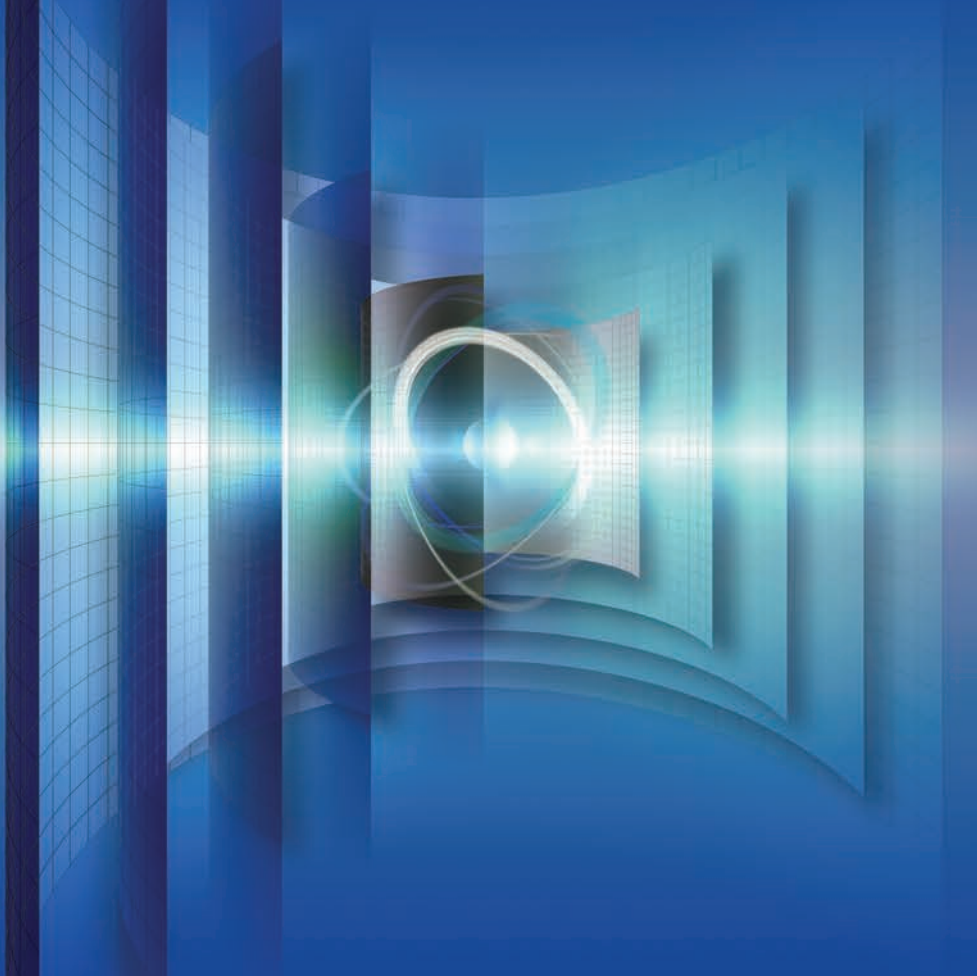
Colección de Seguridad Física Nuclear del OIEA N° 33-T

Orientaciones Técnicas

Seguridad informática de sistemas de instrumentación y control en 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.

SEGURIDAD INFORMÁTICA DE SISTEMAS DE INSTRUMENTACIÓN Y CONTROL EN INSTALACIONES NUCLEARES

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

AFGANISTÁN
ALBANIA
ALEMANIA
ANGOLA
ANTIGUA Y BARBUDA
ARABIA SAUDITA
ARGELIA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIYÁN
BAHAMAS
BAHREIN
BANGLADESH
BARBADOS
BELARÚS
BÉLGICA
BELICE
BENIN
BOLIVIA, ESTADO PLURINACIONAL DE
BOSNIA Y HERZEGOVINA
BOTSWANA
BRASIL
BRUNEI DARUSSALAM
BULGARIA
BURKINA FASO
BURUNDI
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
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
NORMAS DE SEGURIDAD DEL OIEA Nº 33-T

SEGURIDAD INFORMÁTICA DE SISTEMAS DE INSTRUMENTACIÓN Y CONTROL EN 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
Marzo de 2024
STI/PUB/1787

SEGURIDAD INFORMÁTICA DE
SISTEMAS DE INSTRUMENTACIÓN Y CONTROL
EN INSTALACIONES NUCLEARES
OIEA, VIENA, 2024
STI/PUB/1787
ISBN 978-92-0-329023-4 (papel)
ISBN 978-92-0-328723-4 (PDF)
ISSN 2521-1803

PRÓLOGO

El OIEA está autorizado por su Estatuto a "establecer o adoptar […] normas de seguridad para proteger la salud y reducir al mínimo el peligro para la vida y la propiedad" —normas que el OIEA debe utilizar en sus propias operaciones y que los Estados pueden aplicar mediante sus disposiciones de reglamentación de la seguridad nuclear y radiológica—. A esos efectos, el OIEA consulta con los órganos competentes de las Naciones Unidas y con los organismos especializados pertinentes. Un amplio conjunto de normas de alta calidad revisadas periódicamente es un elemento clave de un régimen de seguridad mundial estable y sostenible, como también lo es la asistencia del OIEA en la aplicación de esas normas.

El OIEA inició su programa de normas de seguridad en 1958. El énfasis puesto en su calidad, idoneidad y mejora continua ha redundado en el uso generalizado de las normas del OIEA en todo el mundo. La Colección de Normas de Seguridad incluye ahora principios fundamentales de seguridad unificados, que representan un consenso internacional acerca de lo que debe constituir un alto grado de protección y seguridad. Con el firme apoyo de la Comisión sobre Normas de Seguridad, el OIEA se esfuerza por promover la aceptación y el uso a escala mundial de sus normas.

Las normas solo son eficaces si se aplican adecuadamente en la práctica. Los servicios de seguridad del OIEA abarcan el diseño, la selección de emplazamientos y la seguridad técnica, la seguridad operacional, la seguridad radiológica, la seguridad en el transporte de materiales radiactivos y la seguridad en la gestión de los desechos radiactivos, así como la organización a nivel gubernamental, las cuestiones relacionadas con reglamentación y la cultura de la seguridad en las organizaciones. Estos servicios de seguridad prestan asistencia a los Estados Miembros en la aplicación de las normas y posibilitan el intercambio de experiencias y conocimientos valiosos.

La reglamentación de la seguridad es una responsabilidad nacional y muchos Estados han decidido adoptar las normas del OIEA para incorporarlas en sus reglamentos nacionales. Para las partes en las diversas convenciones internacionales sobre seguridad, las normas del OIEA son un medio coherente y fiable de asegurar el cumplimiento eficaz de las obligaciones emanadas de esas convenciones. Los órganos reguladores y los explotadores de todo el mundo también aplican las normas para mejorar la seguridad en la generación de energía nucleoeléctrica y en las aplicaciones de la energía nuclear en la medicina, la industria, la agricultura y la investigación.

La seguridad no es un fin en sí misma, sino un requisito indispensable para la protección de las personas de todos los Estados y del medio ambiente, ahora y en el futuro. Los riesgos relacionados con la radiación ionizante deben evaluarse

y controlarse sin restringir indebidamente la contribución de la energía nuclear al desarrollo equitativo y sostenible. Los Gobiernos, los órganos reguladores y los explotadores de todo el mundo deben velar por que los materiales nucleares y las fuentes de radiación se utilicen con fines beneficiosos y de manera segura y ética. Las normas de seguridad del OIEA están concebidas para facilitar esa tarea, y aliento a todos los Estados Miembros a hacer uso de ellas.

NOTA EDITORIAL

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 en el Estado. Las orientaciones en las que se usan formas verbales condicionales tienen por fin presentar buenas prácticas internacionales e indicar un consenso internacional en el sentido de que es necesario que los Estados adopten las medidas recomendadas o medidas alternativas equivalentes.

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

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

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

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

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

ÍNDICE

1. INTRODUCCIÓN

ANTECEDENTES

1.1. Los sistemas de instrumentación y control (I+C) desempeñan una función esencial en la labor de garantizar la explotación segura de las instalaciones nucleares. Dado que las tecnologías digitales siguen evolucionando y ampliando su capacidad, se las está incorporando e integrando cada vez más en los sistemas de I+C[1]. Las nuevas instalaciones nucleares y los diseños modernos de instalaciones nucleares utilizan sistemas de I+C digitales sumamente integrados para manejar de manera eficiente y simultánea inmensas cantidades de datos de procesos que, a su vez, requieren menos interacción e intervención humanas que los anteriores sistemas de I+C. Las tecnologías digitales también se suelen introducir en los sistemas de I+C durante la modernización de las instalaciones existentes. No obstante, la aplicación de tecnologías digitales dentro de los sistemas de I+C ha hecho que estos sistemas sean vulnerables a ciberataques.

1.2. Un ciberataque es un acto doloso llevado a cabo por personas u organizaciones que tiene como objetivo la información de carácter estratégico o los recursos de información de carácter estratégico con la intención de robar, alterar, impedir el acceso a un objetivo concreto o destruirlo mediante el acceso no autorizado a un sistema susceptible (o mediante acciones dentro de ese sistema). Los recursos de información de carácter estratégico comprenden los sistemas de control, las redes, los sistemas de información y cualquier otro medio electrónico o físico. Los adversarios han lanzado ciberataques exitosos dirigidos a sistemas de I+C; uno de ellos fue el ciberataque mediante el gusano informático Stuxnet, que provocó la destrucción de equipo en una instalación nuclear [1].

1.3. Los ciberataques a los sistemas de I+C pueden poner en peligro la seguridad tecnológica y física de las instalaciones nucleares. Pueden contribuir a la comisión de actos de sabotaje o ayudar en la retirada no autorizada de material nuclear. Los efectos de los ciberataques a los sistemas de I+C relacionados con la seguridad tecnológica pueden provocar numerosas consecuencias, como la pérdida temporal del control de procesos o consecuencias radiológicas inaceptables. El conocimiento público de ataques que afectan a los sistemas de

[1] En el resto de la presente publicación, el término “sistema de I+C” se utiliza para hacer alusión a los sistemas de instrumentación y control que utilizan tecnologías digitales, que dependen de estas o que están respaldados por estas.

I+C también pueden socavar la confianza en la seguridad tecnológica y física de las instalaciones nucleares.

1.4. En el párr. 4.10 de las *Recomendaciones de Seguridad Física Nuclear sobre la Protección Física de los Materiales y las Instalaciones Nucleares (INFCIRC/225/Rev.5)* [2] se establece la necesidad de proteger los sistemas computarizados (incluidos los sistemas de I+C). El texto pertinente es del siguiente tenor:

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

1.5. La publicación *Seguridad informática en las instalaciones nucleares* [3] de la *Colección de Seguridad Física Nuclear del OIEA* Nº 17 proporciona orientación específica para las instalaciones nucleares sobre la implantación de un programa de seguridad informática a fin de apoyar la orientación que se señala en la ref. [2]. La ref. [3] también proporciona información detallada sobre terminología fundamental, como "seguridad informática", "seguridad de la TI" y "ciberseguridad". Los términos "seguridad de la TI" y "ciberseguridad" se consideran sinónimos de "seguridad informática" a los efectos de esta publicación y no se utilizarán.

1.6. La seguridad informática ha de tenerse en cuenta, de manera explícita, en todas las fases del ciclo de vida de los sistemas de I+C. El término "ciclo de vida", (por oposición al término "vida útil") implica que la vida del sistema es verdaderamente cíclica (como sucede en el reciclado o en el reprocesamiento), y en particular que, en el nuevo sistema, se utilizan elementos del sistema antiguo. La ref. [4] contiene un listado de actividades habituales del ciclo de vida de los sistemas de I+C.

1.7. Históricamente, la seguridad informática no se tenía muy en cuenta en el diseño de los sistemas de I+C de las instalaciones nucleares, puesto que se presuponía que los sistemas cableados o analógicos eran invulnerables a los ciberataques debido a su rígida implantación, a su aislamiento y a la separación de los sistemas, así como a una comunicación interactiva prácticamente inexistente, especialmente con redes o sistemas externos. La transición hacia la tecnología digital ha cambiado la naturaleza de los sistemas de I+C en las instalaciones

nucleares al posibilitar la interconexión de sistemas de I+C reprogramables (a distancia o localmente) y funcionalmente distintos.

1.8. El mayor uso de componentes y dispositivos digitales versátiles y programables ha reducido la diversidad de los sistemas de I+C. Ello incluye el uso de elementos y enfoques comunes en todo un abanico de aplicaciones industriales (por ejemplo, los protocolos de comunicación). Los actos dolosos[2] dirigidos a estas tecnologías comunes en otras industrias también podrían afectar a una instalación nuclear.

1.9. Las personas autorizadas, ya sea en el emplazamiento o en un lugar remoto, en tanto que tienen acceso lógico o físico a los sistemas de I+C, pueden entrañar, como agentes internos, una amenaza para la seguridad tecnológica y física de una instalación nuclear. Estos agentes internos pueden ser empleados de la instalación o personal contratado por proveedores, contratistas o suministradores que tal vez puedan aprovecharse de su acceso autorizado para cometer actos dolosos. La necesidad de proteger los sistemas computarizados frente a las amenazas de agentes internos se reconoce en la ref. [5].

OBJETIVO

1.10. Esta publicación tiene por objetivo proporcionar orientaciones sobre seguridad informática a fin de proteger los sistemas de I+C en las instalaciones nucleares frente a actos dolosos que podrían impedir que esos sistemas llevaran a cabo sus funciones relacionadas con la seguridad tecnológica y física. Si bien esta publicación se centra en la operación físicamente segura de estos sistemas, la aplicación de estas orientaciones también puede contribuir a mejorar la seguridad tecnológica y el desempeño operacional de las instalaciones nucleares.

1.11. Esta publicación está destinada a las autoridades competentes, como órganos reguladores, así como a personal encargado de la gestión, las operaciones, el mantenimiento y la ingeniería de instalaciones nucleares; proveedores, contratistas y suministradores de sistemas de I+C; diseñadores de sistemas de I+C; laboratorios de investigación, y otras entidades a las que atañe la seguridad tecnológica y física de las instalaciones nucleares.

[2] Los sucesos causados por un error humano o por fallos aleatorios de equipos o componentes no se incluyen en el concepto de actos dolosos.

ALCANCE

1.12. El alcance de esta publicación es la aplicación de medidas de seguridad informática a los sistemas de I+C que desempeñan funciones de seguridad tecnológica, seguridad física[3] o funciones auxiliares en instalaciones nucleares. Estas medidas están destinadas a proteger los sistemas de I+C frente a actos dolosos perpetrados por personas u organizaciones. En esta publicación también se aborda la aplicación de esas medidas a los entornos de desarrollo, simulación y mantenimiento de estos sistemas.

1.13. Las orientaciones que se proporcionan en esta publicación son aplicables a los sistemas de I+C de nuevas[4] instalaciones nucleares y a nuevos sistemas de I+C de instalaciones existentes. Se espera que estas orientaciones se apliquen en la mayor medida posible a los sistemas de I+C antiguos de instalaciones existentes, también en los casos en que no se utiliza tecnología digital.

1.14. Si bien no se trata explícitamente en esta publicación, otros sistemas de interfaz y sistemas de tecnología de la información y las comunicaciones (TIC), como los sistemas de comunicaciones y de control de los trabajos, pueden introducir riesgos en los sistemas de I+C. Estos riesgos deben tenerse en cuenta al diseñar y aplicar medidas de seguridad informática para los sistemas de I+C en una instalación. Las medidas de seguridad informática para estos sistemas pueden ser distintas de las aplicadas a los sistemas de I+C y han de evaluarse y adaptarse de manera oportuna.

1.15. En la presente publicación no se proporcionan orientaciones amplias sobre consideraciones de seguridad tecnológica para los sistemas de I+C. Esas orientaciones pueden encontrarse en las refs. [4 y 6]. Además, esta publicación no define ni modifica la terminología técnica empleada en normas de seguridad del OIEA y otras publicaciones del OIEA relacionadas con la seguridad. Estos términos se destacan en esta publicación, cuando se utilizan, y sus definiciones se pueden encontrar en el *Glosario de seguridad del OIEA* [7].

---

[3] Entre los sistemas que proporcionan funciones de seguridad física se encuentran los utilizados para la protección física y para la contabilidad y el control de materiales nucleares.

[4] Una instalación nueva es una instalación que aún está pendiente de completar la fase de puesta en servicio.

ESTRUCTURA

1.16. Tras esta introducción, esta publicación se articula en cuatro secciones. En la sección 2 se presenta un panorama general de los sistemas de I+C que se utilizan en las instalaciones nucleares y la función que desempeña la seguridad informática para proteger estos sistemas frente a ciberataques. En la sección 3 se expone la relación entre la seguridad informática y la seguridad de los sistemas de I+C. En la sección 4 se presentan orientaciones sobre la seguridad informática que han de aplicarse en las distintas fases del ciclo de vida de los sistemas de I+C, incluso durante la clausura de una instalación.

2. CONCEPTOS CLAVE PARA LA SEGURIDAD INFORMÁTICA DE LOS SISTEMAS DE I+C

2.1. Los sistemas de I+C en las instalaciones nucleares se utilizan para monitorizar y controlar procesos y equipo. Estos sistemas incluyen:

a) sistemas de control de supervisión y adquisición de datos (SCADA);
b) sistemas de control distribuido;
c) sistemas de control digital centralizado;
d) sistemas de control compuestos de controladores lógicos programables;
e) microcontroladores y dispositivos "inteligentes", y
f) sistemas que utilizan dispositivos lógicos programados (por ejemplo, matrices de puertas programables *in situ*, dispositivos lógicos programables complejos y circuitos integrados de aplicación específica).

