Evaluación de la seguridad física informática en las instalaciones nucleares

IAEA
Organismo Internacional de Energía Atómica

COLECCIÓN DE SEGURIDAD FÍSICA NUCLEAR DEL OIEA Y PUBLICACIONES CONEXAS

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.

Las publicaciones de la *Colección de Seguridad Física Nuclear del OIEA* se clasifican en las subcategorías siguientes:

- Las **Nociones Fundamentales de Seguridad Física Nuclear** 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** 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** 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** 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.

Otras publicaciones sobre seguridad física nuclear que no contienen orientaciones del OIEA se publican fuera del marco de la *Colección de Seguridad Física Nuclear del OIEA*.

PUBLICACIONES CONEXAS

El OIEA también establece normas de seguridad destinadas a proteger la salud y reducir al mínimo el peligro para la vida y propiedad, que se publican en la ***Colección de Normas de Seguridad del OIEA***.

El OIEA facilita la aplicación de las orientaciones y las normas y pone a disposición información relacionada con las actividades nucleares pacíficas, fomenta su intercambio y sirve de intermediario para ello entre sus Estados Miembros.

Los informes sobre seguridad y protección en las actividades nucleares se publican como **Informes de Seguridad**, en los que se ofrecen ejemplos prácticos y métodos detallados que se pueden utilizar en apoyo de las normas de seguridad.

Otras publicaciones del OIEA relacionadas con la seguridad, se publican como títulos de **Preparación y Respuesta para Casos de Emergencia**, **Informes Técnicos** y documentos técnicos **TECDOC**. El OIEA publica asimismo informes sobre accidentes radiológicos, manuales de capacitación y manuales prácticos, así como otros títulos especiales relacionados con la seguridad.

La ***Colección de Energía Nuclear del OIEA*** comprende publicaciones de carácter informativo destinadas a fomentar y facilitar la investigación, el desarrollo y la aplicación práctica de la energía nuclear con fines pacíficos. Incluye informes y guías sobre la situación y los adelantos de las tecnologías, así como experiencias, buenas prácticas y ejemplos prácticos en relación con la energía nucleoeléctrica, el ciclo del combustible nuclear, la gestión de desechos radiactivos y la clausura.

EVALUACIÓN DE LA SEGURIDAD FÍSICA INFORMÁTICA EN LAS 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
CAMBOYA
CAMERÚN
CANADÁ
CHAD
CHILE
CHINA
CHIPRE
COLOMBIA
CONGO
COREA, REPÚBLICA DE
COSTA RICA
CÔTE D'IVOIRE
CROACIA
CUBA
DINAMARCA
DJIBOUTI
DOMINICA
ECUADOR
EGIPTO
EL SALVADOR
EMIRATOS ÁRABES UNIDOS
ERITREA
ESLOVAQUIA
ESLOVENIA
ESPAÑA
ESTADOS UNIDOS DE AMÉRICA
ESTONIA
ETIOPÍA
EX REPÚBLICA YUGOSLAVA DE MACEDONIA
FEDERACIÓN DE RUSIA
FIJI
FILIPINAS
FINLANDIA
FRANCIA
GABÓN
GEORGIA
GHANA
GRECIA
GUATEMALA
GUYANA
HAITÍ
HONDURAS
HUNGRÍA
INDIA
INDONESIA
IRÁN, REPÚBLICA ISLÁMICA DEL
IRAQ
IRLANDA
ISLANDIA
ISLAS MARSHALL
ISRAEL
ITALIA
JAMAICA
JAPÓN
JORDANIA
KAZAJSTÁN
KENYA
KIRGUISTÁN
KUWAIT
LESOTHO
LETONIA
LÍBANO
LIBERIA
LIBIA
LIECHTENSTEIN
LITUANIA
LUXEMBURGO
MADAGASCAR
MALASIA
MALAWI
MALÍ
MALTA
MARRUECOS
MAURICIO
MAURITANIA
MÉXICO
MÓNACO
MONGOLIA
MONTENEGRO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NICARAGUA
NÍGER
NIGERIA
NORUEGA
NUEVA ZELANDIA
OMÁN
PAÍSES BAJOS
PAKISTÁN
PALAU
PANAMÁ
PAPUA NUEVA GUINEA
PARAGUAY
PERÚ
POLONIA
PORTUGAL
QATAR
REINO UNIDO DE GRAN BRETAÑA E IRLANDA DEL NORTE
REPÚBLICA ÁRABE SIRIA
REPÚBLICA CENTROAFRICANA
REPÚBLICA CHECA
REPÚBLICA DE MOLDOVA
REPÚBLICA DEMOCRÁTICA DEL CONGO
REPÚBLICA DEMOCRÁTICA POPULAR LAO
REPÚBLICA DOMINICANA
REPÚBLICA UNIDA DE TANZANÍA
RUMANIA
RWANDA
SAN MARINO
SANTA SEDE
SAN VICENTE Y LAS GRANADINAS
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONA
SINGAPUR
SRI LANKA
SUDÁFRICA
SUDÁN
SUECIA
SUIZA
SWAZILANDIA
TAILANDIA
TAYIKISTÁN
TOGO
TRINIDAD Y TABAGO
TÚNEZ
TURKMENISTÁN
TURQUÍA
UCRANIA
UGANDA
URUGUAY
UZBEKISTÁN
VANUATU
VENEZUELA, REPÚBLICA BOLIVARIANA DE
VIET NAM
YEMEN
ZAMBIA
ZIMBABWE

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

EVALUACIÓN DE LA SEGURIDAD FÍSICA INFORMÁTICA EN LAS INSTALACIONES NUCLEARES

ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA
VIENA, 2018

DERECHOS DE AUTOR

EVALUACIÓN DE LA SEGURIDAD FÍSICA INFORMÁTICA EN LAS INSTALACIONES NUCLEARES

IAEA-TDL-006
ISBN 978-92-0-306617-4

Impreso por el OIEA en Austria
Enero de 2018

PRÓLOGO

La finalidad de la seguridad física nuclear es prevenir y detectar actos dolosos que se relacionen con materiales nucleares, otros materiales radiactivos, o las instalaciones y actividades conexas, y darles respuesta si se producen. Las computadoras, los sistemas informáticos y los componentes digitales desempeñan un papel cada vez más importante en la gestión de la información de carácter estratégico, la seguridad tecnológica nuclear, la seguridad física nuclear y la contabilidad y el control de los materiales en esas instalaciones. Una vulneración de los sistemas informáticos podría repercutir negativamente en la seguridad física nuclear, en forma directa e indirecta, y favorecer la comisión de actos dolosos.

La *Colección de Seguridad Física Nuclear del OIEA* se ocupa de los aspectos de la seguridad física nuclear que tienen que ver con la prevención y detección de actos dolosos relacionados con materiales nucleares, otros materiales radiactivos o las instalaciones conexas, como los robos, el sabotaje, el acceso no autorizado y las transferencias ilegales, y con la respuesta a esos actos. En apoyo de las orientaciones publicadas en la *Colección de Seguridad Física Nuclear del OIEA*, que representan el consenso internacional, el OIEA produce también otras publicaciones que ofrecen un asesoramiento especializado adicional sobre temas específicos.

La publicación Nº 17 de la *Colección de Seguridad Física Nuclear del OIEA,* titulada *Seguridad informática en las instalaciones nucleares*, proporciona orientaciones sobre el establecimiento de un programa de seguridad física informática en una instalación nuclear o radiológica. Sobre la base de la orientación facilitada en esa obra, la presente publicación ofrece una metodología para evaluar la seguridad física informática en las instalaciones nucleares. La realización periódica de esas evaluaciones y la pronta aplicación de las medidas correctivas necesarias son esenciales para proteger las computadoras y los activos informáticos. La metodología que aquí se describe puede aplicarse tanto en la autoevaluación interna como en las evaluaciones externas. Esta publicación tiene por objeto ayudar a los evaluadores a planificar y realizar evaluaciones adaptadas a las distintas instalaciones y organizaciones.

La presente publicación se preparó con la asistencia de más de treinta expertos en el curso de tres reuniones de consultores y varias otras reuniones de expertos, con aportaciones de más de diez Estados Miembros.

NOTA EDITORIAL

Esta publicación se ha preparado a partir del material original aportado por los colaboradores y no ha sido editada por el personal de los servicios editoriales del OIEA. Las opiniones expresadas son las de los colaboradores y no reflejan necesariamente las del OIEA o las de los Gobiernos de sus Estados Miembros.

Ni el OIEA ni sus Estados Miembros asumen responsabilidad alguna por las consecuencias que puedan derivarse del uso de esta publicación. Esta publicación no aborda cuestiones de responsabilidad, jurídica o de otra índole, por actos u omisiones por parte de persona alguna.

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.

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

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

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

ÍNDICE

1. INTRODUCCIÓN

1.1. ANTECEDENTES

La seguridad física informática es vista, cada vez más, como un componente clave de la seguridad física nuclear. Con los avances de la tecnología, aumentará el uso de computadoras y sistemas informáticos en todos los aspectos de las operaciones de las instalaciones, incluidos los sistemas de seguridad tecnológica y física. En la publicación Nº 20 de la *Colección de Seguridad Física Nuclear del OIEA*, titulada *Objetivo y elementos esenciales del régimen de seguridad física nuclear de un Estado*, se subraya la importancia de las actividades de garantía de la ciberseguridad que determinan y abordan las cuestiones y los factores que podrían afectar a la capacidad de proporcionar una seguridad física nuclear adecuada [1]. Este aspecto se trata también en la publicación Nº 13 de la *Colección de Seguridad Física Nuclear*, titulada *Recomendaciones de Seguridad Física Nuclear sobre la Protección Física de los Materiales y las Instalaciones Nucleares* (INFCIRC/225/Revision 5) [2], en que se afirma que:

> "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." (Ref. [2], párrs. 4.10/5.19)

Un proceso de evaluación riguroso y completo puede ayudar a fortalecer la eficacia del programa de seguridad física informática de una instalación (y de un Estado). La publicación Nº 17 de la *Colección de Seguridad Física Nuclear*, titulada *Seguridad informática en las instalaciones nucleares* [3], ofrece orientaciones para el desarrollo y la gestión de un programa de ese tipo. Muchas otras publicaciones tratan sobre la seguridad física de la información y los sistemas informáticos y sobre la realización de auditorías o evaluaciones, entre ellas:

- La serie ISO/IEC 27000 [4 a 8], que versa sobre la gestión de la seguridad física de la información;
- La norma ISO 19011:2011 [9], que ofrece un marco para la auditoría;
- La Publicación Especial del NIST 800-115, titulada *Technical Guide to Information Security Testing and Assessment* [10].

La presente publicación se ha elaborado para atender a la necesidad de orientación específica en el ámbito nuclear que cumpla con las normas internacionales, las orientaciones del Organismo Internacional de Energía Atómica (OIEA) y la buena práctica reconocida.

1.2. PROPÓSITO

En esta publicación se describe una metodología para evaluar la seguridad física informática en las instalaciones nucleares. La metodología puede adaptarse fácilmente para efectuar evaluaciones en instalaciones en que haya otros materiales radiactivos.

Las orientaciones se han redactados de modo que se puedan aplicar en múltiples contextos, por ejemplo en:

- una misión específica del servicio de asesoramiento sobre seguridad física informática, organizada por el OIEA a petición de un Estado Miembro;
- un módulo específico sobre seguridad física informática integrado en otras misiones organizadas por el OIEA, por ejemplo una misión del Servicio Internacional de Asesoramiento sobre Protección Física (IPPAS) en que el dominio de la protección física sea el objeto de la evaluación;

— evaluaciones realizadas por una autoridad competente nacional en emplazamientos e instalaciones de un Estado;
— autoevaluaciones realizadas a nivel de una instalación o de una organización;
— una evaluación de la seguridad física informática de los proveedores y terceros que presten apoyo a instalaciones nucleares.

La metodología permite evaluar las prácticas existentes en una instalación con el fin de fortalecer la organización y sus procedimientos y prácticas. Tiene en cuenta las orientaciones impartidas en las publicaciones de la *Colección de Seguridad Física Nuclear del OIEA*, las normas internacionales y la buena práctica apoyada por la comunidad internacional. Está estructurada como un examen de alto nivel del marco para la seguridad física informática, con un examen a nivel funcional de las medidas y los procedimientos establecidos para ejecutar ese marco, prestando atención específica a las funciones de seguridad nuclear tecnológica y física que puedan ofrecer los sistemas informáticos.

Cada evaluación puede requerir una adaptación a las circunstancias del caso y una clara descripción del resultado previsto. Por ejemplo, el resultado previsto de una evaluación realizada por una autoridad competente puede ser un informe sobre la manera en que la entidad explotadora cumple sus obligaciones reglamentarias y jurídicas. Este informe difícilmente propondrá soluciones a los problemas, pero puede exigir que se adopten medidas con arreglo a las prioridades establecidas por la autoridad competente y que se realice una evaluación de seguimiento. En cambio, un grupo asesor que efectúe una evaluación puede tener que recomendar posibles soluciones, además de exponer sus conclusiones. También es probable que un grupo asesor tome en consideración las prioridades y las actividades de seguimiento; y el ámbito de la evaluación podría especificar que el grupo de evaluación colabore con la entidad explotadora en la realización del análisis y en la elaboración de un plan de acción.

Es importante que los objetivos y los resultados previstos de la evaluación se acuerden y enuncien claramente en la reunión preparatoria.

La finalidad principal de la presente publicación es ayudar al grupo encargado de la evaluación a establecer un plan de evaluación adaptado a cada instalación en particular. Lo que se pretende no es ofrecer una lista de verificación completa, sino que el grupo de evaluación, basándose en su experiencia, utilice estas orientaciones para verificar que su examen sea completo y conforme con los objetivos de la evaluación y los recursos asignados.

1.3. ÁMBITO DE APLICACIÓN

La presente publicación se centra en la evaluación de la práctica en materia de seguridad física informática en todos los tipos de instalación nuclear, como las centrales nucleares, las instalaciones del ciclo del combustible, los reactores de investigación y otras. Aunque la manipulación de otros materiales radiactivos, el transporte y las operaciones conexas no se examinan específicamente en esta publicación, los principios y procesos en ella descritos pueden adaptarse fácilmente para que se apliquen a la evaluación de esas actividades.

La presente publicación solo trata específicamente de los aspectos de la seguridad física de la información que se relacionan con las computadoras. Por ejemplo, no se examinan la clasificación, el marcado ni los requisitos relativos al manejo de la información.

La evaluación se basa en exámenes, entrevistas y observaciones, y normalmente no incluye el ensayo activo de los sistemas. En particular, la evaluación detallada en estas orientaciones no comprende pruebas de penetración ni la conexión de dispositivos de prueba a los sistemas. Los miembros del grupo de evaluación no se servirán directamente de ningún equipo del lugar de la

evaluación, pero el grupo podrá pedir ver los registros de sistema activos o los archivos de configuración de un sistema de producción en servicio. Si es necesario, y sin rebasar el ámbito de la evaluación, el grupo solicitará a la instalación que ejecute determinadas tareas operacionales, y en el marco de una autoevaluación o mediante servicios prestados por una organización externa, cuando así se solicite, podrán realizarse ensayos activos. Cuando se efectúen ensayos activos en un sistema de producción en servicio, se deberá proceder con extremo cuidado.

La metodología descrita en la presente publicación se ha concebido para una situación ideal: un grupo de tres o cuatro evaluadores, con una o dos semanas de tiempo disponibles en el emplazamiento para llevar a cabo la evaluación. Sin embargo, también se examina cómo podría adaptarse la metodología si, por falta de tiempo y de recursos, no es posible desplegar ese nivel de esfuerzo.

1.4. ESTRUCTURA

La presente publicación ofrece primero un panorama general de la metodología y luego da orientaciones detalladas para las distintas etapas de la evaluación. Se divide en las siguientes secciones:

— La sección 2 contiene un panorama general de la metodología de evaluación y describe las etapas y los pasos más importantes.

— La sección 3 describe con más pormenores las actividades preparatorias que se pueden realizar antes de una evaluación.

— La sección 4 explica en detalle la metodología de evaluación.

— La sección 5 ofrece orientaciones detalladas sobre la realización de la evaluación, con ejemplos de las preguntas que se deben formular y la información que se debe tomar en consideración durante el proceso.

— La sección 6 trata sobre las actividades que se llevarán a cabo normalmente durante la conclusión de la evaluación y en el seguimiento posterior.

— El anexo I contiene consejos y buenas prácticas para realizar evaluaciones de sistemas de control industrial.

— El anexo II ofrece un modelo de formulario para que los miembros del grupo tomen notas durante el trabajo sobre el terreno.

— El anexo III presenta un modelo para el informe final.

— El anexo IV enumera las consideraciones que la organización anfitriona ha de tener en cuenta al abordar los resultados del informe.

La figura 1 muestra las etapas básicas de la planificación de la evaluación y el cronograma proyectado.

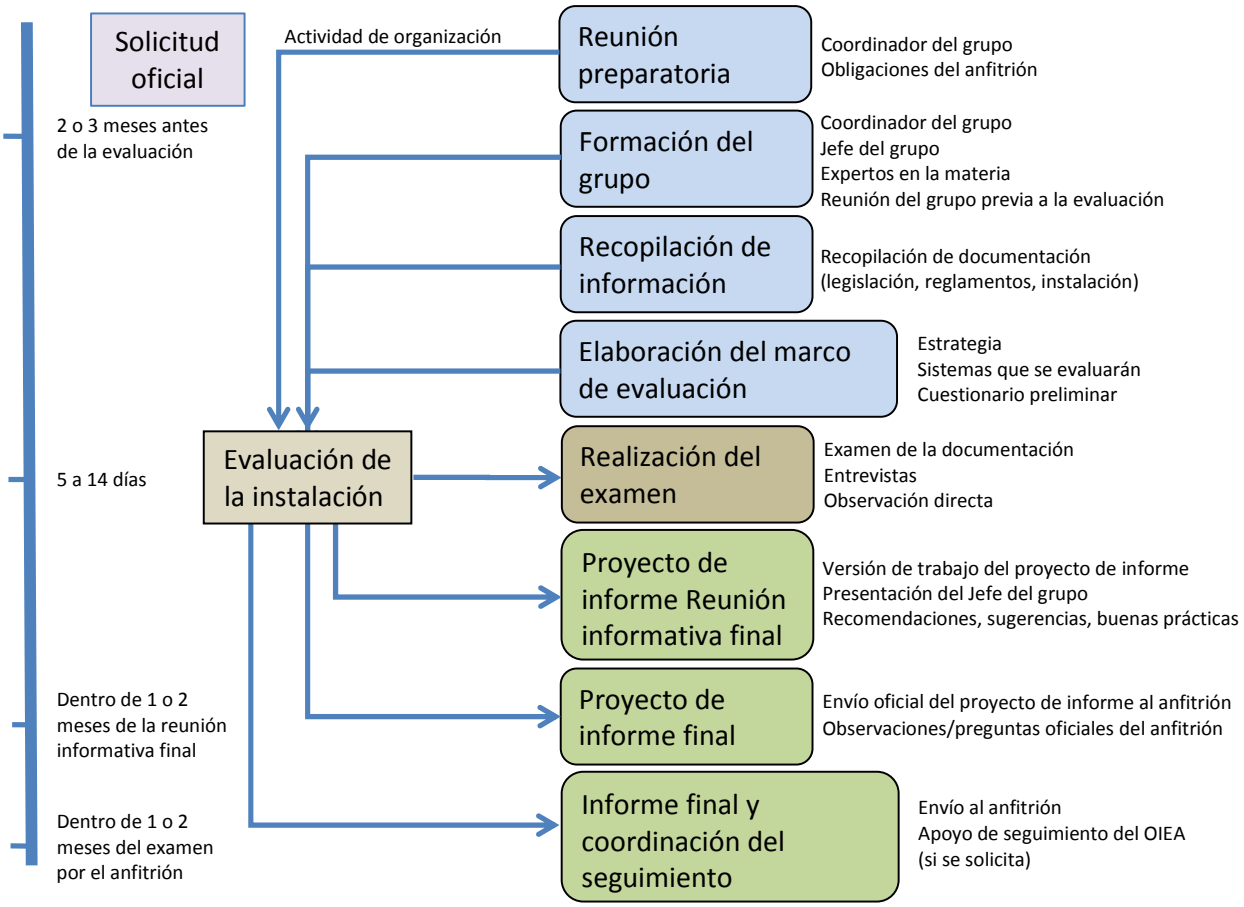

Fig. 1. Pasos y cronograma de la evaluación. El cronograma puede ajustarse en función de los recursos y el tiempo disponibles.

