se asigna a los sistemas digitales de la central respecto a los cuales el hecho de que su integridad o disponibilidad se vean comprometidas no afecta a la seguridad tecnológica, a la disponibilidad de la central o al rendimiento de la instalación.

II-5. Además de estos criterios generales, la definición de los niveles de seguridad informática puede incluir una lista de funciones típicas de la instalación o tipos de sistemas que son específicos de cada nivel. Esta lista podría simplificar la asignación de niveles de seguridad informática a los sistemas.

II-6. La clasificación de niveles de seguridad informática se centra en las posibles consecuencias relacionadas con el hecho de que se comprometan los sistemas informáticos (véase la referencia [II-2]). En muchos casos, la información adquirida o calculada por un sistema digital también puede ser obtenida con herramientas analógicas o por una persona, en cuyo caso el nivel de seguridad informática puede ser menos estricto (y, por tanto, menos restrictivo para el funcionamiento normal).

II-7. Cuando se utilizan varios activos digitales distintos para la misma función, es necesario elegir un sistema primario que apoye la función y asignarlo a un nivel de seguridad informática acorde con las consecuencias que puedan producirse en caso de que se vea comprometido.

REFERENCIAS DEL ANEXO II

[II–1] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Important to Safety — General Requirements for Systems, IEC 61513:2011, IEC, Geneva (2011).

[II–2] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems — Requirements for Security Programmes for Computer-Based Systems, IEC 62645:2014, IEC, Geneva (2014).

Anexo III

EJEMPLO DE APLICACIÓN DE NIVELES Y ZONAS DE SEGURIDAD INFORMÁTICA

INFORMACIÓN GENERAL

III-1. El presente anexo proporciona un ejemplo de la aplicación de niveles y zonas de seguridad informática. El cuadro III-1 proporciona una lista de los sistemas utilizados en este ejemplo y muestra la correspondencia de los niveles de seguridad informática con las zonas físicas y lógicas utilizadas en este ejemplo.

III-2. En el caso de sistemas simples, que constan de un número reducido de activos en ubicaciones físicas bien definidas, la aplicación de los niveles de seguridad informática y de las zonas físicas y lógicas es sencilla. Ello resulta más complicado en el caso de sistemas complejos que se extienden por toda la instalación o de zonas físicas que contienen sistemas que es necesario asignar a múltiples niveles de seguridad física, como la sala de control principal.

SALA DE CONTROL PRINCIPAL

III-3. Normalmente, la sala de control principal contiene controles para muchas categorías diferentes de sistemas que tienen distintos requisitos de seguridad física (por ejemplo, sistemas de seguridad tecnológica, suministro de vapor (caldera), sistemas eléctricos, sistemas auxiliares, sistemas informáticos). Las interfaces persona-máquina de todos los sistemas de la instalación se encuentran total o parcialmente en la sala de control principal. Estos sistemas e interfaces persona-máquina suelen utilizar activos digitales para realizar sus funciones.

III-4. En las instalaciones antiguas, esto crea dificultades en la aplicación de la seguridad informática por varios motivos:

a) Las consolas de interfaces persona-máquina más antiguas suelen incluir controles para varios sistemas, especialmente para la parte no nuclear de la central y sistemas auxiliares. Esta agregación puede dificultar el aislamiento y la separación de estos sistemas. En algunos casos, pueden combinarse funciones de la instalación realizadas por sistemas asignados a distintos niveles de seguridad informática en una sola consola de la interfaz persona-

máquina, a la que es necesario aplicar el nivel de seguridad física más estricto.

b) Los activos digitales situados dentro del espacio físico de la sala de control principal y sus salas de equipos tendrían asignados, utilizando el enfoque de niveles y zonas de seguridad informática, diferentes niveles de seguridad informática. Por ejemplo, un sistema de protección del reactor puede tener asignado el nivel más estricto (p. ej., nivel de seguridad 1), mientras que una computadora personal que permita al explotador acceder al correo electrónico puede tener asignado el nivel menos estricto (p. ej., nivel de seguridad 5).

c) El personal que realiza actividades autorizadas en un sistema dentro de la sala de control principal puede tener acceso a otros equipos dentro de dicha sala.

III-5. Se presenta el siguiente ejemplo ilustrativo para explicar posibles soluciones de seguridad informática a los problemas descritos anteriormente, en relación con los conceptos que se detallan en la figura 1 del texto principal.