Los sistemas similares que controlan plantas industriales suelen recibir la denominación de "sistemas de control industrial".

2.2. Los sistemas de I+C están diseñados para ofrecer un comportamiento tecnológica y físicamente seguro, fiable y determinista de la instalación nuclear, tanto en condiciones de funcionamiento normal como anormal[5]. Las consideraciones de diseño y las medidas destinadas a mejorar la seguridad tecnológica también pueden proporcionar beneficios para la seguridad física.

[5] En el *Glosario de seguridad del OIEA* [7] se hace alusión al funcionamiento anormal como sinónimo de "incidente operacional previsto". Para la presente publicación, el primer término se considera más fácil de entender.

Por ejemplo, medidas de diseño como el desempeño determinista, la evitación de fallos, la detección de fallos, los enfoques de tolerancia a fallos, la gestión de la configuración, la verificación y validación independientes, y otros métodos de ensayo avanzados pueden proporcionar cierta defensa frente a intentos dolosos de alterar el comportamiento de los sistemas de I+C.

2.3. El diseño de la arquitectura global de I+C en las instalaciones nucleares incorpora conceptos que pueden contribuir a la seguridad informática mitigando los efectos de un mal funcionamiento[6] intencionado o accidental, como la independencia, la redundancia, la defensa en profundidad de la seguridad y la diversidad[7]. El término "defensa en profundidad de la seguridad" se utiliza en esta publicación para hacer alusión a la defensa en profundidad que se define en el *Glosario de seguridad del OIEA* [7], a fin de distinguirlo de la aplicación de "defensa en profundidad", un concepto similar pero centrado en la seguridad física (según se define en *Nociones Fundamentales de Seguridad Física Nuclear* [8]) en la aplicación de medidas de seguridad informática que se describen en la sección 4.

2.4. La aplicación de estos conceptos en la arquitectura general de I+C y otras medidas de diseño deberían evaluarse para determinar su contribución a la seguridad informática. Por ejemplo, es probable que la diversidad del diseño o la tecnología reduzca vulnerabilidades comunes entre los sistemas clave de seguridad o control; sin embargo, puede añadir vulnerabilidades que sean únicas para cada sistema individual.

2.5. Las orientaciones que figuran en esta publicación se aplican a todos los sistemas de I+C asociados a instalaciones nucleares, salvo que se indique lo contrario.

---

[6] El término "mal funcionamiento" se utiliza en este documento para hacer alusión a situaciones que no se han contemplado con anterioridad (es decir, no son incidentes operacionales previstos), pero con respecto a las cuales el sistema de I+C no funciona según lo previsto.

[7] En la presente publicación, la independencia, la redundancia, la defensa en profundidad de la seguridad y la diversidad aluden a conceptos específicos que se utilizan en el *Glosario de seguridad del OIEA* [7].

SEGURIDAD INFORMÁTICA DE LOS SISTEMAS DE I+C

2.6. En el párrafo 2.2 de la ref. [2] se indica que

"El *régimen de protección física*[8] de un Estado debería tratar de alcanzar estos objetivos mediante:

— la prevención de los *actos dolosos* por medio de la disuasión y la protección de la información de carácter estratégico;
— la gestión de los *actos dolosos* frustrados o consumados mediante un sistema integrado de *detección*, dilación y respuesta, y
— la mitigación de las consecuencias de los *actos dolosos*."

2.7. Entre los ejemplos de cómo la prevención, la gestión y la mitigación se pueden aplicar a la seguridad informática de los sistemas de I+C figuran los siguientes:

— la prevención: instalar dispositivos a prueba de fallos que bloqueen las comunicaciones no autorizadas de datos para reducir la posibilidad de ciberataques basados en la red que perjudicarían al sistema de I+C;
— la gestión, incluida la detección, la dilación y la respuesta: mediante la inspección de los archivos de registro de sucesos del sistema, el operador tal vez pueda detectar precursores y poner en marcha medidas protectoras antes de que comience un acto doloso que pueda perjudicar a la seguridad tecnológica o la seguridad física de una instalación, y
— la mitigación y la recuperación: si se descubre que un sistema de I+C está infectado con un programa malicioso, una vez se haya detenido la propagación de dicho programa, el operador determinaría si es necesario aplicar medidas de control compensatorias (por ejemplo, actualización de las firmas de antivirus, instalación o mejora de sistemas de prevención o detección de intrusiones o ambos) para evitar la reinfección, llevar a cabo una reconstrucción del sistema, verificar la eficacia de las medidas de control compensatorias, restaurar el sistema y volverlo a poner en funcionamiento, tras realizar un análisis detallado de la seguridad y actividades de verificación de la integridad del sistema, si fuese preciso.

2.8. En ocasiones, la protección de los sistemas de I+C frente al comprometimiento se basa en la hipótesis de que una sola medida preventiva

[8] Históricamente, el término "protección física" se ha utilizado para describir lo que ahora se conoce como la seguridad física nuclear de los materiales y las instalaciones nucleares.

es suficiente, como aislar los sistemas de otras redes. Sin embargo, es probable que esa hipótesis dé lugar a la aplicación insuficiente de medidas de gestión y mitigación, por lo que un fallo de esta única medida de seguridad informática podría comprometer el sistema protegido.

2.9. Para los sistemas generales de TIC se han elaborado numerosos enfoques, métodos, técnicas, normas y directrices diferentes en materia de seguridad informática. Algunos de estos no son directamente aplicables a los sistemas de I+C de las instalaciones nucleares, pues estos presentan necesidades específicas de seguridad informática que no tienen en común con los sistemas de TIC.

2.10. No obstante, dado que la seguridad informática de los sistemas de I+C no se puede separar por completo de la seguridad informática de los sistemas de TIC, los operadores y los reguladores deberían elaborar políticas, requisitos, medidas y prácticas de seguridad informática que contemplen los sistemas de I+C y los sistemas de TIC de una forma integrada.

2.11. Muchos sistemas de I+C tienen un ciclo de vida de decenios, incluidos períodos durante los cuales puede que no haya soporte del proveedor o este soporte sea inadecuado para satisfacer los requisitos de seguridad informática[9] relacionados con los sistemas. Comprende el soporte proporcionado por el proveedor original y por terceros asociados. Por ejemplo, con el paso del tiempo, es posible que los programas de antivirus no proporcionen una protección suficiente frente a la explotación de vulnerabilidades de los sistemas de I+C, debido a la pérdida de la compatibilidad del *hardware* o el *software* o el hecho de que ya no se proporcionan actualizaciones de firmas.

2.12. En la mayoría de las aplicaciones, los sistemas de I+C funcionan en tiempo real y las acciones de estos sistemas se llevan a cabo dentro de estrictos intervalos de tiempo. Entre los ejemplos de esas acciones de los sistemas de I+C en instalaciones nucleares figuran el control de las operaciones normales, medidas protectoras, medidas de limitación y la señalización de alarmas a los operadores. Las medidas de seguridad informática no deberían obstaculizar, prevenir ni retrasar la ejecución de medidas operacionales ni de seguridad necesarias. Las medidas de seguridad informática de los sistemas de I+C modernos se pueden utilizar para prevenir, detectar y retrasar actos dolosos y para responder a ellos y mitigar sus consecuencias; no obstante, se debe tener cuidado para garantizar que

[9] En esta publicación, el término “requisitos de seguridad informática” hace alusión a requisitos específicos por escrito impuestos por la autoridad competente pertinente o por el operador para satisfacer los requisitos reglamentarios.

las medidas de respuesta no obstruyan las funciones de seguridad tecnológica acreditadas ni coloquen al sistema fuera de su base de diseño[10].

2.13. Las medidas de seguridad informática que se aplican de forma retrospectiva o que se ejecutan mal pueden introducir más complejidad en el diseño del sistema de I+C, lo que puede aumentar la probabilidad de fallo o mal funcionamiento del sistema de I+C.

2.14. El elemento esencial 9 de las *Nociones Fundamentales de Seguridad Física Nuclear* [8] señala la utilización de enfoques basados en el conocimiento de los riesgos para asignar recursos y realizar actividades relacionadas con la seguridad física nuclear. Un diseño elaborado utilizando un enfoque basado en el conocimiento de los riesgos que tenga en cuenta consideraciones de seguridad física desde el inicio del proceso de diseño puede ser más sencillo y más robusto debido a la integración de las características de seguridad, la eliminación de funcionalidades innecesarias (por ejemplo, el acceso remoto) o al fortalecimiento del sistema.

MEDIDAS DE SEGURIDAD INFORMÁTICA

2.15. Las medidas de seguridad informática se utilizan para prevenir, detectar y retrasar actos dolosos y para responder a ellos, además de para mitigar las consecuencias de esos actos. Estas medidas también se utilizan para garantizar que los actos no dolosos no degraden la seguridad física ni aumenten la vulnerabilidad de los sistemas computarizados frente a actos dolosos.

2.16. Las medidas de seguridad informática que abordan las vulnerabilidades del sistema o que proporcionan capas de protección de defensa se pueden clasificar en una de las tres categorías siguientes: medidas de control técnico, medidas de control físico o medidas de control administrativo. Cuando se vaya a desarrollar una seguridad informática integrada para sistemas de I+C, se deberían tener en cuenta las tres categorías y se debería seleccionar una combinación adecuada.

---

[10] En la base de diseño de los elementos importantes para la seguridad se deberá especificar la capacidad, fiabilidad y funcionalidad necesarias para los correspondientes estados operacionales, las condiciones de accidente y las condiciones surgidas de peligros internos y externos, a fin de cumplir los criterios de aceptación específicos durante la vida útil de la instalación nuclear. El término “base de diseño” se define de forma más amplia en el *Glosario de seguridad del OIEA* [7]. La base de diseño para los sistemas de I+C se describe con más detalle en la sección 3 de la ref. [4].

2.17. Las medidas de control técnico son el *hardware* y/o el *software* empleados para prevenir y detectar una intrusión u otro acto doloso y mitigar las consecuencias y recuperarse de estos. Con respecto a las medidas de control técnico, al evaluar su eficacia en comparación con las medidas de control físico o administrativo, se debería contemplar la capacidad que tienen aquellas para proporcionar medidas protectoras continuas y automáticas.

2.18. Las medidas de control físico son barreras físicas que protegen los instrumentos, los sistemas computarizados y los activos de apoyo frente a daños físicos y al acceso físico no autorizado. Entre las medidas de control físico cabe mencionar las cerraduras, los encajonamientos físicos, los dispositivos de indicación de manipulación ilícita, las salas de aislamiento, las puertas y los guardias.

2.19. Las medidas de control administrativo son políticas, procedimientos y prácticas concebidos para proteger los sistemas computarizados proporcionando instrucciones para las acciones de los empleados y del personal de terceros. Especifican las acciones que los empleados y el personal de terceros pueden, deben o tienen prohibido llevar a cabo. Las medidas de control administrativo para instalaciones nucleares comprenden medidas de control operacional y de la gestión.

APLICACIÓN DE UN ENFOQUE GRADUADO

2.20. El operador debería imponer requisitos de seguridad informática conforme a un enfoque graduado basado en el conocimiento de los riesgos; ese enfoque debería tener en cuenta lo siguiente:

— la importancia de las funciones de los sistemas de I+C tanto para la seguridad tecnológica (es decir, la clasificación de la seguridad) como para la seguridad física;
— las amenazas detectadas y evaluadas que afectan a la instalación;
— el atractivo del sistema de I+C para posibles adversarios;
— las vulnerabilidades del sistema de I+C;
— el entorno operativo, y
— las posibles consecuencias que podrían, directa o indirectamente, derivarse del comprometimiento del sistema.

Ese enfoque podría basarse en los resultados de una evaluación de riesgos de la seguridad informática.

2.21. En un enfoque graduado, los requisitos de seguridad informática se definen en proporción a las posibles consecuencias de un ataque. Las posibles consecuencias del comprometimiento de una función del sistema de I+C son, ordenadas del peor al mejor escenario, las siguientes:

— la función es indeterminada. Los efectos del comprometimiento dan lugar a una alteración no observada del diseño o de la función del sistema;
— la función tiene comportamientos o acciones imprevistos que son observables para el operador;
— la función falla, y
— el desempeño de la función es el previsto, lo que significa que el comprometimiento no perjudica a la función del sistema (es decir, es tolerante a fallos).

2.22. Los niveles de seguridad informática deberían aplicarse a los sistemas de I+C según se señala en esta publicación, de manera que se permita la aplicación de un enfoque graduado en materia de seguridad informática.

2.23. En la ref. [3] se puede observar un ejemplo de la aplicación de un enfoque graduado utilizando niveles de seguridad[11]. Por su parte, en la ref. [9] se puede observar un ejemplo de la aplicación de un enfoque graduado para la seguridad.

NIVELES DE SEGURIDAD INFORMÁTICA

2.24. Los niveles de seguridad informática y las clases de seguridad son conceptos distintos pero conexos. La clasificación de la seguridad de un elemento importante para la seguridad se basa en la importancia para la seguridad de sus funciones, así como en las posibles consecuencias de su fallo.

2.25. A cada función de un sistema de I+C asociada a una instalación se le suele asignar un nivel de seguridad informática para indicar el grado de protección de seguridad informática que necesita. Cada nivel necesitará distintos conjuntos de medidas de seguridad informática para satisfacer los requisitos de seguridad informática pertinentes. Los niveles de seguridad se suelen definir según los objetivos de seguridad de una organización. En la ref. [10] se proporciona más información sobre la aplicación de niveles y zonas de seguridad.

[11] En esta publicación, “niveles de seguridad” y “zonas de seguridad” se refieren a niveles de seguridad informática y zonas de seguridad informática.

2.26. Se señalan los subsistemas y componentes de los sistemas de I+C cuyo mal funcionamiento pueda afectar a la seguridad tecnológica nuclear (incluida la mitigación de accidentes), a la seguridad física nuclear y a la contabilidad y control de materiales nucleares y se les asignan niveles de seguridad según su contribución a la función del sistema de I+C.

2.27. El operador asigna un nivel de seguridad a un sistema, subsistema o componente de I+C en función de las posibles consecuencias de su fallo o mal funcionamiento, incluido el mal funcionamiento de un modo que difiere de su diseño o de los modos de fallo concebibles que se detectarían en un análisis de la seguridad de la instalación. El nivel de seguridad informática asignado a un sistema, subsistema o componente de I+C es específico para ese sistema, subsistema o componente y es independiente de su entorno.

ZONAS DE SEGURIDAD INFORMÁTICA

2.28. El concepto de zona de seguridad implica el agrupamiento lógico y/o físico de sistemas computarizados que tienen requisitos de seguridad informática comunes, debido a propiedades inherentes de los sistemas o a sus conexiones con otros sistemas. Todos los sistemas ubicados dentro de una única zona están protegidos con el mismo nivel de seguridad, es decir, el nivel asignado a la función del sistema de I+C con el nivel de seguridad más estricto dentro de la zona. El agrupamiento de sistemas de I+C en zonas de seguridad puede simplificar la aplicación y la gestión de las medidas de seguridad informática.

2.29. Las consideraciones para la aplicación de zonas de seguridad deberían cumplir los siguientes criterios:

— los sistemas que pertenecen a la misma zona tienen necesidades similares con respecto a las medidas de seguridad informática;
— los sistemas que pertenecen a la misma zona forman una zona de confianza a efectos de comunicación interna entre esos sistemas (es decir, zona de confianza interna);
— cada zona consta de sistemas que tienen la misma importancia o una importancia comparable en lo que respecta a la seguridad física y tecnológica de la instalación, o pertenecen a una zona de confianza interna;
— se mantienen los requisitos de la arquitectura de seguridad del sistema (por ejemplo, redundancia, diversidad, separación geográfica y eléctrica, criterio del fallo único);

— en los límites de zona se aplican medidas de control técnico para restringir la circulación de datos y la comunicación entre sistemas ubicados dentro de distintas zonas (por ejemplo, lugar remoto) o a los que se han asignado distintos niveles de seguridad;
— los medios extraíbles, los dispositivos móviles y otro equipo temporal que precisen de acceso lógico o físico a un sistema únicamente se utilizan dentro de una sola zona o de un conjunto concreto de zonas, y
— las zonas se pueden dividir en subzonas para mejorar la configuración.

2.30. Cuando se utilicen zonas de seguridad en una instalación, a algunos sistemas o componentes de I+C se les podría asignar una zona a la que se haya asignado un nivel de seguridad más estricto que su propio nivel de seguridad inherente. Por ejemplo, a un dispositivo de comunicación que realiza únicamente funciones de seguridad tecnológica o física de un nivel inferior se le puede asignar el mismo nivel de seguridad que al sistema de protección del reactor, en el caso de que se encuentre ubicado dentro de la zona de seguridad del sistema de protección del reactor. Esta asignación se debe a la posibilidad de uso doloso del dispositivo para comprometer los componentes del sistema de protección del reactor, que son sumamente importantes para la seguridad. Además, el uso de la zona de seguridad del sistema de protección del reactor permite la creación de una zona de confianza interna, con lo cual se garantiza que no deberán aplicarse medidas de seguridad informática adicionales entre los componentes del sistema de protección del reactor y el dispositivo de comunicación.