2. PANORAMA GENERAL DE LA METODOLOGÍA Y EL PROCESO DE EVALUACIÓN

2.1. OBJETIVOS

El objetivo de esta metodología de evaluación es ayudar a los Estados Miembros y a las entidades explotadoras a establecer, aplicar, mantener y, cuando sea el caso, reforzar la seguridad física informática de sus instalaciones, y ayudar también a sus autoridades competentes a evaluar la eficacia de las medidas adoptadas. La presente publicación ofrece orientación de alto nivel para diseñar y realizar una evaluación en instalaciones nucleares o en instalaciones con otros materiales radiactivos, pero no pretende proporcionar una lista de verificación completa para llevar a cabo la evaluación. Su finalidad principal es prestar asesoramiento a algunas de las entidades y personas siguientes, o a todas ellas:

- las entidades explotadoras de las instalaciones, sobre cómo establecer un programa de seguridad física informática para hacer frente a las ciberamenazas pertinentes y estructurarlo de modo que se adapte a su evolución;
- las autoridades nacionales, sobre cómo traducir las recomendaciones internacionales en requisitos específicos aplicables al sistema de seguridad física informática del Estado para las instalaciones con materiales nucleares u otros materiales radiactivos;
- las entidades explotadoras de las instalaciones, sobre los distintos métodos para cumplir con las recomendaciones y las buenas prácticas internacionales;
- las autoridades competentes nacionales y las entidades explotadoras de las instalaciones, sobre cómo realizar una evaluación objetiva de la situación de su marco de seguridad física informática y de la aplicación de las orientaciones y las buenas prácticas internacionales;
- el personal clave de la autoridad competente nacional y de las entidades explotadoras de las instalaciones, brindándoles la oportunidad de examinar sus prácticas junto con expertos con experiencia en las prácticas aplicadas en el mismo campo en otros lugares;
- los especialistas en seguridad física informática de los Estados Miembros, ofreciéndoles oportunidades de ampliar su experiencia y sus conocimientos en su campo de especialización.

Además, la evaluación puede utilizarse para determinar las buenas prácticas, que podrán luego comunicarse a otras instalaciones y/o a otros Estados Miembros para su mejora a largo plazo.

2.2. CONSIDERACIONES SOBRE LA REGLAMENTACIÓN

La presente publicación puede servir de guía de referencia a las autoridades competentes que realicen evaluaciones *in situ* de la seguridad física informática. Además, la autoridad competente puede otorgar reconocimiento a una instalación que lleve a cabo una autoevaluación, o exigir la realización de autoevaluaciones periódicas. La autoridad competente puede exigir también la evaluación de un emplazamiento por una parte independiente y/o un tercero.

En el proceso preparatorio se determinan las normas y reglamentos específicos que se emplearán para formular las conclusiones, recomendaciones y sugerencias. La autoridad competente puede pedir que se presente la siguiente información como parte de la evaluación y del informe final:

- la lista de los hallazgos;

— el plan de acción de la instalación para resolver los hallazgos, con las medidas que se adoptarán y los plazos;

— pruebas de un sistema de seguimiento que vigile y rastree la resolución de los distintos hallazgos;

— si es necesario, informes periódicos sobre el estado de las medidas para resolver hallazgos específicos.

La autoridad competente podrá utilizar estos resultados de la inspección como base para las inspecciones futuras en el emplazamiento.

2.3. PROCESO DE EVALUACIÓN

Los elementos y el flujo del proceso de una evaluación se ilustran en la figura 2. Este proceso se examinará en detalle en esta sección.

La presente publicación ofrece orientaciones y recomendaciones sobre cómo planificar una evaluación y constituir un grupo de evaluación. Una buena evaluación requiere la asignación de recursos adecuados, la constitución de un grupo de evaluación competente y la cooperación de la instalación.

A continuación se presentan las esferas representativas de una evaluación y se proporcionan orientaciones para la recopilación de información sobre la base del concepto de los dominios funcionales y los dominios de la seguridad física. El grupo de evaluación crea un marco de evaluación — un plan sistemático para evaluar la instalación — teniendo en cuenta los objetivos de la planificación, las orientaciones del OIEA, las normas industriales, las guías de reglamentación, la buena práctica, etc. No se ofrece una lista de verificación específica para ello, porque cada evaluación es especial y requiere una adaptación a las circunstancias del caso.

Según la naturaleza de la evaluación y las limitaciones de tiempo, los miembros del grupo de evaluación pueden ajustar el ámbito de la evaluación para que corresponda a la situación y a las necesidades particulares de la instalación. Todos los aspectos de la seguridad física informática incluidos en el ámbito de la evaluación deberán estudiarse a fondo para poder emitir una opinión fundamentada sobre la situación del programa de seguridad física informática en ese momento.

Al realizar una evaluación, el grupo debe reunir suficiente información para evaluar las prácticas de seguridad física informática de la instalación en el nivel adecuado. Estas orientaciones contienen consejos para la recopilación de información y recomendaciones sobre los aspectos más importantes.

El grupo de evaluación debe actuar con espíritu crítico al evaluar el marco de seguridad física informática de la instalación, y emitir juicios basados en observaciones fundamentadas y no en supuestos. El grupo puede también formular recomendaciones y sugerencias para introducir mejoras y reconocer las buenas prácticas de la instalación. Es importante que el grupo tenga en cuenta que puede haber diferentes enfoques aceptables de la aplicación de la seguridad física (a menos que la autoridad competente haya impuesto un enfoque específico).

El producto de la evaluación es el informe final y, normalmente, también una reunión informativa final. Junto con informar sobre los hallazgos de la evaluación, el informe final contiene recomendaciones y sugerencias que podrían contribuir a mejorar los sistemas o procesos examinados. También puede contener un examen de las repercusiones de los hallazgos en la seguridad tecnológica y física global de la instalación. Se recomienda que se determinen las buenas prácticas y se comuniquen a otras instalaciones y/o Estados Miembros.

Durante la reunión informativa final, el Jefe del grupo presentará los hallazgos de la evaluación y, en particular, las recomendaciones y sugerencias del grupo. Es importante que el Jefe del grupo comunique también el contexto de los hallazgos y toda información conexa que sea pertinente. Se aconseja que los resultados, y especialmente los 'informes calificados', se presenten siempre con su contexto y fundamentación.

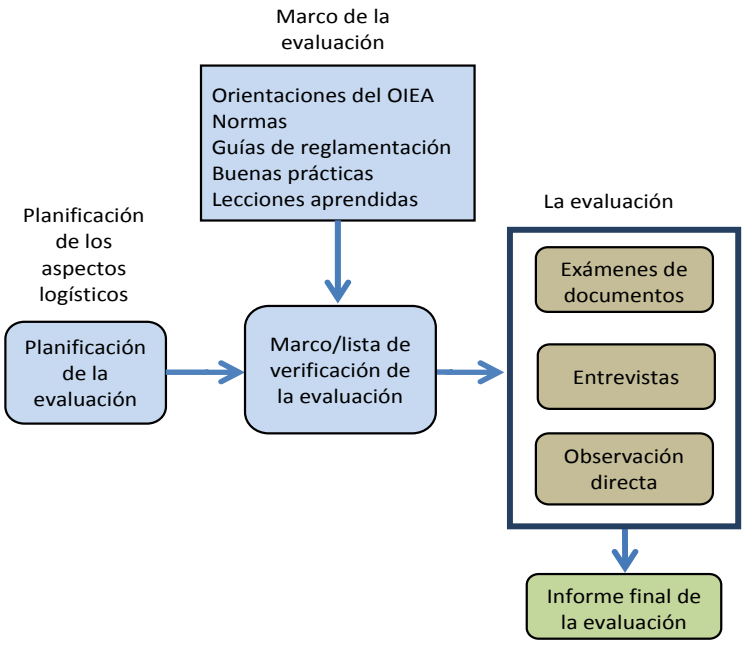

Fig.2. Componentes de la evaluación.

2.4. DOMINIOS DE LA EVALUACIÓN

El enfoque de la evaluación de la seguridad física informática se compone de dos elementos básicos: un examen global del programa de seguridad física informática, y uno o varios exámenes a nivel de los sistemas. La evaluación proporciona una instantánea de las prácticas de seguridad física informática aplicadas en la instalación. El concepto que se presenta en esta publicación da lugar a un examen tanto de las operaciones funcionales de la instalación como de su seguridad física informática en los distintos dominios. Esto ayuda a garantizar la cobertura de todos los procesos y sistemas que cumplen funciones principales en relación con las operaciones, la empresa, la seguridad tecnológica, la seguridad física y la respuesta a emergencias.

2.4.1. Dominios funcionales

En general, los sistemas informáticos de las instalaciones nucleares pueden adscribirse a uno o varios de los cinco dominios funcionales que se describen en la presente sección. La evaluación puede adaptarse de modo que abarque solo uno o algunos de estos dominios (véanse más detalles en la sección 2.6, sobre la escalabilidad). Una evaluación completa de la seguridad física informática debería comprender los cinco dominios:

i. Dominio de las operaciones: los sistemas informáticos utilizados para explotar la entidad evaluada, que incluyen los sistemas de instrumentación, control y adquisición de datos. Otros sistemas que se han de considerar son los que se necesitan para el funcionamiento de la propia instalación, como la calefacción, la refrigeración, la ventilación, la iluminación y los sistemas elevadores.

ii. Dominio de la empresa: los sistemas informáticos utilizados para la administración y el funcionamiento empresarial de la entidad. Un ejemplo típico es el sistema de permisos de trabajo. Normalmente, el dominio de la empresa tiene conexiones con redes externas que pueden relacionarse también con otros dominios.

iii. Dominio de la seguridad tecnológica: los sistemas informáticos que son fundamentales para la seguridad tecnológica de las instalaciones y para proteger a las personas y el medio ambiente contra los riesgos radiológicos y las actividades que pudieran generar esos riesgos. Incluyen, por ejemplo, los sistemas de prevención y protección utilizados para la parada de una central nuclear.

iv. Dominio de la protección física: los sistemas informáticos utilizados para proteger y vigilar los materiales nucleares y radiológicos de la entidad. Incluyen los sistemas de control del acceso y los sistemas de protección física para la monitorización del perímetro, así como los sistemas de contabilidad y control de los materiales nucleares.

v. Dominio de la respuesta a emergencias: los sistemas informáticos utilizados para la detección, la respuesta y la mitigación en caso de incidentes de emergencia que amenacen la seguridad pública, la salud y el medio ambiente. Por ejemplo, pueden utilizarse sistemas informáticos en la monitorización radiológica y del medio ambiente, la alarma y extinción de incendios y las comunicaciones de emergencia.

2.4.2. Dominios de la seguridad física

Los dominios de la seguridad física son los aspectos de alto nivel en que debe centrarse la atención al examinar la seguridad física informática. Ayudan a proporcionar al grupo que evalúa un dominio funcional una meta integral para su examen de las prácticas de seguridad física. Estos dominios, adaptados a partir de los que se describen en la norma IEC/ISO 27002 [6], son los siguientes:

i. Política de seguridad física;

ii. Gestión de la seguridad física informática;

iii. Gestión de los activos;

iv. Seguridad física de los recursos humanos;

v. Protección física;

vi. Gestión de las comunicaciones y las operaciones;

vii. Control del acceso informático;

viii. Adquisición, desarrollo y mantenimiento de los sistemas informáticos;

ix. Gestión de los incidentes de seguridad física informática;

x. Gestión de la continuidad;

xi. Cumplimiento.

La publicación Nº 17 de la *Colección de Seguridad Física Nuclear del OIEA*, *Seguridad informática en las instalaciones nucleares* [3], y la serie IEC/ISO 27000 [4 a 8] proporcionan conjuntamente una base inicial para la evaluación. El grupo de evaluación puede tomar en consideración también las normas, buenas prácticas y lecciones aprendidas respecto de los sistemas de control industrial al elaborar su plan de evaluación (posiblemente una lista de verificación). En la sección 5 se describen con más detalle los distintos dominios de la seguridad física y se ofrece orientación para evaluarlos. En el anexo I figuran ejemplos de lecciones aprendidas de la evaluación de sistemas de control industrial.

2.5. TÉCNICAS DE EVALUACIÓN

El grupo de evaluación utilizará algunas de las técnicas siguientes, o todas ellas, a fin de adquirir la información que necesite para elaborar sus conclusiones y recomendaciones:

- El examen de documentos y registros, por ejemplo de la legislación, los reglamentos o la instalación.
- Entrevistas con el personal de las organizaciones pertinentes, por ejemplo con el personal de la autoridad competente, los operadores de la instalación y representantes de otras organizaciones.
- La observación directa de la organización, sus prácticas y sistemas, y la aplicación de medidas de seguridad física informática.

2.5.1. Examen de documentos y registros

El proceso de recopilación de información entraña el examen, estudio o análisis de los documentos y registros de la instalación que esta proporcione o que se recopilen en ella. El propósito es:

- evaluar el cumplimiento de los procedimientos internos en las disposiciones adoptadas y en la seguridad física informática;
- evaluar el cumplimiento de las leyes, políticas, requisitos reglamentarios y orientaciones nacionales;
- determinar la conformidad con las orientaciones internacionales pertinentes, como las orientaciones del OIEA, las normas ISO/IEC y la buena práctica;
- determinar si las disposiciones adoptadas y las medidas de seguridad física informática son acordes con la buena práctica nacional e internacional;
- analizar su pertinencia para la situación de la amenaza existente en ese momento (p. ej., la amenaza base de diseño);
- seleccionar los procesos y/o sistemas que se evaluarán detalladamente *in situ* en los dominios funcionales elegidos o pertinentes.

Los documentos y registros pueden ser, entre otros, cualesquiera de los siguientes:

- la política;
- los procedimientos;
- los formularios de la empresa;
- guías de reglamentación/leyes;
- informes de evaluación anteriores (evaluaciones externas, autoevaluaciones, etc.);
- registros (p. ej., de la capacitación, de las inspecciones, etc.);
- páginas web (de Internet y de la intranet);
- materiales didácticos (de orientación para los nuevos empleados, sobre la seguridad física informática, etc.);
- las listas de inventarios de computadoras;
- las listas de control del acceso;
- los archivos de configuración;
- los diagramas de redes;
- los diagramas de la instalación;
- registros operacionales;
- conjuntos de reglas (como cortafuegos, sistemas de detección de intrusiones, enrutadores, etc.).

En la sección 5 se enumeran los documentos y registros que se recomienda examinar para cada dominio de la seguridad física y se ofrecen pistas que indican los elementos específicos a los que hay que prestar atención al examinar los documentos para determinar si cumplen con las buenas prácticas.

2.5.2. Entrevistas

Las entrevistas y conversaciones con personas o grupos de la instalación y/o de la autoridad pertinente dan otro nivel de información para la evaluación. De hecho, si se realizan de forma adecuada, estas entrevistas son posiblemente la parte más importante de la evaluación. Tras el examen de los materiales escritos pertinentes, pueden celebrarse entrevistas con el personal de la instalación al objeto de:

- obtener información adicional;
- verificar que los procedimientos escritos se comprendan y se apliquen tal como están establecidos;
- detectar problemas relacionados con la evaluación dimanantes de medidas o sesiones informativas anteriores;
- recabar opiniones personales;
- formarse un juicio de la base de conocimientos, la capacitación y los recursos de la entidad que se está evaluando;
- respaldar, confirmar o poner en tela de juicio observaciones hechas durante la labor de observación *in situ* de las medidas de seguridad física informática existentes;
- determinar el flujo de información de la organización y los procesos efectivos.

Las entrevistas ofrecen también a los miembros del grupo de evaluación la oportunidad de intercambiar información importante con sus contrapartes en la instalación. Una conversación de intercambio de ideas suele ser el mejor método para una entrevista. El enfoque de confrontación puede no ser productivo. Si es necesario, debe facilitarse un intérprete para evitar errores en la comunicación. Hay que tener cuidado de seleccionar al personal adecuado para las entrevistas, a fin de mantener el nivel de intercambio de información que corresponda. Por ejemplo, la administración no será necesariamente capaz de abordar los procesos de aplicación técnica. El personal que se recomienda entrevistar comprende, entre otras, a las siguientes personas:

i. Administración
   - el jefe del emplazamiento;
   - el director o los directores de la instalación;
   - el director de seguridad física;
   - el director de seguridad tecnológica;
   - el director o los directores de seguridad física de la información/los sistemas informáticos/la tecnología de la información;
   - el jefe de tecnología de la información;
   - el director de recursos humanos;
   - el director de operaciones de emergencia;
   - otro personal directivo que proceda.

ii. Especialistas técnicos
   - los administradores de sistemas;
   - el supervisor del mantenimiento de la I+C;

— el ingeniero de sistemas (de cada sistema seleccionado);
— los operadores técnicos.

iii. Otro personal

— el personal de garantía de la calidad;
— los operadores de consolas.

Antes de la entrevista, el grupo de evaluación debe tener preparado un conjunto de preguntas iniciales o de temas por tratar. Las preguntas bien formuladas pueden ayudar a evaluar:

— el conocimiento y cumplimiento de la política y los procedimientos;
— la capacitación y la eficacia de la seguridad física;
— la formación y la conciencia de la seguridad física;
— la percepción de la amenaza y de los riesgos;
— la capacidad de respuesta a incidentes;
— la claridad de las funciones y responsabilidades;
— la eficacia de la cultura de la seguridad física;
— la detección y notificación de los problemas;
— las medidas de confidencialidad;
— la aplicación de la buena práctica;
— la selección de medidas y soluciones técnicas que se deban aplicar.

Específicamente, un interrogatorio eficaz permite:

— aclarar las cuestiones que hayan surgido durante el examen de los documentos recopilados;
— verificar que el personal a cargo o responsable de aplicar los procedimientos comprenda las políticas de seguridad física relacionadas con la aplicación;
— verificar que ese personal comprenda los procedimientos de aplicación y esté debidamente capacitado y cualificado para desempeñar las funciones y/o actividades correspondientes a su cargo.

Se alienta a que se celebren entrevistas abiertas y dinámicas, que dejen espacio para preguntas espontáneas y para el intercambio de información, además de las preguntas predeterminadas.

En la sección 5 figuran ejemplos de preguntas relativas a cada dominio de la seguridad física, que el grupo de evaluación podrá utilizar y adaptar a sus necesidades específicas.

2.5.3. Observación directa

La observación directa de las medidas de seguridad física informática y de la aplicación de los procedimientos en una instalación es un aspecto importante de la evaluación. Una parte sustancial del período de evaluación *in situ* puede estar dedicado a observar esas medidas y procedimientos en la práctica. Se sugiere que las observaciones incluyan el uso de los procedimientos, los planes del emplazamiento, las instrucciones, la presentación de informes ordinarios y específicos y las medidas de control de la calidad.

Las actividades del emplazamiento que se recomienda observar durante la evaluación comprenden, entre otras cosas:

— la gestión de la configuración y de los activos;
— la securización de los sistemas;
— los procesos de seguridad física;

— el control del acceso físico y lógico;
— la separación de las funciones;
— la seguridad física del personal;
— la monitorización y el registro de sucesos;
— la arquitectura de red;
— el uso de la buena práctica;
— las visitas de inspección/verificaciones de los sistemas.

También es importante examinar el uso de controles compensatorios, cuando, ante la imposibilidad de establecer un control de seguridad física, se haya implantado otro que cumpla el mismo objetivo de seguridad. La actividad observada puede compararse con lo dispuesto en los procedimientos o reglas de la instalación, las orientaciones establecidas y la buena práctica del sector. Las observaciones permitirán así a los miembros del grupo formarse un juicio sobre la eficacia de la capacidad de la instalación de aplicar el programa de seguridad física informática.

En la sección 5 se enumeran las actividades que conviene observar en cada dominio de la seguridad física.

2.6. ESCALABILIDAD

Según la naturaleza de la evaluación, puede ser razonable o deseable limitar su alcance a algunas de las áreas funcionales incluidas en la presente guía. La orientación que se da en esta publicación es flexible y puede aplicarse a diferentes escalas, con distintos enfoques y marcos cronológicos, según el nivel de la evaluación.

2.7. CONSIDERACIONES RELATIVAS A LA SEGURIDAD FÍSICA DE LA INFORMACIÓN

En la evaluación se examinarán la información y los activos de información de carácter estratégico. Los informes y los documentos de trabajo pueden contener información de ese tipo, cuya divulgación no autorizada podría comprometer la seguridad física nuclear y tener consecuencias graves. Por ello, es indispensable que el material preparatorio, las notas técnicas, los borradores de los informes y el informe final se clasifiquen, marquen, manipulen, almacenen, transmitan y destruyan debidamente aplicando los procedimientos pertinentes para la información de carácter estratégico de la instalación anfitriona. El tratamiento y la seguridad física de esa información deben examinarse durante la reunión preparatoria y determinarse antes del inicio de la evaluación.

