Planificación de la respuesta a incidentes de 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.

PLANIFICACIÓN DE LA RESPUESTA A INCIDENTES DE 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''.

PLANIFICACIÓN DE LA RESPUESTA A INCIDENTES DE SEGURIDAD FÍSICA INFORMÁTICA EN LAS INSTALACIONES NUCLEARES

ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA
VIENA, 2018

DERECHOS DE AUTOR

PLANIFICACIÓN DE LA RESPUESTA A INCIDENTES DE SEGURIDAD FÍSICA INFORMÁTICA EN LAS INSTALACIONES NUCLEARES
IAEA-TDL-005
ISBN 978-92-0-306717-1

Impreso por el OIEA en Austria
Febrero 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 puede 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. La seguridad física no se limita solo a la prevención; también incluye la detección y la respuesta. Todo propietario o explotador de un sistema necesita tener procesos y planes de contingencia para detectar los incidentes de seguridad física informática que pudieran tener efectos adversos en los sistemas de protección física, seguridad tecnológica nuclear y contabilidad y control de los materiales nucleares, o conducir a la divulgación no autorizada de información de carácter estratégico, y para dar respuesta a esos incidentes.

El propósito de la presente publicación es ayudar a los Estados Miembros a elaborar planes de contingencia completos para los incidentes de seguridad física informática que puedan repercutir en la seguridad nuclear física y/o tecnológica. La publicación ofrece una descripción de cómo establecer una capacidad de respuesta a incidentes de seguridad física informática como parte de un programa de seguridad física informática, con las sugerencias pertinentes, y examina las funciones y responsabilidades del propietario del sistema, de la entidad explotadora, de la autoridad competente y de la autoridad técnica nacional en la respuesta a un incidente de seguridad física informática que pueda tener repercusiones en la seguridad física nuclear.

La presente publicación se preparó con la asistencia de más de veinte expertos en el curso de dos reuniones de consultores y una serie de exámenes externos, con aportaciones de más de 12 Estados miembros y organizaciones internacionales.

ÍNDICE

1. INTRODUCCIÓN 1

1.1. Antecedentes 1
1.2. Propósito 1
1.3. Ámbito de aplicación 2
1.4. Estructura 3

2. CONCEPTOS Y CONTEXTO 4

2.1. Panorama general 4
2.2. Visión general de la respuesta a incidentes de seguridad física informática 6
2.3. Niveles de la respuesta a incidentes de seguridad física informática 6

3. POLÍTICA, FUNCIONES Y RESPONSABILIDADES 8

3.1. Panorama general 8
3.2. Políticas de respuesta a incidentes de seguridad física informática 8
3.3. Grupo de respuesta a incidentes de seguridad física informática (CSIRT) 11
3.4. Plan de respuesta a incidentes de seguridad física informática 14
3.5. Procesos y procedimientos de la entidad explotadora 17

4. FASES DE LA RESPUESTA A UN INCIDENTE DE SEGURIDAD FÍSICA INFORMÁTICA . 21

4.1. Panorama general 21
4.2. Preparación 21
4.3. Detección y análisis 23
4.4. Mitigación (contención, erradicación y recuperación) 25
4.5. Actividad posterior al incidente 26
4.6. Comunicación de información 28

5. ANÁLISIS DE LOS INCIDENTES DE SEGURIDAD FÍSICA INFORMÁTICA 29

5.1. Panorama general 29
5.2. Categorización de la gravedad 29
5.3. Consecuencias de los incidentes de seguridad física informática para la seguridad tecnológica 34
5.4. Pérdida o vulneración de información de carácter estratégico 36
5.5. Análisis de la amenaza 36
5.6. Caracterización técnica 37
5.7. Niveles de progresión 38
5.8. Flujo del proceso y progresión 39

REFERENCIAS 45

GLOSARIO 47

ANEXO I INDICADORES DE INCIDENTES 49

ANEXO II GUÍA PARA EL ANÁLISIS DE INCIDENTES 51

ANEXO III CONSIDERACIONES ESPECIALES PARA LOS SISTEMAS DE CONTROL INDUSTRIAL 54

ANEXO IV ESCENARIOS DE INCIDENTES 55

ANEXO V INFORMACIÓN SOBRE LOS INCIDENTES 57

ANEXO VI RECOLECCIÓN DE PRUEBAS 59

ANEXO VII EJEMPLOS DE CARACTERIZACIONES TÉCNICAS 62

ANEXO VIII EJEMPLO DE UNA POLÍTICA DE RESPUESTA A INCIDENTES DE SEGURIDAD FÍSICA INFORMÁTICA 64

1. INTRODUCCIÓN

1.1. ANTECEDENTES

Un régimen de seguridad física nuclear debería garantizar que en todos los niveles apropiados de una organización existan sistemas y medidas para detectar y evaluar los *sucesos relacionados con la seguridad física nuclear*[1] y notificarlos a las *autoridades competentes* que proceda a fin de que pueda ponerse en marcha una respuesta adecuada [1]. La elaboración de un marco nacional para la gestión de la respuesta a un suceso de esa índole es una parte importante de un régimen nacional de seguridad física nuclear.