3. ENFOQUE BASADO EN EL CONOCIMIENTO DE LOS RIESGOS PARA LA SEGURIDAD INFORMÁTICA DE LOS SISTEMAS DE I+C

3.1. Un enfoque basado en el conocimiento de los riesgos para la seguridad informática de los sistemas de I+C puede utilizar evaluaciones de riesgos a fin de hallar las vulnerabilidades a ciberataques que guardan relación con estos sistemas y determinar las consecuencias que pudieran derivarse de la explotación exitosa de estas vulnerabilidades. Las medidas de seguridad informática se pueden asignar posteriormente en función de los resultados de las evaluaciones de riesgos.

3.2. Dado que los sistemas de I+C suelen ser esenciales para la seguridad de una instalación, conocer la seguridad tecnológica nuclear puede ayudar a evaluar

los riesgos, elaborar medidas de seguridad informática para el sistema de I+C, evaluar los posibles conflictos entre la seguridad tecnológica y la seguridad física, y estudiar cómo se podrían resolver esos conflictos. Por ejemplo, adversarios podrían sabotear una instalación mediante un ciberataque a los sistemas de I+C de una instalación, provocando con ello posibles consecuencias para la seguridad tecnológica y física. Esos ataques podrían provocar fallos de los sistemas de I+C o podrían hacer que los sistemas de I+C funcionasen de forma distinta a su comportamiento previsto o a sus modos de fallo analizados. Los actos dolosos pueden afectar a un solo sistema de I+C o a múltiples sistemas de I+C. Por ejemplo, pueden eludir múltiples niveles de la defensa en profundidad de la seguridad o provocar fallos simultáneos en estos[12]. Los actos dolosos también pueden combinar ciberataques con elementos de ataques físicos.

3.3. Una seguridad informática inadecuada o un sistema de I+C comprometido puede menoscabar la seguridad de una instalación. Por ejemplo, si un sistema de I+C se viera comprometido, un adversario podría obtener datos que proporcionasen la información crítica necesaria para planificar un ataque o modificar datos que facilitasen el sabotaje de los sistemas de la instalación o la retirada no autorizada de materiales nucleares. También, un ciberataque que diera lugar a un acto de sabotaje podría desencadenar un accidente o degradar el desempeño de una función de seguridad tecnológica. Ese ataque también podría provocar una pérdida de la disponibilidad del sistema.

3.4. Los ciberataques a los sistemas de I+C también podrían provocar consecuencias que posibilitaran la retirada no autorizada de material nuclear de una instalación. Los sistemas de I+C que llevan a cabo funciones de protección física o de contabilidad y control de materiales nucleares pueden verse afectados por ciberataques, que podrían poner a una instalación en una situación que no se haya contemplado en el plan de seguridad física del emplazamiento. Un acto doloso también podría combinar un ciberataque a estos sistemas con elementos de ataques físicos con el objetivo de conseguir la retirada no autorizada de material nuclear.

3.5. Por lo tanto, las medidas de seguridad informática para los sistemas de I+C deben abordar tanto los ciberataques que causen sabotaje de forma directa como aquellos que recopilen información que podría facilitar el sabotaje de la instalación nuclear o la retirada no autorizada de material nuclear.

---

[12] En la ref. [7] se detallan los cinco niveles de la defensa en profundidad de la seguridad tecnológica nuclear.

INTERRELACIÓN CON LA GESTIÓN DE RIESGOS DE SEGURIDAD INFORMÁTICA DE LA INSTALACIÓN

3.6. El operador debería contar con un proceso de gestión de riesgos de seguridad informática de la instalación para aplicar seguridad informática a fin de proteger las funciones que desempeñan los sistemas de I+C. Este proceso se utiliza para señalar las vulnerabilidades[13] de la instalación a ciberataques y para determinar la consecuencia del comprometimiento exitoso de una o más funciones de los sistemas de I+C (que puede incluir la explotación de vulnerabilidades).

3.7. Los productos de los procesos de la gestión de riesgos de seguridad informática de la instalación deberían incluir la determinación de las funciones de la instalación que realicen los sistemas de I+C —como los sistemas de apoyo y complementarios— que, en el caso de que se viesen comprometidas, podrían perjudicar a la seguridad tecnológica, la seguridad física del material nuclear o la gestión de accidentes. El análisis de la seguridad de la instalación se puede utilizar como aporte para la gestión de riesgos de seguridad informática de la instalación; ahora bien, el análisis de la seguridad por sí solo no es suficiente porque no aborda todas las situaciones de mal funcionamiento. El mal funcionamiento provocado por ciberataques podría colocar a la instalación en situaciones que no se hayan contemplado en el análisis de la seguridad.

3.8. Los productos de los procesos de la gestión de riesgos de seguridad informática de la instalación deberían señalar las posibles consecuencias relacionadas con la seguridad tecnológica nuclear, con la seguridad física nuclear y con la contabilidad y control de materiales nucleares resultantes del comprometimiento del sistema a raíz de un ciberataque a los sistemas de I+C. Al analizar las consecuencias de un ataque a un sistema de I+C, se debería contemplar la posibilidad de que el ataque podría formar parte de un ataque mayor que afecte a multitud de sistemas de I+C o podría ser un ciberataque combinado con un ataque físico. Este análisis podría utilizarse para asignar los niveles de seguridad adecuados a sistemas y componentes individuales de I+C según las posibles consecuencias de su fallo o mal funcionamiento.

3.9. Los niveles de seguridad asignados a los sistemas de I+C se pueden asociar con un listado jerárquico de posibles consecuencias para la seguridad tecnológica y la seguridad física. Por ejemplo, se podrían utilizar los estados de una central, las consecuencias del sabotaje, las jerarquías de la categorización del material

[13] Salvo que se indique lo contrario, en el *Glosario de seguridad* [7] se proporcionan la jerarquía y las definiciones en relación con los estados de una central.

nuclear o una combinación de estos, como en los ejemplos de los párrs. 3.10 a 3.13 y 3.15.

3.10. Por motivos de seguridad tecnológica, los estados de una central se podrían utilizar para señalar las posibles consecuencias para la seguridad derivadas de un ciberataque a los sistemas de I+C. Por ejemplo, los estados de una central se podrían asociar con los siguientes niveles de seguridad de los sistemas de I+C, ordenados de la situación con la consecuencia más leve a la situación con la consecuencia más grave:

1) funcionamiento normal: un ciberataque a sistemas de I+C no puede provocar que la instalación opere fuera de los límites y condiciones especificados para la operación normal;
2) incidente operacional previsto: un ciberataque a sistemas de I+C puede hacer que el estado de la central se desvíe de su operación normal de una forma prevista, pero que, en vista de disposiciones de diseño adecuadas, no cause ningún daño significativo a elementos importantes para la seguridad ni conduzca a condiciones de accidente;
3) accidente base de diseño[14]: un ciberataque a sistemas de I+C puede causar condiciones de accidente que permanezcan dentro de la base de diseño de la instalación y en las cuales el daño al material nuclear (u otro material radiactivo) y la emisión de material radiactivo no sobrepasen los límites autorizados;
4) condiciones adicionales de diseño: un ciberataque a sistemas de I+C puede causar condiciones de accidente que no se contemplen en la previsión de los accidentes base de diseño, pero que sí sean tenidas en cuenta en el proceso de diseño de la instalación, con la aplicación de métodos de mejor estimación, y en las cuales las emisiones de material radiactivo no sobrepasen los límites aceptables. Las condiciones adicionales de diseño podrían incluir condiciones de accidente severo.

3.11. Las consecuencias del sabotaje contra las funciones realizadas por los sistemas de I+C también podrían asociarse con niveles de seguridad. Ese enfoque implicaría que el Estado debería definir el umbral de consecuencias radiológicas inaceptables (URC), según se recomienda en el párr. 3.44 de la ref. [2]. La definición del umbral de URC se puede basar en criterios cuantitativos o cualitativos, que se pueden expresar en términos de emisiones de radionucleidos (por ejemplo, una emisión que supere cierta cantidad concreta), dosis (por

[14] La jerarquía y el texto que la acompaña correspondiente al accidente base de diseño y las condiciones adicionales de diseño se han extraído de la ref. [7].

ejemplo, una emisión que conduzca a una dosis de radiación que supere un valor concreto con respecto a una persona ubicada en un punto concreto, normalmente fuera del emplazamiento) o condiciones de la instalación (por ejemplo, un acto de sabotaje que pueda provocar un daño significativo al núcleo en un reactor). Como se señala en la ref. [11], párrs. 3.94 y 95:

> "los blancos cuyo sabotaje pueda causar una emisión radiológica sustancial que afecte de manera importante a la población y el medio ambiente fuera de los límites de la instalación nuclear (consecuencias de alto riesgo) requerirán el nivel más alto de protección. [En la ref. [2]], las consecuencias radiológicas de los sucesos de esta gravedad se califican como 'graves' o 'de riesgo'.

Por consiguiente, el Estado debería definir también el umbral de las consecuencias radiológicas de alto riesgo".

3.12. En la ref. [11] se proporciona un ejemplo de lista jerárquica de posibles consecuencias de un sabotaje. A continuación se presenta un resumen de ese contenido en relación con las funciones de los sistemas de I+C, en el que las consecuencias están ordenadas de la más leve a la más grave:

— Consecuencia radiológica por debajo del umbral de URC: los blancos que representan estas consecuencias leves necesitan un nivel de protección correspondientemente bajo.
— Las URC se pueden clasificar en tres categorías, ordenadas desde las consecuencias más leves hasta las más graves:
  - nivel de consecuencias C: un acto de sabotaje que podría dar lugar a dosis para las personas en el emplazamiento que exijan la adopción de medidas protectoras urgentes para reducir al mínimo los efectos para la salud en el emplazamiento;
  - nivel de consecuencias B: un acto de sabotaje que podría dar lugar a dosis o contaminación fuera del emplazamiento que exijan la adopción de medidas protectoras urgentes para reducir al mínimo los efectos para la salud fuera del emplazamiento (también se pueden considerar consecuencias radiológicas graves), y
  - nivel de consecuencias A: un acto de sabotaje que podría tener efectos deterministas graves en la salud fuera del emplazamiento (probablemente también se habrán de considerar consecuencias radiológicas graves).

3.13. Los niveles de seguridad también se podrían asociar a la posibilidad de la retirada no autorizada de material nuclear. Las posibles consecuencias de

ciberataques a sistemas de I+C que realicen funciones de protección física o de contabilidad y control de materiales nucleares se podrían asociar a niveles de seguridad basándose en la categoría del material que podría ser objeto de retirada no autorizada. En el cuadro I de la ref. [2] se proporcionan los criterios para categorizar el material nuclear y, además, se señalan recomendaciones para la protección física a partir de esta categorización.

3.14. Actualmente no existe consenso internacional sobre un modelo de jerarquía completamente integrada de todas las consecuencias para la seguridad tecnológica y la seguridad física derivadas de accidentes y sucesos de seguridad física nuclear provocados por ciberataques. No obstante, el operador o el Estado debería elaborar esa jerarquía a escala nacional.

3.15. Al evaluar el conjunto de consecuencias provocadas por un ciberataque a los sistemas de I+C de instalaciones también se pueden contemplar otras consecuencias, como la pérdida de reputación. En la ref. [12] se puede encontrar un listado de posibles consecuencias.

3.16. Las tácticas y las técnicas de los adversarios cambian constantemente y las instalaciones nucleares deberían promover una cultura de la seguridad física nuclear que examine constantemente los riesgos de seguridad informática y que permita la adaptabilidad del programa de seguridad informática de la instalación. La cultura de la seguridad física nuclear se explica más detalladamente en la ref. [13].

3.17. Se deberían analizar la configuración de los sistemas y las actividades asociadas a los sistemas de I+C mejorados con equipo digital, a fin de detectar cambios en las rutas lógicas y físicas que puedan ofrecer oportunidades que un adversario podría explotar. Estas actividades asociadas a los sistemas de I+C comprenden las actividades de mantenimiento temporales, los procesos de compras, el soporte de proveedores, la comunicación con dispositivos de campo y las actualizaciones de *software* manuales.

3.18. La gestión de riesgos de seguridad informática de una instalación es un proceso iterativo y cíclico que podría incluir un análisis inicial, la detección y evaluación de amenazas, la definición de niveles de seguridad, un examen periódico y un análisis actualizado. Debería haber un proceso de aceptación definido para examinar y verificar los resultados de los análisis nuevos o actualizados.

3.19. En el caso de instalaciones nuevas, la gestión de riesgos de seguridad informática de la instalación se debería llevar a cabo como parte del proceso de diseño y debería aceptarse antes de la finalización de la fase inicial de puesta en servicio.

3.20. En el caso de instalaciones existentes, las aportaciones a la versión nueva o actualizada de la gestión de riesgos de seguridad informática de una instalación pueden incluir análisis de seguridad, detalles de la arquitectura de seguridad y de procesos y los productos previamente aceptados de la gestión de riesgos de seguridad informática de la instalación.

INTERRELACIÓN CON LA GESTIÓN DE RIESGOS DE SEGURIDAD INFORMÁTICA DEL SISTEMA

3.21. En la gestión de riesgos de seguridad informática del sistema se deberían utilizar los productos de la gestión de riesgos de seguridad informática de la instalación (si se dispusiera de ellos) y los documentos sobre la base de diseño de los sistemas de I+C como aportaciones para determinar el riesgo para la seguridad que entrañan los ciberataques a sistemas, subsistemas o componentes — individuales o múltiples— de I+C. Los riesgos de seguridad informática evaluados para los sistemas de I+C deberían analizarse y documentarse.

3.22. Para la evaluación y gestión de los riesgos de seguridad informática del sistema de I+C, el operador debería asignar funciones y responsabilidades durante todo el ciclo de vida del sistema de I+C. La seguridad informática requiere medidas específicas por parte de organizaciones y grupos multidisciplinarios. Por ejemplo, el operador puede establecer grupos de trabajo encargados de gestionar procesos y actividades de seguridad informática, así como de obtener autorizaciones.

3.23. El operador debería llevar un inventario del sistema de I+C en el que se incluya el *software*, los subsistemas y los componentes y que se actualice y se mantenga durante todo el ciclo de vida del sistema. El operador debería utilizar este inventario cuando realiza la gestión de riesgos de seguridad informática.

3.24. Se deberían evaluar los componentes del sistema de I+C y se les debería asignar el nivel de seguridad adecuado según la gestión de riesgos de seguridad informática del sistema. Con respecto a estos componentes, se deberían señalar las consecuencias para la seguridad tecnológica y física que podrían derivarse del mal funcionamiento o de una situación de comprometimiento. En el caso de

que se implanten zonas de seguridad dentro de la instalación, se debería asignar y señalar la zona de seguridad.

3.25. Al realizar la gestión de riesgos de seguridad informática del sistema, el operador debería contemplar la posibilidad de que se produzcan ciberataques en cada una de las fases del ciclo de vida del sistema de I+C. En la evaluación, el operador también debería contemplar que los ciberataques pueden afectar a un solo sistema o a múltiples sistemas y que esos ciberataques se podrían combinar con otras formas de actos dolosos que provoquen daños físicos. En la gestión de riesgos de seguridad informática del sistema también se deberían tener en cuenta los actos dolosos que podrían cambiar las señales de procesos, los datos de configuración de equipo o el *software*.

3.26. Además, en la gestión de riesgos de seguridad informática del sistema se deberían contemplar todos los vectores de ataque que se podrían utilizar para introducir datos maliciosos o código malicioso en el sistema de I+C. Por ejemplo, se podría introducir código malicioso en el sistema de I+C a través de conexiones de comunicación, productos suministrados y servicios prestados, o dispositivos portátiles que se conecten temporalmente al equipo objetivo.

3.27. La gestión de riesgos de seguridad informática del sistema debería determinar la probabilidad de que se produzca cada posible consecuencia asociada al sistema de I+C; para ello, se deberían utilizar como aportaciones los siguientes elementos: la disponibilidad de vectores de ataque específicos que podrían emplearse para introducir datos maliciosos o código malicioso en el sistema de I+C; la aplicación y eficacia de medidas de seguridad informática; capacidades de amenaza, y otra información asociada.

3.28. La gestión de riesgos de seguridad informática del sistema es un proceso iterativo y cíclico que, de forma similar a la gestión de riesgos de seguridad informática de la instalación, comprende un análisis inicial, la aplicación de medidas de seguridad informática, un examen periódico y un análisis actualizado. Se podría considerar necesario realizar un examen de la gestión de riesgos de seguridad informática del sistema cuando se dé una de las siguientes situaciones:

— se revisa la gestión de riesgos de seguridad informática de la instalación o el análisis de seguridad de la instalación;
— se realizan modificaciones en el sistema;
— se producen sucesos o incidentes de seguridad importantes, o
— se detectan nuevas amenazas o vulnerabilidades o cambios en estas.

3.29. La gestión de riesgos de seguridad informática del sistema debería detectar acciones u omisiones humanas que puedan afectar a la seguridad física.

ASIGNACIÓN DE MEDIDAS DE SEGURIDAD INFORMÁTICA

3.30. Las orientaciones de los párrs. 3.31 a 3.34 se aplican a todos los sistemas, subsistemas y componentes de I+C a los cuales se puede aplicar un enfoque graduado conforme a su nivel de seguridad asignado.

3.31. A cada sistema, subsistema o componente de I+C se le debería asignar un nivel de seguridad acorde con las posibles consecuencias de su fallo o mal funcionamiento tanto para la seguridad tecnológica como para la seguridad física.

3.32. La aplicación de medidas de seguridad informática a cada sistema de I+C se debería determinar según su nivel de seguridad asignado o según el nivel de seguridad de la zona de seguridad en la que está ubicado, tomándose de estos dos niveles el que sea más estricto.