Los miembros del grupo que distribuyan sus notas técnicas a otros miembros a fin de recabar sus comentarios deberán adoptar precauciones especiales para garantizar la seguridad física de la información de carácter estratégico. También es necesario considerar, antes de la evaluación, los tipos de dispositivos electrónicos o medios de almacenamiento que se utilizarán para tomar notas y para preparar los borradores y las versiones finales de los informes.

Se recomienda que la seguridad física de estos materiales se base en el principio de la ‘necesidad de conocer’, es decir, que el acceso a ellos se restrinja a las personas de probidad demostrada que necesiten realmente conocerlos.

Según el contexto de la evaluación, puede ser necesario que los miembros del grupo de evaluación firmen un acuerdo de confidencialidad o de no divulgación.

3. ACTIVIDADES PREPARATORIAS

3.1. ALCANCE DEL EXAMEN

Dado el número de sistemas informáticos existentes en las instalaciones nucleares y la amplitud de los dominios funcionales y de la seguridad física que se deben evaluar, puede ser imposible realizar un examen completo de todo el programa de seguridad física informática en una misma evaluación. Por consiguiente, el primer paso es que la instalación anfitriona decida el alcance y los objetivos de la evaluación y los explique al Coordinador o al Jefe del grupo, según proceda. En la sección 4 se presenta el concepto de los componentes modulares de ciertos dominios funcionales de la instalación. Este enfoque permite a los planificadores de la evaluación determinar los componentes prioritarios de una evaluación específica.

3.2. REUNIÓN PREPARATORIA

La reunión preparatoria, en que participan el Coordinador y el Jefe del grupo, se celebra normalmente dos o tres meses antes de la evaluación en los locales de la instalación anfitriona, para que puedan participar representantes de todas las partes interesadas. Lo que se desea lograr en esa reunión es una clara comprensión del proceso y la metodología de la evaluación, con inclusión de las actividades de preparación, los mecanismos de realización de la evaluación y la labor ulterior de preparación del informe. Posteriormente podrá distribuirse un acta de la reunión.

En la reunión se examinará lo siguiente:

- las principales características del programa de evaluación;
- el objetivo y alcance de la evaluación;
- el formato y contenido previstos del informe;
- el alcance y el nivel del análisis que se incluirá en el informe;
- los requisitos de tratamiento y seguridad física de la información que se aplicarán al informe y a las notas técnicas;
- la preparación para la evaluación, incluida una lista de los documentos requeridos;
- la preparación de un paquete de información preliminar para el grupo de evaluación;
- el apoyo logístico necesario, como la oficina del grupo, una impresora, una fotocopiadora y un medio de transporte local;
- la prestación de servicios de traducción/interpretación;
- el tratamiento de los documentos confidenciales de la instalación evaluada;
- los procedimientos que seguirá el grupo de evaluación — con inclusión de las medidas que se adoptarán de inmediato y del punto de contacto dentro de la entidad anfitriona al que se deberá dar aviso — si se detecta alguna de las situaciones siguientes:
  - una vulneración real o potencial de un sistema,
  - una negligencia culpable,
  - un problema de seguridad tecnológica importante,
  - un problema de seguridad física importante;
- la finalización del calendario de la evaluación;
- la posible composición del grupo de evaluación;
- las posibles actividades de seguimiento.

3.3. OBLIGACIONES DEL ANFITRIÓN

El anfitrión se considera el patrocinador de la actividad. Puede ser la administración de la propia instalación o un organismo gubernamental, en el caso del examen de una instalación, o un organismo gubernamental, si la actividad de evaluación se centra en un examen a nivel del Estado. Como parte de las conversaciones durante la reunión preparatoria, el Coordinador y el Jefe del grupo llegarán a acuerdos con el anfitrión para la prestación de los servicios de apoyo necesarios en el lugar de la evaluación. En las misiones internacionales, las evaluaciones de la seguridad física informática se realizan normalmente en inglés. El anfitrión deberá proporcionar los servicios de interpretación necesarios para que los miembros del grupo puedan realizar su trabajo.

Es importante que el anfitrión conceda al grupo de evaluación el uso exclusivo de una zona de reunión segura durante todo el período de la evaluación. Esta zona de reunión segura debe ser suficientemente grande para que el grupo pueda trabajar y mantener conversaciones con un grado razonable de privacidad. También puede ser deseable tener acceso a Internet, lo que deberá señalarse en la reunión preparatoria inicial. Se recomienda que se pongan a disposición de los miembros del grupo una impresora y una fotocopiadora. Los documentos pertinentes que se deban examinar en la reunión preparatoria se facilitarán en el idioma que acuerden el anfitrión y el grupo de evaluación. El grupo necesitará contar durante todo el período de evaluación con un contenedor, o un área con medidas de protección física adicionales, para el almacenamiento seguro de los documentos o activos que puedan contener información confidencial o de carácter estratégico.

A fin de ahorrar tiempo durante la evaluación, y de que los miembros del grupo puedan hacerse una idea completa del contexto de esta y de los requisitos reglamentarios, es conveniente que el anfitrión proporcione los documentos pertinentes para su distribución a los miembros del grupo con al menos dos meses de antelación a la visita del grupo, teniendo en cuenta que algunos documentos pueden no estar fácilmente disponibles hasta la llegada a la instalación. Todos los documentos que se obtengan del anfitrión deberán tratarse de conformidad con lo que hayan acordado el anfitrión y el grupo.

Según el alcance de la evaluación, esos documentos podrían comprender lo siguiente:

i. Legislación nacional:
   - — las leyes que regulen la seguridad física informática en las instalaciones nucleares; una sinopsis de las responsabilidades y la estructura (con indicación de los departamentos pertinentes) de las diferentes organizaciones gubernamentales que se ocupan de las cuestiones de seguridad física informática y de cómo se interrelacionan esas organizaciones;
   - — los reglamentos sobre la seguridad física informática de las instalaciones nucleares;
   - — las orientaciones normativas pertinentes sobre las instalaciones nucleares;
   - — las características de la amenaza base de diseño.

ii. Organizaciones y procedimientos de las autoridades reguladoras:
   - — su estructura, organización y dotación de personal; una descripción de los procedimientos de concesión de licencias, cuando proceda;
   - — las prácticas de inspección;
   - — una lista de los reglamentos, las guías de reglamentación, los códigos y las normas aplicables.

iii. Descripción, organización y procedimientos de seguridad física informática de la instalación:

— la política de seguridad física global (o las secciones pertinentes de esta);
— los planes de seguridad física informática;
— las funciones y responsabilidades en materia de seguridad física;
— el programa de capacitación y sensibilización sobre la seguridad física;
— el inventario de los activos digitales y una descripción de cómo y por qué están incluidos en el programa de seguridad física informática de la instalación;
— la participación de terceros;
— la evaluación del riesgo, incluida una descripción de cómo se seleccionan los controles de seguridad física;
— la categorización de los sistemas de seguridad tecnológica;
— los procedimientos de seguridad tecnológica que guardan relación con la seguridad física;
— el diseño de la arquitectura de red;
— los dispositivos para los límites entre los dominios de red, incluidas las políticas de flujo de datos para esos dispositivos;
— la documentación técnica de los sistemas;
— los informes de evaluación ya existentes (preparados por la propia instalación o por terceros);
— los procedimientos y registros de la respuesta a incidentes de seguridad física informática;
— los informes sobre incidentes de seguridad física informática, y las medidas correctivas adoptadas;
— los documentos sobre la gestión de la configuración, incluidos los análisis de la seguridad física relacionados con cambios en la configuración.

3.4. FORMACIÓN DEL GRUPO

3.4.1. Composición del grupo

El grupo puede estar integrado por un Coordinador, un Jefe (cuando proceda), tres o más expertos y, posiblemente, un redactor técnico que ayude al grupo a elaborar las notas técnicas y el informe final de la evaluación. La composición del grupo podrá adaptarse según el alcance de la evaluación.

El Coordinador o el Jefe del grupo seleccionarán a los expertos que formarán parte del grupo, con el acuerdo del anfitrión. Estos expertos deberán tener un nivel elevado y reconocido de conocimientos y experiencia en la seguridad física informática, junto con una especialización en uno o varios de los ámbitos de las operaciones de la instalación, la seguridad tecnológica, la seguridad física, la tecnología de la información y la ingeniería de la instalación, para respaldar la evaluación de los dominios funcionales. Los miembros del grupo deben poder comprometerse a dedicar un determinado período de tiempo a la preparación, la propia evaluación y la elaboración del informe final. Es útil para la evaluación que por lo menos uno de los miembros del grupo esté familiarizado con el diseño de la instalación explotada por el anfitrión.

Además, se recomienda que los miembros del grupo se seleccionen de modo que estén representados diferentes enfoques nacionales de la reglamentación y la aplicación, como la legislación pertinente, la regulación de las actividades nucleares, la explotación de las instalaciones y el análisis de los sistemas de seguridad física informática. Además de su campo de especialización particular, cada experto tendrá probablemente conocimientos sobre

otros enfoques nacionales y otras esferas pertinentes. De esta forma, el grupo podrá ofrecer la mejor evaluación y el mejor asesoramiento posibles sobre la seguridad física informática.

Se podrá invitar a un observador del anfitrión a que participe en la evaluación junto con el grupo. Ello puede resultar útil para facilitar el intercambio de información.

3.4.2. Coordinador del grupo

El Coordinador acompañará al grupo durante toda la evaluación para velar por la coordinación con las contrapartes en la entidad anfitriona y prestar el apoyo logístico y de otra índole que pueda ser necesario. En el caso de las misiones de los servicios de asesoramiento del OIEA, el Coordinador distribuirá a todos los miembros del grupo la edición vigente de los documentos pertinentes sobre la evaluación y cualquier otro material que proceda, además de los documentos que facilite de antemano el país anfitrión, para que puedan familiarizarse con los documentos que utilizarán durante toda la misión.

El Coordinador del grupo tiene la responsabilidad global de la coordinación de la evaluación y la presentación del informe final correspondiente.

Sus responsabilidades comprenden lo siguiente:

- coordinar la labor preparatoria y concertar los arreglos necesarios para la evaluación;
- establecer el enlace con las contrapartes adecuadas en la entidad anfitriona que serán las principales personas de contacto del grupo de evaluación durante la misión;
- designar, junto con la entidad anfitriona si es el caso, a un experto en seguridad física informática para que sea el Jefe del grupo durante la evaluación;
- organizar, junto con el Jefe del grupo, una reunión preparatoria con el anfitrión;
- seleccionar, con la aprobación de la entidad anfitriona, a los miembros del grupo;
- coordinar los arreglos logísticos en apoyo del grupo de evaluación, incluido el suministro de los documentos informativos pertinentes;
- tener conocimiento de las normas pertinentes de la instalación respecto de la seguridad tecnológica, la seguridad física, la seguridad del personal y cualquier otro requisito aplicable, y comunicar esta información al grupo de evaluación.

3.4.3. Jefe del grupo

El Jefe del grupo es particularmente importante para el éxito de la evaluación. Las personas seleccionadas para este cargo deben tener dotes de liderazgo reconocidas y una experiencia muy amplia en todas las actividades de examen que pueda tener que realizar el grupo de evaluación. Lo ideal es que el Jefe del grupo tenga experiencia en la realización de evaluaciones de la seguridad física informática en instalaciones nucleares.

Normalmente, el Jefe del grupo tiene la responsabilidad global de las siguientes tareas:

- representar al grupo en las interacciones con sus contrapartes en la entidad anfitriona;
- dirigir la reunión preparatoria y las reuniones informativas inicial y final;
- determinar las normas de actuación de todos los miembros del grupo;
- informar a los miembros del grupo sobre la evaluación, incluidos sus objetivos y procesos;
- velar por que los miembros del grupo tengan la información necesaria para estar debidamente preparados para la evaluación;

— dirigir la elaboración detallada de las actividades y los plazos de la evaluación;
— coordinar y supervisar las actividades de examen del grupo, lo que incluye celebrar reuniones diarias del grupo, velar por que se cumplan los plazos, mantener informadas a sus contrapartes, resolver las cuestiones que requieran la adopción de decisiones y preparar la reunión final;
— coordinar el examen de todas las notas técnicas;
— coordinar la preparación del proyecto de informe;
— presentar los resultados de la evaluación en la reunión informativa final;
— producir el informe final;
— velar por que los miembros del grupo tengan conocimiento de las cuestiones de confidencialidad y manejen la información en consecuencia;
— velar por que los miembros del grupo tengan conocimientos y capacitación sobre todas las normas pertinentes de la instalación que se relacionen con la seguridad tecnológica, la seguridad física, la seguridad del personal y cualquier otro requisito aplicable.

3.4.4. Miembros del grupo

Los miembros del grupo realizarán la evaluación, recopilando información, llevando a cabo los análisis y haciendo aportaciones al informe final. Tendrán conocimientos especializados en la seguridad física informática y competencias técnicas adicionales en relación con el funcionamiento de la organización o instalación.

Las responsabilidades y funciones de los miembros del grupo comprenden lo siguiente:

— efectuar los exámenes de los documentos y registros;
— participar en las reuniones y conversaciones con las contrapartes de la entidad anfitriona, según proceda;
— asistir a las reuniones del grupo y participar en el desarrollo de las actividades de evaluación;
— comparar sus conclusiones/hallazgos con los de los otros miembros del grupo;
— elaborar notas técnicas sobre la aplicación de las medidas de seguridad física informática en la instalación anfitriona, sobre la base de las exposiciones, la documentación, las entrevistas y la observación directa de la organización y sus prácticas;
— evaluar los sistemas de los dominios funcionales en relación con los controles de los dominios de la seguridad física;
— ser conscientes del acuerdo relativo a la confidencialidad concertado con la entidad anfitriona y manejar la información en consecuencia;
— conocer y cumplir las normas pertinentes de la instalación con respecto a la seguridad tecnológica, la seguridad física, la seguridad del personal y otros requisitos aplicables.

3.4.5. Redactor técnico

Un redactor técnico puede ser útil para apoyar al grupo en la finalización puntual del informe de evaluación y prestar asistencia a sus miembros en la elaboración de las notas técnicas. El redactor técnico asiste a todas las reuniones, sesiones informativas y entrevistas para tomar notas que complementen la información recopilada por el grupo. Durante toda la evaluación, el redactor técnico reúne las aportaciones por escrito de los miembros del grupo y las formatea y edita según corresponda. Sus responsabilidades y funciones comprenden lo siguiente:

— participar en las actividades del grupo;
— tomar notas detalladas y/o prestar asistencia a los miembros del grupo en su preparación para las actividades de observación y las entrevistas;
— junto con el grupo y su jefe, elaborar el informe de evaluación;
— ser consciente del acuerdo de confidencialidad concertado con la entidad anfitriona y manejar toda la información en consecuencia;
— conocer y cumplir todas las normas pertinentes de la instalación con respecto a la seguridad tecnológica, la seguridad física, la seguridad del personal y otros requisitos aplicables.

3.5. REUNIÓN DEL GRUPO PREVIA A LA EVALUACIÓN

Se recomienda que el grupo se reúna antes del comienzo de la evaluación a fin de establecer la coordinación entre sus miembros. Esto es particularmente importante si los integrantes del grupo no han trabajado juntos con anterioridad, como ocurrirá en las misiones internacionales a cargo de expertos de diferentes países. Incluso si los miembros del grupo trabajan juntos con regularidad, puede ser conveniente celebrar una reunión previa a la evaluación para examinar y aclarar los detalles específicos de esa evaluación en particular.

Según la naturaleza de la misión o evaluación, esta reunión podría celebrarse con varios meses de antelación o inmediatamente antes del comienzo de la evaluación.

El Coordinador y el Jefe del grupo dirigirán esta reunión, cuyo orden del día podría contener los siguientes puntos:

i. Presentación de los miembros del grupo;
ii. Antecedentes de la evaluación:
    a) Alcance de la evaluación;
    b) Programa y plazos de las actividades de evaluación;
iii. Información básica sobre los miembros del grupo:
    a) Competencias y conocimientos de los miembros del grupo;
    b) Expectativas de los miembros del grupo;
iv. Examen de los factores peculiares de la evaluación y de las instalaciones nucleares que se visitarán;
v. Examen del proceso de evaluación detallado;
vi. Elaboración detallada de las funciones, las responsabilidades y los focos de atención de cada miembro del grupo.

3.6. PROGRAMA DE LA EVALUACIÓN

El programa de la evaluación dependerá en gran medida de que se realice solo en un emplazamiento o en muchos, y de que se trate de una evaluación autónoma o de un módulo de otra evaluación, una misión o un servicio de asesoramiento. En el cuadro 1 se propone un programa hipotético para una evaluación autónoma de la seguridad física informática, en que la mayoría de los días se trabajará *in situ* y un redactor técnico actualizará diariamente el proyecto de informe.

CUADRO 1. PROGRAMA HIPOTÉTICO DE UNA EVALUACIÓN

Día 1
El grupo celebra la reunión previa a la evaluación y una sesión de orientación
Día 2
El grupo recibe la capacitación necesaria para entrar en la instalación anfitriona
Reunión inicial con la instalación anfitriona
Inicio de la evaluación
Reunión de rendición de cuentas y preparación para el día siguiente
El redactor técnico prepara el informe diario sobre la base de la rendición de cuentas
El Jefe del grupo informa a un director que representa a la entidad anfitriona, si es necesario
Del día 3 hasta el día final -2
Inicio de la evaluación
Reunión de rendición de cuentas y preparación para el día siguiente
El redactor técnico prepara el informe diario sobre la base de la rendición de cuentas y compila las notas y los informes diarios
El Jefe del grupo informa a un director que representa a la entidad anfitriona, si es necesario
Día final -1
Los miembros del grupo examinan y resumen la evaluación
El redactor técnico prepara un informe de salida para el examen de los miembros del grupo
El Jefe del grupo prepara una presentación para la reunión informativa final
El Jefe del grupo informa a un director que representa a la entidad anfitriona, si es necesario
Día final
Reunión informativa final — se informa a la entidad anfitriona sobre el resultado de la evaluación

3.6.1. Reuniones del grupo

Las reuniones diarias del grupo, que normalmente se celebran al final del día, son útiles para examinar las actividades de la jornada, evaluar los avances, debatir los hallazgos/conclusiones de los miembros del grupo y proporcionar al redactor técnico la información que necesite sobre las actividades del día.

Esas reuniones pueden servir también para preparar las actividades del día siguiente, por ejemplo mediante:

- el examen de las partes pertinentes de las directrices para la evaluación y/o del material preparatorio;
- la confección de una lista de preguntas sobre cada tema;
- la planificación de las actividades de observación sobre el terreno;
- la determinación de las principales cuestiones que tendrán prioridad al día siguiente.

4. METODOLOGÍA DE LA EVALUACIÓN

4.1. PANORAMA GENERAL DE LA METODOLOGÍA

Una forma típica de iniciar una evaluación es examinando las prácticas de seguridad física informática de la instalación desde una perspectiva global. A continuación, puede hacerse un análisis más detallado de determinados procesos y sistemas, aplicando el enfoque que se describe en la sección 4.3.1, que se basa en dividir las prácticas de seguridad física informática en dominios funcionales y dominios de la seguridad física. Este proceso ayudará a afinar la evaluación de la eficacia y calidad de todo el programa de seguridad física informática.

4.2. EVALUACIÓN DEL PROGRAMA GLOBAL DE SEGURIDAD FÍSICA INFORMÁTICA

En la fase de recopilación de información, la evaluación del programa global de seguridad física entraña un examen de las políticas, los planes, los procedimientos, la aplicación y los organigramas pertinentes. Luego, las entrevistas y las observaciones sobre el terreno ayudarán a evaluar mejor las prácticas de seguridad física informática. Cuatro aspectos conforman el panorama global que deberá examinarse: el enfoque de la administración, los procesos de seguridad física informática, la gestión de la amenaza y de sus consecuencias y la gestión del riesgo.

En las secciones siguientes se exponen los criterios indicativos en que podría basarse la evaluación de cada uno de estos aspectos.