La seguridad física informática es vista, cada vez más, como un componente clave de la seguridad física nuclear que plantea un conjunto especial de retos para las instalaciones que manipulan *materiales nucleares* y *otros materiales radiactivos* y para las actividades conexas tales como el transporte. La preocupación principal es un *acto doloso* que directa o indirectamente ponga en peligro la seguridad física de los *materiales nucleares* y/o radiactivos.

El objetivo más importante de la seguridad física informática es prevenir la *vulneración* de los sistemas informáticos, pero las organizaciones tienen también que estar preparadas para actuar si un adversario externo o interno consigue comprometer sus sistemas. Las instalaciones y las organizaciones estatales necesitan tener un plan de contingencia para los *sucesos relacionados con la seguridad física nuclear* que incluya los incidentes de seguridad física informática y la respuesta correspondiente. Este plan tendrá por finalidad aislar el peligro, mitigar el daño, dar aviso a las *autoridades competentes* y realizar los procesos de restauración.

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] se afirma que "[d]ebería 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."

La protección no puede limitarse a la prevención. También tiene que incluir la detección y la respuesta. Todo propietario o explotador de un sistema necesita tener procesos y planes de contingencia para detectar los incidentes de seguridad física informática que pudieran tener efectos adversos en los sistemas utilizados para la protección física, la seguridad tecnológica nuclear, y la contabilidad y el control de los *materiales nucleares*, o conducir a la divulgación no autorizada de *información de carácter estratégico*, incluida la información que pueda facilitar futuros atentados, y dar respuesta a esos incidentes.

1.2. PROPÓSITO

El propósito de la presente publicación es ayudar a los Estados Miembros a elaborar planes de contingencia completos para los incidentes de seguridad física informática que puedan repercutir negativamente en la seguridad nuclear física y/o tecnológica.

[1] Los términos que aparecen en cursiva se definen en el Glosario que se encuentra al final del cuerpo de esta publicación.

Esta publicación complementa la documentación ya existente al abordar el carácter especial de los *materiales nucleares* y *otros materiales radiactivos* y los requisitos de seguridad física específicos para estos materiales. Ofrece orientaciones sobre los elementos clave para elaborar y aplicar una respuesta completa a un incidente de seguridad física informática (es decir, un ciberataque) que pueda comprometer o menoscabar la seguridad física nuclear. La publicación abarca lo siguiente:

- la caracterización de los incidentes de seguridad física informática;
- la definición de la política de respuesta y de las funciones y las responsabilidades correspondientes;
- la ejecución del Plan de Respuesta a Incidentes de Seguridad Física Informática;
- la comunicación de los incidentes de seguridad física informática;
- consideraciones relativas a los sistemas de control industrial;
- consideraciones relativas a los sistemas de información;
- consideraciones relativas a los sistemas de protección física;
- consideraciones relativas a la seguridad física nuclear.

1.3. ÁMBITO DE APLICACIÓN

La presente publicación está destinada a las personas u organizaciones que participan en la elaboración, aplicación o ejecución de planes de contingencia para incidentes de seguridad física informática que puedan tener un impacto en la seguridad nuclear física y/o tecnológica. Las orientaciones ofrecidas en esta publicación pueden ser de utilidad a las siguientes personas y entidades:

- las *autoridades competentes*, incluidos los órganos reguladores;
- el personal directivo de las instalaciones, empresas y organizaciones que intervienen en el uso, almacenamiento o transporte de *materiales nucleares* u *otros materiales radiactivos*;
- las *entidades explotadoras* y su personal;
- los contratistas u otros terceros que trabajen para las autoridades, las organizaciones o las *entidades explotadoras* de las instalaciones;
- otras entidades que puedan desempeñar un papel en la respuesta a incidentes de seguridad física informática, como los organismos de las fuerzas del orden nacionales e internacionales;
- autoridades técnicas nacionales y/o regionales tales como las organizaciones de grupos de respuesta a emergencias informáticas (CERT).

Las orientaciones que se proporcionan se relacionan específicamente con los incidentes de seguridad física informática que se producen o inician en la *entidad explotadora*, en la entidad licenciataria o en organizaciones de apoyo tales como las entidades proveedoras o de apoyo de mantenimiento. Sin embargo, esta publicación podría ser utilizada también por las *autoridades competentes* y las autoridades técnicas para desarrollar procesos y capacidades de respuesta a los incidentes que se produzcan o inicien en sus respectivas organizaciones o emplazamientos.