3.33. Para cada nivel de seguridad se deberían señalar y definir requisitos de seguridad informática. Se debería evaluar la eficacia de las medidas por las que se aplican estos requisitos, a fin de garantizar que se proporcione protección suficiente para los sistemas de I+C en función del nivel de seguridad al que hayan sido asignados.

3.34. En el caso de que las medidas de seguridad informática no puedan proporcionar protección suficiente a los sistemas de I+C en cada nivel de seguridad, se debería estudiar la adopción de más medidas o de medidas alternativas; por ejemplo, características de protección física a nivel de la instalación, funciones electrónicas independientes, rediseño del sistema o medidas administrativas que eliminen vulnerabilidades concretas o que reduzcan las consecuencias de un mal funcionamiento.

INTERRELACIONES ENTRE LA SEGURIDAD TECNOLÓGICA Y LA SEGURIDAD FÍSICA

3.35. Como se señala en la ref. [8], párr. 1.2:

> “La seguridad física y la seguridad tecnológica tienen en común la finalidad de proteger a las personas, los bienes, la sociedad y el medio ambiente.

Las medidas de seguridad física y las de seguridad tecnológica tienen que concebirse y aplicarse en forma integrada para poder generar sinergia entre estas dos esferas y, además, de modo que las medidas de seguridad física no comprometan la seguridad tecnológica y las medidas de seguridad tecnológica no comprometan la seguridad física."

En las refs. [4, 6] se puede encontrar más orientación sobre consideraciones de seguridad para los sistemas de I+C.

3.36. La idoneidad de una determinada medida de seguridad informática dependerá de consideraciones de seguridad tecnológica, de seguridad física y operacionales. Para asignar medidas de seguridad informática a los sistemas de I+C, es necesaria la aportación del personal encargado de la seguridad tecnológica, la seguridad física y las operaciones. Las medidas de seguridad informática no pueden existir al margen de las cuestiones de seguridad tecnológica, y las características de seguridad tecnológica no pueden existir al margen de las cuestiones de seguridad física. Por ejemplo, por motivos de seguridad tecnológica, ciertas funciones de seguridad física (por ejemplo, la recopilación de registros de auditoría o la generación de alarmas de seguridad física) podrían tener que aplicarse en sistemas separados que puedan monitorizar los sistemas de I+C pero no perjudican a la capacidad del sistema para desempeñar sus funciones esenciales. También, la realización de exploraciones activas de seguridad física únicamente cuando los sistemas de I+C no se encuentren en funcionamiento podría satisfacer los objetivos de seguridad física y, a su vez, limitar su efecto sobre los sistemas operacionales.

3.37. Las medidas de seguridad informática diseñadas de forma inadecuada podrían introducir posibles modos de fallo en el sistema, aumentar la probabilidad de operación espuria y obstaculizar la capacidad del sistema para realizar su función de seguridad tecnológica de forma fiable. Por ejemplo, si la implantación de un sistema de detección de *software* malicioso o de virus dentro del sistema I+C se diseñase de forma inadecuada, esto podría aumentar la complejidad del sistema de I+C, aumentar la latencia del sistema de I+C y hacer que este fuera vulnerable a su explotación. Sin embargo, una medida de control técnico bien diseñada que garantice que únicamente el *software* verificado y validado pueda ejecutarse en un sistema de I+C podría mejorar la capacidad del sistema para llevar a cabo su función de seguridad tecnológica de forma fiable y, a su vez, podría proporcionar beneficios considerables en materia de seguridad física.

3.38. Muchas funciones que se diseñan en los sistemas de I+C por motivos de seguridad tecnológica también pueden presentar beneficios para la seguridad

física. Eso sucede, por ejemplo, cuando se comprueba la validez, autenticidad e integridad de los datos recibidos antes de utilizarlos en una función del sistema de I+C.

3.39. Puede haber situaciones en las que una medida de seguridad informática no se pueda aplicar conforme al nivel de seguridad asignado al sistema de I+C; por ejemplo, debido a conflictos con funciones esenciales de seguridad tecnológica; no obstante, estas excepciones se deberían analizar y justificar minuciosamente.

3.40. El conjunto íntegro de medidas de seguridad informática del sistema de I+C debería funcionar de forma combinada y evitar (o no introducir) puntos individuales de fallo.

3.41. La estrategia de seguridad tecnológica podría tener el potencial de perjudicar a la seguridad física. Por ejemplo, el diseño de la seguridad tecnológica suele implicar la asignación de funciones a diferentes subsistemas (o procesadores) para aislar los efectos de los fallos, y la adopción de sistemas redundantes y diversos para que los fallos aislados no comprometan las funciones importantes. Estas estrategias incrementan el número de subsistemas en los sistemas de I+C, lo cual, a su vez, aumenta el número de blancos para ciberataques. Por lo tanto, se deberían tomar medidas para reducir el riesgo de que un ciberataque provoque la pérdida de la diversidad o la redundancia de los sistemas. Las medidas de seguridad informática no deberían introducir nuevas vulnerabilidades que puedan provocar fallos habituales entre estos sistemas redundantes y diversos.

CONSIDERACIONES DE SEGURIDAD TECNOLÓGICA PARA LAS MEDIDAS DE SEGURIDAD INFORMÁTICA

3.42. Las orientaciones que figuran en los párrs. 3.43 a 3.52 se aplican a todos los sistemas de I+C que son importantes para la seguridad tecnológica.

3.43. La aplicación de medidas de seguridad informática no debería perjudicar a las funciones esenciales de seguridad tecnológica y al desempeño del sistema de I+C.

3.44. Ni el funcionamiento normal ni anormal de cualquier medida de seguridad informática debería perjudicar a la capacidad de un sistema de I+C para llevar a cabo su función de seguridad tecnológica.

3.45. El operador debería señalar, documentar y contemplar en los análisis de peligros del sistema los modos de fallo de las medidas de seguridad informática y la forma en que estos modos de fallo afectarían a las funciones de los sistemas de I+C.

3.46. Las medidas de seguridad informática que protegen la interfaz humano–sistema no deberían perjudicar la capacidad del operador para mantener la seguridad tecnológica de la instalación. El operador también debería contemplar efectos adversos como la interceptación y modificación de datos de procesos que se envíen a la interfaz humano–sistema (por ejemplo, la falsificación de paquetes) con el objetivo de impedir que el operador active una función de seguridad tecnológica (por ejemplo, parada manual de emergencia) o que retrase esa activación.

3.47. Las medidas de seguridad informática que no se puedan integrar de manera práctica en el sistema de I+C deberían aplicarse separadas del sistema de I+C. Tal vez sean necesarias más medidas de control administrativo para utilizar y mantener estos dispositivos separados.

3.48. Las medidas de seguridad informática integradas en sistemas de I+C deberían elaborarse según las orientaciones sobre sistemas de gestión que figuran en la ref. [14] o un sistema de gestión alternativo equivalente y deberían tener el mismo nivel de aptitud que el sistema en el que se encuentran las medidas de seguridad informática.

3.49. En el caso de que haya un conflicto entre la seguridad tecnológica y la seguridad física, se deberían mantener las consideraciones de diseño empleadas para garantizar la seguridad tecnológica, siempre que el operador busque una solución compatible para satisfacer los requisitos de seguridad informática. Se deberían aplicar medidas de seguridad informática compensatorias para reducir el riesgo a un nivel aceptable; esas medidas deberían estar respaldadas por una justificación y un análisis de riesgos de seguridad física integrales. Las medidas aplicadas no deberían basarse únicamente en medidas de control administrativo durante un período prolongado. Nunca se debería aceptar la ausencia de una solución de seguridad física.

3.50. El operador debería asignar con claridad la responsabilidad principal del diseño, la selección y la aplicación de medidas de seguridad informática; no obstante, esta responsabilidad principal debería ser un esfuerzo colaborativo entre el personal encargado de las actividades relacionadas con el diseño del sistema de I+C, el mantenimiento, la seguridad tecnológica y la seguridad física.

3.51. El análisis del diseño del sistema de I+C debería demostrar que las medidas de seguridad informática integradas en el sistema de I+C y las aplicadas como dispositivos separados no perjudicarán a las funciones de seguridad tecnológica acreditadas de los sistemas y componentes que son importantes para la seguridad tecnológica.

3.52. El mantenimiento de las medidas de seguridad informática no debería perjudicar a la disponibilidad de los sistemas de I+C.

4. LA SEGURIDAD INFORMÁTICA EN EL CICLO DE VIDA DE LOS SISTEMAS DE I+C

4.1. El diseño de sistemas de I+C para instalaciones nucleares debería gestionarse a través del sistema de gestión integrada de la instalación[15], a fin de garantizar que se contemplen y apliquen todos los requisitos de seguridad informática en todas las fases del ciclo de vida de los sistemas de I+C y que se satisfagan estos requisitos en el diseño final. En la ref. [14] se establecen los Requisitos de Seguridad Generales para los sistemas de gestión de instalaciones nucleares. Además, el párr. 3.12 a) de la ref. [8] hace alusión a la importancia de la seguridad física nuclear de los sistemas de gestión integrada. La ref. [3] proporciona más información sobre la relación general entre los sistemas de gestión y la seguridad informática.

4.2. En el párr. 2.13 de la ref. [4] se indica que:

> "en los sistemas de instrumentación y control digitales, demostrar que el producto resultante es apto para su finalidad depende en gran medida, aunque no exclusivamente, del uso de un proceso de desarrollo de alta calidad que establezca la especificación y la aplicación disciplinadas de los requisitos de diseño."

[15] Según la ref. [7], el sistema de gestión es un "conjunto de elementos interrelacionados e interactuantes (sistema) destinado a establecer políticas y objetivos y a posibilitar que se logren dichos objetivos de manera eficiente y eficaz". En la presente publicación, el término comprende la estructura organizativa y la cultura, las políticas y los procesos organizativos, incluidos los destinados a señalar y asignar recursos (por ejemplo, personal, equipo, infraestructura y el entorno laboral) para el desarrollo de sistemas de I+C.

El párr. 2.14 añade que:

> "en el ámbito de la energía nucleoeléctrica, así como en otros ámbitos fundamentales de la seguridad tecnológica como el ámbito aeroespacial, se han aplicado procesos de desarrollo que se representan habitualmente como modelos del ciclo de vida, que describen las actividades para el desarrollo de sistemas electrónicos y las relaciones entre estas actividades. … Normalmente, las actividades relacionadas con una determinada etapa de desarrollo se agrupan en la misma fase del ciclo de vida."

La seguridad informática debería tenerse en cuenta en todas las fases del ciclo de vida de los sistemas de I+C.

4.3. Como se señala en el párr. 2.17 de la ref. [4]:

> "se necesitan tres niveles fundamentales de ciclos de vida para describir el desarrollo de los sistemas de I+C:
>
> — un ciclo de vida de la arquitectura global de I+C [16];
> — uno o más ciclos de vida de los sistemas individuales de I+C, y
> — uno o más ciclos de vida de los componentes individuales: los ciclos de vida de los componentes se suelen gestionar en el marco del desarrollo de plataformas y son independientes de los ciclos de vida de la arquitectura global y de los ciclos de vida de los sistemas individuales. Los ciclos de vida de los componentes de los sistemas digitales se suelen dividir en ciclos de vida separados para el desarrollo de *hardware* y *software*."

4.4. Los desarrolladores y los operadores de un sistema suelen determinar la definición de modelos de ciclo de vida y las actividades agrupadas dentro de cada fase de un ciclo de vida; sin embargo, la definición y aplicación debería ser una tarea multidisciplinaria en la que participen muchos otros ámbitos, incluido el de la seguridad informática. Por lo general, la responsabilidad principal con respecto a los sistemas de I+C recae en los desarrolladores hasta que los sistemas se transfieren a la entidad operadora para su instalación, integración y puesta en servicio.

---

[16] Como se señala en el párr. 3.10 de la ref. [4], "la arquitectura global de I+C es la estructura organizativa de los sistemas de I+C de la central."

4.5. Dado que el ciclo de vida de los sistemas de I+C puede extenderse varios decenios, distintas entidades pueden desempeñar la función de desarrolladores u otras funciones durante el ciclo de vida de un sistema. Por ejemplo, no es infrecuente que un proveedor lleve a cabo el desarrollo original y que el comprador desarrolle modificaciones más adelante, sobre todo si las modificaciones son de poca importancia. El hecho de que distintas entidades desarrollen estas modificaciones no elimina la necesidad de aplicar medidas de seguridad informática en todas las fases del ciclo de vida de los sistemas de I+C.

4.6. A la mayor brevedad posible, la seguridad informática se debería planificar de forma coherente para todos los ciclos de vida de la arquitectura, el sistema y los componentes de I+C. En esta planificación se deberían especificar las medidas de seguridad informática que han de aplicarse en cada fase para proteger la arquitectura, los sistemas y los componentes de I+C frente a ciberataques que puedan poner en peligro las funciones que son importantes para la seguridad tecnológica. Se debería contemplar la posibilidad de que las funciones de seguridad tecnológica o las medidas de seguridad informática cambien en fases posteriores.

4.7. Durante el proceso de desarrollo del sistema de I+C se debería tratar de reducir al mínimo las posibles vulnerabilidades y debilidades de la seguridad informática y se deberían señalar las posibles vulnerabilidades y debilidades residuales de cada fase del ciclo de vida del sistema de I+C.

4.8. Si bien los modelos de ciclo de vida se pueden organizar de muchas formas, en la presente publicación se utilizan las siguientes fases hipotéticas del ciclo de vida a modo de marco para describir consideraciones de seguridad informática durante el ciclo de vida de los sistemas de I+C:

— planificación del proceso;
— base de diseño;
— arquitectura global de I+C y asignación funcional;
— especificación de los requisitos del sistema de I+C;
— selección de elementos predesarrollados;
— diseño e implantación detallados;
— integración del sistema;
— validación del sistema;
— instalación, integración y puesta en servicio;
— operaciones y mantenimiento;
— modificación, y
— clausura.

4.9. Además de estas fases, el ciclo de vida de los sistemas de I+C también conlleva muchas actividades que son comunes a todas las fases de los ciclos de vida. Las actividades comunes que son importantes para la seguridad informática son:

— la garantía de la calidad;
— la gestión de la configuración;
— la verificación y validación[17];
— la evaluación de la seguridad, y
— la documentación.

4.10. Los requisitos de seguridad informática y las actividades correspondientes a cada fase de un ciclo de vida deberían ser proporcionales a las consecuencias resultantes del acceso, uso, divulgación, manipulación, interrupción o destrucción no autorizados o inadecuados del sistema de I+C. También se debería tener en cuenta el comprometimiento de cualquier sistema, sistema de apoyo o información que pudiera perjudicar a la seguridad tecnológica o la seguridad física.

4.11. El resto de esta sección se divide en subsecciones en las que se analizan orientaciones generales en materia de seguridad informática que se aplican a todas las fases de los ciclos de vida, y orientaciones sobre seguridad física que son específicas para las fases individuales de los ciclos de vida. En esta exposición, las fases se analizan solo una vez, pero las orientaciones deberían aplicarse a cualquier ciclo de vida en el que se encuentre la fase de la que se trate.

ORIENTACIONES GENERALES PARA LA SEGURIDAD INFORMÁTICA

4.12. En la política de seguridad informática de una instalación nuclear se especifican los objetivos globales de seguridad informática de esa instalación. En lo relativo a la planificación de la seguridad informática de la instalación y de los sistemas, estos objetivos se especifican en la política en términos claros,

[17] En el *Glosario de seguridad del OIEA* [7] se define tanto "verificación" como "validación". La verificación de un sistema informático es el "*proceso* por el que se garantiza que una fase del ciclo de vida de un *sistema* informático cumple los requisitos impuestos por la fase anterior". La validación de un sistema informático es el "*proceso* de ensayo y evaluación de un *sistema* informático integrado (equipo y programas informáticos) para asegurar que se cumplen los requisitos funcionales, de comportamiento y de interfaz."

específicos y —en la medida de lo posible— medibles. Los objetivos de la instalación se traducen en objetivos de los sistemas. En la ref. [3] se proporciona más orientación sobre la seguridad informática en las instalaciones nucleares.

4.13. En la política de seguridad informática se deberían incluir elementos que aborden la seguridad física de los sistemas de I+C y, en consecuencia, la política debería aplicarse a cualquier entidad que sea responsable de actividades del ciclo de vida de los sistemas de I+C. Estas entidades comprenden operadores, proveedores, contratistas y suministradores que diseñan, aplican y compran sistemas, *software* y componentes de I+C.

4.14. Cada entidad encargada de llevar a cabo actividades del ciclo de vida de los sistemas de I+C debería señalar y documentar las normas y procedimientos que cumplen con las políticas de seguridad física aplicables, a fin de garantizar que el *hardware*, el *software* y el *firmware* reduzcan al mínimo el código no documentado (por ejemplo, código de puertas traseras), el código malicioso (por ejemplo, intrusiones, virus, gusanos, troyanos y bombas lógicas) y otras funciones o aplicaciones no deseadas, innecesarias o no documentadas, con el objetivo de reducir al mínimo el número de posibles vías a través de las que se pueda producir un ciberataque.

4.15. La política, el programa, las normas asociadas y los procedimientos aplicables en materia de seguridad informática deberían abordar cada fase individual del ciclo de vida de los sistemas de I+C a fin de proteger los sistemas de I+C de la instalación frente a su comprometimiento.

4.16. Las políticas, el programa, las normas y los procedimientos en materia de seguridad informática, así como todas las medidas de seguridad informática, deberían cumplir todos los requisitos reglamentarios y de seguridad informática.