III-6. La aplicación de zonas de seguridad informática a la sala de control principal (conjuntamente con los sistemas de protección física y de protección contra incendios) resulta difícil debido a la necesidad de monitorizar y gestionar de manera centralizada las funciones de la instalación. El concepto de zonas de seguridad informática permite establecer límites físicos y/o lógicos, lo cual puede contribuir a subsanar estas limitaciones. La relación se ilustra en la figura III–1.

III-7. Se supone que la sala de control principal (y las salas dentro de la zona protegida que contienen equipos electrónicos) está clasificada y protegida como zona vital. Esto implica que el sabotaje de los equipos de la sala de control principal podría llegar a tener consecuencias radiológicas inaceptables.

III-8. El cuadro III-1 presenta un ejemplo de un subconjunto de sistemas que es necesario monitorizar o utilizar o que requieren comunicaciones desde la sala de control principal.

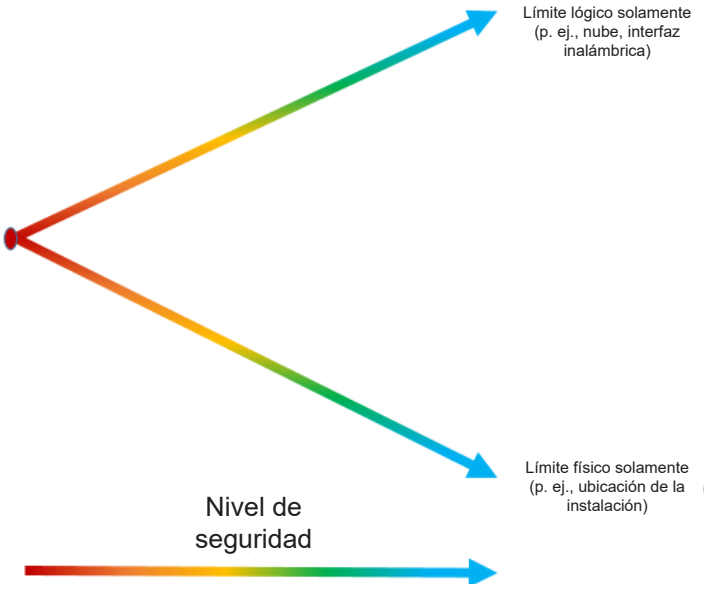


Figura III-1. Requisitos de zona relativos a los límites físicos y lógicos en función del nivel de seguridad informática.

ZONAS SITUADAS FUERA DE LA SALA DE CONTROL PRINCIPAL QUE SE MONITORIZAN DESDE EL INTERIOR DE ESTA

Sistema de protección del reactor (nivel 1 de seguridad informática)

III-9. En el cuadro III-1, el nivel de seguridad informática más estricto (nivel 1) exige que se especifiquen estrictamente los límites lógicos y físicos de las zonas de seguridad informática y que dichos límites no se solapen entre sí. Por ejemplo, la red específica puede limitarse a ubicaciones situadas dentro de la zona vital (o equivalente).

III-10. Es necesario controlar estrictamente el acceso físico y lógico a las zonas que tengan asignado el nivel 1 de seguridad informática. El acceso físico puede controlarse mediante una barrera sólida con control del acceso y detección de intromisiones que cumpla los requisitos recomendados en la referencia [III-1], y el acceso lógico puede controlarse mediante una vía de comunicación de datos unidireccional a prueba de fallos (por ejemplo, un diodo de datos) con arreglo a la orientación incluida en la presente publicación y la referencia [III-2].

CUADRO III-1. LISTA DE SISTEMAS: EJEMPLO DE APLICACIÓN DE NIVELES Y ZONAS DE SEGURIDAD INFORMÁTICA

Sistema	Función más significativa	Nivel de seguridad informática	Límite lógico	Límite físico
Sistema de instrumentación y control para la protección del reactor	Prevenir condiciones de accidente	1	Red interna específica desacoplada mediante diodo de datos Sin conectividad de red externa	Equipos situados en una única zona vital solamente Medida de seguridad informática (diodo de datos) situada en zona vital
Sistema de instrumentación y control para la limitación del reactor	Controlar la reactividad	2	Redes específicas, desacopladas mediante diodo de datos, cortafuegos u otros dispositivos de seguridad	Equipos situados en una o varias zonas vitales Los cables de red, equipo o enrutamiento fuera de zonas vitales se han reforzado físicamente (p. ej., paneles o conductos protegidos)
Sistema de instrumentación y control para la información de procesos	Proporcionar alarmas y notificaciones al explotador sobre el entorno y el estado de la instalación	3	Redes interconectadas con la interfaz persona-máquina Nota: Puede tratarse de una consola independiente o adicional de la interfaz persona-máquina en la sala de control principal	Equipos y redes situados en zona protegida y/o zonas vitales

CUADRO III-1. LISTA DE SISTEMAS: EJEMPLO DE APLICACIÓN DE NIVELES Y ZONAS DE SEGURIDAD INFORMÁTICA (cont.)