Estas orientaciones pueden adaptarse para que se ajusten a las necesidades de las organizaciones y/o los Estados Miembros, en cumplimiento de sus leyes y reglamentos nacionales.

1.4. ESTRUCTURA

La presente publicación consta de cinco secciones y ocho anexos. Las cuatro secciones restantes son las siguientes:

- Sección 2. Conceptos y contexto: en esta sección se introducen los conceptos básicos utilizados en toda la publicación.
- Sección 3. Política, funciones y responsabilidades: en esta sección se establecen la política, las funciones y las responsabilidades para la preparación y ejecución de planes de contingencia.
- Sección 4. Fases de la respuesta a un incidente: en esta sección se describe en detalle el proceso de respuesta a un incidente informático, con las distintas fases de la respuesta.
- Sección 5. Análisis del incidente: en esta sección se examinan los múltiples aspectos del análisis del impacto que se ha de hacer ante un incidente de seguridad física informática y se detalla el flujo de actividades durante la respuesta.

Los ocho anexos proporcionan información adicional sobre los siguientes aspectos:

- los indicadores de incidentes;
- una guía para el análisis de incidentes;
- las consideraciones especiales para los sistemas de control industrial;
- los escenarios de incidentes;
- la información sobre los incidentes;
- la recolección de pruebas;
- ejemplos de caracterizaciones técnicas;
- un ejemplo de una política de respuesta a un incidente de seguridad física informática.

2. CONCEPTOS Y CONTEXTO

2.1. PANORAMA GENERAL

Las *instalaciones nucleares*, las instalaciones en que hay *otros materiales radiactivos*, y las instalaciones, organizaciones y actividades conexas tienen la responsabilidad de proteger la información y los activos de información de carácter estratégico cuya *vulneración* pueda repercutir en la seguridad física nuclear. Esto comprende la elaboración de planes de contingencia y de respuesta, así como el desarrollo de las capacidades necesarias para hacer frente a *actos dolosos*, incluido los ciberataques.

Para planificar la respuesta a los incidentes de seguridad física informática, es necesario primero entender y definir qué son esos incidentes y cuándo pueden dar lugar a un *suceso relacionado con la seguridad física nuclear*. En la presente sección se aclara el significado de algunos términos importantes utilizados en esta publicación, y cómo se aplican los principales conceptos de la planificación de la respuesta a incidentes de seguridad física informática al ámbito de la seguridad física nuclear.

Los términos 'computadora' y 'sistema informático' se refieren en esta publicación a los dispositivos de computación, comunicación e instrumentación y control que conforman los elementos funcionales de la *instalación nuclear*. Comprenden las computadoras de mesa, los grandes sistemas de computadoras, los servidores y los dispositivos de red, y los componentes de orden más bajo, como los sistemas empotrados y los controladores lógicos programables (PLC). [3]

Un sistema de control es una categoría específica de sistema de computación o en red que responde a señales de entrada del proceso o de un operador y genera señales de salida, velando así por que el proceso siga funcionando de la manera deseada.

Los sistemas de control incluyen los sistemas de instrumentación y control (I+C) utilizados en la explotación de una central nuclear o de una instalación del ciclo del combustible o de almacenamiento para respaldar una serie de funciones. Estos sistemas se conocen con distintos nombres en el sector. En el presente documento se empleará la expresión 'sistemas de control industrial' (SCI). Estos sistemas 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. [4]

Un incidente de seguridad física informática es cualquier suceso que tenga consecuencias reales o potenciales para un sistema informático o una red de computadoras. Esto incluye también el acto de infringir una política de seguridad física explícita o implícita.

El Convenio sobre la Ciberdelincuencia [5], del Consejo de Europa, categoriza los incidentes de seguridad física informática en términos de delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos. Las categorías establecidas en este Convenio son las siguientes:

1. Acceso ilícito: Acceso ilegítimo a la totalidad o a una parte de un sistema informático.

2. Interceptación ilícita: Interceptación ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos.

3. Interferencia en los datos: Comisión ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.

4. Interferencia en el sistema: Obstaculización grave e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.

5. Abuso de los dispositivos: Producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:

— un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos en las anteriores categorías 1 a 4;

— una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático, con el fin de utilizarlos para la comisión de cualquiera de los delitos contemplados en las anteriores categorías 1 a 4.

Los incidentes de seguridad física informática pueden comprometer la confidencialidad, integridad y disponibilidad de un sistema informático y de los datos que procesa, almacena o transmite. Un incidente de seguridad física podría ser también una violación —o la amenaza inminente de una violación— de una política de seguridad física explícita o implícita, una política de usos aceptables o una práctica de seguridad física estándar. Aunque algunos sucesos adversos (p. ej., inundaciones, incendios, apagones eléctricos o calor excesivo) pueden causar una parada de los sistemas, estos no son *actos dolosos* de personas u organizaciones y, por lo tanto, no se consideran incidentes de seguridad física informática.