4.17. Las políticas, las normas y los procedimientos de seguridad informática se pueden proporcionar dentro del programa de seguridad de los sistemas de I+C de una entidad o se pueden incorporar a los planes del ciclo de vida de los sistemas de I+C. En la práctica, a menudo se adopta un enfoque mixto.

ASPECTOS DE LA POLÍTICA DE SEGURIDAD INFORMÁTICA RELACIONADA CON LOS SISTEMAS DE I+C

4.18. En la política de seguridad informática de instalaciones nucleares se debería describir la aplicación de un enfoque graduado en materia de implantación de

medidas de seguridad informática para los sistemas de I+C. El enfoque graduado se debería aplicar de conformidad con la importancia de la seguridad tecnológica y la seguridad física de cada función de los sistemas de I+C (por ejemplo, conforme al nivel de seguridad asignado de cada sistema). La dirección debería establecer y hacer cumplir objetivos claros de la política seguridad informática que sean coherentes con los objetivos globales de seguridad tecnológica y seguridad física de la instalación, y abordar de manera específica la seguridad de los sistemas de I+C. En la ref. [3] se señalan con más detalle consideraciones generales relativas a la política y al programa de seguridad informática.

4.19. La política de seguridad informática debería incluir consideraciones importantes para los sistemas de I+C, como:

— el control del acceso, incluido el control del acceso tanto físico como lógico, y la utilización de privilegios mínimos;
— la gestión de la configuración y de los activos, como la gestión de contraseñas, la gestión de parches, el uso del sistema, el fortalecimiento del sistema, el control de la configuración, restricciones sobre el uso de dispositivos móviles y medios extraíbles, dispositivos y redes inalámbricos y el acceso remoto;
— las actividades de verificación de la integridad del sistema y de los componentes;
— los procesos de compras;
— la gestión de riesgos y amenazas, incluidos los procesos para recopilar, analizar, documentar y compartir con otras personas que tengan que conocer información sobre vulnerabilidades, debilidades y amenazas y tomar medidas al respecto;
— la respuesta a incidentes y la recuperación, y
— las auditorías y las evaluaciones.

4.20. En la política de seguridad informática se deberían asignar funciones y responsabilidades a entidades o personas que lleven a cabo actividades del ciclo de vida de los sistemas de I+C.

PROGRAMA DE SEGURIDAD INFORMÁTICA

4.21. Cada entidad que tenga la responsabilidad de llevar a cabo actividades del ciclo de vida de los sistemas de I+C debería elaborar e implantar un programa de seguridad informática integrado o separado en el que se aborden los sistemas de I+C.

4.22. En el programa de seguridad informática se deberían definir las funciones y responsabilidades de cada fase del ciclo de vida de los sistemas de I+C en relación con cada sistema de I+C.

4.23. En el programa de seguridad informática se debería especificar que las entidades responsables apliquen el concepto de defensa en profundidad y señalen medidas de seguridad informática aplicables para los sistemas de I+C conforme a su nivel de seguridad asignado.

4.24. En el programa de seguridad informática se debería especificar la aplicación de medidas de seguridad informática destinadas a brindar protección frente a actos dolosos por parte de agentes internos y frente a la manipulación del sistema de I+C (incluida su integridad) en cada una de las fases del ciclo de vida del sistema de I+C.

4.25. En el programa de seguridad informática se debería especificar que el acceso al sistema, a los componentes, al *software,* a los datos de configuración y a los instrumentos de I+C esté controlado durante todas las fases del ciclo de vida del sistema de I+C. Entre los ejemplos de prácticas del control del acceso figuran el principio de privilegios mínimos y la necesidad de saber.

4.26. En el programa de seguridad informática se debería abordar la confidencialidad de las medidas de seguridad informática, como la protección de la documentación conexa, en consonancia con el nivel de seguridad de los sistemas de I+C a los que se haga alusión en la documentación.

4.27. El programa de seguridad informática debería abordar las posibles vulnerabilidades y debilidades de seguridad informática de cada fase del ciclo de vida de los sistemas de I+C.

4.28. En el programa de seguridad informática se debería señalar el proceso por el cual se clasifica como información de carácter estratégico y se compartimenta[18] la información sobre la seguridad de los sistemas de I+C como, por ejemplo, información detallada relativa a vulnerabilidades halladas en los sistemas de I+C de la instalación o las defensas concretas que se utilizan para proteger los sistemas. Según se define en la ref. [8], la información de carácter estratégico es "información, sea cual sea su forma, comprendidos los programas informáticos,

[18] Por "compartimentar" se entiende dividir información en partes controladas por separado, a fin de evitar que agentes internos reúnan toda la información necesaria para intentar cometer un acto doloso.

cuya revelación, modificación, alteración o destrucción no autorizadas, o cuya denegación de utilización podría comprometer la seguridad física nuclear".

4.29. Se alienta firmemente a las instalaciones nucleares y las entidades asociadas a poner en común información no estratégica sobre vulnerabilidades para que las instalaciones estén mejor preparadas en el caso de que se distribuya y comparta información sobre vulnerabilidades de los sistemas de I+C entre posibles adversarios. En la ref. [15] se proporcionan orientaciones sobre la seguridad física de la información nuclear (incluida su clasificación).

4.30. En el programa de seguridad informática relativo a los sistemas de I+C se debería especificar la obligación de realizar y documentar exámenes y evaluaciones periódicos de la seguridad informática en cada fase del ciclo de vida.

4.31. En el programa de seguridad informática se deberían especificar las medidas de seguridad informática que proporcionen un entorno seguro en el que se puedan realizar actividades de desarrollo.

4.32. En el caso de los sistemas de I+C antiguos, puede haber una mayor dependencia de medidas de control administrativo y de aislamiento que en los sistemas contemporáneos. En el programa de seguridad informática se deberían determinar y mantener medidas de seguridad informática compensatorias adicionales que sean necesarias para garantizar la seguridad informática de los sistemas de I+C antiguos.

ENTORNO DE DESARROLLO SEGURO

4.33. Las orientaciones de los párrs. 4.34 a 4.40 se aplican al desarrollo de todos los sistemas, subsistemas y componentes de I+C a los cuales se aplica un enfoque graduado en materia de seguridad informática conforme a su nivel de seguridad asignado.

4.34. El desarrollo de sistemas de I+C se debería llevar a cabo en un entorno de desarrollo seguro. Esta recomendación se aplica tanto a los emplazamientos internos como externos. Al asignar un nivel de seguridad a este entorno se debería contemplar el nivel de seguridad del sistema en el entorno objetivo, el nivel de seguridad de otros sistemas desarrollados o almacenados dentro del entorno de desarrollo común y los instrumentos de desarrollo. Las medidas de seguridad informática del entorno se deberían evaluar para confirmar la conformidad con los requisitos del nivel de seguridad asignado.

4.35. El entorno de desarrollo seguro debería incluir medidas de control administrativo, como el control de la configuración y la gestión de activos.

4.36. Se deberían utilizar medidas de control físico para controlar el acceso a entornos de desarrollo seguros.

4.37. Se debería verificar el equipo de prueba y de soporte que se utilice en los entornos de desarrollo de sistemas de I+C para confirmar que el uso de este equipo no proporciona vías que permitan introducir datos ni código maliciosos en el entorno de desarrollo seguro.

4.38. Debería haber medidas de seguridad informática para controlar el traslado de datos y dispositivos en relación con todas las fases de desarrollo, a fin de garantizar que no se introduzcan datos ni código maliciosos en el entorno de desarrollo seguro y proteger la información de carácter estratégico asociada a los sistemas de I+C. Estas medidas de seguridad informática deberían incluir medidas de control administrativo y técnico, como restricciones de uso y procedimientos para el control de medios extraíbles y dispositivos móviles. El entorno de desarrollo seguro se debería reconocer como un entorno distinto que esté separado, tanto física como lógicamente, de los entornos operacionales y empresariales.

4.39. Se deberían aplicar medidas de seguridad informática para proteger la integridad del entorno de desarrollo seguro, así como de las aportaciones y los productos del diseño (por ejemplo, datos, archivos de configuración, actualizaciones de *software* y parches de *software*) durante las transferencias entre el entorno de desarrollo seguro y el entorno objetivo. Estas medidas podrían incluir sistemas de configuración de activos automatizados en los que se haya confirmado mediante su análisis el beneficio de la seguridad para el entorno de desarrollo seguro y el entorno objetivo.

4.40. Los instrumentos de terceros o de proveedores que se utilicen para el desarrollo de sistemas de I+C se deberían probar, validar y proteger en proporción con el nivel de seguridad asignado del entorno de desarrollo.

PLANES DE CONTINGENCIA

4.41. Las entidades que lleven a cabo una o más actividades del ciclo de vida de los sistemas de I+C deberían elaborar planes y procedimientos de contingencia para impedir el aumento gradual y la progresión de comportamientos anómalos

y para recuperarse de incidentes de seguridad informática. Estos planes y procedimientos de contingencia se deberían examinar, aplicar periódicamente y actualizar cuando se descubran deficiencias.

4.42. El operador debería elaborar un plan de respuesta a incidentes de seguridad informática que conste de procedimientos en los que se definan, se señalen y se responda a posibles comportamientos anormales o sospechosos que se detecten en los sistemas de I+C y sistemas asociados.

4.43. En el plan de respuesta a incidentes de seguridad informática se debería abordar la recopilación de información y los requisitos jurídicos de la conservación de pruebas durante sucesos de seguridad a fin de apoyar el análisis de investigación.

4.44. En el plan de respuesta a incidentes de seguridad informática se debería asignar personal al grupo de respuesta a incidentes de seguridad informática de la instalación. Este grupo debería estar disponible en la instalación para responder a cualquier incidente de seguridad informática que se detecte. Entre el personal asignado pueden estar quienes tengan conocimientos especializados específicos en sistemas de I+C o en seguridad informática.

4.45. Las copias de respaldo y restauración de los sistemas de I+C que son importantes para los planes y procedimientos de contingencia deberían incluir el *software*, los datos esenciales y los archivos de configuración. Estas copias deberían guardarse en un lugar físico separado del lugar de origen, a fin de protegerlas frente a fallos de causa común. Se deberían utilizar medidas de seguridad informática para proteger estas copias frente al robo, la manipulación ilícita y la eliminación o la destrucción.

PROVEEDORES, CONTRATISTAS Y SUMINISTRADORES DE SISTEMAS DE I+C

4.46. En los párrs. 4.47 a 4.53, por “proveedores”, “contratistas” y “suministradores” se entiende quienes suministran a la instalación nuclear equipo digital, *software* y servicios para los sistemas de I+C a los que se aplica un enfoque graduado en materia de seguridad informática conforme al nivel de seguridad asignado al sistema. El operador debería hacer cumplir la aplicación de las orientaciones que figuran en los párrs. 4.47 a 4.53 mediante la concertación de un contrato con los proveedores, contratistas o suministradores en cuestión.

4.47. Las entidades de proveedores y subproveedores deberían contar con procesos de seguridad informática sólidos y verificables.

4.48. Los proveedores, contratistas y suministradores deberían cumplir todos los requisitos de seguridad informática aplicables. Esto incluye la aplicación de medidas de seguridad informática especificadas por el operador, durante el soporte proporcionado en el emplazamiento o en el lugar de trabajo del proveedor, contratista o suministrador y durante cualquier traslado o almacenamiento de los bienes comprados.

4.49. El proveedor, contratista o suministrador debería contar con un proceso de gestión de la seguridad informática.

4.50. El operador debería especificar de forma clara y en un contrato los requisitos de seguridad informática aplicables en emplazamientos en los que un proveedor, contratista o suministrador realice actividades con sistemas de I+C, en función del nivel de seguridad asignado al sistema, subsistema o componente.

4.51. Debería haber un proceso que posibilite que el operador y el proveedor, contratista o suministrador se notifiquen entre sí sobre vulnerabilidades y coordinen labores de respuesta y mitigación.

4.52. El proveedor, contratista o suministrador debería demostrar que cuenta con un mecanismo verosímil para recibir notificaciones de vulnerabilidades, evaluarlas y notificarlas a la instalación nuclear durante todo el período del servicio contractual. Esta consideración puede prorrogarse más allá de cualquier período normal de garantía, a fin de dar soporte al ciclo de vida del equipo instalado. En estos casos, el mecanismo debería estar incluido respecto del período prorrogado dentro de las obligaciones contractuales acordadas por los proveedores, contratistas o suministradores.

4.53. Se deberían realizar auditorías y evaluaciones de los proveedores, contratistas o suministradores encargados del diseño, desarrollo, integración y mantenimiento de los sistemas de I+C y los resultados de esas auditorías y evaluaciones deberían notificarse al operador.

CAPACITACIÓN EN SEGURIDAD INFORMÁTICA

4.54. Todo el personal que realice trabajos relacionados con sistemas de I+C, incluidos los trabajos relacionados con información de carácter estratégico

asociada a estos sistemas, debería recibir capacitación periódica sobre concienciación y procedimientos en materia de seguridad informática.

4.55. Todo el personal que tenga acceso físico o lógico a sistemas de I+C debería estar cualificado conforme a sus responsabilidades en materia de seguridad informática y, para conservar su cualificación, debería recibir capacitación especializada sobre la seguridad de los sistemas de I+C basada en sus funciones y responsabilidades.

4.56. Todo el personal que tenga acceso físico o lógico a sistemas de I+C debería estar capacitado hasta un nivel de competencia adecuado a sus funciones, a fin de respaldar tareas de seguridad informática y reconocer posibles incidentes de seguridad informática. Estas personas pueden estar informadas sobre las repercusiones de los cambios que se hagan bien en el sistema de I+C al que tienen acceso o en sus medidas de seguridad informática asociadas.

4.57. El personal señalado como miembros del grupo de respuesta a incidentes de seguridad informática debería recibir capacitación sobre la detección de incidentes de seguridad informática y la respuesta a estos. Esta tarea puede conllevar la utilización de un banco de pruebas de sistemas de I+C como componente del programa de capacitación sobre la seguridad de los sistemas de I+C.

4.58. El personal de ingeniería, operaciones y mantenimiento debería estar capacitado para mantener las funciones tanto de la seguridad tecnológica como de la seguridad física de los sistemas de I+C.

4.59. El personal encargado del diseño de los sistemas de I+C debería recibir capacitación sobre el diseño y la programación seguros de sistemas de I+C para instalaciones nucleares (por ejemplo, cómo contemplar la seguridad en el diseño de *software*).

ELEMENTOS COMUNES DE TODAS LAS FASES DEL CICLO DE VIDA

4.60. En la mayoría de los casos, los Requisitos de Seguridad para el sistema de gestión [14] y la orientación general que figura en las Guías de Seguridad conexas [16, 17] proporcionan orientaciones suficientes para las actividades de

los sistemas de gestión relacionadas con la seguridad informática en todas las fases del ciclo de vida de los sistemas de I+C. No obstante, hay unas pocas áreas que exigen orientaciones más específicas.

Sistemas de gestión

4.61. Las orientaciones que figuran en los párrs. 4.62 a 4.70 se aplican a todas las entidades que realizan una o más actividades del ciclo de vida de los sistemas de I+C a los que se les aplica un enfoque graduado en materia de seguridad informática conforme al nivel de seguridad asignado al sistema.

4.62. Al redactar requisitos reglamentarios y/o de seguridad informática en relación con sistemas de gestión, se deberían consultar los Requisitos de Seguridad 6 a 8 que figuran en los párrs. 4.8 a 4.20 de la ref. [14] para sistemas de gestión.

4.63. Toda entidad que se encargue de desarrollar, desplegar, operar, mantener o retirar sistemas o componentes de I+C debería contemplar la seguridad informática de los sistemas de I+C en sus sistemas de gestión integrada.

4.64. El sistema de gestión integrada de la instalación debería ser compatible con los procesos y los procedimientos de seguridad informática.

4.65. Las actividades del ciclo de vida se deberían realizar dentro del marco de un sistema de gestión que proporcione disposiciones adecuadas para la seguridad de los sistemas y los componentes de I+C.

4.66. Debería haber procesos y procedimientos auditables para confirmar que los sistemas, subsistemas y componentes de I+C que son importantes para mantener la seguridad informática siguen desempeñando sus funciones de seguridad física durante su vida operacional.

4.67. Se debería prever la realización de exámenes de la seguridad de los sistemas de I+C (por ejemplo, inspecciones de la configuración) durante todo el ciclo de vida de los sistemas de I+C, a fin de demostrar que se han seguido los procedimientos de seguridad y que se ha alcanzado el nivel requerido con respecto al trabajo realizado (por ejemplo, no se han añadido más componentes).

4.68. Se deberían realizar inspecciones independientes[19] para comprobar que los procesos y los procedimientos de seguridad informática se llevan a cabo según lo estipulado en el plan de garantía de la calidad del operador.

4.69. Se deberían elaborar y conservar registros detallados de las actividades del ciclo de vida, de tal manera que se puedan examinar estos registros y se puedan comparar con requisitos de seguridad informática en cualquier momento. Estos registros deberían incluir todos los incidentes de seguridad informática y las medidas de respuesta y de contingencia adoptadas tras los incidentes.

4.70. Las personas autorizadas que tengan acceso lógico o físico privilegiado a sistemas de I+C deberían estar sujetas a evaluaciones de fiabilidad, a capacitación sobre seguridad informática y a observaciones sobre su comportamiento en consonancia con el programa de mitigación de agentes internos de la instalación u otro programa equivalente (véase la ref. [5]).