4.2.1. Enfoque de la administración

Uno de los elementos clave de un buen programa de seguridad física informática es la aceptación de la política de seguridad física informática en todos los niveles de la administración y de las operaciones y su aplicación en la práctica. El programa no tendrá éxito si no cuenta con el firme apoyo de la administración. Los criterios indicativos a este respecto comprenden lo siguiente:

i. Un compromiso demostrado de la administración a todos los niveles.

ii. Una definición clara de los objetivos de seguridad física informática.

iii. La definición de funciones y responsabilidades claras que garantizan que los procesos de seguridad física informática, incluidas las funciones y responsabilidades específicas:

   a) abarcan todos los dominios funcionales;
   b) se establecen con la debida coordinación entre los dominios funcionales pertinentes;
   c) prevén una organización adecuada (incluido un Oficial de seguridad física informática, o un cargo equivalente).

iv. Una administración que da acceso a recursos adecuados (humanos, financieros, de tiempo asignado, de competencias, etc.).

v. Procesos de gestión que incluyen la evaluación interna y medidas de garantía de la calidad.

vi. La garantía del cumplimiento del marco regulador.

4.2.2. Procesos de seguridad física informática

Este aspecto se refiere al uso y aplicación de medidas de seguridad física informática en la puesta en práctica de la política correspondiente. Comprende la aplicación de controles técnicos, controles administrativos y controles físicos para prevenir los sucesos relacionados con la seguridad física informática, y detectarlos y darles respuesta cuando se producen. Los criterios indicativos a este respecto comprenden lo siguiente:

— La existencia de una política y de un programa de seguridad física informática.

— La existencia de un conjunto estructurado, oficializado y documentado de procesos destinados a velar por la seguridad física informática.

— La existencia de procesos que permiten un examen y una mejora constantes, por ejemplo exámenes periódicos, auditorías, procedimientos de mantenimiento claros y autoevaluaciones, etc.

— La existencia de procesos que, en la medida de lo posible, son proactivos y no reactivos.

4.2.3. Gestión de la amenaza y de sus consecuencias

Utilizando fuentes de información fidedignas, las autoridades adecuadas del Estado — y las instalaciones, cuando corresponde — definen la amenaza y las capacidades a ese respecto elaborando una evaluación de la amenaza y, si procede, una amenaza base de diseño. Las consideraciones relativas a la amenaza incluyen el análisis de los adversarios que tienen una capacidad cibernética creíble. Se aconseja que la amenaza se examine y evalúe continuamente para detectar todo indicio de cambios que puedan afectar a la seguridad física informática de la organización o instalación. Los criterios indicativos y las preguntas a este respecto comprenden lo siguiente:

— La existencia en la organización de un proceso de gestión maduro que aborda las amenazas, las vulnerabilidades y las posibles consecuencias.

— ¿Cuáles referencias y qué metodología se utilizan?

— ¿Cuál es el alcance del análisis de la amenaza (la organización, una parte de la organización, un sistema, etc.)?

— Cómo se realizó, documentó y utilizó el análisis junto con los controles de seguridad física de referencia.

— Si se han identificado y evaluado los posibles blancos para determinar si requieren protección contra las amenazas a la seguridad física nuclear.

— Si las evaluaciones incluyen un análisis de las posibles consecuencias de ciberataques contra esos blancos.

— Con respecto a la forma en que se realizan las evaluaciones de la amenaza, con qué frecuencia tienen lugar los exámenes ordinarios y las actualizaciones.

— Si el programa de respuesta a incidentes apoya los procesos de mitigación, continuidad y recuperación que se han definido para los casos de vulneración de los sistemas informáticos.

4.2.4. Gestión del riesgo y adhesión a los principios de seguridad física fundamentales

El Estado y la instalación deben velar por que el programa de seguridad física informática sea capaz de fijar y mantener el riesgo de vulneración de los sistemas informáticos en un nivel aceptable por medio de la gestión del riesgo. El programa de seguridad física informática debe, además, detallar la aplicación de los principios fundamentales de la seguridad física, incluido el

uso de un enfoque graduado y de la defensa en profundidad, para proteger los activos contra los sucesos relacionados con la seguridad física nuclear en consonancia con el nivel de las consecuencias o efectos que esos sucesos puedan tener. Los criterios indicativos y las preguntas a este respecto comprenden lo siguiente:

— Si las medidas de seguridad física informática se basan en un enfoque graduado. En particular, si los niveles de seguridad física se han asignado aplicando reglas o procesos claros (p. ej., sobre la base de la seguridad tecnológica, la amenaza base de diseño, un análisis de las posibles consecuencias, etc.). ¿Se aplican efectivamente esas reglas o procesos?
— ¿Cómo se aplica la defensa en profundidad a los componentes y sistemas informáticos?
— ¿Cómo influyen las evaluaciones del riesgo en el enfoque graduado?
— ¿Aborda el enfoque graduado todos los elementos identificados en la evaluación del riesgo?

4.3. MATRIZ DE EVALUACIÓN

4.3.1. Introducción

Un elemento central de la presente metodología es la evaluación de los dominios funcionales y los dominios de la seguridad física (descritos en la sección 2.4). En el cuadro 2 se presenta una matriz que correlaciona ambos tipos de dominios que se han de evaluar y permite comprobar que la evaluación abarque las esferas de interés directo con suficiente profundidad. La matriz de evaluación contiene:

— los cinco dominios funcionales principales en las columnas;
— los dominios de la seguridad física (adaptados a partir de los dominios establecidos en la serie ISO 27000) en las filas.

El objeto de esta matriz es ayudar a:

— determinar el alcance de la evaluación;
— estructurar los resultados de los análisis y observaciones, en la etapa de recopilación de información y sobre el terreno;
— proporcionar al grupo de evaluación un análisis suficientemente amplio que le permita hacer una evaluación bien fundamentada;
— visualizar los resultados de la evaluación.

4.3.2. Dominios funcionales

La evaluación global comprende un análisis de los cinco dominios funcionales: las operaciones, la empresa, la seguridad tecnológica, la protección física y la respuesta a emergencias. En algunos casos es posible hacer una evaluación de alcance más limitado, que se centre en un subconjunto de estos dominios (p. ej., en una misión típica del IPPAS solo se evaluará la protección física).

A continuación figura una lista indicativa de las familias de sistemas o funciones que se han de evaluar para cada uno de los cinco dominios funcionales. Esta lista varía, y puede adaptarse a la instalación concreta que se deba evaluar. También puede adaptarse en función del alcance de la evaluación y del tipo de instalación. Esta selección podrá modificarse en el curso de la evaluación, si es necesario, para incluir elementos adicionales que se hayan encontrado en las actividades *in situ*. Los siguientes son ejemplos de los sistemas o funciones correspondientes a cada dominio:

Dominio de las operaciones

- sistemas de control de procesos: sistemas de instrumentación y control (I+C) para el control de la central;
- sistemas de I+C de la sala de control, incluidos los sistemas de alarma;
- sistemas informáticos de proceso que reúnen y preparan la información para la sala de control;
- sistemas de I+C para la manipulación y el almacenamiento del combustible;
- gestión/mantenimiento de la configuración;
- acceso remoto y red privada virtual (VPN) para el entorno operacional;
- infraestructura de comunicación de voz y datos;
- sistemas de funcionamiento y control de la infraestructura;
- entornos de ensayo y desarrollo de los sistemas de operaciones.

Dominio de la empresa

- infraestructura de comunicación de voz y datos;
- sistemas de gestión de los recursos humanos y los repositorios de datos;
- sistemas técnicos/de ingeniería;
- sistemas de órdenes de trabajo y permisos de trabajo;
- sistemas de compras;
- sistemas de oficina.

Dominio de la seguridad tecnológica

- sistemas de protección: sistemas de I+C utilizados para las medidas de protección del reactor o de la central que se activan automáticamente;
- sistemas de medidas de seguridad: sistemas de I+C que ejecutan medidas de seguridad, iniciadas ya sea por los sistemas de protección o manualmente;
- elementos de apoyo de los sistemas de seguridad: I+C para los sistemas de suministro de energía eléctrica de emergencia.

Dominio de la protección física

- monitorización del perímetro/detección de intrusiones;
- sistemas de control del acceso;
- sistemas de contabilidad y control de inventarios (distintos de los que se utilizan para los materiales nucleares);
- sistemas de contabilidad y control de los materiales nucleares;
- infraestructura de comunicación de voz y datos;
- sistemas de alarma;
- base de datos de las autorizaciones de seguridad física, utilizada para velar por que el personal tenga las aprobaciones adecuadas.

Dominio de la respuesta a emergencias

- monitorización del medio ambiente;
- monitorización radiológica;
- sistemas de protección contra incendios;
- infraestructura de comunicación de voz y datos.

En el informe final se indicará cuáles sistemas y funciones se evaluaron, y cuáles se consideró que no correspondían al ámbito de la evaluación.

4.3.3. Dominios de la seguridad física

A diferencia del caso de los dominios funcionales, la evaluación puede tener que abordar el conjunto completo de los once dominios de la seguridad física para que el examen tenga una cobertura suficientemente amplia. Como se señaló anteriormente, estos once dominios se han tomado de la serie ISO/IEC 27000 [4 a 8] y se han adaptado para su uso en las evaluaciones de la seguridad física informática en instalaciones nucleares. En la sección 5 se ofrecen orientaciones específicas para evaluar cada uno de estos dominios con respecto a la seguridad física nuclear. Esa lista es indicativa, y no prescriptiva.

En el cuadro 2 figura una matriz cruzada de los dominios funcionales y de la seguridad física, que puede utilizarse para hacer un seguimiento de la cobertura de la evaluación y cerciorarse de que se ha hecho un examen completo de las esferas de interés. El uso de una matriz de este tipo queda a discreción del grupo de evaluación. Además de indicar la cobertura de la evaluación, la matriz puede ayudar a visualizar las observaciones en los diferentes dominios, lo que a su vez ayudará a determinar las tendencias o lagunas en la cobertura de la seguridad física.

CUADRO 2. MATRIZ DE COBERTURA DE LOS DOMINIOS.

Dominios funcionales **Dominios de la seguridad física**	**Operaciones**	**Empresa**	**Seguridad tecnológica**	**Protección física**	**Respuesta a emergencias**
Política de seguridad física					
Gestión de la seguridad física informática					
Gestión de los activos					
Seguridad física de los recursos humanos					
Protección física					
Gestión de las comunicaciones y las operaciones					
Control del acceso					
Adquisición, desarrollo y mantenimiento					
Gestión de incidentes de seguridad física informática					
Gestión de la continuidad					
Cumplimiento					

5. ORIENTACIONES PARA LA EVALUACIÓN, POR DOMINIO DE LA SEGURIDAD FÍSICA

5.1. PANORAMA GENERAL

En la presente sección se ofrecen orientaciones y buenas prácticas relacionadas con cada uno de los once dominios de la seguridad física para su uso como posibles criterios de valoración durante la evaluación. Esta orientación no está concebida para ser usada directamente como una lista de verificación, pero puede emplearse para crear un plan de evaluación adaptado a las circunstancias concretas. Durante la evaluación, los miembros del grupo deben prestar atención no solo a cada dominio por separado, sino también a la integración de todos ellos y a su impacto total en el programa global de seguridad física informática.

5.2. POLÍTICA DE SEGURIDAD FÍSICA

5.2.1. Descripción del dominio

Este dominio de la seguridad física proporciona dirección y apoyo a la administración para la mejora de la seguridad física informática en consonancia con la seguridad nuclear tecnológica y física y con las leyes, los reglamentos y los requisitos empresariales pertinentes.

La administración necesita establecer una dirección de política clara, acorde con la seguridad nuclear tecnológica y física, y demostrar su apoyo y adhesión a la seguridad física informática implantando y manteniendo una política al respecto en toda la organización.

La política de seguridad física informática se debe definir, comunicar, documentar y revisar periódicamente. Se recomienda que la política tenga en cuenta los cinco dominios funcionales nucleares: las operaciones, la empresa, la seguridad tecnológica, la protección física y la respuesta a emergencias.

Documentos y registros de interés

- Política/plan de seguridad física informática;
- Política/plan de seguridad física de la instalación;
- Comunicación de la política de seguridad física informática a los empleados;
- Registro de las auditorías de la seguridad física informática;
- Registro de los exámenes y actualizaciones de la política de seguridad física;
- Registro de los ejercicios de seguridad física informática.

Pistas para el análisis de los documentos y registros

- ¿Se ha definido la política de seguridad física?
- ¿Es coherente esta política con las otras políticas de la instalación?
- ¿Cómo se comunica la política de seguridad física a los empleados?
- ¿Cómo se demuestra el compromiso de la administración?
- ¿Con qué frecuencia se examina la política para introducir cambios? ¿Existe un registro de esos exámenes?
- ¿Cómo evalúa la administración la eficacia de la política?
- ¿Aborda la política de seguridad física los cinco dominios funcionales nucleares?
- Si existen excepciones a la política de seguridad física, ¿están documentadas?

— ¿Se comunica la política de seguridad física a terceros (subcontratistas, etc.)?
— ¿Responde la política a las orientaciones vigentes sobre la buena práctica?
— ¿Se establecen claramente en la política los objetivos de seguridad física?
— ¿Están claramente definidas las responsabilidades y asignadas las correspondientes facultades?

Ejemplos de preguntas para las entrevistas

— ¿Conocen los empleados la política de seguridad física?
— ¿Entienden las funciones y responsabilidades (incluidas las propias)?
— ¿Tienen acceso a la política de seguridad física?
— ¿Cómo se aplica la política de seguridad física en las guías o instrucciones específicas para su trabajo?

Aspectos que conviene observar

— Procesos específicos que se relacionen con la aplicación de la política;
— Cuando proceda, verifíquese la coherencia entre las políticas.

Pistas para el análisis sobre el terreno

— Formúlense las mismas preguntas a personas de distintos departamentos y diferentes niveles de la organización.

5.3. GESTIÓN DE LA SEGURIDAD FÍSICA INFORMÁTICA

Descripción del dominio

La organización debe establecer un marco de gestión de la seguridad física informática.

La administración debe aprobar la política de seguridad física informática, asignar las funciones y responsabilidades, y examinar la aplicación de las medidas de seguridad física informática en toda la organización. De hecho, este puede ser un componente de una política de seguridad física más amplia. Se alienta a que se adopte un enfoque multidisciplinario en todos los departamentos de la organización (p. ej., de la TI y la I+C/ingeniería).

Documentos y registros de interés

— Política/plan de seguridad física informática;
— Organigramas y descripciones de puestos;
— Política y procedimientos que detallen la estructura orgánica;
— Lista del oficial o los oficiales de seguridad física informática y los miembros del grupo de seguridad física informática;
— Descripción del proceso de autorización para las modificaciones de la política y los procedimientos de seguridad física informática;
— Procedimiento y proceso de autorización para adquirir nuevo equipo de procesamiento de información;
— Programa y política de capacitación, y los registros correspondientes.

Pistas para el análisis de los documentos y registros

- ¿Cuáles son los objetivos de seguridad física informática?
- ¿Dónde recaen en la jerarquía de la organización las responsabilidades por la seguridad física informática?
- ¿Cuál es la estructura del grupo de seguridad física informática?
- Para todos los dominios funcionales tiene que haber un oficial a cargo de la seguridad física informática. Si existe más de uno de estos oficiales, las responsabilidades y líneas de comunicación deben estar claramente definidas. Se requieren interfaces claramente establecidas, con las respectivas funciones y responsabilidades;
- ¿Está incluida en los procedimientos de modificación la seguridad física informática?
- ¿Existe una formación especializada para las personas con funciones de seguridad física?
- ¿Quién tiene que recibir capacitación, con qué frecuencia se imparte esa capacitación, y qué porcentaje del personal ha recibido la capacitación requerida?

Ejemplos de preguntas para las entrevistas

- ¿Sabe usted quién es su oficial de seguridad física informática y cómo ponerse en contacto con él o ella?
- ¿Cuáles son los procedimientos de referencia para la seguridad física informática?
- ¿Celebra el grupo de seguridad física informática reuniones ordinarias? ¿Se levantan actas de estas reuniones? ¿Cuál es el proceso para comunicar al grupo de seguridad física informática los sucesos o incidentes o los cambios que puedan comprometer la seguridad física?
- ¿Cuál es el proceso (es decir, cuáles son las herramientas o procedimientos) para proteger la información de carácter estratégico?
- ¿Qué capacitación ha recibido el personal en seguridad física informática? ¿Es esta una capacitación continua?
- ¿Se ha efectuado un análisis de competencias de la organización interna existente para determinar las posibles lagunas en las capacidades? ¿Qué se ha hecho con respecto a esas lagunas?

Aspectos que conviene observar

- ¿Tienen los especialistas en seguridad física informática una formación externa pertinente en su especialidad?
- ¿Cómo se hace el rastreo y el seguimiento de las tareas de seguridad física informática (p. ej., mediante puntos de acción asignados a partir de las actas de las reuniones)?
- ¿Hay una persona a cargo de las auditorías/evaluaciones de la seguridad física informática? ¿Se prevén auditorías o evaluaciones en la planificación anual?

Pistas para el análisis sobre el terreno

- Se aconseja que los miembros del grupo de seguridad física informática participen en la evaluación;
- ¿Es visible la seguridad física informática en todos los niveles de la administración y el personal?

5.4. GESTIÓN DE LOS ACTIVOS

Descripción del dominio

Este dominio de la seguridad física tiene el objetivo de proteger los activos de la organización. Comprende la responsabilidad por la gestión de los activos, un inventario del equipo y los programas informáticos autorizados, una lista del equipo y los programas informáticos no autorizados, y la clasificación informática (de los sistemas importantes para la seguridad tecnológica y/o física).

Todos los activos deben tener un propietario exclusivo que tendrá la responsabilidad de asignar los controles apropiados.

Documentos y registros de interés

- Política y procedimientos que describan en detalle el sistema de gestión de activos;
- Inventario de los activos (sistemas informáticos, equipo de red, programas informáticos, versiones);
- Procedimientos y criterios para identificar las computadoras incluidas en el programa de seguridad física informática, si se aplica;
- Listado/diagrama de la ubicación física de los activos inventariados;
- Procedimientos de inventario, con inclusión de la periodicidad y de los registros de las actualizaciones del inventario;
- Diagrama funcional de los sistemas y los activos informáticos conexos;
- Diagrama del modelo de zonas (si se aplica);
- Política y procedimiento para clasificar la información de carácter estratégico.

Pistas para el análisis de los documentos y registros

- Si la gestión de los activos abarca todo el ciclo de vida de estos;
- ¿Qué parte de la organización levantó el inventario?
- ¿Quién mantiene el inventario?
- ¿Quién tiene acceso a él?
- Rastreabilidad de los cambios;
- Protección del inventario (incluidas las copias de respaldo);
- ¿Cómo se lleva a cabo la clasificación de los activos? ¿Se documenta? ¿Cuál es la calidad?
- ¿Están los activos asignados a una zona y se gestionan con arreglo a un 'modelo de zonas'?
- ¿Se han definido 'niveles de seguridad física'? ¿Cuáles son las medidas de seguridad física aplicadas a cada nivel?
- ¿Hay niveles de seguridad física asignados a zonas específicas? ¿En qué se basa esa asignación?
- ¿Corresponde la ubicación física a lo señalado en el inventario?
- ¿En qué medida corresponde el modelo de zonas a la ubicación física de un sistema?
- ¿Cómo están etiquetados los activos según la clasificación por dominio funcional?
- ¿Cómo se traduce la clasificación en zonas lógicas (compárese con el enfoque graduado)?
- ¿Está el equipo conectado a más de una zona?

— ¿Se han evaluado las medidas de protección física en términos de la seguridad física informática?
— ¿En qué grado dependen las medidas de protección física de sistemas informáticos y/o de red?

Ejemplos de preguntas para las entrevistas

— ¿Cuáles son las medidas de seguridad física para el nivel observado?
— ¿Tiene usted acceso a la lista de inventario de activos, o puede tenerlo?
— ¿Se permite tener dispositivos externos o privados, y en qué circunstancias? (Pregúntese por los controles de seguridad física establecidos)
— ¿Cómo se resuelven las cuestiones relativas al ciclo de vida (cómo se escoge y mantiene el nuevo equipo y cuál es el proceso de retirada del servicio)?
— ¿Cómo se trata el equipo de propiedad de terceros?

Aspectos que conviene observar

— Verifíquense algunos dispositivos en relación con el diagrama de red;
— ¿Está conectada la computadora a la red adecuada?
— ¿Está correctamente etiquetado el dispositivo, según la política establecida?
— ¿Se aplican las medidas de seguridad física a ese activo?
— Verifíquese la correspondencia del inventario con el equipo *in situ* (p. ej., mediante una verificación aleatoria);
— Contrólese la gestión de las versiones y de la configuración de los parámetros;
— ¿Cómo se gestiona la confidencialidad de los activos y del inventario?
— ¿Desde dónde y cómo se llevan a cabo la administración y el mantenimiento de los activos conectados a una red?