Sistema	Función más significativa	Nivel de seguridad informática	Límite lógico	Límite físico
Sistemas de instrumentación y control para la automatización operacional	Controlar los sistemas de la parte no nuclear de la central	3	Redes interconectadas con la interfaz persona-máquina Nota: Puede tratarse de una consola independiente o adicional de la interfaz persona-máquina en la sala de control principal, o combinarse con un sistema de instrumentación y control para la información de procesos	Equipos y redes situados en zona protegida y/o zonas vitales
Ofimática	Realizar funciones relacionadas con el personal	4	No se permite ninguna conexión lógica (interfaz por cable, inalámbrica o portátil) con ninguna zona (sistema) de nivel 1, 2 o 3	Se permite en zona de acceso limitado, zona protegida y zonas vitales
Sistemas de telecomunicación	Llamar a las fuerzas de respuesta u otros organismos externos, según convenga	4	No se permite ninguna conexión lógica (interfaz por cable, inalámbrica o portátil) con ninguna zona asignada al nivel 1, 2 o 3	Se permiten en todos los lugares necesarios para los objetivos del explotador

CUADRO III-1. LISTA DE SISTEMAS: EJEMPLO DE APLICACIÓN DE NIVELES Y ZONAS DE SEGURIDAD INFORMÁTICA (cont.)

Sistema	Función más significativa	Nivel de seguridad informática	Límite lógico	Límite físico
Dispositivos informáticos móviles personales	No se exige ninguna — solo exenciones	5	Solo se permiten en redes de nivel 5 No pueden estar próximos a ninguna zona asignada al nivel 1, 2 o 3	No se permiten en zonas vitales

III-11. Por lo general, los sistemas que realizan la función de la instalación relativa a prevenir condiciones de accidente (por ejemplo, en un sistema de protección del reactor) se asignarán al nivel de seguridad informática más estricto. El equipo que facilita la función estará situado en una zona vital cercana al reactor, pero se monitorizará a través de una interfaz persona-máquina en la sala de control principal. Esto crea un posible problema con respecto a la aplicación de zonas de seguridad informática, ya que la interconexión entre el sistema de protección del reactor y la interfaz persona-máquina podría enrutarse fuera de las zonas vitales (por ejemplo, en la zona protegida), lo que infringiría el requisito de seguridad física.

III-12. Una solución sería separar la función de monitorización de la función de prevención de las condiciones de accidente. Esto permitiría la separación lógica mediante un diodo de datos entre los activos digitales de la zona vital que previenen las condiciones de accidente y los situados fuera de la zona vital utilizados para fines de monitorización en la sala de control principal. Esta solución solo sería eficaz si la función para prevenir las condiciones de accidente fuera independiente y no necesitara ninguna medida o información desde fuera de los sistemas asignados para su realización.

III-13. Los activos digitales a los que se atribuya la prevención de condiciones de accidente se asignarán al nivel de seguridad informática más estricto (nivel 1) sobre la base de la función de la instalación. Estos activos digitales se ubicarán en una zona vital fuera de la sala de control principal. Los activos digitales a los que se atribuya la monitorización del sistema de protección del reactor (por ejemplo,

la consola de la interfaz persona-máquina del sistema de protección del reactor en la sala de control principal) se asignarán al nivel 2 (o superior) de seguridad.

ZONAS SITUADAS FUERA DE LA SALA DE CONTROL PRINCIPAL CUYAS OPERACIONES SE REALIZAN DESDE EL INTERIOR DE ESTA

Sistema de instrumentación y control para la limitación del reactor (nivel 2 de seguridad informática)

III-14. Con arreglo al cuadro III-1, los activos digitales que realizan funciones asignadas al nivel 2 de seguridad han de estar en una zona vital y tener un acceso físico y lógico sometido a un control estricto. Sin embargo, por motivos operacionales, la función de control de la reactividad necesita la entrada de comandos desde la sala de control principal (por ejemplo, instrucciones para aumentar o disminuir la potencia).