Exámenes y auditorías de la seguridad informática

4.71. Las orientaciones que figuran en los párrs. 4.72 a 4.77 se aplican a todas las entidades que realizan una o más actividades del ciclo de vida relacionadas con los sistemas de I+C a los que se les aplica un enfoque graduado en materia de seguridad informática conforme a su nivel de seguridad asignado.

4.72. Se deberían realizar periódicamente exámenes y auditorías de la seguridad informática de los sistemas de I+C y de las actividades asociadas para verificar que se cumplen los reglamentos, la política de seguridad informática y las buenas prácticas en materia de seguridad informática de los sistemas de I+C.

4.73. Los exámenes de seguridad informática de los sistemas de I+C deberían ser independientes y los deberían realizar examinadores cualificados internos y/o externos.

4.74. Se deberían definir y documentar políticas y procedimientos en los que se incluyan funciones y responsabilidades para la realización de esos exámenes.

4.75. Los exámenes de la seguridad informática de los sistemas de I+C deberían verificar la aplicación y la eficacia de sus medidas de seguridad informática asociadas.

---

[19] Por “independientes” se entiende que las inspecciones las lleva a cabo una persona o entidad distinta de la parte que se somete al examen.

4.76. No se deberían llevar a cabo pruebas de evaluación de intrusiones en sistemas de I+C operacionales. La prueba de evaluación de intrusiones implica tratar de explotar una vulnerabilidad (por ejemplo, como en una prueba de penetración) que pueda cambiar las condiciones operacionales o la configuración del sistema de I+C fuera de su base de diseño. El operador debería contemplar el uso de métodos controlados para llevar a cabo pruebas sin carga útil mientras la instalación se encuentre en una situación en la que se eviten UCR; por ejemplo, cuando la instalación se encuentre en régimen de parada o cuando se le haya retirado el combustible. En las políticas y procedimientos de la instalación se debería abordar la realización y ejecución de estas pruebas. Estas pruebas se deberían diseñar de forma específica para cada sistema. El grupo de respuesta a incidentes de seguridad informática debería participar en las pruebas de evaluación de intrusiones.

4.77. Los registros de los exámenes de seguridad informática y los datos de análisis asociados se deberían archivar, conservar y proteger durante todo el ciclo de vida del sistema de I+C.

Gestión de la configuración para la seguridad informática

4.78. Las orientaciones que se proporcionan en los párrs. 4.79 a 4.87 se aplican a todos los sistemas, subsistemas y componentes de I+C a los que se haya asignado un nivel de seguridad.

4.79. Las actividades de control de la configuración del *software* pueden ayudar a prevenir y detectar incidentes de seguridad informática, aunque estas actividades no tienen como finalidad principal abordar objetivos específicos de la seguridad física nuclear. Se debería analizar y confirmar el beneficio para la seguridad informática que se obtiene al realizar estas actividades antes de dar esos beneficios por sentado. Por ejemplo, mediante estas actividades se podría detectar un incidente de seguridad informática, pero el tiempo de inicio de la respuesta al incidente detectado probablemente sería insuficiente para proteger el sistema en comparación con el tiempo de respuesta en un sistema de seguridad informática que incorpore medidas de seguridad informática en capas con elementos de respuesta automáticos.

4.80. Los cambios no gestionados en la configuración del *software* son una fuente importante de nuevas vulnerabilidades y situaciones impredecibles. Normalmente, el sistema de gestión de la configuración que se emplea para los sistemas de I+C es un sistema genérico que también gestiona muchos otros tipos de sistemas. Sin embargo, el sistema de gestión de la configuración se debería

utilizar de tal manera que incorpore conocimientos tanto de los sistemas de I+C como de sus medidas de seguridad informática.

4.81. La gestión de la configuración depende de la gestión del cambio, que es un proceso que pretende garantizar que, cuando se cambie un sistema informático, se utilicen procesos de diseño aprobados y la verificación y validación adecuadas. También incluye el control de documentos que respaldan estos procesos. En el párr. 5.26 de la publicación *Aplicación del sistema de gestión de instalaciones y actividades, Colección de Normas de Seguridad del OIEA* Nº GS-G-3.1 [16], se señala lo siguiente:

> "los tipos de documentos que se habrá de controlar deberían ser, pero sin limitarse a ellos: los documentos que definen el sistema de gestión; los requisitos en materia de seguridad; las instrucciones de trabajo; los informes de evaluación; los planos; los ficheros de datos; las especificaciones; los códigos informáticos; los pedidos y documentos conexos; y los documentos del suministrador".

4.82. Las medidas de seguridad informática para los sistemas de I+C que utilicen el proceso de gestión de la configuración de la instalación deberían ser coherentes con los requisitos de control de la configuración de la instalación aplicables al sistema de I+C asociado.

4.83. La gestión de la configuración para las medidas de seguridad informática asociadas a sistemas de I+C debería garantizarse durante todo el ciclo de vida de estos sistemas.

4.84. La gestión de la configuración para las medidas de seguridad informática asociadas a sistemas de I+C debería incluir técnicas y procedimientos para analizar los efectos de los cambios de la configuración, aprobar cambios de la configuración, garantizar que las versiones de *software* se combinen correctamente, emitir documentos de diseño y *software* para su uso, y establecer y mantener un registro cronológico de cambios de la configuración (por ejemplo, qué versiones de instrumentos de *software* se utilizan en un punto concreto del diseño).

4.85. La identificación, el almacenamiento y la emisión para el uso de componentes de I+C y medidas de control técnico asociadas deberían estar protegidos frente al comprometimiento.

4.86. Los documentos de configuración para las medidas de seguridad informática asociadas a sistemas de I+C deberían conservarse y protegerse del acceso no autorizado y de su comprometimiento. Esta información debería clasificarse como información de carácter estratégico y el acceso a ella debería limitarse a los casos en que es necesario conocerla.

4.87. Durante el desarrollo, el transporte, la instalación y las operaciones, se deberían aplicar medidas de control técnico al *software* y a los archivos de configuración a fin de limitar el acceso a ellos y garantizar su integridad.

Verificación y validación

4.88. Las orientaciones que se proporcionan en los párrs. 4.89 a 4.94 se aplican a todos los sistemas, subsistemas y componentes de I+C a los que se haya asignado un nivel de seguridad.

4.89. Cada fase del proceso de desarrollo de los sistemas de I+C utiliza información de fases anteriores y proporciona resultados para que se utilicen como aportación a fases posteriores. La verificación se debería realizar tras finalizar una fase del proceso de desarrollo y antes de avanzar a la siguiente fase del proceso de desarrollo; además, debería incluir una evaluación de las medidas de seguridad informática.

4.90. Antes de finalizar la fase de puesta en servicio del proceso de desarrollo del sistema de I+C, se debería realizar la validación del sistema de I+C con el objetivo de garantizar que se cumplan los requisitos de seguridad informática y, al mismo tiempo, se sigan cumpliendo los requisitos funcionales, de comportamiento y de interfaz. Con ello se pretende proporcionar un alto grado de garantía de que el sistema desempeñará su función según lo exigido. Grupos o personas que sean independientes de los diseñadores y desarrolladores deberían llevar a cabo la validación de las medidas de seguridad informática. El alcance de la validación independiente y el grado de independencia, por ejemplo, deberían ser aptos para el nivel de seguridad asignado al sistema o componente en cuestión, al margen de que la validación la realice personal del proveedor, contratista o suministrador o expertos externos ajenos al proveedor, contratista o suministrador.

4.91. Las actividades de verificación y validación deberían demostrar que el sistema de I+C cumple los requisitos de seguridad informática pertinentes.

4.92. El operador debería verificar y validar cada medida de control técnico para confirmar que le proporciona al sistema de I+C la protección deseada y que no

reduce la fiabilidad de sus funciones de seguridad tecnológica ni de seguridad física.

4.93. Las medidas de seguridad informática se deberían verificar y validar utilizando un nivel de esfuerzo proporcional al nivel de seguridad asignado al sistema de I+C asociado o utilizando un nivel de esfuerzo proporcional a la clasificación de seguridad del sistema de I+C; para determinar cuál de los dos utilizar, se debería optar por el que sea más estricto.

4.94. Las actividades de verificación y validación deberían señalar, registrar y documentar las vulnerabilidades, debilidades y otras anomalías que se hayan detectado y su resolución. Dado el tamaño y la complejidad de los sistemas computarizados más modernos, puede que sea difícil garantizar que los resultados de estas actividades sean exhaustivos o exitosos en la labor de descubrir todas las anomalías. Por ejemplo, los instrumentos automatizados para realizar exámenes de código de *software* dependen de la plataforma y del lenguaje de programación utilizados, y puede que solo tengan éxito en parte. Además, tal vez no sea posible examinar ciertos sistemas operativos, código máquina y funciones de bibliotecas invocables (*callable libraries*), que pueden contener vulnerabilidades que se podrían explotar.

Evaluaciones de la seguridad informática

4.95. Las orientaciones que se proporcionan en los párrs. 4.96 a 4.100 se aplican a todos los sistemas, subsistemas y componentes de I+C a los que se haya asignado un nivel de seguridad.

4.96. Se deberían realizar evaluaciones de la seguridad informática con respecto a cada fase del ciclo de vida del sistema de I+C, a fin de detectar posibles amenazas, así como vulnerabilidades y debilidades.

4.97. Se debería monitorizar la información pública o la información de fuentes de libre acceso, así como las fuentes de proveedores, contratistas o suministradores y expertos, a fin de detectar de inmediato cambios en el panorama de amenazas y nuevas vulnerabilidades.

4.98. Se deberían evaluar las amenazas y las vulnerabilidades nuevas o cambiadas para valorar su posible efecto sobre la seguridad informática de los sistemas de I+C. Se deberían adoptar medidas correctivas (por ejemplo, modificación de las características de seguridad) en el caso de que estos cambios pudieran dar lugar a posibles violaciones de la seguridad o a riesgos inaceptables para la instalación.

4.99. Toda entidad que se encargue de desarrollar, desplegar, operar, mantener o deshabilitar un sistema o componentes de I+C debería llevar a cabo evaluaciones y auditorías periódicas de la seguridad informática.

4.100. Los resultados de las evaluaciones de la seguridad informática se deberían utilizar para actualizar la gestión de riesgos de seguridad informática del sistema.

Documentación

4.101. Las orientaciones que se proporcionan en los párrs. 4.102 a 4.106 se aplican a todos los sistemas, subsistemas y componentes de I+C a los que se haya asignado un nivel de seguridad.

4.102. La documentación relativa a la seguridad informática de los sistemas de I+C ayuda a evitar ambigüedades y facilita la utilización correcta y sin errores, la vigilancia, la resolución de problemas, el mantenimiento, la modificación y la modernización futuras del sistema, y la capacitación del personal de la instalación y de apoyo técnico.

4.103. Se debería generar documentación para registrar información suficiente relacionada con la seguridad informática de los sistemas de I+C, a fin de demostrar que el diseño, la aplicación y el mantenimiento de las medidas de seguridad informática se ajustan al nivel de protección requerido en consonancia con el nivel de seguridad asignado.

4.104. Para cada una de las fases del ciclo de vida de los sistemas de I+C, se deberían establecer documentos de aportación y documentos de productos de la seguridad informática.

4.105. La documentación debería garantizar la trazabilidad de los requisitos de seguridad informática en todas las actividades del ciclo de vida de los sistemas de I+C. Se debería registrar la adición, modificación y supresión de medidas de seguridad informática relacionadas con sistemas de I+C.

4.106. La documentación debería estar protegida frente a la divulgación no autorizada, la manipulación ilícita y la eliminación, y la destrucción, en proporción al nivel de seguridad asignado del sistema de I+C asociado.

Base de diseño

4.107. Las orientaciones de los párrs. 4.108 a 4.114 se aplican a todos los sistemas, subsistemas y componentes de I+C a los cuales se puede aplicar un enfoque graduado conforme a su nivel de seguridad asignado.

4.108. En el párr. 3.11 de la ref. [4] se indica que "la base de diseño señala las funciones, las condiciones y los requisitos de la arquitectura global de I+C y de cada sistema de I+C individual." Así pues, esta información se utiliza para asignar requisitos de seguridad informática a cada sistema de I+C y a los sistemas de seguridad física de apoyo. La base de diseño también se utiliza para establecer especificaciones en cuanto al diseño, la aplicación, la construcción, la realización de pruebas y el desempeño relacionados con las medidas de seguridad informática.

4.109. La base de diseño de la arquitectura global de I+C y de cada sistema de I+C debería utilizarse para fundamentar el diseño de las medidas de seguridad informática que se han de aplicar para satisfacer los requisitos reglamentarios en materia de seguridad informática (como la amenaza base de diseño o la evaluación de la amenaza). En la ref. [18] se proporciona más orientación sobre la amenaza base de diseño (incluidas las evaluaciones de la amenaza y las exposiciones alternativas de la amenaza).

4.110. En la base de diseño se deberían señalar consideraciones e hipótesis sobre el diseño de la seguridad informática de los sistemas de I+C y de los sistemas de seguridad física de apoyo.

4.111. El nivel de protección que ha de aplicarse a cada sistema de I+C se debería definir en la base de diseño, en consonancia con el nivel de seguridad asignado que se señale en la gestión de riesgos de seguridad informática de la instalación y del sistema.

4.112. La base de diseño debería especificar los requisitos para las medidas de seguridad informática, incluidas las medidas de control técnico, físico y administrativo.

4.113. La base de diseño debería especificar requisitos de seguridad tecnológica que permitan la realización de actividades de validación eficaces, con el objetivo de impedir que las medidas de seguridad informática afecten negativamente al comportamiento en materia de seguridad de los sistemas de I+C.

4.114. La base de diseño se debería mantener y actualizar periódicamente para reflejar los cambios en los requisitos reglamentarios de seguridad informática o los riesgos.

Control del acceso

4.115. Las orientaciones de los párrs. 4.116 a 4.120 se aplican a todos los sistemas, subsistemas y componentes de I+C a los cuales se aplica un enfoque graduado en materia de seguridad informática conforme a su nivel de seguridad asignado.

4.116. Se debería controlar el acceso físico y lógico a los sistemas de I+C con el objetivo de prevenir el acceso no autorizado a estos. El acceso privilegiado a los sistemas de I+C debería estar estrictamente controlado, de modo que únicamente el personal autorizado tenga acceso a la configuración, el *software* o el *hardware* existentes o pueda realizar cambios en estos. Este acceso se puede restringir según la función laboral que desempeñe el personal autorizado, tanto en cuanto a la duración como al número de sistemas a los que se pueda acceder.

4.117. El número de puntos de acceso a redes y dispositivos se debería reducir al mínimo posible, a fin de reducir a la mínima expresión el número de posibles vectores de ataque.

4.118. La comunicación digital se debería restringir a los usos autorizados y se debería monitorizar a fin de detectar cualquier actividad anómala. Cuando se detecte una actividad anómala, se deberían adoptar medidas adecuadas.

4.119. Con respecto a los sistemas de I+C a los que se haya asignado el nivel de seguridad más estricto, se debería contemplar el uso de métodos de autenticación multifactor en los casos en que esos métodos sean compatibles con interacciones dependientes del tiempo entre el personal de la instalación y el sistema de I+C.

4.120. Se deberían elaborar y actualizar periódicamente procedimientos para gestionar y asignar funciones y derechos de acceso con respecto al sistema y cuentas de usuario. En los procedimientos se debería tener en cuenta el principio del privilegio mínimo. Este proceso puede indicarse o integrarse en el programa de seguridad informática de la instalación y el sistema de gestión integrada de la instalación.

Protección de la confidencialidad de la información

4.121. Las orientaciones de los párrs. 4.122 a 4.125 se aplican a todos los sistemas, subsistemas y componentes de I+C a los cuales se puede aplicar un enfoque graduado conforme a su nivel de seguridad asignado.

4.122. Cuando se aplican medidas de protección física y de seguridad informática insuficientes para proteger la confidencialidad de la información, se pueden producir divulgaciones no autorizadas de información que podrían comprometer la protección física o la seguridad informática del sistema o de la instalación. En la publicación de la *Colección de Seguridad Física Nuclear del OIEA* 23-G [15] se indica lo siguiente:

> "La información es conocimiento, independientemente de la forma en que exista o se exprese. Comprende ideas, conceptos, sucesos, procesos, pensamientos, hechos y patrones. Puede registrarse en un material como el papel, una película o un medio magnético u óptico, o conservarse en sistemas electrónicos."

4.123. La información relacionada con los sistemas de I+C (por ejemplo, bases de datos, archivos y documentación asociados; componentes de cambios; simuladores) debería señalarse, y cuando proceda, clasificarse como información de carácter estratégico y asegurarse con medidas adecuadas. Las refs. [12, 15] proporcionan más información sobre recomendaciones para proteger la información de carácter estratégico.

4.124. Se deberían utilizar medidas de seguridad informática para proteger la confidencialidad de la información asociada a los sistemas de I+C, que puede comprender información sobre el diseño, la fabricación, la instalación y la operación de los sistemas de I+C y del equipo conexo.

4.125. El operador debería aplicar medidas de control técnico, físico y administrativo para prevenir, detectar y responder a la divulgación no autorizada o la filtración de información de carácter estratégico relacionada con los sistemas de I+C.

Monitorización de la seguridad

4.126. Las orientaciones de los párrs. 4.127 a 4.130 se aplican a todos los sistemas, subsistemas y componentes de I+C a los cuales se puede aplicar un enfoque graduado conforme a su nivel de seguridad asignado.

4.127. Se deberían especificar requisitos de seguridad informática que guarden relación con la monitorización de la seguridad de los sistemas de I+C y que sean coherentes con los niveles de seguridad que se han asignado a los sistemas.