Pistas para el análisis sobre el terreno

— ¿Corresponde la ubicación física a lo señalado en el inventario?
— ¿Corresponde el modelo de zonas a la ubicación física de los sistemas (o de partes de estos)?
— ¿Cómo están etiquetados los activos según la clasificación por dominio funcional?
— ¿Cómo se traduce la clasificación en zonas lógicas o niveles de seguridad física (compárese con el enfoque graduado)?
— ¿Está el equipo conectado a más de una zona?

5.5. SEGURIDAD FÍSICA DE LOS RECURSOS HUMANOS

Descripción del dominio

El objetivo de este dominio de la seguridad física es velar por que los empleados, los contratistas y los terceros usuarios — es decir, todo el personal con responsabilidades dentro de la organización — comprendan sus funciones y responsabilidades respecto del uso de las computadoras y de la seguridad física informática. Las responsabilidades referentes a la seguridad física deben aclararse antes de la contratación, establecerse como condiciones del empleo y mantenerse durante todo el empleo o contrato de la persona.

Es aconsejable aplicar la evaluación de la probidad (denominada también investigación del personal) a todos los candidatos a un empleo, contratistas y terceros usuarios, según corresponda a su nivel de acceso a datos y sistemas de carácter estratégico. También se recomienda que los empleados, contratistas y terceros usuarios de instalaciones de procesamiento de información firmen un acuerdo sobre sus funciones y responsabilidades de seguridad física y participen en programas de capacitación adecuados a sus responsabilidades. Este aspecto puede estar sujeto a la legislación nacional pertinente, que deberá tomarse en consideración.

El programa de sensibilización sobre la seguridad física informática es un proceso continuo promovido por la administración.

Documentos y registros de interés

- Política y procedimientos relativos al uso y la seguridad física de los sistemas informática para los empleados, contratistas y subcontratistas;
- Registros que indiquen la gestión del personal en lo referente al uso y la seguridad física de los sistemas informáticos;
- Medidas adoptadas para controlar la compatibilidad de los privilegios con la categoría de los empleados (la gestión de los derechos de acceso con arreglo a la función);
- Política y procedimiento para la capacitación del personal (de orientación, según la función, de actualización de los conocimientos);
- Registros de la certificación/cualificación y requisitos para la colocación profesional de los miembros del grupo de seguridad física informática.

Pistas para el análisis de los documentos y registros

- ¿Con qué frecuencia se somete el personal a programas de sensibilización sobre la seguridad física informática?
- ¿Cuál es el procedimiento para tener acceso a las computadoras, las aplicaciones y los datos?
- ¿Cuál es el proceso para tener acceso a datos y aplicaciones de carácter estratégico?
- ¿Cómo se evalúa la eficacia de la cultura de la seguridad física informática?
- ¿Existe un directorio del personal en línea? ¿En qué formato, y qué información contiene?
- ¿Cuál es la política de la empresa con respecto al uso de los medios sociales?
- ¿Para cuáles empleados se exige la verificación de la probidad?
- ¿Cuáles son las consecuencias si se violan los procedimientos de seguridad física?
- ¿Son adecuadas las sanciones previstas, y se aplican correctamente? ¿Se recompensa debidamente el buen comportamiento?
- ¿Se han definido un ‘aviso del acuerdo de uso’ o una ‘política de usos aceptables de la tecnología’? Estas medidas pueden aplicarse mediante una pantalla de inicio que se abra al acceder a una cuenta informática;
- ¿Tienen las computadoras, cuando procede, un protector de pantalla con contraseña? ¿Cuál es el tiempo fijado para su activación?

Ejemplos de preguntas para las entrevistas

- ¿Con qué frecuencia se somete el personal a programas de sensibilización sobre la seguridad física informática?
- ¿Cuál es el procedimiento para obtener acceso a las computadoras, las aplicaciones y los datos?
- ¿Cuál es el proceso para obtener acceso a datos y aplicaciones de carácter estratégico?
- ¿Cuál es el proceso para informar sobre un posible incidente de seguridad física informática?
- ¿Cómo se estimula la notificación por el propio personal interesado de los posibles incidentes de seguridad física informática?
- ¿Cuáles son las consecuencias si se violan los procedimientos de seguridad física?

Aspectos que conviene observar

- Contrólense el acuerdo de acceso a las computadoras y/o la política del usuario;
- Verifíquense las certificaciones/los registros de la capacitación sobre seguridad física informática;
- Verifíquense las características de las cuentas en función del trabajo desempeñado en una muestra aleatoria de empleados/contratistas (p. ej., contrólese la autorización oficial en el caso de los empleados que tengan que ver con un sistema de seguridad tecnológica);
- Contrólese el estado de la cuenta de los empleados que han dejado recientemente la organización;
- ¿Son adecuadas las sanciones previstas, y se aplican correctamente? ¿Se recompensa debidamente el buen comportamiento?
- ¿Presentan todas las computadoras un 'aviso del acuerdo de uso' o la 'política de usos aceptables de la tecnología' durante el acceso a las cuentas?
- Cuando procede, ¿tienen las computadoras un protector de pantalla con contraseña? ¿Cuál es el tiempo fijado para su activación?

Pistas para el análisis sobre el terreno

- ¿Podrían una persona, o unas cuantas personas, plantear el riesgo de un punto único de fallo en el proceso?
- ¿Cómo se gestionan los derechos de acceso de las personas trasladadas o despedidas?
- ¿Cómo promueve la organización una cultura activa de la seguridad física informática en la empresa? ¿La hace extensiva a los comportamientos fuera del entorno laboral, por ejemplo al uso de los medios sociales?

5.6. PROTECCIÓN FÍSICA

Descripción del dominio

Este dominio de la seguridad física tiene el objetivo de velar por la protección física de los activos informáticos. Procura prevenir el acceso físico no autorizado a los sistemas cuyo sabotaje pudiera perturbar o interrumpir los servicios o el flujo de la información. La prevención y los controles de seguridad física deben basarse en una evaluación del riesgo y aplicarse utilizando un enfoque graduado. Debe prestarse la debida atención a mitigar la amenaza procedente de agentes internos.

En el caso de los sistemas de I+D, la aplicación de controles físicos es a menudo la única forma de controlar el acceso; en estos sistemas, los controles técnicos pueden no existir o no ser adecuados.

Documentos y registros de interés

- Política/plan de seguridad (o protección) física de la instalación;
- Política/plan de seguridad física informática;
- Diagrama funcional de los sistemas y los activos informáticos conexos;
- Diagrama de la disposición física de las instalaciones;
- Listado/diagrama de la ubicación física de los activos inventariados;
- Diagrama/listado de los controles físicos;
- Diagramas de los cables o conexiones físicas de las redes;
- Procedimientos para los procesos pertinentes de control del acceso físico y la gestión de las listas de acceso;
- Registros del control del acceso físico a espacios y equipos;
- Organigrama y descripciones de puestos.

Pistas para el análisis de los documentos y registros

- Coherencia entre los controles técnicos, los controles administrativos y los controles físicos;
- Coherencia entre el carácter estratégico de las funciones y la protección física de los sistemas o componentes utilizados;
- Idoneidad de la seguridad física informática de los sistemas a cargo de la protección física;
- Idoneidad de la seguridad física informática de los sistemas responsables del control ambiental;
- Verificación de la separación física adecuada de las redes, componentes o equipos con diferentes niveles de seguridad física;
- ¿Se ha caracterizado la amenaza, y son adecuados los controles que se aplican?
- Determinación de las restricciones del acceso que se basan exclusivamente en procedimientos (es decir, en controles administrativos).

Ejemplos de preguntas para las entrevistas

- ¿Cuáles son las áreas designadas como zonas controladas/estratégicas?
- Describa los mecanismos técnicos y de procedimiento para el control del acceso a cada zona controlada/estratégica;
- ¿Son adecuadas las medidas de protección física para los sistemas informáticos de interés?
- ¿Cuáles son las amenazas físicas percibidas por la organización (también en términos de los recursos y motivos, y sin olvidar la amenaza interna)?
- ¿Cuál es la política de acceso o de escolta de terceros que trabajen en zonas controladas?
- ¿Cuál es la política respecto de los reproductores portátiles y los dispositivos electrónicos de mano en las zonas controladas?
- ¿Cuál es el proceso de disposición final del equipo informático averiado o sustituido?

— ¿Cuál es el proceso de disposición final de los medios electrónicos?

— ¿Cuál es el procedimiento para sacar equipo informático y medios electrónicos del emplazamiento (p. ej., para llevarse una computadora portátil a casa por motivos de trabajo)?

— ¿Cuál es el procedimiento para entrar con equipo externo (es decir, no perteneciente a la instalación), como una computadora portátil o un lápiz de memoria, que se necesite para el trabajo?

— ¿Cuáles son los controles físicos y administrativos relacionados con la protección del entorno informático?

Aspectos que conviene observar

— Obsérvense los medios y procedimientos de control del acceso en acción;

— Verifíquese que el personal autorizado para acceder físicamente a los activos informáticos sea el mínimo necesario. Debe llevarse una lista de control del acceso que indique las personas con acceso físico autorizado, y esa lista debe estar a disposición del personal de seguridad;

— Obsérvense la protección de los alambres y cables, los gabinetes eléctricos, los soportes de bobinas de cables y los tableros de distribución, y cómo están atados los cables. Téngase presente que el equipo de las redes puede estar situado en zonas de usos múltiples, y no sólo en las salas de servidores. ¿Se encuentra el equipo en una zona segura? ¿Quién tiene acceso a ella?

— ¿Qué dispositivos de seguridad física del equipo se utilizan (dispositivos de detección de manipulaciones ilícitas, dispositivos de bloqueo físico, alarmas, vigilancia por vídeo, etc.)?

— Obsérvese la aplicación de las medidas de procedimiento para la protección (el uso de placas, escoltas, líneas pintadas que no se deben cruzar, la aplicación de la regla de las dos personas, etc.);

— Obsérvese el uso de dispositivos de TI personales, como teléfonos inteligentes, computadoras portátiles, tabletas, reproductores portátiles, etc.);

— Obsérvese la ubicación de los terminales de computadoras: ¿están situados de modo que se impida la vista no autorizada de las pantallas y los teclados?

— ¿Se dejan medios informáticos sobre los escritorios, sin supervisión?

— ¿Cuáles medidas de seguridad se aplican en torno a la infraestructura de apoyo de la infraestructura informática (como los controles de seguridad física de la ventilación y la refrigeración, el suministro eléctrico principal y de reserva, etc.)?

— ¿Cómo se realizan el etiquetado, el inventario y el rastreo de las distintas partes del equipo?

Pistas para el análisis sobre el terreno

— Realícese un análisis conjunto de los controles físicos y los controles administrativos;

— Examínese la amenaza interna, y qué se puede lograr con el acceso físico a los recursos informáticos;

— Obsérvese a las personas que entran con dispositivos informáticos personales, como teléfonos inteligentes, computadoras portátiles, tabletas, reproductores portátiles, etc.);

— Verifíquese la coherencia del control del acceso lógico y el control del acceso físico;

— Contrólese si el acceso físico a (determinados) sistemas de I+C está conectado a una alarma. ¿Dónde suena la alarma? ¿Cuál es la actuación normal ante una alarma?

5.7. GESTIÓN DE LAS COMUNICACIONES Y LAS OPERACIONES INFORMÁTICAS

Descripción del dominio

El principal objetivo de este dominio de la seguridad física es controlar la infiltración y exfiltración de datos desde y hacia los sistemas informáticos incluidos en el programa de seguridad física informática, para protegerlos contra la introducción de nuevas vulnerabilidades y controlar los procedimientos operacionales a fin de velar por que el sistema funcione y esté protegido como corresponde. Otro objetivo es proteger la integridad de las computadoras y las comunicaciones.

Documentos y registros de interés

- Diagramas de flujo de datos que indiquen la interconexión de las redes y el flujo de datos;
- Política y procedimiento para la gestión de la configuración;
- Diagrama de la arquitectura de red;
- Política y procedimiento para la reconfiguración de las computadoras o redes;
- Política y procedimiento para la securización de los sistemas informáticos;
- Política y procedimiento para los medios digitales: acceso, etiquetado, almacenamiento, transporte y sanitización;
- Política y procedimiento para la verificación y validación de los controles de seguridad física aplicados a las computadoras y las redes incluidas en los programas de seguridad física informática;
- Registros de la cualificación/certificación de las personas que realizan las pruebas de verificación y validación;
- Política y procedimiento para la divulgación de información al exterior/al público (p.ej., en el sitio web de la empresa);
- Política y procedimiento para el manejo de la información de dominio público;
- Política y procedimiento para la gestión de la prestación de servicios por terceros respecto de todas las clases de computadoras y redes incluidas en el programa de seguridad física informática;
- Acuerdos con terceros referentes a las redes de la instalación a las que pueden acceder los terceros y a sus soluciones de seguridad física;
- Política y procedimiento para tratar con contratistas externos;
- Política y procedimiento para la vigilancia y evaluación continuas del programa de seguridad física informática;
- Política y procedimiento para el intercambio digital de información dentro de la propia instalación y con instalaciones externas;
- Política y procedimiento para las exenciones del programa de seguridad física informática, incluido el registro de esas exenciones;
- Política y procedimiento para el uso de dispositivos inalámbricos, dispositivos móviles y medios extraíbles;
- Política y procedimiento para las restricciones del uso y la aplicación de tecnologías inalámbricas;

— Política y procedimiento para realizar escaneos con el fin de detectar conexiones inalámbricas y puntos de acceso inalámbricos no autorizados;

— Política y procedimiento para gestionar el descubrimiento de conexiones o puntos de acceso inalámbricos no autorizados;

— Política y procedimiento para el uso de dispositivos informáticos portátiles, incluidos los teléfonos móviles;

— Política y procedimiento para la vigilancia y evaluación continuas de las conexiones a redes inseguras y falsas;

— Política y procedimiento, y descripción de los métodos utilizados, para detectar el uso no autorizado de sistemas y/o redes, o el acceso a ellos;

— También puede ser útil realizar una búsqueda en la información de libre acceso para evaluar la información de dominio público sobre la instalación u organización que pudiera plantear un riesgo para la seguridad física informática.

Pistas para el análisis de los documentos y registros

— Examínense los procedimientos aprobados que aplica el personal de operación y mantenimiento para la seguridad física intrínseca, y su compatibilidad con la política y el plan de seguridad física;

— ¿Incluyen los procedimientos de seguridad física los diferentes modos de operación de la instalación, para cubrir los distintos problemas de seguridad física a los que pueden dar lugar?

— ¿Cubren los procedimientos recopilados los aspectos de la seguridad física para los que se elaboraron?

— ¿Ha realizado la instalación anfitriona un análisis efectivo para cerciorarse de que esos controles de seguridad física funcionan y protegen tal como debieran?

— ¿Ha evaluado la instalación anfitriona los efectos que tendría la elusión de los controles de seguridad física en el dominio de la gestión de las comunicaciones y las operaciones?

— ¿Ha evaluado la instalación anfitriona los efectos que tendría la elusión de los controles de seguridad física relacionados con actividades realizadas a distancia o por terceros (incluido el mantenimiento)?

— ¿Ha configurado la instalación anfitriona sus computadoras del modo adecuado para reducir las vulnerabilidades conocidas en ese momento?

— ¿Se aplica el concepto del ‘mínimo privilegio’?

— ¿Tiene la instalación anfitriona un programa de análisis y ensayos de la seguridad física (que utilice un análisis de la vulnerabilidad, pruebas de penetración u otros medios) para estudiar las posibles vulnerabilidades conocidas y desconocidas? ¿Cuál es el alcance del programa de ensayos?

— ¿Se exige a los contratistas y subcontratistas que apliquen la política de seguridad física informática?

Ejemplos de preguntas para las entrevistas

— ¿Cuál es el procedimiento para salir del emplazamiento con equipo y medios informáticos (p.ej., para llevarse un computador portátil a casa por motivos de trabajo)?

— ¿Cuál es el procedimiento para entrar en el emplazamiento con equipo externo (es decir, no perteneciente a la instalación), como una computadora portátil, un lápiz de memoria o un teléfono inteligente, que se necesite en el trabajo?

Aspectos que conviene observar

— Verifíquese que la instalación anfitriona haya configurado sus computadoras aplicando el principio del mínimo privilegio y un proceso para analizar y mitigar las vulnerabilidades conocidas en ese momento;

— Obsérvese el resultado de los procedimientos;

— Identifíquese toda indicación de entidades o de conectividad externas (p. ej., con fines de respaldo o vigilancia);

— Realícense inspecciones al azar en busca de computadoras portátiles y dispositivos móviles y pregúntese por su uso;

— Verifíquese la congruencia entre los sistemas, las aplicaciones, la arquitectura de red y otros elementos documentados y los que se encuentra efectivamente en el emplazamiento.

Pistas para el análisis sobre el terreno

— Examínese si el análisis del riesgo abarca realmente todos los riesgos relacionados con las comunicaciones por red y los dispositivos móviles;

— Considérese la siguiente pregunta: ¿Cuál es el principal reto pendiente?

5.8. CONTROLES DEL ACCESO INFORMÁTICO

Descripción del dominio

El objetivo de este dominio de la seguridad física es controlar (por medios técnicos y administrativos) el acceso lógico a los sistemas informáticos o a la información electrónica.

Este dominio se ocupa de los requisitos relacionados con el control del acceso, la gestión del acceso de los usuarios, las responsabilidades del usuario, el control del acceso a las redes, el control del acceso al sistema operativo, el control del acceso a las aplicaciones y la información, y la computación móvil y el teletrabajo.

El acceso a los sistemas informáticos (los sistemas de I+C, los sistemas de supervisión, los sistemas técnicos, los sistemas de seguridad física y los sistemas empresariales) se controla con arreglo a lo establecido en el plan de seguridad física informática.

Las reglas para el control del acceso lógico a computadoras y redes se establecen mediante un proceso de autorización oficial.

Documentos y registros de interés

— Plan de seguridad física informática;

— Política y procedimiento para el control del acceso informático (gestión de los derechos, gestión de las cuentas);

— Registro de los resultados de las auditorías del control del acceso, si se han efectuado;

— Política y procedimiento para examinar la autorización del acceso a los sistemas, incluidos los privilegios;

— Organigrama para la gestión de los derechos de administrador de los sistemas informáticos;
— Política y procedimiento para las contraseñas (complejidad, duración, y política de bloqueo de la cuenta);
— Política y procedimiento para la concesión y documentación de los privilegios;
— Descripción de los mecanismos de autenticación empleados;
— Registros del control del acceso y documentación de la vigilancia;
— Política y procedimiento para la autorización y contabilidad de cuentas;
— Política de acceso a las redes — seguridad física de los conmutadores, conectores no conectados, etc.;
— Política de acceso a las redes — uso de LAN virtuales;
— Topologías de las redes y el tráfico;
— Política relativa a las puertas de enlace de seguridad — listas de control del acceso en los enrutadores, normas de contrafuegos;
— Diagrama/listado de los puntos de acceso inalámbrico;
— Política y procedimiento para el acceso remoto (quién, cuándo, por qué motivo, para cuáles servicios);
— Política y procedimiento para el uso y la seguridad física de los módems;
— Política y procedimiento para las cuentas de administrador o de altos privilegios.

Pistas para el análisis de los documentos y registros

— En los casos en que no sea posible aplicar las medidas técnicas de control del acceso requeridas (como las contraseñas) en determinados componentes de la I+C, por motivos ya sea técnicos o de ejecución operacional, verifíquese que se empleen medidas correctivas (p. ej., procedimientos adaptados, seguridad física aumentada, seguridad física del personal, detección de intrusiones y medidas de auditoría) que sean acordes con el nivel de seguridad física del sistema de I+C;
— Compruébese la coherencia entre los controles técnicos, los controles administrativos y los controles físicos;
— Para los sistemas de I+C, préstese particular atención a los métodos y los casos de acceso remoto en que se hayan aplicado tecnologías inalámbricas y móviles;
— En las tecnologías inalámbricas, ¿existe una política de uso para el acceso y un programa de evaluación que garantice su cumplimiento?
— Verifíquese si se aplican políticas de 'segregación de funciones' y 'mínimo privilegio' de tipo técnico o administrativo. Concretamente, para los sistemas de I+C y los sistemas heredados esenciales, si no se aplican esas políticas, verifíquese que existan medidas correctivas.