III-15. Los equipos están situados en zonas vitales, y la infraestructura de red (cableado, conmutadores y paneles) está reforzada cuando se encuentra en zonas menos seguras (por ejemplo, si los cables de red pasan por la zona protegida). Dado que la entrada de comandos es necesaria (es decir, comunicaciones iniciadas desde la sala de control principal al equipo), no es posible la instalación de un diodo de datos para controlar el acceso lógico.

III-16. Una solución sería aislar física y lógicamente la zona que contiene activos de red y digitales que apoyan estas comunicaciones de comandos respecto de otras zonas asignadas a niveles de seguridad inferiores (niveles 3 a 5). Ello permitiría una separación lógica entre otros sistemas a niveles inferiores. Esta solución solo será eficaz si la función para prevenir las condiciones de accidente es independiente y no necesita ninguna medida o información que esté fuera de los sistemas asignados para su realización.

III-17. El mismo razonamiento y solución pueden aplicarse también al sistema de instrumentación y control para la información de procesos y a los sistemas de instrumentación y control para la automatización operacional asignados al nivel 3 de seguridad informática.

ZONAS O DISPOSITIVOS CON CONECTIVIDAD EXTERNA

Ofimática y sistemas de telecomunicaciones (nivel 4 o 5 de seguridad informática)

III-18. Con arreglo al cuadro III-1, la ofimática y los sistemas de telecomunicaciones facilitan funciones necesarias que requieren conectividad externa. Ello permite al explotador acceder a información y recursos que puedan ser necesarios en determinados casos y condiciones.

III-19. Estas conexiones externas, a Internet y a otros servicios, redes y dispositivos, pueden aumentar el riesgo a menos que se establezcan medidas para garantizar que no se pueda intercambiar información entre estas fuentes externas y sistemas que realicen funciones de la instalación asignados a niveles de seguridad superiores. Se necesitan medidas sólidas para eliminar o restringir el acceso a interfaces portátiles, conexiones por cable e inalámbricas y otros medios a través de los cuales pueda intercambiarse información con activos digitales que tengan conectividad externa, así como para aplicar zonas de seguridad informática delimitadas de forma estricta para dichos activos digitales mediante mecanismos de desacoplamiento sólidos. La separación de las zonas de seguridad dentro de la sala de control principal se examina en mayor detalle en los párrafos III-21 a III-27.

Dispositivos informáticos móviles personales (no asignados)

III-20. Se supone que los dispositivos informáticos móviles personales y *software* no se han reforzado para eliminar la capacidad de intercambiar información cuando estén cerca de activos digitales asignados. Por consiguiente, los dispositivos informáticos móviles personales no están permitidos en la sala de control principal (ni en las salas de equipos conexas).

SEPARACIÓN DE LAS ZONAS DE SEGURIDAD DENTRO DE LA SALA DE CONTROL PRINCIPAL

III-21. Como se indica en el párrafo III-13, los activos digitales suelen realizar múltiples funciones de la instalación que requerirían diferentes niveles de seguridad informática, y es probable que dichos activos digitales se encuentren dentro de la sala de control principal. Esta proximidad aumenta el riesgo de que estos activos se vean comprometidos por ciberataques.

III-22. Ello es especialmente cierto si no se han establecido controles físicos que protejan el acceso a los activos digitales y las interfaces entre estos. En tal caso, un agente interno que tenga acceso lógico o físico a la zona de la sala de control principal podría comprometer sin restricciones los activos digitales de esa zona.

III-23. Los activos digitales (y sistemas) ubicados en la sala de control principal realizan funciones que a menudo requieren información de otros activos digitales o requieren la adopción de medidas por parte del personal de operación. Si el sistema de protección del reactor se ha separado lógica y físicamente de la sala de control principal como en el ejemplo anterior (por ejemplo, mediante un diodo de datos para la monitorización), las otras funciones principales de seguridad que hay que tener en cuenta son el control de la reactividad y la eliminación del calor del núcleo.

III-24. Los sistemas que realizan estas funciones de seguridad suelen asignarse al nivel 2 de seguridad informática. Con arreglo al cuadro III-1, el nivel 2 de seguridad informática requiere límites de zona estrictos, pero estos pueden ser una combinación de límites físicos y lógicos.