4.128. Cuando la monitorización de sistemas de I+C exija el nivel de seguridad más alto o un nivel de seguridad alto, en las medidas de seguridad informática desplegadas se deberían emplear principios de independencia[20] o de diversidad, a fin de detectar el comprometimiento o el mal funcionamiento. Se deberían proporcionar interfaces de usuario para la monitorización de la seguridad, indicaciones de comprometimiento, instrumentación de registro y alarmas en lugares adecuados, que deberían ser aptas y suficientes para apoyar la monitorización eficaz de la seguridad informática en todos los estados de la central.

4.129. Se deberían establecer requisitos para monitorizar el estado de las medidas de control técnico o físico, a fin de facilitar la adopción de cualquier medida necesaria de seguridad tecnológica o seguridad física.

4.130. Los sistemas de I+C y las medidas de seguridad informática asociadas se deberían monitorizar y registrar constantemente. El análisis debería señalar el acceso no autorizado o cambios realizados sin autorización. Se debería proteger la integridad de estos registros.

Consideraciones para la arquitectura global de defensa de la seguridad informática

4.131. Las orientaciones que se proporcionan en los párrs. 4.132 a 4.140 se aplican a todos los sistemas, subsistemas y componentes de I+C a los que se haya asignado un nivel de seguridad.

4.132. El operador debería especificar una arquitectura global de defensa para la seguridad informática de los sistemas de I+C en la que todos los sistemas de I+C tengan un nivel de seguridad asignado y estén protegidos conforme a los requisitos aplicables.

4.133. La arquitectura de defensa se debería utilizar para facilitar y mantener la capacidad de los sistemas de I+C en cuanto a la prevención, detección, dilación y mitigación de ciberataques, así como a la recuperación en caso de ciberataque.

[20] Un ejemplo de independencia es la segregación de los sistemas de monitorización del sistema de I+C, lo que permitiría separar las funciones.

La arquitectura de defensa incluye, entre otras cosas, límites formales lógicos o físicos como las zonas de seguridad en la que se despliegan las medidas de defensa[21]. Al implantar esa arquitectura, los operadores deberían plantearse limitar los elementos dinámicos tanto de las redes compuestas como de sus sistemas individuales, a fin de aumentar la determinación de su comportamiento. Esta mayor determinación puede ayudar a aplicar medidas de seguridad informática eficaces para la detección de posibles incidentes de seguridad informática.

4.134. Se deberían aplicar límites de seguridad informática entre los sistemas, subsistemas y componentes de I+C que tengan distintos niveles de seguridad y que estén protegidos con distintas medidas de seguridad informática. Los límites de seguridad informática son los límites lógicos y físicos de un sistema o de un conjunto de sistemas en el mismo nivel de seguridad y, por lo tanto, se pueden asegurar mediante la aplicación de medidas de defensa comunes (por ejemplo, zonas de seguridad informática).

4.135. Se debería controlar la circulación de datos entre zonas de seguridad a las que se hayan asignado niveles de seguridad distintos y entre sistemas de I+C individuales en el mismo nivel de seguridad conforme a un enfoque basado en el conocimiento de los riesgos, a fin de garantizar que la arquitectura de defensa siga siendo eficaz.

4.136. Los sistemas de I+C que requieran el nivel de seguridad más alto (es decir, el nivel de seguridad más estricto) únicamente se deberían conectar a sistemas que necesiten niveles de seguridad más bajos (es decir, niveles de seguridad más débiles) a través de vías de comunicación de datos unidireccionales, deterministas y a prueba de fallos[22]. La dirección de estas vías de datos debería limitarse a la transmisión de datos desde dispositivos que requieran el nivel de seguridad más estricto hasta los dispositivos a los que se hayan asignado niveles de seguridad más débiles. Se recomienda encarecidamente no aplicar excepciones; estas solo se pueden contemplar de forma individualizada y estricta y cuando estén respaldadas por una justificación y un análisis de riesgos de seguridad física completos[23].

---

[21] Un ejemplo de ese tipo de arquitectura de defensa es aquella que incluye una serie de niveles de defensa concéntricos de seguridad creciente y que contempla tanto los componentes del *hardware* como del *software*.

[22] En el nivel de seguridad más estricto no se puede aplicar el acceso remoto a los sistemas, debido a la limitación unidireccional del tráfico saliente del sistema de I+C.

[23] Algunos Estados Miembros están convencidos de que no se deberían permitir excepciones en ningún caso.

4.137. Los dispositivos digitales o las redes de comunicación que se utilicen para las actividades de monitorización, mantenimiento y recuperación no deberían eludir las medidas de control técnico utilizadas para proteger las vías de comunicación entre dispositivos con distintos niveles de seguridad.

4.138. Los sistemas a los que se haya asignado el nivel de seguridad más estricto deberían estar ubicados dentro de los límites de la zona más segura. Las funciones de comunicaciones inalámbricas son problemáticas cuando se aplican en sistemas de I+C a los que se ha asignado el nivel de seguridad más estricto, puesto que es difícil proporcionar un límite seguro para esas comunicaciones.

4.139. Las comunicaciones de datos entre los sistemas de I+C de la instalación y el centro de emergencia (ya sea en el emplazamiento o fuera de este) deberían estar protegidas y controladas por medidas de seguridad informática.

4.140. Para las medidas de control técnico aplicadas en cada zona de seguridad o en el límite de la zona de seguridad se deberían emplear tecnologías distintas de las implantadas en niveles o límites de seguridad adyacentes. De este modo se garantizará el uso de tecnologías diversas para proteger a los sistemas de I+C.

Defensa en profundidad frente al comprometimiento

4.141. Las orientaciones de los párrs. 4.142 a 4.151 se aplican a todos los sistemas, subsistemas y componentes de I+C a los cuales se puede aplicar un enfoque graduado conforme a su nivel de seguridad asignado.

4.142. La defensa en profundidad frente al comprometimiento implica establecer distintas capas defensivas de medidas de seguridad informática que tengan que fallar o ser eludidas para que un ciberataque progrese y afecte a un sistema de I+C. Por lo tanto, la defensa en profundidad se logra no solo aplicando múltiples capas de defensa (por ejemplo, zonas de seguridad dentro de una arquitectura de defensa de seguridad informática), sino también estableciendo y manteniendo un programa sólido de medidas de seguridad informática que permitan la evaluación, prevención y detección de ataques a los sistemas de I+C, así como la protección contra estos y la respuesta, mitigación y recuperación para casos de ataque a esos sistemas. Por ejemplo, si se produjera un fallo en la prevención (por ejemplo, la vulneración de una política) o se eludieran los mecanismos de protección (por ejemplo, por un nuevo virus no detectado aún como un ciberataque), seguirían existiendo mecanismos para detectar cualquier alteración no autorizada de un sistema de I+C afectado y para responder ante ella.

4.143. Ningún fallo individual que se produzca dentro de las capas de defensa o a través de estas debería invalidar ni hacer ineficaz la seguridad informática global de los sistemas de I+C. Por ejemplo, la explotación de una vulnerabilidad crítica dentro de un dispositivo común de protección de redes utilizado en dos lugares unidos de forma lógica pero físicamente separados tendría la posibilidad de facilitar un ataque eludiendo múltiples capas de medidas de seguridad informática.

4.144. Se deberían designar y operar sistemas de I+C y componentes digitales conexos de conformidad con el concepto de defensa en profundidad frente al comprometimiento.

4.145. Se debería asignar personal a la realización de medidas de seguridad que complementen las medidas de control técnico. Se debería analizar y justificar el equilibrio entre la actividad humana y las medidas de control técnico.

4.146. Se debería adoptar un enfoque sistemático para señalar y documentar acciones humanas que puedan perjudicar a la seguridad de los sistemas de I+C en cada fase del ciclo de vida de estos sistemas.

4.147. Se debería utilizar un enfoque basado en el conocimiento de los riesgos para determinar la provisión adecuada de seguridad para los sistemas de I+C, como la aplicación de medidas de control técnico y la defensa en profundidad frente al comprometimiento. Las capas de las medidas de seguridad informática utilizadas para aplicar la defensa en profundidad frente al comprometimiento deberían aplicarse conforme a la gestión de riesgos de seguridad informática de la instalación y de los sistemas.

4.148. Cada capa de defensa debería estar protegida de ciberataques que se originen en capas adyacentes.

4.149. Los mecanismos de protección utilizados para el aislamiento entre capas de defensa deberían mitigar los fallos de causa común.

4.150. Las capas de defensa y las contramedidas asociadas deberían prevenir o retrasar el avance de los ataques.

4.151. Las capas de defensa deberían ser eficaces durante todo el ciclo de vida del sistema de I+C y se deberían contemplar en el diseño, la configuración, la modificación y la asignación de parámetros de los componentes del sistema.

Especificación de requisitos de seguridad informática

4.152. Se deberían establecer y documentar los requisitos de seguridad informática relativos a la arquitectura de defensa y a los sistemas y componentes individuales de I+C. Estos requisitos para la arquitectura de defensa deberían elaborarse a partir de la base de diseño de los sistemas de I+C.

4.153. Los requisitos de seguridad informática relativos a los sistemas, subsistemas y componentes de I+C deberían contemplar los requisitos funcionales y de comportamiento, la configuración de los sistemas, la cualificación, la ingeniería de factores humanos, las definiciones y comunicaciones de datos, la documentación, la instalación y puesta en servicio, la operación y el mantenimiento.

4.154. En la elaboración de requisitos de seguridad informática para los sistemas de I+C se debería tener en cuenta la gestión de riesgos de seguridad informática de la instalación y de los sistemas. Los requisitos de seguridad informática se deberían examinar y actualizar a partir de cambios en los productos de la gestión de riesgos de seguridad informática de la instalación y de los sistemas.

4.155. La combinación de los requisitos de seguridad informática para la arquitectura de defensa y para los sistemas individuales de I+C debería cumplir con la base de diseño establecida para la arquitectura global de I+C.

Selección de elementos predesarrollados

4.156. Las orientaciones de los párrs. 4.157 a 4.164 se aplican a todos los sistemas, subsistemas y componentes de I+C a los cuales se puede aplicar un enfoque graduado.

4.157. Los elementos predesarrollados podrían comprender dispositivos electrónicos, *software* predesarrollado, artículos comerciales de distribución general, dispositivos digitales compuestos de *hardware* y *software* (incluido el *firmware*), dispositivos de *hardware* configurados con lenguaje de descripción de *hardware* o bloques funcionales predesarrollados.

4.158. Los elementos predesarrollados podrían incluir *hardware* y *software* predesarrollados (incluido el *firmware*) de entidades que no cuenten con un

programa adecuado de seguridad informática o que no estén dispuestas a compartir información detallada sobre su programa de seguridad informática. En esos casos, es preciso analizar las características de seguridad informática de los elementos y justificar su uso dentro de sistemas de I+C o de sistemas auxiliares.

4.159. Es probable que la propiedad intelectual del *software* predesarrollado y de los artículos comerciales de distribución general esté protegida y que no se pueda disponer de su código fuente para actividades de verificación amplias. Por lo tanto, es probable que el operador no cuente con ningún método fiable para determinar de forma amplia las vulnerabilidades de seguridad de estos productos. En esos casos, se necesitarán medidas de seguridad informática compensatorias, salvo que el desarrollador de aplicaciones modifique estos productos.

4.160. Se deberían aplicar medidas de seguridad informática para garantizar que las características del *software* predesarrollado y de los artículos comerciales de distribución general no puedan hacer que los sistemas de I+C dejen de satisfacer sus requisitos de seguridad informática. Por ejemplo, puede haber orientaciones para reducir la cantidad de código que se ejecuta, para impedir que haya puntos de entrada a disposición de usuarios no autorizados y para eliminar funcionalidades innecesarias, lo que reduciría al mínimo la superficie de ataque (es decir, se lograría el fortalecimiento del sistema). No obstante, la aplicación de estas medidas de seguridad informática únicamente puede proporcionar una protección limitada y, por ello, el operador debería aplicar otras medidas de seguridad informática compensatorias.

4.161. Para seleccionar y configurar componentes o *software* predesarrollados se debería utilizar un proceso de cualificación de la seguridad que sea proporcional al nivel de seguridad del sistema de I+C.

4.162. Se debería verificar el uso de *software* predesarrollado y de artículos comerciales de distribución general para garantizar que los productos satisfagan los requisitos de seguridad informática de los sistemas de I+C.

4.163. El operador debería determinar cuál es la documentación que necesita para la cualificación de los productos de *software* predesarrollado. No se debería confiar en medidas de control técnico cuya eficacia no se pueda verificar.

4.164. En el *software* predesarrollado o en los artículos comerciales de distribución general que se puedan configurar, se deberían eliminar las funciones o los servicios que no se necesiten.

Diseño e implantación de sistemas de I+C

4.165. Las orientaciones de los párrs. 4.166 a 4.174 se aplican a todos los sistemas, subsistemas y componentes de I+C a los cuales se puede aplicar un enfoque graduado conforme a su nivel de seguridad asignado.

4.166. En la fase de implantación del sistema de I+C (*hardware* y *software* integrados), el diseño del sistema se transforma a código, estructuras de bases de datos y representaciones conexas ejecutables por la máquina. La implantación trata de la configuración e instalación de *hardware*, la codificación y realización de pruebas de *software*, y la configuración e instalación de la comunicación (incluida, cuando se decida, la incorporación de *software* y artículos comerciales de distribución general reutilizados).

4.167. En las fases de diseño e implantación del ciclo de vida de los sistemas de I+C, se deberían señalar los requisitos de seguridad informática de los sistemas de I+C y se debería verificar su aplicación.

4.168. Los requisitos señalados en la especificación de los sistemas de I+C se deberían traducir a elementos de diseño específico en la descripción de diseño de los sistemas. Estos elementos de diseño específico deberían incluir disposiciones que se han de aplicar dentro del diseño del sistema de I+C o a través de medidas de seguridad informática aplicadas de forma externa al sistema de I+C.

4.169. Los elementos de diseño de la seguridad informática de los sistemas de I+C deberían abordar el control del acceso físico y lógico a las funciones de los sistemas, al uso de los servicios de los sistemas de I+C y a la comunicación de datos con otros sistemas.

4.170. El acceso físico y lógico a un sistema de I+C debería controlarse en función del nivel de seguridad asignado a ese sistema. Por ejemplo, los sistemas a los que se haya asignado el nivel de seguridad más estricto deberán tener unos requisitos de seguridad informática para el control de acceso multifactor, como el control del acceso que requiera una combinación de conocimientos (por ejemplo, una contraseña), objetos (por ejemplo, una tarjeta inteligente) y características personales (por ejemplo, huellas dactilares).

4.171. Los sistemas de I+C deberían diseñarse de modo que incluyan características que proporcionen resistencia o protección frente al comprometimiento.

4.172. Las medidas de diseño deberían proporcionar confianza suficiente de que la seguridad de un sistema al que se ha asignado un determinado nivel de seguridad no se ve reducida por conexiones a sistemas a los que se han asignado niveles de seguridad más débiles.

4.173. Se deberían diseñar combinaciones adecuadas de medidas de control administrativo (por ejemplo, un programa de seguridad informática) y medidas de control físico para reducir la susceptibilidad de un sistema de I+C respecto a un ciberataque.

4.174. Los componentes de los sistemas de I+C se deberían asignar e instalar en lugares de la instalación que aseguren físicamente el equipo y sus comunicaciones de redes con otros sistemas; por ejemplo, colocar todas las conexiones de datos para los sistemas y componentes dentro de recintos seguros.

Integración de los sistemas de I+C

4.175. Las orientaciones que se proporcionan en los párrs. 4.176 a 4.178 se aplican a todos los sistemas, subsistemas y componentes de I+C.

4.176. La integración de los sistemas de I+C es el proceso de combinar el *hardware* y el *software* (incluido el *firmware*) de los sistemas de I+C en un solo sistema. A menudo, los proveedores, contratistas o suministradores realizarán una prueba de la integración de cada sistema individual que producen, así como de una combinación de sistemas dentro de su alcance, antes de enviar sus productos al emplazamiento de la instalación. Mediante esta prueba se verifica el correcto funcionamiento de los componentes del *software* y la correcta interrelación entre componentes dentro del sistema de I+C.

4.177. Dentro del ciclo de vida del sistema de I+C, durante la fase de integración del sistema, ya se debería contar con medidas integradas de control técnico, que deberían estar configuradas conforme a las especificaciones antes de realizar las pruebas.

4.178. Durante la prueba de integración, el proveedor, contratista o suministrador debería confirmar que las medidas de seguridad informática integradas producen resultados según lo especificado y no perjudican la capacidad de los sistemas de I+C para desempeñar sus funciones esenciales.

Validación del sistema

4.179. Las orientaciones que se proporcionan en los párrs. 4.180 a 4.185 se aplican a todos los sistemas, subsistemas y componentes de I+C a los que se haya asignado un nivel de seguridad.

4.180. Las actividades de validación del sistema suelen producirse simultáneamente con otras fases del ciclo de vida. Una vez se ha finalizado la integración del sistema, se suele realizar una validación parcial del sistema mediante, por ejemplo, aportaciones simuladas. Las actividades de validación suelen realizarse como parte de las fases de instalación, integración del sistema de I+C y puesta en servicio. La validación se considera culminada cuando se pone en funcionamiento un sistema para operaciones normales de la instalación.

4.181. Durante la validación de cada sistema, subsistema y componente de I+C, se debería demostrar la aplicación de los requisitos de seguridad informática y de los elementos de configuración. Probar las funciones de seguridad física tiene por objetivo garantizar que los requisitos de seguridad informática de los sistemas de I+C estén validados mediante la ejecución de pruebas de integración, de sistemas y de aceptación cuando sea práctico y necesario.