Ejemplos de preguntas para las entrevistas

— ¿A cuáles sistemas accede el personal que realiza determinadas funciones?
— ¿A cuáles de estos sistemas se accede a distancia? ¿Con qué frecuencia se accede a ellos? ¿Por qué se accede a distancia?
— Contrólese si hay delegaciones o concesiones de derechos de acceso no previstas en el procedimiento;

— ¿Cuál es la percepción de la política de control del acceso? ¿Es demasiado estricta o demasiado laxa? ¿Responde a las necesidades operacionales?

— Determínense las cuestiones o los problemas que surgen con frecuencia en el control del acceso y que no se resuelven adecuadamente (se sortean);

— ¿Cuál es el proceso para la concesión/obtención del acceso informático? ¿Cuáles son los procesos de revocación y renovación?

— Determínese si se eluden los controles del acceso para aumentar la eficiencia operacional (o por comodidad) en algunos casos;

— ¿Qué incidentes — o incluso anécdotas — han ocurrido con el control del acceso?

— ¿Tiene el administrador dos cuentas (de administrador y de usuario)?

— ¿Cómo gestiona la organización los cambios en la situación del personal (p.ej., los cambios de departamento, los cambios de funciones, etc.)?

Aspectos que conviene observar

— Solicítese que se demuestren los medios y procedimientos de aplicación del control del acceso;

— Verifíquese si existen formas de delegar o conceder derechos de acceso que no estén previstas en el procedimiento establecido;

— Verifíquense las listas de control del acceso lógico para comprobar que el número de personas con acceso autorizado se mantenga en el mínimo necesario;

— Realícense inspecciones en busca de módems y puntos de acceso inalámbrico;

— Contrólese la actividad inalámbrica;

— Realícense inspecciones en busca de puertos de conexión accesibles;

— Determínense los posibles puntos de conexión para la monitorización pasiva;

— Búsquense sistemas y estaciones de trabajo no bloqueados;

— Búsquense sistemas sin contraseña, con cuentas por defecto o con una contraseña obvia;

— Verifíquese si existen banderolas que informan a los usuarios sobre los tipos de uso autorizados;

— Verifíquese cómo se logra la segregación de la red (segregación lógica, segregación física, aislamiento físico total);

— Contrólense la arquitectura de red y especialmente las interfaces entre los dominios de la seguridad física;

— Determínense las vías por las que se podrían comprometer los sistemas críticos (seguridad tecnológica, control) desde redes empresariales o corporativas, o de otras formas;

— Determínense las cuestiones o los problemas que surgen con frecuencia en el control del acceso y que no se resuelven adecuadamente (se sortean);

— Búsquense mecanismos de autenticación no documentados;

— Investíguense los procedimientos de inicio de sesión; ¿existe un mecanismo claro de autenticación de textos?

— ¿Hay cuentas y contraseñas compartidas entre el personal? ¿Se utilizan cuentas colectivas?

— Pídase el programa de actividades para el período de la evaluación, y selecciónense algunas actividades para su observación, como el parcheado, la parametrización, la instalación de programas informáticos, etc.

Pistas para el análisis sobre el terreno

- ¿Cuántas contraseñas diferentes tiene que utilizar una persona en las operaciones cotidianas? ¿Cuántas en operaciones especiales? (Demasiadas contraseñas pueden conducir al uso de notas adhesivas, etc.)
- ¿Cierra el personal la sesión o bloquea su cuenta cuanto deja su computador, si se aplica?
- ¿Cómo se maneja la rastreabilidad, si se utilizan cuentas colectivas/compartidas?
- ¿Cómo se garantiza la complejidad de la contraseña?
- ¿Cómo es la coherencia entre el control del acceso lógico y el del acceso físico?

5.9. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS INFORMÁTICOS

Descripción del dominio

El objetivo de este dominio de la seguridad física es garantizar la seguridad física y la integridad de los sistemas informáticos que se adquieren, y las actividades de mantenimiento que debe realizar el proveedor cuando el sistema se ha puesto en servicio. Los controles de seguridad física incluidos en este dominio comprenden la protección de la cadena de suministro, las verificaciones de la corrección de los programas informáticos, la integración de mecanismos de seguridad física, los ensayos de fábrica y las pruebas de aceptación.

Debe tomarse especial nota de las actividades de mantenimiento de los sistemas informáticos. Estas actividades deben evaluarse para comprobar que existan suficientes controles que protejan contra la introducción de vulnerabilidades o software maligno. Además, se aconseja que se evalúe la tempestividad y eficacia de las actividades de mantenimiento de los sistemas informáticos, como el parcheado.

Documentos y registros de interés

- Política y procedimiento para la adquisición de sistemas y servicios, incluida la elaboración de los requisitos de seguridad física para los sistemas adquiridos o desarrollados;
- Descripción de los requisitos relativos al establecimiento de medidas de seguridad física para la protección contra la vulnerabilidad y la introducción de amenazas a través de la cadena de suministro;
- Descripción de los requisitos de que los proveedores empleen métodos de calidad y validación de los programas informáticos para reducir al mínimo el software defectuoso o mal diseñado;
- Descripción o demostración del modo en que la instalación vela por que los nuevos sistemas adquiridos contengan suficiente información sobre el diseño o los medios de seguridad física, o ambas cosas, para poder aplicar y mantener los controles de seguridad requeridos;
- Descripción o demostración de los requisitos de seguridad física para crear, ejecutar y documentar pruebas de seguridad y planes de evaluación que garanticen que los productos adquiridos cumplen con todos los requisitos de seguridad física especificados;
- Descripción o demostración de los requisitos de seguridad física para mantener la integridad del sistema adquirido hasta su entrega en la instalación. Descripción de cómo verifica y controla la instalación que el programa de seguridad física aplicado al sistema informático antes de su entrega sea como mínimo del mismo nivel que el que se aplicará cuando esté en funcionamiento;

— Plan y resultados de los ensayos de verificación y validación del código con arreglo a los requisitos del diseño y la configuración de la seguridad física;

— Procedimientos para las pruebas de aceptación del equipo informático/electrónico;

— Documento sobre los requisitos de aplicación y mantenimiento de medidas de seguridad física informática;

— Plan y resultados de los ensayos de validación para evaluar la eficacia de las medidas de seguridad física informática aplicadas;

— Diseño y metodología para la seguridad física informática, que describan las características de seguridad física incorporadas en el diseño a fin de cumplir los requisitos establecidos para las computadoras;

— Registros del mantenimiento de los sistemas informáticos;

— Programas de mantenimiento que indiquen las tareas relacionadas con la seguridad física informática por orden de prioridad.

Pistas para el análisis de los documentos y registros

— Verifíquese que la seguridad física informática está siendo gestionada debidamente por las terceras partes interesadas;

— Verifíquese la seguridad física a lo largo de la cadena de adquisición y desarrollo, tomando en consideración que puede haber numerosos contratistas, subcontratistas, etc.

Ejemplos de preguntas para las entrevistas

— ¿Qué controles se aplican al equipo en el emplazamiento antes de su instalación y durante ella?

— ¿Cuáles ensayos se realizan para evaluar las funciones de seguridad física — en los locales del proveedor y después de la instalación?

— ¿Qué controles existen para velar por que no se introduzcan en el sistema vulnerabilidades o exploits tales como software maligno durante las actividades de mantenimiento?

— ¿Cómo se vigilan en el emplazamiento las actividades de mantenimiento realizadas por terceros?

— Pruebas de las inspecciones de la seguridad física en el emplazamiento del proveedor y del registro del cumplimiento de los requisitos de seguridad física.

Aspectos que conviene observar

— ¿Qué controles se aplican al equipo en el emplazamiento antes de su instalación y durante ella?

— ¿Cómo se comunica la información de carácter estratégico entre el proveedor y la instalación?

Nota: Este dominio es difícil de observar sobre el terreno, ya que se relaciona principalmente con terceros y con un período anterior a la entrega de los sistemas.

Pistas para el análisis sobre el terreno

— Obsérvese una actividad de mantenimiento de la seguridad física realizada por personal interno o por terceros contratistas.

5.10 GESTIÓN DE INCIDENTES DE SEGURIDAD FÍSICA INFORMÁTICA

Descripción del dominio

Los incidentes de seguridad física informática pueden ocurrir aun cuando la organización se empeñe al máximo por evitarlos. El objetivo de este dominio de la seguridad física es velar por que existan procesos para la mitigación de los posibles efectos y la comunicación eficaz de esos incidentes.

Según la publicación Nº 17 de la *Colección de Seguridad Física Nuclear del OIEA* [3], un incidente de seguridad física informática es un suceso que pone en peligro, real o potencialmente, la confidencialidad, integridad o disponibilidad de un sistema de información basado en una computadora, en red o digital, o de la información procesada, almacenada o transmitida por dicho sistema, o bien que constituye una violación o un riesgo inminente de violación de las políticas o los procedimientos de seguridad, o de las políticas sobre usos aceptables.

Documentos y registros de interés

- Política y procedimiento para la gestión de incidentes;
- Plan de comunicación de incidentes;
- Solicitudes al servicio de asistencia de TI (resguardos);
- Demostración de la evaluación de la seguridad física en sucesos no planificados de parada de la instalación o de los sistemas (evaluaciones de la causa raíz);
- Ejemplo o modelo de un informe de incidente (de preferencia, un informe real);
- Procedimiento/consideraciones con respecto a los efectos transdominio de la respuesta a un incidente (por ejemplo, las medidas adoptadas en un sistema de TI empresarial después de un incidente de seguridad física pueden no ser aceptables en un entorno de I+C);
- Plan y procedimientos de respuesta a incidentes;
- Registros y medidas subsiguientes resultantes de la realización de ejercicios para evaluar la eficacia del plan de respuesta a incidentes.

Pistas para el análisis de los documentos y registros

- ¿Se tienen debidamente en cuenta en la gestión de incidentes de seguridad física informática las amenazas externas y las amenazas internas (es decir, las causadas por agentes internos)?
- ¿Existe un sistema de clasificación claro para caracterizar los incidentes?
- ¿Existe un procedimiento claramente definido para la progresión en la respuesta a un incidente (criterios, puntos de contacto)?
- El proceso de comunicación se ocupa de las comunicaciones internas (entre otros, con los responsables de la gestión general de los incidentes en la instalación) y de las comunicaciones externas (los vínculos con los grupos de respuesta a emergencias informáticas (CERT) y las autoridades nacionales e internacionales);
- ¿Se han elaborado procedimientos de investigación forense, preservación de huellas, etc. y adaptado para que respalden la investigación?
- Evalúense el proceso de rehabilitación, y la definición y aplicación de medidas correctivas;
- Compruébese la coherencia entre la gestión del incidente y la gestión de la continuidad;

— Compruébese el enlace entre los responsables de la gestión del incidente de seguridad física informática y los responsables de la gestión general de los incidentes en la instalación;

— ¿Ha ejecutado la instalación los planes y procedimientos de respuesta a incidentes como parte de su ejercicio de autoevaluación (en simulaciones o simulacros)?

— ¿Ha participado la instalación en algún ejercicio coordinado de respuesta a incidentes de seguridad física informática junto con organizaciones externas?

— ¿Se han incorporado los requisitos de la preservación de pruebas y la cadena de custodia en el plan y los procedimientos de respuesta a incidentes de seguridad física informática?

Ejemplos de preguntas para las entrevistas

— Contrólese el conocimiento del procedimiento, y en particular del punto de contacto, de los empleados y contratistas en caso de incidente de seguridad física;

— Describa qué constituye un incidente de seguridad física. ¿Cómo se categorizan los incidentes de seguridad física?

— ¿Cuándo, y en qué circunstancias, debe notificarse un incidente? ¿Cuáles entidades externas deben ser informadas?

— ¿Qué procedimiento debe aplicar un empleado o contratista que descubra una desviación en la aplicación de los controles de seguridad física?

— ¿Ha sufrido la instalación algún incidente de seguridad física (informática)?

— ¿Puede describir qué se ha hecho o modificado después de un incidente de seguridad física informática reciente?

— ¿Se consideran eficaces los procesos existentes? ¿Cuáles aspectos siguen siendo problemáticos?

— ¿Cómo y con qué frecuencia se ejercitan los planes y procedimientos de respuesta a incidentes?

— ¿Ha participado la instalación en algún ejercicio coordinado de respuesta a incidentes informáticos a nivel de una instalación, del Estado o internacional?

Aspectos que conviene observar

— Solicítese una demostración del sistema específico de seguimiento de la gestión de incidentes (en papel o en una aplicación informática).

Pistas para el análisis sobre el terreno

— Evalúese si el personal ha recibido suficiente capacitación en el procedimiento.

5.11 GESTIÓN DE LA CONTINUIDAD

Descripción del dominio

El objetivo general de este dominio de la seguridad física es la continuidad y el restablecimiento de las funciones de importancia crítica de una instalación después de una perturbación importante de los sistemas y procesos informáticos normales. Estas perturbaciones pueden ser causadas por peligros naturales, errores humanos y actos dolosos.

Obsérvese que la sección sobre la gestión de incidentes de seguridad física informática se refiere a la respuesta inicial y la mitigación en caso de incidente, mientras que el presente dominio se centra en la continuidad y en el proceso de recuperación.

Documentos y registros de interés

- Políticas y procedimientos para la gestión de la continuidad;
- Lista de las aplicaciones y sistemas que tienen una gestión de la continuidad, y lista de sus propietarios y/o de las responsabilidades;
- Continuidad de los registros de capacitación en las operaciones (incluidos los informes de ejercicios);
- Continuidad del plan de operaciones.

Pistas para el análisis de los documentos y registros

- Determínese cómo está integrada la gestión de la continuidad relacionada con la seguridad física informática en los programas de continuidad de las operaciones existentes en la instalación (p. ej., a través de un plan de continuidad de las actividades en el emplazamiento);
- Obsérvese que la gestión de la continuidad se tiene en cuenta en el diseño básico y las especificaciones técnicas de los sistemas de seguridad y funcionamiento de la I+C. Se recomienda que estas especificaciones se tomen en consideración al evaluar la gestión de la continuidad de los sistemas de seguridad y funcionamiento de la I+C. Esto puede no aplicarse a otros dominios funcionales. Para los sistemas de I+C que cumplan funciones de seguridad tecnológica o física importantes, dos características de diseño fundamentales que deben considerarse al determinar las medidas de gestión de la continuidad son el tiempo medio entre fallos y el tiempo medio de reparación;
- ¿Están identificados los subsistemas y las interdependencias importantes? ¿Son suficientes los acuerdos contractuales para respaldar los objetivos de la continuidad?
- ¿Tienen los sistemas y las funciones importantes un nivel apropiado de diversificación y redundancia?
- ¿Se tiene debidamente en cuenta la dimensión dolosa (el ataque intencional, en contraposición a un fallo accidental) en la gestión de la continuidad?
- Compruébese la coherencia entre la gestión del incidente y la gestión de la continuidad.

Ejemplos de preguntas para las entrevistas

- Verifíquese si los planes de ensayos para la continuidad y recuperación de los sistemas informáticos y los procedimientos de recuperación (p. ej., la restauración y actualización de los datos entre la parada y el reinicio) se conocen, aplican y revisan;
- ¿Ha recibido el personal capacitación en la recuperación de sistemas y la gestión de la continuidad? ¿Quién la ha recibido? ¿Cómo se trata en la gestión de la continuidad la cuestión de la prioridad en el acceso y los recursos durante una degradación operacional?
- ¿Ha realizado la instalación ejercicios de capacitación centrados en la recuperación de sistemas y la gestión de la continuidad en el caso de un suceso cibernético?
- ¿Existen sistemas de respaldo para cumplir las funciones informáticas importantes en caso de incidente/accidente?
- ¿Cuáles controles de seguridad se aplican a los sistemas de respaldo?

— ¿Cuál es el nexo arquitectónico con los sistemas de respaldo?
— ¿Existen procedimientos para operar tras la pérdida de las funciones informáticas?

Aspectos que conviene observar

— Verifíquese que los empleados tienen acceso a los procedimientos de continuidad pertinentes;
— La evaluación podría seleccionar un subconjunto de controles de la gestión de la continuidad para examinarlos, como los procedimientos de respaldo y de restauración, los medios de comunicación alternativos (en particular para la respuesta a una emergencia) y los acuerdos de priorización de los contratistas;
— Solicítese el informe del ejercicio más reciente;
— Obsérvense las instalaciones de control alternativo y de respaldo, si existen.

Pistas para el análisis sobre el terreno

— Obsérvese la ejecución de un procedimiento de recuperación, ya sea en el sistema, en un laboratorio de desarrollo o mediante un proceso "en papel";
— ¿Está actualizada la información sobre la configuración de la central? ¿Con qué mecanismo/proceso se actualiza?
— Determínese la pertinencia de la priorización del acceso y los recursos durante una degradación operacional con respecto a los objetivos generales de la instalación.

5.12 CUMPLIMIENTO

Descripción del dominio

Si la evaluación corre a cargo de la autoridad competente, o si se trata de una autoevaluación, el cumplimiento de las obligaciones establecidas en las leyes, estatutos, reglamentos o contratos pertinentes con respecto a la seguridad física informática puede estar incluido en el alcance de la evaluación.

El objetivo de este dominio de la seguridad física es verificar que el programa de seguridad física informática esté en conformidad con esas obligaciones establecidas en las leyes, estatutos, reglamentos o contratos pertinentes.

Obsérvese que este dominio no se aplica en algunos contextos; esto puede tomarse en consideración cuando se planifique el alcance de la evaluación.

Documentos y registros de interés

— Documentos sobre las obligaciones jurídicas, estatutarias, reglamentarias o contractuales que aborden aspectos de la seguridad física informática;
— Informe(s) sobre el cumplimiento de la reglamentación (interno(s) o externo(s));
— Procedimiento/proceso de certificación, si es pertinente para la seguridad física informática;
— Componente de seguridad física informática de la amenaza base de diseño;
— Documentos de orientación sobre el diseño y la modificación de los sistemas (las secciones sobre las restricciones de cumplimiento).

Pistas para el análisis de los documentos y registros

— Cada dominio funcional puede tener diferentes criterios y restricciones de cumplimiento;

— Además, según el país y el tipo de instalación de que se trate, puede ser necesario tener en cuenta varios marcos reguladores, de organismos de diferente nivel en el Estado (p. ej., del organismo regulador de la seguridad tecnológica y de un organismo de seguridad física);

— Algunos aspectos de la seguridad física informática pueden estar integrados en documentos de ámbito más amplio; por ejemplo, puede haber secciones dedicadas a la seguridad física informática en las normas de seguridad tecnológica aplicables;

— ¿Cómo están integrados los requisitos jurídicos y reglamentarios en la política, la organización y los procedimientos referentes a la seguridad física?

— ¿Hay listas de los documentos pertinentes, o claras remisiones a ellos, en la política de seguridad física?

— Los sistemas de I+C suelen tener sus propios documentos de orientación sobre el diseño y la modificación, pero el grupo de evaluación puede analizar esos aspectos en otros dominios (p. ej., la contabilidad de los materiales nucleares o los sistemas relacionados con la respuesta a emergencias).

Ejemplos de preguntas para las entrevistas

— ¿Cómo se definen, rastrean y aplican los requisitos reglamentarios?

— ¿Quién se encarga de esas tareas (definición, rastreo y aplicación)?

— Explique cómo se validan las modificaciones sobre el terreno para determinar sus efectos en el cumplimiento de las obligaciones jurídicas, estatutarias, reglamentarias y contractuales.

Aspectos que conviene observar

— La evaluación podría seleccionar un subconjunto de requisitos de seguridad física informática a partir de las obligaciones jurídicas, estatutarias, reglamentarias y contractuales y validar su aplicación sobre el terreno.

Pistas para el análisis sobre el terreno

— Comiéncese con una pequeña muestra representativa; si se descubren varias discrepancias, se podrá reexaminar la muestra y añadir elementos adicionales.

6. INFORME FINAL Y ACTIVIDADES POSTERIORES A LA EVALUACIÓN

6.1. ELABORACIÓN DEL INFORME FINAL

Uno de los aspectos más importantes de la evaluación es el examen de las observaciones, la determinación de los hallazgos, y la formulación de recomendaciones y sugerencias a la entidad anfitriona. Esta información se recoge en el informe final y se presenta en una reunión informativa final con la instalación o entidad anfitriona.

El formato y el contenido del informe pueden variar según el propósito de la evaluación, pero hay elementos que siempre están presentes, como un resumen ejecutivo, una introducción, y las secciones sobre los resultados y las conclusiones. En el anexo III se ofrece un modelo para el informe de la evaluación. La figura 3 ilustra el proceso de preparación y desarrollo del informe.