III-25. La asignación de los activos digitales de la sala de control principal a zonas se complica aún más por la necesidad de que las funciones informáticas corporativas (por ejemplo, correo electrónico, Internet, gestión de operaciones) apoyen a los operadores de la sala de control principal. La instalación de activos digitales para respaldar estas funciones puede crear una situación en la que se proporcionen sistemas asignados a los niveles de seguridad 2 y 5 al mismo personal en la sala de control principal, si bien es necesario cumplir el requisito de separar los activos digitales que realizan funciones de la instalación que se hayan asignado a diferentes niveles de seguridad.

III-26. En este ejemplo, pueden adoptarse las siguientes soluciones:

a) Las redes lógicas nunca se conectan directamente y siempre emplean mecanismos de desacoplamiento sólidos. Las redes de nivel 2 de seguridad no se extienden más allá de la sala de control principal (y las salas de equipos conexas dentro de la zona protegida) sin que existan dichos mecanismos de desacoplamiento.
b) Las redes lógicas están separadas y definidas con claridad, y la responsabilidad sobre ellas puede asignarse a distintas dependencias institucionales (por ejemplo, tecnología de la información, ingeniería).
c) Pueden establecerse medidas de control físico para crear subzonas dentro de la sala de control principal. Puede tratarse de paneles bloqueados,

bloqueadores de interfaces portátiles (por ejemplo, bloqueadores de puertos), conductos de red seguros y/o zonas de acceso limitado dentro de la sala de control principal.

III-27. Habida cuenta de las soluciones propuestas anteriormente, el uso de controles lógicos y físicos permitiría la existencia de múltiples niveles de seguridad informática dentro de una única zona física (por ejemplo, la sala de control principal). Sin embargo, con la instalación de medidas de seguridad informática adicionales, la sala de control principal puede dividirse en varias subzonas, cada una de las cuales tiene asignado su propio nivel de seguridad.

REFERENCIAS DEL ANEXO III

[III–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.

[III–2] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018).

GLOSARIO

activos digitales de carácter estratégico. Recursos de información de carácter estratégico que son sistemas informáticos o forman parte de ellos.

agente interno. Persona que tiene autorización para acceder bien a instalaciones conexas o actividades conexas, o bien a información de carácter estratégico o recursos de información de carácter estratégico, y que podría cometer o facilitar la comisión de actos delictivos o actos intencionales no autorizados que estén relacionados con material nuclear, otros materiales radiactivos, instalaciones conexas o actividades conexas, o que se dirijan contra ellos, u otros actos que según determine el Estado tengan un impacto negativo en la seguridad física nuclear.

amenaza base de diseño. Conjunto de atributos y características de posibles agentes internos y/o adversarios externos que podrían intentar una retirada no autorizada o un acto de sabotaje, utilizado como referencia a la hora de diseñar y evaluar un sistema de protección física.

arquitectura defensiva de seguridad informática. Estructura de los sistemas informáticos establecida con arreglo a las medidas, limitaciones y requisitos de diseño que han de imponerse durante el ciclo de vida de un sistema, de modo que los sistemas que realizan funciones de la instalación de constatada importancia para la seguridad tecnológica y la seguridad física de esta y que están asignados a niveles de seguridad informática a nivel de la instalación tengan el nivel de protección necesario.

ataque combinado. Acto doloso en el que se utilizan, de forma coordinada, un ciberataque y un ataque físico.

ciberataque. Acto doloso realizado con la intención de robar, alterar o destruir un blanco específico, o de impedir el acceso a este, accediendo sin autorización a un sistema informático vulnerable (o actuando en su interior).

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

detección. Proceso del sistema de protección física que empieza cuando se percibe un acto potencialmente doloso o no autorizado y termina con una evaluación de la causa de la alarma.