4.182. Las actividades de validación del sistema deberían confirmar la eficacia de las medidas de seguridad informática y comprobar los posibles efectos —directos o indirectos— sobre las funciones de seguridad tecnológica.

4.183. Se debería demostrar que cada medida de control técnico aplicada en el sistema de I+C produce los resultados previstos y no aumenta el riesgo de vulnerabilidades de seguridad ni reduce la fiabilidad de las funciones de seguridad tecnológica.

4.184. La validación de las medidas de seguridad informática de los sistemas de I+C debería incluir una evaluación de la configuración de los sistemas (incluida toda la conectividad externa), pruebas de cualificación del *software*, pruebas de cualificación de los sistemas y pruebas de aceptación en fábrica de los sistemas. La validación de estas medidas de seguridad informática se puede respaldar mediante pruebas de los sistemas de I+C con las que se detecten posibles vulnerabilidades o se caractericen comportamientos o acciones imprevistos.

4.185. Las pruebas de validación de los sistemas se deberían llevar a cabo dentro de un entorno seguro. Por ejemplo, los dispositivos de pruebas —como simuladores o emuladores— se deberían asegurar mediante medidas de seguridad

informática. La rigurosidad de las medidas de seguridad informática debería ser proporcional al nivel de seguridad asignado al sistema de I+C.

Instalación, integración global de los sistemas de I+C y puesta en servicio

4.186. Durante la instalación y la puesta en servicio, el operador debería realizar un examen de aceptación sobre la corrección de las medidas de control físico y técnico en el entorno objetivo, teniendo en cuenta la integración global de los sistemas de I+C[24].

4.187. La instalación del sistema de I+C, la integración global de los sistemas de I+C y la puesta en servicio deberían realizarse en un entorno seguro. Al asignar un nivel de seguridad a este entorno se debería contemplar el nivel de seguridad del sistema en el entorno objetivo y el nivel de seguridad de los instrumentos utilizados en la instalación y la puesta en servicio.

4.188. El entorno seguro se debería proteger con medidas de seguridad informática que sean proporcionales al nivel de seguridad asignado al sistema de I+C y a los procesos de seguridad que se lleven a cabo para lograr la instalación y la puesta en servicio. En algunos casos se deberían establecer medidas compensatorias de control administrativo y físico para controlar el acceso al entorno seguro, así como a equipo y fuentes de datos asociados.

4.189. Se debería verificar el equipo utilizado en el entorno seguro a fin de confirmar que no ofrece vías que permitan la introducción de datos ni código maliciosos en el entorno ni en los componentes del sistema de I+C.

4.190. Debería haber medidas de seguridad informática para controlar y monitorizar la entrada y salida de datos y activos digitales en el entorno seguro.

Operaciones y mantenimiento

4.191. Las orientaciones de los párrs. 4.192 a 4.205 se aplican a todos los sistemas, subsistemas y componentes de I+C a los cuales se puede aplicar un enfoque graduado conforme a su nivel de seguridad asignado.

---

[24] En la presente publicación, por “integración global de los sistemas de I+C” se entiende la integración de todos los sistemas de I+C de una instalación y es un concepto distinto a “integración del sistema de I+C”, tratado con anterioridad en esta publicación.

4.192. Las operaciones y las actividades de mantenimiento continúan durante todo el ciclo de vida del sistema de I+C y ya se han abordado en las secciones anteriores que tratan sobre la planificación de procesos y actividades comunes para todas las fases del ciclo de vida. Cuando se inicia la fase de operaciones y mantenimiento de un sistema, la entidad operadora debería responsabilizarse íntegramente de la seguridad informática en relación con la ejecución de las operaciones y de las actividades de mantenimiento.

4.193. Las actividades de mantenimiento son actividades de las que precisa el operador para mantener los sistemas o los componentes en buenas condiciones de funcionamiento. Estas actividades de mantenimiento deberían extenderse a las medidas de control técnico y físico que proporcionan seguridad informática a los sistemas de I+C; estas actividades pueden comprender las siguientes tareas:

— mantenimiento preventivo o pruebas periódicos;
— acciones para detectar, impedir o mitigar la degradación de componentes, y
— acciones para diagnosticar, reparar, renovar o sustituir componentes defectuosos por componentes idénticos.

4.194. Se deberían aplicar medidas de seguridad informática a las operaciones y actividades de mantenimiento, a fin de asegurar que no se vean comprometidos los componentes y los sistemas.

4.195. La fase de operaciones implica el uso del sistema de I+C por parte del operador en el entorno operativo al que está destinado. Durante la fase de operaciones, el operador debería:

— comprobar que el sistema de I+C está intacto; para ello debería valerse de técnicas como pruebas y monitorización periódicas, examen de los registros del sistema y monitorización en tiempo real, cuando sea posible;
— evaluar el impacto que tienen en la seguridad del sistema de I+C los cambios del sistema de I+C que se realicen dentro del entorno operativo;
— evaluar el efecto de cualquier propuesta de cambio sobre la seguridad del sistema de I+C;
— evaluar procedimientos operacionales con respecto al cumplimiento del uso previsto;
— analizar riesgos de seguridad que afecten al operador y al sistema;
— evaluar nuevas limitaciones de seguridad del sistema;
— evaluar la corrección y la usabilidad de los procedimientos operacionales;

— realizar autoevaluaciones y auditorías periódicas de la seguridad de los sistemas informáticos, que son componentes clave de un buen programa de seguridad, y
— evaluar los informes disponibles de incidentes con respecto a nuevas amenazas y vulnerabilidades.

4.196. Las operaciones y las actividades de mantenimiento se deberían analizar para asegurarse de que se apliquen medidas de seguridad informática con el fin de prevenir la introducción de *software* malicioso en el sistema de I+C.

4.197. Las actividades de mantenimiento deberían atenerse a los requisitos de seguridad informática de los sistemas de I+C existentes, salvo que se haya de cambiar esos requisitos como parte de la actividad de mantenimiento. En algunos casos, tal vez haya que retirar o deshabilitar temporalmente medidas de seguridad informática para permitir la ejecución de las tareas de mantenimiento necesarias. Durante el período en que no se disponga de medidas de seguridad informática, el sistema se encontrará sometido a mayores riesgos y se deberían aplicar medidas compensatorias.

4.198. La realización de actividades de calibración, pruebas y mantenimiento podría conllevar el uso de medios extraíbles y dispositivos móviles que se conecten temporalmente a los sistemas y componentes de I+C digitales. Las medidas de seguridad informática relacionadas con estas actividades deberían contemplar lo siguiente:

— la aplicación de medidas de control técnico y administrativo eficaces para el manejo tecnológica y físicamente seguro de los dispositivos digitales;
— la verificación de la integridad de todos los valores de consigna para el control, con el objetivo de prevenir cambios no deseados y protegerlos de ellos, y
— el uso de personal cualificado (incluido el personal de terceros) que haya recibido capacitación en la realización de estas actividades conforme a requisitos de seguridad informática.

4.199. Se deberían deshabilitar las interfaces o se debería restringir el acceso a ellas cuando no sean necesarias o no se estén utilizando (por ejemplo, conexión de computadoras para tareas de mantenimiento y desarrollo).

4.200. Debería haber medidas de seguridad informática para prevenir el acceso innecesario o no autorizado.

4.201. Debería haber procesos o aplicaciones de monitorización para verificar la configuración del *software* actual comparándola con configuraciones conocidas.

4.202. El acceso remoto se debería restringir en la mayor medida posible. Cuando se necesite el acceso remoto, se debería contemplar el riesgo de esas conexiones y es preciso aplicar medidas de seguridad informática adicionales. Esa conectividad debería mantenerse únicamente durante el tiempo necesario para su finalidad concreta.

4.203. Se deberían controlar cuidadosamente las actividades de operación y mantenimiento mediante procesos de órdenes de trabajo formales y procedimientos de mantenimiento formales. Por ejemplo, se debería contemplar un sistema de control —como la norma de actuación por pareja— para tareas como la realización de cambios de configuración en sistemas de I+C operacionales.

4.204. Las actividades de operación no deberían requerir cambios en las medidas de seguridad informática de los sistemas de I+C.

4.205. Los instrumentos de operación y mantenimiento del sistema que se puedan emplear para comprometer el sistema de I+C deberían estar protegidos de forma proporcional al nivel de seguridad del sistema de I+C asociado. Por ejemplo, los instrumentos que se utilicen en un sistema al que se haya asignado un nivel de seguridad más estricto no se deberían utilizar en un sistema al que se haya asignado un nivel de seguridad más débil.

Modificación de los sistemas de I+C

4.206. Aplicar medidas de seguridad informática a sistemas de I+C antiguos en una instalación nuclear existente no es siempre una tarea sencilla. Por ejemplo, pueden surgir las siguientes dificultades:

— tal vez no se pueda modificar la arquitectura de I+C antigua sin afectar al comportamiento determinista de los sistemas de I+C antiguos;
— es posible que las tecnologías existentes que se utilicen para el almacenamiento de datos o programas, las interfaces o la comunicación no permitan su modificación;
— tal vez las estructuras y la disposición de la instalación existentes no tengan margen para medidas de protección física suficientes, y

— tal vez las medidas de control técnico contemporáneas que proporcionan funciones de monitorización de la seguridad no sean compatibles con las tecnologías implantadas en los sistemas de I+C antiguos.

4.207. Durante la modernización de una instalación nuclear que conlleve la sustitución de sistemas de I+C antiguos por sistemas de I+C modernos, el operador debería tener en cuenta la posibilidad de que tal vez deban mantenerse las interfaces antiguas con los sistemas de la instalación originales y otros sistemas y de que tal vez se introduzcan nuevas vulnerabilidades y debilidades debido a la tecnología o al diseño nuevos.

4.208. Las modificaciones de los sistemas de I+C cambian el sistema o su documentación. Estos cambios se pueden categorizar de la siguiente manera:

— cambios o mejoras (correctivas o adaptativas);
— migración (es decir, el traslado de un sistema a un nuevo entorno operativo), y
— sustitución (es decir, la retirada de soporte activo por parte de la entidad de operación y mantenimiento, la sustitución parcial o total por un sistema nuevo o la instalación de un sistema mejorado).

4.209. Las modificaciones de los sistemas de I+C pueden deberse a requisitos o ser específicas para corregir errores (correctivas), para adaptarse a un entorno operativo modificado (adaptativas) o para responder a más solicitudes o mejoras del operador.

4.210. Cuando se realicen modificaciones en un sistema de I+C, se debería incluir una evaluación de la seguridad del sistema de I+C modificado; por ejemplo, mediante la actualización de la gestión de riesgos de seguridad informática del sistema.

4.211. La seguridad informática debería considerarse parte del proceso de gestión del cambio. Este incluye cambios en el *software* y el *hardware* de los sistemas de I+C.

4.212. Para asegurarse de que con las modificaciones no se hayan introducido vulnerabilidades en el entorno de la instalación, el operador debería evaluar la propuesta de cambios en el sistema de I+C —incluido su efecto sobre el programa de seguridad informática y sobre la seguridad del sistema de I+C existente—, evaluar anomalías que se descubran durante la operación, evaluar las necesidades

de migración y evaluar las modificaciones realizadas, incluidas las actividades de validación y verificación.

4.213. Las medidas de seguridad informática deberían evaluarse conforme se describe en los párrs. 4.206 a 4.212 anteriores, y deberían revisarse para reflejar los requisitos de seguridad informática resultantes del proceso de modificación, según proceda.

4.214. Durante la modificación, los requisitos de seguridad informática de los sistemas de I+C existentes deberían permanecer en vigor, salvo que se haya de cambiar esos requisitos como parte de la actividad de modificación.

4.215. Se debería contar con una gestión de la configuración para las medidas de seguridad informática, a fin de prevenir la introducción de *software* no autorizado en los sistemas de I+C.

4.216. Al realizar la migración de sistemas, el operador debería verificar que los sistemas migrados cumplen los requisitos de seguridad informática del sistema de I+C.

4.217. Los artefactos que se derivan del desarrollo, la instalación y la realización de pruebas se deberían retirar del sistema y de sus archivos de configuración, antes de la puesta en servicio para su funcionamiento.

4.218. Las modificaciones en los sistemas de I+C se deberían tratar como procesos de desarrollo y se deberían verificar y validar.

4.219. Todas las modificaciones en el sistema de I+C y en sus componentes, incluidas las relativas a las configuraciones del *software*, del *hardware* y del sistema, deberían tener en cuenta las posibles vulnerabilidades y amenazas para la seguridad física que pueden surgir no solo durante la ejecución de estas actividades, sino también a consecuencia de las modificaciones.

4.220. Muchos activos digitales y componentes asociados, incluidos los medios de almacenamiento extraíbles, tienen la capacidad de conservar datos digitales cuando se retiran de un sistema. Estos datos digitales pueden incluir datos lógicos o residuales preprogramados del sistema, como lecturas de sensores, señales de control, datos analíticos y tráfico de redes. Estos datos tal vez se puedan extraer de los componentes desechados.

4.221. Debería haber medidas de control administrativo y técnico para impedir que los datos que permanezcan en los componentes desechados se puedan utilizar con el fin de ayudar a desarrollar un *exploit* informático. Se deberían destruir los componentes o se deberían retirar los datos de forma segura, salvo que los datos residuales que se encuentren en los componentes que se vayan a desechar se hayan evaluado para demostrar que no suponen ningún riesgo de comprometimiento en materia de seguridad.

4.222. En el caso de las modificaciones que conlleven la sustitución de sistemas de I+C, el operador debería llevar a cabo actividades como la limpieza de datos, la sobreescritura completa o la destrucción de discos, a fin de garantizar que no se puedan recuperar datos del sistema de I+C sustituido una vez que se haya retirado del servicio.

CLAUSURA

4.223. Durante la fase de clausura, antes de que se hayan retirado de la instalación los materiales nucleares, otros materiales radiactivos y los activos de información de carácter estratégico, el operador debería evaluar el efecto que tendría la sustitución o la retirada de las funciones de seguridad física del sistema de I+C existentes del entorno operativo.

4.224. En esta evaluación, el operador debería incluir el efecto que tendría en las interfaces del sistema de seguridad y no seguridad el hecho de retirar las funciones de seguridad física del sistema.

4.225. El operador debería documentar los métodos por los cuales se mitigará cualquier cambio en las funciones de seguridad física del sistema de I+C (por ejemplo, sustitución de las funciones de seguridad física, aislamiento de otros sistemas de seguridad tecnológica e interacciones del operador o deshabilitación de las funciones de interfaz del sistema de I+C).

4.226. Los procedimientos de seguridad deberían conservar elementos que garanticen la limpieza del *hardware* y de los datos hasta que se haya finalizado la clausura de una instalación.

REFERENCIAS

[1] ALBRIGHT, D., BRANNAN, P., WALROND, C., Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report (2011), http://isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/8

[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, *Seguridad informática en las instalaciones nucleares*, *Colección de Seguridad Física Nuclear del OIEA* Nº 17, OIEA, Viena, 2013.

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-39, IAEA, Vienna (2016).

[5] 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*, OIEA, Viena, 2022.

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Instrumentation and Control Systems and Software Important to Safety for Research Reactors, IAEA Safety Standards Series No. SSG-37, IAEA, Vienna (2015).

[7] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Glosario de Seguridad del OIEA: Terminología empleada en seguridad nuclear y protección radiológica, Edición de 2018*, OIEA, Viena, 2022.

[8] 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.

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Use of a Graded Approach in the Application of the Safety Requirements for Research Reactors, IAEA Safety Standards Series No. SSG-22, IAEA, Vienna (2012).

[10] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants - Instrumentation and Control Systems - Requirements for Security Programmes for Computer-based Systems, IEC 62645:2014, IEC, Geneva (2014).

[11] 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.

[12] INTERNATIONAL STANDARDS ORGANIZATION, Information Technology – Security Techniques – Information Security Risk Management, ISO/IEC:27005:2011, ISO, Geneva (2011).

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

[14] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Liderazgo y gestión en pro de la seguridad*, *Colección de Normas de Seguridad del OIEA* Nº GSR Part 2, OIEA, Viena, 2017.
[15] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Seguridad física de la información nuclear, Colección de Seguridad Física Nuclear del OIEA* Nº 23-G, OIEA, Viena, 2018.
[16] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Aplicación del sistema de gestión de instalaciones y actividades, Colección de Normas de Seguridad del OIEA* Nº GS-G-3.1, OIEA, Viena, 2016.
[17] 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.
[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).

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

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 seguridad informática representa un área compleja que se enfrenta a mayores vectores de amenazas dentro de los entornos tecnológicos dinámicos. La seguridad informática en las instalaciones nucleares se complica aún más debido a la integración de sistemas de instrumentación y control (I+C) en el marco de la gestión de la seguridad informática. La presente publicación proporciona orientaciones que abordan el desafío que supone la aplicación de medidas de seguridad informática a los sistemas de I+C en las instalaciones nucleares, incluida la fundamentación técnica y metodologías para la aplicación de medidas de seguridad informática a sistemas de I+C que proporcionan seguridad tecnológica, seguridad física o funciones auxiliares en instalaciones nucleares. Estas medidas tienen la finalidad de proteger los sistemas de I+C frente a actos dolosos perpetrados por personas u organizaciones. En esta publicación también se trata la aplicación de esas medidas a los entornos de desarrollo, simulación y mantenimiento de estos sistemas.

ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA
VIENA