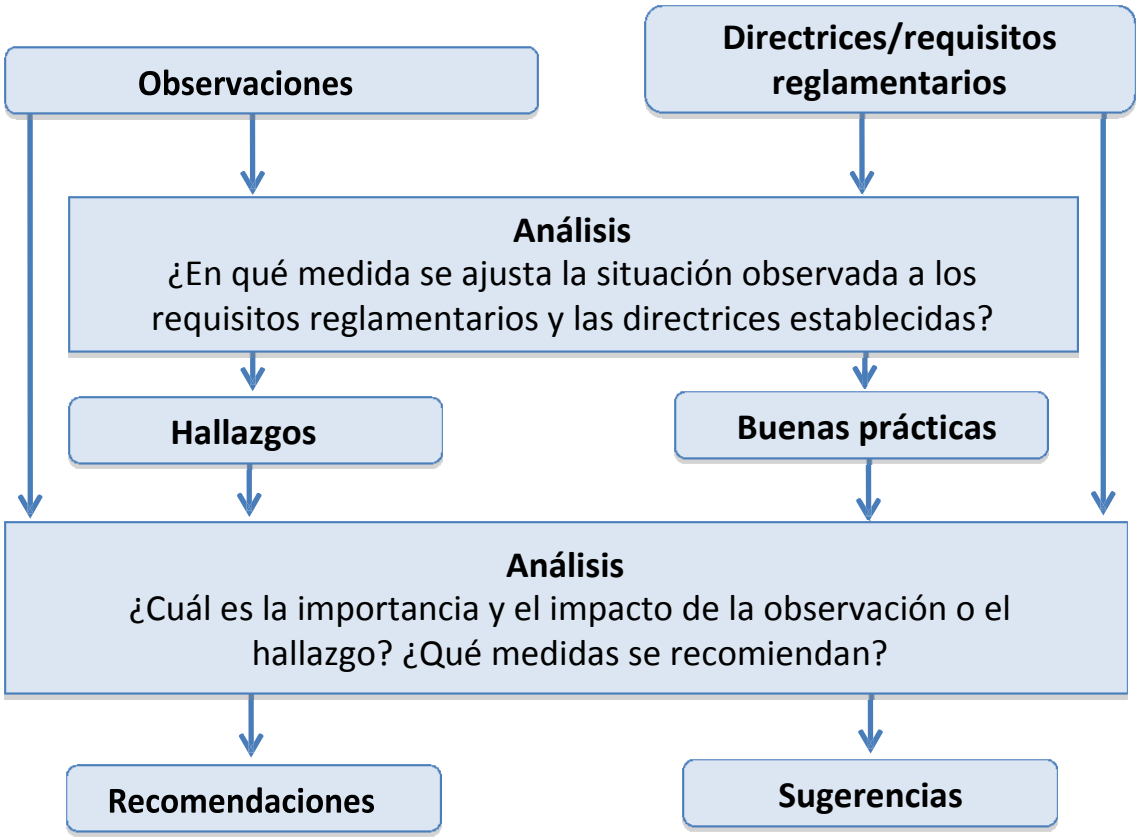

Fig 3. Proceso de análisis de la evaluación.

El componente de recopilación de datos de la evaluación consiste en registrar las observaciones de datos de interés hechas durante el examen de los documentos y registros, las entrevistas y la labor de observación directa. Las observaciones son importantes en sí mismas, pero a veces constituyen también colectivamente un indicador de tendencias en la instalación u organización que puede ser necesario corregir. Durante el examen de las notas de campo pueden agruparse las observaciones parecidas para descubrir tendencias o casos recurrentes.

A continuación, las observaciones se analizan, comparándolas con los requisitos establecidos en los reglamentos nacionales, los procedimientos de la organización y/o las normas internacionales, según corresponda. Se determina la existencia de un hallazgo cuando se detecta el incumplimiento, o una desviación, de un procedimiento reglamentario o interno. La base para determinar que existe un hallazgo tiene que haber sido definida claramente y acordada en las reuniones de planificación preliminares.

También es importante entender que la lista de hallazgos es solo una instantánea de la instalación, basada en un cierto número de observaciones realizadas por el grupo de evaluación. En el análisis de las observaciones y la determinación de los hallazgos deben tenerse en cuenta múltiples factores, entre ellos:

- la profundidad y amplitud de la evaluación;
- la habilidad y experiencia del grupo de evaluación;
- el nivel de acceso ofrecido al grupo de evaluación;
- el nivel de recursos proporcionado para la evaluación, por ejemplo, el tiempo y el número de evaluadores.

Por consiguiente, los hallazgos constituirán una muestra selectiva y no una representación exhaustiva de las prácticas de seguridad física informática de la organización. Un hallazgo confirma la existencia de un problema, pero la ausencia de hallazgos no significa que no existan problemas de seguridad física informática.

Las observaciones no siempre dan lugar a hallazgos, y no todos los hallazgos son adversos. Otro resultado posible es la determinación de una 'buena práctica', es decir, de un proceso o procedimiento de la organización que ofrece un método novedoso y eficaz para cumplir objetivos de seguridad física. Tales prácticas deben definirse y comunicarse como posibles ejemplos para que otras organizaciones mejoren sus propios programas de seguridad física.

Además de los hallazgos y las buenas prácticas, el grupo de evaluación puede también proporcionar otras orientaciones, recomendaciones y sugerencias en el informe en relación con los hallazgos.

Las recomendaciones son orientaciones para el cumplimiento de los requisitos jurídicos y reglamentarios (las leyes o reglamentos nacionales) y/o las normas internacionales, cuando procede. Normalmente, las recomendaciones no indican cómo corregir un problema, sino solo que existe un problema que hay que corregir.

Las sugerencias proporcionan un nivel adicional de información con respecto a un hallazgo, que incluye estrategias correctoras o de mitigación. Esa información no se deriva necesariamente de las orientaciones reglamentarias, sino más bien de las normas técnicas y las buenas prácticas industriales.

Las sugerencias pueden incluir medidas tales como:

- modificaciones del equipo y la instalación de dispositivos y medios adicionales para mejorar la seguridad física;
- mejoras de los procedimientos y medidas administrativas;
- el establecimiento de controles y frenos adicionales;
- la rectificación de deficiencias descubiertas en los procedimientos operacionales;
- la rectificación de deficiencias descubiertas en los documentos de política;
- la capacitación del personal en el desempeño de funciones generales y específicas;
- la introducción de cambios en el entorno de trabajo;
- la introducción de cambios en la planificación y programación del trabajo y/o en las personas asignadas a determinadas tareas.

6.1.1. Análisis de la importancia

En una evaluación, a menudo no basta con determinar la existencia de un hallazgo; al final, es necesario estudiar el impacto o la posible consecuencia de ese hallazgo. La entidad anfitriona tiene que examinar el impacto o la importancia del hallazgo para la seguridad física y

tecnológica. El análisis del impacto puede realizarse a múltiples niveles. El primer nivel examina el impacto del hallazgo por sí solo, procurando determinar específicamente su efecto o importancia en relación con los atributos de la confidencialidad, la integridad y la disponibilidad. El segundo nivel del análisis adopta un enfoque sistemático y examina los hallazgos en su conjunto y el efecto global que pueden tener en una instalación u organización. Este análisis no es trivial y puede requerir la participación de un grupo multidisciplinario que examine todas las ramificaciones de interés para la seguridad tecnológica, la seguridad física, las operaciones, etc.

Normalmente, el grupo de evaluación no aplica este nivel de análisis para un examen reglamentario, en que el análisis se deja en manos de la entidad anfitriona. Sin embargo, ese análisis puede llevarse a cabo conjuntamente con el grupo de evaluación en el caso de las autoevaluaciones o de las misiones de asesoramiento técnico por terceros. Estas evaluaciones requieren una cantidad considerable de tiempo y recursos.

6.2. ELEMENTOS PARA LA PREPARACIÓN DEL INFORME

Según los acuerdos que se hayan concertado respecto de la evaluación, el informe puede presentarse durante la evaluación, por ejemplo proporcionando un proyecto de informe para la reunión informativa final, o con posterioridad a esta.

Con respecto al contenido del informe, deben tenerse en cuenta las siguientes consideraciones:

- Los miembros del grupo deben ser objetivos y basar sus conclusiones en el examen de los documentos pertinentes, las entrevistas del personal clave y la observación directa;
- Los miembros del grupo deben consultar con las contrapartes de la entidad anfitriona para aclarar toda cuestión que no esté clara y asegurarse de que la han entendido correctamente;
- Los miembros del grupo deben consultarse entre sí, y particularmente con el Jefe del grupo, y compartir los resultados de sus hallazgos a fin de evitar la duplicación, las incoherencias y las cuestiones que puedan incidir en otros hallazgos;
- Las conclusiones de los miembros del grupo — en particular las que den lugar a recomendaciones y sugerencias y al reconocimiento de buenas prácticas — deben documentarse en forma concisa y respaldarse con una ‘base’ que sirva de fundamento para justificar una determinada recomendación, sugerencia o buena práctica;
- Debe examinarse el grado de sensibilidad del informe final, sobre la base del carácter estratégico de su contenido, de las vulnerabilidades que pueda revelar (y de las posibles consecuencias de ello), y de cualquier política nacional o de la organización sobre la información de carácter estratégico que se aplique. El grado de sensibilidad del informe deberá estar claramente marcado en el documento, y el informe deberá manejarse en consecuencia.

Cuando comunique un hallazgo, el informe deberá ser claro y, de ser posible, indicar lo siguiente:

- la función y los dominios de la seguridad física pertinentes (puede haber múltiples dominios afectados);
- la orientación y/o la buena práctica utilizada para la evaluación (citando la referencia, si se trata de una orientación);
- el hallazgo;
- el posible impacto del hallazgo (lo que podría considerarse como una clasificación de su gravedad, p. ej., administrativo, de menor importancia, importante, grave, etc.);
- la solución o medida correctiva recomendada.

Los hallazgos pueden también agregarse por funciones y dominios de la seguridad física, para obtener una calificación o evaluación general de esferas colectivas.

El informe indica el grado de confianza del grupo en que la valoración fue suficientemente amplia como para proporcionar una evaluación fiel de la instalación.

Los ámbitos que no se hayan evaluado deberán indicarse.

Con respecto al formato y el estilo del informe, pueden ser útiles las consideraciones siguientes:

- Un resumen inicial que exponga a grandes rasgos las impresiones generales del grupo puede ser útil para poner en perspectiva el examen más detallado de las distintas esferas que se encontrará en las páginas siguientes.
- El lenguaje utilizado tiene que ser sencillo, claro, conciso, objetivo e impersonal.
- Se pueden insertar diagramas y fotografías en las secciones que corresponda. Las figuras que ilustran la estructura de un gobierno u organización — y los diagramas o fotografías que ilustran una deficiencia o una buena práctica — son particularmente útiles.
- Las unidades orgánicas, los cargos y los sistemas deben designarse por sus nombres oficiales (o sus traducciones oficiales).
- Las abreviaciones deben acompañarse de la expresión por extenso la primera vez que se utilicen, y enumerarse y definirse en un cuadro aparte, para facilitar la consulta.

6.3. SESIÓN INFORMATIVA FINAL

Los participantes en la sesión informativa final serán personas pertenecientes a la entidad evaluada, pero también podrán estar presentes otras partes. Si es necesario, el Jefe del grupo de evaluación informará a la entidad evaluada de cualquier situación registrada durante la evaluación que pueda menoscabar la confianza en las conclusiones de la evaluación. Esta reunión será oficial, por lo que deberá levantarse un acta y una lista de los presentes.

REFERENCIAS

[1] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Objetivo y elementos esenciales del régimen de seguridad física nuclear de un Estado*, *Colección de Seguridad Física Nuclear del OIEA* Nº 20, OIEA, Viena (2014).

[2] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Recomendaciones de Seguridad Física Nuclear sobre la Protección Física de los Materiales y las Instalaciones Nucleares*, *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 ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary, ISO/IEC 27000:2009, ISO, Geneva (2009).

[5] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Information Security Management Systems — Requirements, ISO/IEC 27001:2005, ISO, Geneva (2005).

[6] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Code of Practice for Information Security Management, ISO/IEC 27002:2005, ISO, Geneva (2005).

[7] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Information Security Risk Management, ISO/IEC 27005:2008, ISO, Geneva (2008).

[8] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Requirements for Bodies Providing Audit and Certification of Information Security Management Systems, ISO/IEC 27006:2007, ISO, Geneva (2007).

[9] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Guidelines for auditing management systems, ISO 19011:2011, ISO, Geneva (2011).

[10] UNITED STATES NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Technical Guide to Information Security Testing and Assessment, NIST Special Publication 800–115, Gaithersburg, Maryland, USA (2008).

GLOSARIO

A continuación se definen algunos términos que se utilizan en la presente publicación. Cuando existen, se han tomado las definiciones dadas en otras publicaciones del OIEA o en normas internacionales. En esos casos, la definición comprende una referencia a la publicación pertinente (que se encontrará en la sección titulada Referencias, al final del cuerpo del documento).

Buena práctica. Programa, actividad, forma de utilizar un equipo u otra práctica que ha demostrado ser excelente y que contribuye directa o indirectamente a la seguridad operacional tecnológica o física, así como al mantenimiento del buen desempeño. Una buena práctica es notablemente superior al comportamiento previsto, y no es simplemente el cumplimiento de los requisitos vigentes.

Computadoras y sistemas informáticos. Dispositivos de computación, comunicación e instrumentación y control que conforman los elementos funcionales de la instalación nuclear. Comprenden no sólo las computadoras de mesa, los grandes sistemas de computadoras, los servidores y los dispositivos de red, sino también los componentes de orden más bajo, como los sistemas empotrados y los PLC (controladores lógicos programables). En los entornos industriales, estos sistemas informáticos pueden denominarse sistemas de control industrial (SCI), y en las centrales nucleares, sistemas de instrumentación y control (I+C) nuclear.

Evaluación. La metodología descrita en esta publicación es una actividad que, en aras de la simplicidad y la coherencia, se denomina 'evaluación' a lo largo de todo el texto. Sin embargo, como se señaló anteriormente, esta metodología puede aplicarse en diversos contextos, y otras descripciones de la actividad, como 'servicio de asesoramiento', 'visita de expertos', 'auditoría' o 'autoevaluación' podrían también ser adecuadas. El empleo del término 'evaluación' no debe interpretarse en el sentido de que otorgue alguna autoridad o responsabilidad adicional al OIEA o a cualquier otra organización que lleve a cabo la actividad.

Hallazgo. Observación que revela una divergencia entre el modo en que se efectúa una operación y el modo en que debería efectuarse, según un requisito reglamentario, una norma o la buena práctica.

Observación. Algo que se determina como resultado del examen de un documento, de una entrevista o de una observación directa.

Recomendación. Medida que refuerza la seguridad física de una instalación nuclear (en el caso de la evaluación de una entidad anfitriona); medida de aplicación obligatoria para poner remedio a un hallazgo (p. ej., cuando procede del órgano regulador de un Estado).

Una recomendación es un consejo que es sumamente conveniente seguir para la actividad o el programa que se está evaluando a fin de mejorar la seguridad física operacional. Se basa en las orientaciones publicadas en la *Colección de Seguridad Física Nuclear del OIEA*, los reglamentos nacionales, las normas o una buena práctica internacional demostrada, y aborda las causas básicas de una cuestión y no sólo los síntomas. Una recomendación engloba con frecuencia un método probado para alcanzar la excelencia, yendo más allá de lo estrictamente necesario. Tiene que ser específica y realista, y apuntar a lograr una mejora tangible.

El uso del término ‘recomendación’ en esta publicación no debe confundirse con su significado equivalente a una orientación que se encuentra en otras publicaciones de la *Colección de Seguridad Física Nuclear*.

Requisito. Base de una evaluación específica, es decir, las reglas, los reglamentos y las normas que deben aplicarse.

Seguridad física informática. Aspecto particular de la seguridad física de la información que se ocupa de los sistemas basados en computadoras, las redes y los sistemas digitales [3].

En esta publicación, la expresión ‘seguridad física informática’ se refiere a la seguridad física de todas las computadoras, tal como se describen más arriba, y de todos los sistemas y redes interconectados. (Las expresiones ‘seguridad física de la TI’ y ‘ciberseguridad’ se consideran sinónimas pero no se utilizan en esta publicación.)

Sugerencia. Medida o mejora propuesta que la instalación nuclear evaluada podría aplicar.

Una sugerencia puede acompañar a una recomendación o ser independiente. A veces contribuirá en forma indirecta a mejorar la seguridad física operacional, pero principalmente tiene por objeto mejorar la eficacia de un funcionamiento que ya es bueno, indicar una aplicación útil de un programa ya existente o señalar una posible alternativa mejor al trabajo que se está realizando. En general, una sugerencia apunta a estimular a la administración y al personal de la instalación a que siga buscando formas de mejorar el desempeño.

ANEXO I
PISTAS PARA LA EVALUACIÓN DEL SISTEMA DE INSTRUMENTACIÓN Y CONTROL

PANORAMA GENERAL DEL SISTEMA DE INSTRUMENTACIÓN Y CONTROL

En el contexto de la presente publicación, los términos 'computadoras' y 'sistemas informáticos' se refieren a los dispositivos de computación, comunicación e instrumentación y control que conforman los elementos funcionales de una instalación nuclear. Comprenden no sólo las computadoras de mesa, los grandes sistemas de computadoras, los servidores y los dispositivos de red, sino también los componentes de orden más bajo, como los sistemas empotrados y los PLC (controladores lógicos programables). Un subconjunto de estos sistemas informáticos incluye el sistema de control digital y el sistema de instrumentación y control. Estos sistemas son particularmente importantes en la evaluación, porque su vulneración puede tener graves efectos en la seguridad física y tecnológica.

El sistema de instrumentación y control (I+C) es el eje operacional de los procesos de la instalación. En la publicación NP–T–3.12 de la *Colección de Energía Nuclear del OIEA* (Ref. [I-1], págs. 2 y 3) se detallan las tres funciones básicas que cumple el sistema de I+C con respecto a los procesos de la central. La primera está dada por sus capacidades sensoriales (p. ej., de medición y vigilancia) que respaldan funciones tales como la monitorización o el control y que permiten al personal determinar el estado de la central. Así, los sistemas de I+C tales como los sensores y detectores son la interfaz directa con los procesos físicos que ocurren en la central nuclear, y sus señales son enviadas a través de los sistemas de comunicación al operador y a las aplicaciones que adoptan decisiones (analógicas o digitales).

La segunda función es el control automático, tanto de la instalación principal como de los numerosos sistemas auxiliares. La tercera función del sistema de I+C es la respuesta a los fallos y los sucesos anómalos, que proporciona seguridad y protege a la central contra las consecuencias de un mal funcionamiento o una deficiencia de sus sistemas o del resultado de errores manuales.

Estos sistemas informáticos y los sistemas conexos (de I+C) utilizados en las funciones operacionales de una central nuclear o de una instalación del ciclo del combustible o de almacenamiento apoyan distintas funciones y se conocen con diferentes nombres en el sector. En la presente publicación se utiliza la expresión 'sistemas de control industrial' (SCI) para hacer referencia a todos esos sistemas, que incluyen los sistemas de adquisición de datos y control de supervisión (SCADA), los sistemas de control distribuido y otras configuraciones de sistemas de control, como los controladores lógicos programables montados en plataformas [I-2].

Los componentes de control de los SCI pueden comprender (Ref. [I-2], págs. 2 a 4):

- terminales remotos para apoyar el control y la monitorización de dispositivos a distancia;
- controladores lógicos programables, que son pequeñas computadoras utilizadas a menudo para el control de procesos industriales;
- dispositivos electrónicos inteligentes, que son sensores/accionadores inteligentes para la adquisición local de datos, la comunicación y el control local;
- una interfaz persona-máquina o una interfaz persona-sistema, que es la interfaz que permite a una persona monitorizar y controlar los procesos de la central.

Estos sistemas son parte de la red de SCI, que también contiene componentes de red estándar y especializados, como enrutadores, cortafuegos, servidores, módems y puntos de acceso remoto.

La red de control tiene luego una interfaz con los componentes de orden inferior, como los sensores y los dispositivos de accionamiento para controlar y/o monitorizar los procesos de la central, como se ilustra en la figura I-1.