— el marco legislativo y regulador y las medidas y los sistemas administrativos que rigen la seguridad física nuclear del material nuclear, otros materiales radiactivos, las instalaciones conexas y las actividades conexas;

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

función de una instalación. Conjunto coordinado de acciones, procesos y operaciones asociados a una instalación nuclear. Su finalidad puede incluir realizar funciones que sean importantes para la seguridad tecnológica nuclear, la seguridad física nuclear, la contabilidad y el control de materiales nucleares o la gestión de información de carácter estratégico, o que estén relacionadas con estos ámbitos. Las funciones de una instalación también incluyen funciones operacionales y administrativas (u organizativas).

gestión de riesgos de seguridad informática. Evaluación y gestión de los riesgos asociados a posibles ciberataques que puedan degradar la seguridad tecnológica nuclear o la seguridad física nuclear. La gestión de riesgos de seguridad informática se realiza a nivel de la instalación y a nivel de sistemas.

incidente de seguridad informática. Hecho que pone o puede poner en peligro la confidencialidad, integridad o disponibilidad de un sistema informático (incluida la información) o que constituye una violación o un riesgo inminente de violación de las políticas de seguridad física.

información de carácter estratégico. Información, cualquiera que sea su forma, incluido el *software*, cuya revelación, modificación, alteración, destrucción o denegación de uso no autorizadas podrían comprometer la seguridad física nuclear.

— las instituciones y organizaciones del Estado encargadas de garantizar la aplicación del marco legislativo y regulador y los sistemas administrativos de seguridad física nuclear, y

— los sistemas de seguridad física nuclear y las medidas de seguridad física nuclear para la prevención y detección de sucesos relacionados con la seguridad física nuclear y la respuesta a ellos.

medidas de control administrativo. Políticas, procedimientos y prácticas que especifican las acciones permitidas, necesarias y prohibidas para proteger los sistemas informáticos, proporcionando instrucciones para las acciones de los empleados y de los proveedores, contratistas y suministradores.

medidas de control físico. Barreras físicas que protegen los instrumentos, los sistemas informáticos y los activos de apoyo frente a daños físicos e impiden el acceso físico no autorizado.

medidas de control técnico. *Hardware* o *software* empleado para prevenir o detectar una intromisión u otro acto doloso, mitigar sus consecuencias y recuperarse tras estos.

medidas de seguridad física nuclear. Medidas que tienen por fin impedir que una amenaza para la seguridad física nuclear culmine en actos delictivos o actos intencionales no autorizados que estén relacionados con material nuclear, otros materiales radiactivos, instalaciones conexas o actividades conexas, o que se dirijan contra ellos, o detectar sucesos relacionados con la seguridad física nuclear o responder a ellos.

medidas de seguridad informática. Medidas destinadas a prevenir, detectar o retrasar actos dolosos u otros actos que podrían comprometer la seguridad informática, responder a ellos y mitigar sus consecuencias.

nivel de seguridad informática. Robustez de la protección necesaria para cumplir los requisitos de seguridad informática con respecto a una función relacionada con la seguridad física nuclear, la seguridad tecnológica nuclear, la contabilidad y el control de materiales nucleares y/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. El programa especifica y detalla los medios para lograr los objetivos de seguridad informática y forma parte del plan general de seguridad física (o está vinculado a él).

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.

régimen de seguridad física nuclear. Régimen que abarca:

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

seguridad informática. Vertiente particular de la seguridad física de la información que se ocupa de la protección de los sistemas informáticos.

sistema de seguridad física nuclear. Conjunto integrado de medidas de seguridad física nuclear.

sistemas informáticos. Tecnologías que generan, procesan, computan, comunican o almacenan información digital, o proporcionan acceso a ella, o que realizan, ofrecen o controlan servicios relacionados con este tipo de información. Estas tecnologías pueden ser físicas o virtuales. Pueden incluir computadoras de mesa, 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.

suceso relacionado con la seguridad física nuclear. Suceso que tiene o puede tener repercusiones para la seguridad física nuclear que es preciso afrontar.

zona de seguridad informática. Grupo de sistemas que tienen límites físicos y/o lógicos comunes — y, de ser necesario, ordenados mediante criterios adicionales — al que se asigna un nivel común de seguridad informática para simplificar la administración, comunicación y aplicación de 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 revisión proporciona orientación sobre cómo establecer o mejorar, desarrollar, aplicar, mantener y sostener la seguridad informática en las instalaciones nucleares. La presente publicación aborda el uso de enfoques basados en el conocimiento de los riesgos para establecer y mejorar políticas y programas de seguridad informática; describe la integración de la seguridad informática en el sistema de gestión
de una instalación, y establece un enfoque sistemático para determinar funciones de la instalación y medidas de seguridad informática adecuadas que protejan los activos digitales de carácter estratégico y la instalación frente a las consecuencias de los ciberataques con arreglo a la evaluación de la amenaza o la amenaza base de diseño.

ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA
VIENA