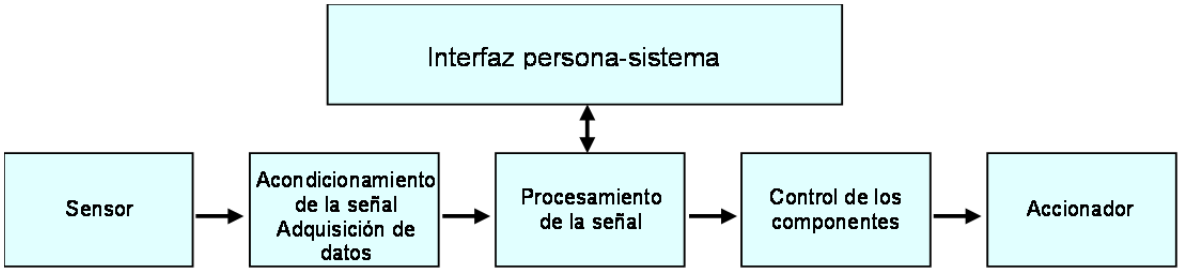

Fig. I-1. Diagrama de bloques de una función de I+C típica [I-1].

Una misma red puede controlar múltiples procesos idénticos. A la inversa, los procesos pueden ser controlados en redes completamente independientes. En la red de control, cada uno de estos componentes es un posible punto vulnerable del sistema y, por lo tanto, debe examinarse a algún nivel en el marco de la evaluación. Una dificultad es que estos componentes no fueron diseñados necesariamente teniendo en cuenta la seguridad física informática.

VULNERABILIDADES COMUNES DE LOS SISTEMAS DE CONTROL

A continuación se enumeran las vulnerabilidades comunes señaladas por el Departamento de Seguridad Nacional de los Estados Unidos [I-3], que pueden tomarse en consideración al elaborar y realizar la evaluación de los SCI y los sistemas de I+C de una central. Ningún elemento debería necesariamente, por sí solo, ser motivo de preocupación; más bien, cada elemento debe considerarse en el contexto global de la evaluación. Las cuestiones que pudieran plantearse pueden haberse resuelto ya con controles compensatorios o con mecanismos de defensa integrados.

Control del acceso

- El acceso no está restringido a los objetos que lo requieren;
- El protocolo de los SCI permite a los anfitriones del SCI leer o sobreescribir archivos en otras computadoras, sin ningún registro;
- La documentación y la información sobre la configuración se comparten libremente (en modo de solo lectura);
- Hay recursos compartidos disponibles en múltiples sistemas;
- Falta una autenticación basada en el cargo para la comunicación entre los componentes del SCI;
- Un usuario a distancia puede cargar un archivo en cualquier lugar de la computadora de destino;
- Los anfitriones del SCI permiten la descarga arbitraria de archivos;
- Los anfitriones del SCI permiten la carga arbitraria de archivos;
- Un cliente a distancia puede poner en marcha cualquier proceso;
- Un servicio del SCI permite el acceso anónimo;
- Hay cuentas de administrador no ‘legales’ y no reveladas para un futuro acceso del proveedor con fines de mantenimiento, actualización o capacitación;

— Se sobreutiliza la cuenta de administrador;
— La explotación a distancia de servicios de aplicación del SCI permite el acceso a nivel de administrador en anfitriones del SCI;
— Un servicio de base de datos funciona como administrador;
— No se requiere autenticación para leer un archivo de configuración de sistemas que contiene detalles sobre las cuentas de los usuarios, incluidas las contraseñas;
— No hay separación de tareas mediante la autorización de acceso asignada;
— No hay un sistema de bloqueo que se active ante intentos fallidos de inicios de sesión.

Contraseñas

— Algunos anfitriones del SCI tienen contraseñas administrativas muy débiles, de tres caracteres;
— Las contraseñas débiles se pueden recuperar y dan acceso de administrador a todos los recursos del sistema;
— Hay varias contraseñas débiles;
— Las contraseñas por defecto no se han cambiado;
— Al nivel de administrador se utilizan nombres de usuarios y contraseñas por defecto;
— Varias cuentas de usuario predefinidas del dispositivo, incluida la cuenta del administrador, tienen asignadas credenciales por defecto;
— Un componente del SCI permite el acceso directamente por Internet con el nombre de usuario y la contraseña por defecto;
— La norma de longitud, seguridad y complejidad de las contraseñas no se aplica;
— Muchas de las cuentas, incluida la cuenta de administrador, no tienen contraseñas con fecha de caducidad;
— No se ha definido una política de bloqueo de cuentas;
— La función de complejidad de la contraseña está desactivada;
— El historial de contraseñas está configurado para que no recuerde ninguna contraseña anterior.

Artefactos de código

El almacenamiento del SCI, por ejemplo del código fuente y la configuración del sistema, en un sistema de archivos compartidos ofrece grandes posibilidades de extracción de información a un adversario. El diseño de muchos SCI incluye recursos compartidos de red abiertos en los anfitriones de los SCI. Los siguientes son ejemplos de posibles hallazgos de la evaluación en relación con esta vulnerabilidad:

— Recursos compartidos de red a disposición del público en anfitriones del SCI. Se descubren recursos compartidos en computadoras de estaciones de trabajo y servidores;
— Recursos compartidos en múltiples sistemas;
— Archivos disponibles para acceso de solo lectura;
— Fugas de información a través de directorios compartidos;
— Gran número de recursos compartidos de red a disposición del público en anfitriones del SCI;
— El código fuente del SCI está compartido en los anfitriones del SCI. El código fuente se puede descargar y utilizar para encontrar vulnerabilidades.

Gestión de parches

Se encuentran versiones antiguas o no parcheadas de aplicaciones de terceros incorporadas en el software del SCI con lo siguiente;

- una versión vulnerable de una base de datos;
- una versión vulnerable de un servidor de la web;
- el OPC (Object Linking and Embedding for Process Control) se basa en la llamada de procedimiento remoto (RPC) y el Modelo de Objetos de Componentes Distribuidos (DCOM); sin parches actualizados, el OPC está expuesto a las vulnerabilidades conocidas de estos dos elementos;
- bibliotecas SSL vulnerables (no parcheadas).

Planificación/política/procedimientos

- Falta de documentación oficial;
- Mantenimiento incorrecto de la documentación sobre seguridad física;
- Falta de un grupo de seguridad física informática;
- Falta de políticas de recuperación en caso de desastre;
- Falta de conocimiento de los procedimientos de recuperación;
- Poca capacidad de respaldo y restauración;

Puntos débiles del diseño de la red

Consideraciones generales

- Falta de un perímetro de seguridad definido;
- Configuración incorrecta de los dispositivos de la red;
- Seguridad de los puertos no habilitada en los dispositivos de la red.

Falta de segmentación de la red

- Redes de control utilizadas para tráfico sin fines de control;
- Servicios de la red de control situados fuera de esta;
- Falta de segmentación interna de la red de producción del SCI: los servidores del ICCP (Inter-Control Center Communications Protocol) no están en una zona desmilitarizada (DMZ);
- Falta de segmentación interna de la red de producción del SCI: un anfitrión con conexiones en serie especiales para la transferencia de datos utiliza una aplicación de alto riesgo fuera de una DMZ;
- Sistemas relacionados con el control a los que se puede acceder desde la LAN corporativa;
- Las evaluaciones de la respuesta a incidentes y las evaluaciones con la herramienta CSET en el emplazamiento identifican los siguientes problemas en múltiples sitios:
- Redes de control utilizadas para tráfico sin fines de control;
- Servicios de la red de control situados fuera de esta.

Cortafuegos/zona desmilitarizada

- Ausencia de cortafuegos;
- Falta de una zona desmilitarizada funcional;

— Cables físicos conectados directamente a la LAN del SCI, sin pasar por el cortafuego;
— El servidor SSH conecta directamente las LAN corporativa y del SCI, sin pasar por el cortafuego;
— La tercera tarjeta de red del servidor del ICCP conecta directamente con la LAN del SCI;
— El acceso a determinados puertos del anfitrión no está restringido a las direcciones IP requeridas;
— Listas de acceso definidas pero no aplicadas. Ningún filtrado de la información entrante;
— Listas de acceso incorrectas para los puertos requeridos;
— Acceso a los servicios de impresoras de la LAN corporativa no restringido por contraseña ni por una lista de control del acceso;
— Un cliente de correo electrónico de la zona desmilitarizada tiene acceso a la LAN corporativa y a Internet;
— Restricciones inadecuadas del acceso de salida;
— Reglas del cortafuego no adaptadas al tráfico del SCI.

Auditorías y rendición de cuentas

— Falta de auditorías/evaluaciones de la seguridad física;
— Registros inexistentes o de mala calidad;
— Comprensión insuficiente de la arquitectura de red;
— Aplicación débil de las políticas de inicio de sesión a distancia;
— Control débil de los medios de entrada y salida;
— Método insuficiente para la vigilancia de los sucesos en la red de control.

REFERENCIAS DEL ANEXO I

[I-1] INTERNATIONAL ATOMIC ENERGY AGENCY, Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants, IAEA Nuclear Energy Series No. NP–T–3.12, IAEA, Vienna (2011).

[I-2] UNITED STATES NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800–82, Gaithersburg, Maryland, USA (2011).

[I-3] UNITED STATES DEPARTMENT OF HOMELAND SECURITY, Common Cybersecurity Vulnerabilities in Industrial Control Systems, US Department of Homeland Security, (2011), available online at: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf

ANEXO II

MODELO DE FORMULARIO PARA LAS OBSERVACIONES

Los siguientes modelos de formulario pueden ayudar a los evaluadores a recopilar y analizar los datos para una evaluación.

Estos modelos y los cuadros de datos son solo ejemplos y pueden modificarse para que respondan a las necesidades del grupo de evaluación.

Las observaciones se utilizarán para elaborar el informe final de la evaluación.

Nombre del evaluador		**Número**			
Fecha y hora					
Lugar	Dónde se efectúa la observación				
Instalación	Si se aplica				
Sistema	Si se aplica				
Dominio de la seguridad física	Según la definición				
Dominio funcional	Según la definición				
Nivel de seguridad física					
Observación:	Descríbase lo que se observó o detectó				
Cómo se detectó	Examen de un documento	Entrevista	Observación	Fuente de libre acceso	Otro:
Propósito	Recomendación	Sugerencia	Buena práctica	Otro :	
Hallazgo*	Descríbase la discrepancia:				
Fundamento*	Referencia a orientaciones del OIEA, una buena práctica, una norma o reglamento, un vector de ataque conocido, etc.				
Causa raíz*	Razón por la que existe el problema				
Dificultad de explotación*	Baja	Moderada	Alta		
Accesibilidad*	Amenaza externa/amenaza interna (a sabiendas o no)				
Impacto potencial*	Descripción del impacto directo e indirecto del hallazgo.				
Grado de importancia*	Categorización del hallazgo según su impacto potencial (las organizaciones pueden elaborar su propia escala de importancia o impacto)				
Acción*	Aplicar una buena práctica, aplicar una norma, aplicar un reglamento, sistema de parches, etc.				
NOTAS:					

* Estos elementos pueden no ser evidentes durante la observación y se podrán añadir más tarde.

Leyenda del formulario de campo

Dominios funcionales

OP: Dominio de las operaciones

EM: Dominio de la empresa

ST: Dominio de la seguridad tecnológica

PF: Dominio de la protección física

RE: Dominio de la respuesta a emergencias

Dominios de la seguridad física

PS: Política de seguridad física

OS: Organización de la seguridad física de la información

GA: Gestión de activos

RH: Seguridad física de los recursos humanos

PF: Protección física

CO: Gestión de las comunicaciones y las operaciones

CA: Control del acceso informático

AD: Adquisición, desarrollo y mantenimiento de sistemas informáticos

GI: Gestión de incidentes de seguridad física informática

GC: Gestión de la continuidad

Dificultad de explotación

Baja	Vulnerabilidad de conocimiento general; existen exploits públicos
Moderada	Algunos detalles se conocen; la prueba del concepto está disponible
Alta	No hay ningún detalle disponible

Tipos de medidas posibles

Modificaciones del equipo e instalación de dispositivos y medios adicionales para prevenir la repetición del mismo suceso o de otros similares.

Mejoras de los procedimientos y medidas administrativas, y frenos y controles adicionales.

Rectificación de deficiencias descubiertas en la documentación operacional (manuales de operaciones).

Rectificación de deficiencias descubiertas en documentos normativos.

Capacitación del personal para que ejecute el trabajo correctamente.

Introducción de cambios en el entorno de trabajo.

Introducción de cambios en la planificación y programación del trabajo y/o en las personas asignadas a determinadas tareas.

ANEXO III

MODELO PARA EL INFORME FINAL

RESUMEN EJECUTIVO

El resumen ejecutivo describe breve y concisamente el contexto, los objetivos, la metodología y los requisitos, las principales recomendaciones y las buenas prácticas.

INTRODUCCIÓN

- Objetivos;
- Alcance;
- Mapa simplificado de la arquitectura de red, para que el grupo de evaluación y la entidad anfitriona tengan la misma visión de los límites de la evaluación;
- Metodología;
- Definiciones (si es necesario).

RESULTADOS DE LA EVALUACIÓN

Hallazgos

- Los hallazgos se obtienen aplicando los filtros de los requisitos a las observaciones. Los hallazgos deben enumerarse;
- Los documentos que contienen los requisitos, como los reglamentos, procedimientos, normas, buenas prácticas y otros deben definirse, y los hallazgos deben remitir al documento correspondiente;
- Las observaciones pueden incluirse o no, pero pueden servir de referencia para los hallazgos (o excluirse, si ya se comunicaron a la instalación).

Recomendaciones, sugerencias y buenas prácticas

- Las recomendaciones (para los hallazgos) y las sugerencias deben definirse y correlacionarse con los requisitos o las directrices incluidos en las referencias;
- Si el que realiza la evaluación es un organismo estatal o un órgano regulador, las recomendaciones pueden definirse con precisión, por ejemplo como directivas, avisos de acción, etc.;
- Las recomendaciones pueden clasificarse con arreglo a un enfoque graduado que se relacione con el riesgo o efecto potencial para la instalación. La base para la clasificación se examinará y acordará en la reunión previa a la evaluación.

Estrategia de mitigación (facultativa)

- La inclusión de una sección sobre una estrategia de mitigación es una opción que puede debatirse antes de la evaluación;
- Si se va incluir una estrategia de mitigación en el informe final, el contenido de esa sección debe examinarse junto con el personal de la instalación.

Análisis del impacto (facultativo)

— El informe puede incluir un análisis del impacto potencial de los hallazgos en las esferas funcionales de la instalación, como la seguridad tecnológica, la seguridad física, la protección radiológica, etc. Este análisis no será un componente de todas las evaluaciones, y el nivel al que se realice deberá examinarse y acordarse en la reunión de planificación.

CONCLUSIÓN

En esta sección se da una visión general del resultado de la evaluación y se reiteran las principales recomendaciones, sugerencias y buenas prácticas para el cumplimiento de los requisitos y el análisis del riesgo de la instalación nuclear. Si el informe final incluye una estrategia de mitigación, puede añadirse aquí un plan de acción principal.

REFERENCIAS

En esta sección se enumeran los documentos/referencias pertinentes utilizados en la evaluación y el análisis:

— requisitos;
— guías de reglamentación;
— normas;
— procedimientos, cualquier otro documento utilizado, etc.;
— entrevistas con los empleados;
— personal directivo entrevistado (directores, ingenieros, técnicos, etc.).

ABREVIACIONES

ANEXO

— Programa de la evaluación;
— Formularios para la observación;
— Formularios para los hallazgos.

ANEXO IV

CONSIDERACIONES PARA ABORDAR LOS RESULTADOS DE LA EVALUACIÓN

En el presente anexo se indican algunos aspectos que la organización anfitriona debería considerar cuando aborde los resultados expuestos en el informe final de la evaluación. El informe contendrá una combinación de hallazgos, observaciones, recomendaciones y sugerencias. Cada organización tendrá sus propios procesos para elaborar un plan de acción sobre la base de esos resultados.

En el examen del informe deben participar diversos niveles de la administración, incluido el personal directivo superior. Esto es importante para que se atribuya el debido peso y se dediquen recursos adecuados a la elaboración de un plan de acción. Algunas de las medidas correctivas o de mitigación serán sencillas, pero otras pueden requerir un análisis detallado. Las siguientes consideraciones pueden ayudar a respaldar el proceso de adopción de decisiones para la elaboración de ese plan de acción.

Impacto

- ¿Cuál es el principal impacto del informe para la organización?
- ¿Cómo afecta el informe al perfil de riesgo global de la organización?

Mitigación

- ¿Qué información adicional se necesita para adoptar una decisión?
- ¿Cuál es la eficacia de la solución propuesta? (¿Cuál es la reducción del riesgo?)
- ¿Es posible tratar múltiples hallazgos con una misma solución?
- ¿Cuáles serán los efectos de la aplicación de la solución recomendada (p. ej., ¿tiene la aplicación de la solución efectos secundarios adversos, tales como la invalidación de la certificación, la licencia o las garantías del sistema?)?
- ¿Impone la solución propuesta algún riesgo adicional o diferente?
- ¿Cuáles serían las medidas alternativas a la solución recomendada?
- ¿Cómo puede verificar la organización que la recomendación propuesta es eficaz?

Plazos para la mitigación

- ¿Cuál es el plazo para aplicar la recomendación? ¿Es suficiente esa acción para hacer frente a la amenaza?
- ¿Qué condiciones especiales se requieren para aplicar la solución (p. ej., una parada o un período de mantenimiento)?
- ¿Puede abordarse el hallazgo utilizando medidas provisionales hasta que sea posible implantar medidas más permanentes?
- ¿Hay en la organización planes de futuros proyectos que subsanen o modifiquen los problemas, o que ofrezcan la oportunidad de resolverlos?

Costos de la mitigación

- ¿Tiene la organización la competencia y los conocimientos técnicos necesarios para aplicar la recomendación?

— ¿Qué incluyen los costos de la solución propuesta?
  — Costos de adquisición;
  — Costos de aplicación;
  — Costos de comunicación para la nueva solución;
  — Costos de capacitación del personal;
  — Costos de capacitación de los usuarios;
  — Costos de productividad y de conveniencia;
  — Costos de auditoría y de verificación de la eficacia;
  — Costos de disposición final al término de la vida útil.

Comunicaciones

— ¿Es útil comunicar a organizaciones externas, por ejemplo a los proveedores, los asociados industriales o las autoridades competentes, determinados resultados del informe?

— Si la evaluación forma parte del proceso regulador, la autoridad competente puede haber establecido requisitos de presentación de informes sobre el plan de acción y las medidas de seguimiento.

Otras consideraciones

— ¿Se trata de un hallazgo recurrente, lo que tal vez signifique que el problema no se trató adecuadamente o que la medida precedente no fue eficaz?

— ¿Indica el conjunto de los hallazgos la existencia de un problema más grande en la organización?

— ¿Cómo puede la organización evitar que este u otros hallazgos conexos se repitan en el futuro?

— ¿Cómo se efectuará el seguimiento de los resultados del informe y del plan de acción dentro de la organización?

PEDIDOS DE PUBLICACIONES

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

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

ALEMANIA

Goethe Buchhandlung Teubig GmbH

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

CANADÁ

Renouf Publishing Co. Ltd

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

Bernan / Rowman & Littlefield

15200 NBN Way, Blue Ridge Summit, PA 17214, EE.UU.
Teléfono: +1 800 462 6420 • Fax: +1 800 338 4550
Correo electrónico: orders@rowman.com • Sitio web: www.rowman.com/bernan

ESTADOS UNIDOS DE AMÉRICA

Bernan / Rowman & Littlefield

15200 NBN Way, Blue Ridge Summit, PA 17214, EE.UU.
Teléfono: +1 800 462 6420 • Fax: +1 800 338 4550
Correo electrónico: orders@rowman.com • Sitio web: www.rowman.com/bernan

Renouf Publishing Co. Ltd

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

FEDERACIÓN DE RUSIA

Scientific and Engineering Centre for Nuclear and Radiation Safety

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

FRANCIA

Form-Edit

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

INDIA

Allied Publishers

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

Bookwell

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

ITALIA

Libreria Scientifica "AEIOU"

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

JAPÓN

Maruzen-Yushodo Co., Ltd

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

REPÚBLICA CHECA

Suweco CZ, s.r.o.

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

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

Dependencia de Mercadotecnia y Venta
Organismo Internacional de Energía Atómica
Vienna International Centre, PO Box 100, 1400 Viena, Austria
Teléfono: +43 1 2600 22529 o 22530 • Fax: +43 1 2600 29302 o +43 1 26007 22529
Correo electrónico: sales.publications@iaea.org • Sitio web: www.iaea.org/books

Organismo Internacional de Energía Atómica
Viena
ISBN 978-92-0-306617-4