Un incidente de seguridad física informática se convierte en un incidente de seguridad física de la información, o en una violación de la seguridad física de la información, cuando entraña una *vulneración* o pérdida real o sospechada de información o datos. Los incidentes más graves de este tipo son los que entrañan *información de carácter estratégico*. Esta se define como la información, en cualquiera de sus formas, incluidos los programas informáticos, cuya divulgación (o modificación, alteración, destrucción o denegación de uso) no autorizada podría comprometer la seguridad física de un Estado, de una instalación relacionada con *materiales nucleares* u *otros materiales radiactivos* o de programas nucleares, o contribuir de otra forma a la comisión de un *acto doloso* contra un emplazamiento, instalación u organización nucleares o contra un transporte de *materiales nucleares*. Son ejemplos de *información de carácter estratégico* el régimen de protección física de una *instalación nuclear*, la localización y el transporte de *materiales nucleares* u *otros materiales radiactivos*, o los detalles sobre el personal de una organización. La publicación Nº 23-G de la *Colección de Seguridad Física Nuclear del OIEA* titulada *Seguridad física de la información nuclear* [6] contiene un examen y da ejemplos de la posible *información de carácter estratégico* para las instalaciones relacionadas con *materiales nucleares* y *otros materiales radiactivos*.

Un *suceso relacionado con la seguridad física nuclear* es un suceso con consecuencias potenciales o reales para la seguridad física nuclear. En la actual era digital, es necesario tomar en consideración la realidad de que un ciberataque puede comprometer la seguridad física nuclear.

Un Grupo de Respuesta a Incidentes de Seguridad Física Informática o CSIRT (Computer Security Incident Response Team) es un grupo local de personas encargadas de responder a los incidentes de seguridad física informática dentro de su propia organización. El tamaño, la composición y las capacidades de los CSIRT varían enormemente, en función de la naturaleza de la organización y de la infraestructura informática.

En la presente publicación, se entiende por autoridad técnica (AT) una organización que posee competencias y recursos especializados para responder a incidentes de seguridad física informática. La AT complementará la capacidad interna de una organización de responder a esos sucesos. La AT puede ser la organización que deba encargarse de la respuesta si un incidente de seguridad física informática sobrepasa la amenaza base de diseño (ABD) definida para los ciberataques. Esto se examina en la publicación Nº 10 de la *Colección de Seguridad Física Nuclear*, titulada *Development, Use and Maintenance of the Design Basis Threat* [7].

Un Grupo de Respuesta a Emergencias Informáticas o CERT (Computer Emergency Response Team) es un ejemplo de una autoridad técnica cuyo único propósito es prestar asistencia y aportar capacidades de respuesta cuando se produce un incidente de seguridad física informática. Los CERT pueden existir a diferentes niveles (nacional, local o sectorial).

2.2. VISIÓN GENERAL DE LA RESPUESTA A INCIDENTES DE SEGURIDAD FÍSICA INFORMÁTICA

La respuesta a incidentes de seguridad física informática no es una actuación particular, sino un enfoque que apoya no solo la detección de un incidente de ese tipo, sino también su mitigación y la recuperación de él cuando se ha producido. Se puede considerar que comprende cuatro fases: la preparación; la detección y el análisis; la contención, erradicación y recuperación; y la actividad posterior al incidente. En la figura 1 se ilustra la secuencia de estas fases. Cada fase se examinará con más detalle en la sección 3.

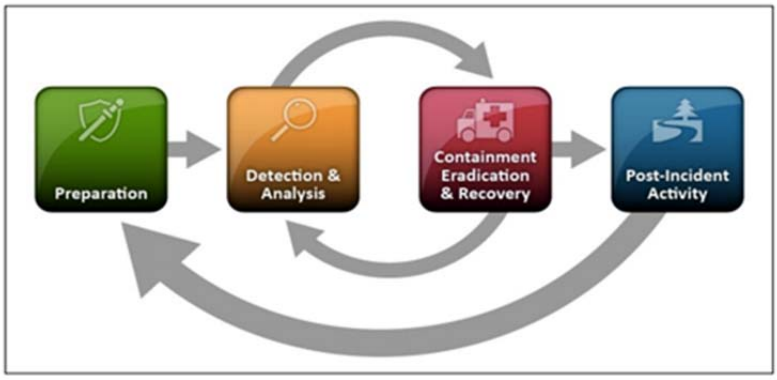

Fig. 1. Fases de la respuesta a incidentes de seguridad física informática [8][2]

2.3. NIVELES DE LA RESPUESTA A INCIDENTES DE SEGURIDAD FÍSICA INFORMÁTICA

Debido a la complejidad de los ciberataques y a las consecuencias que pueden tener, un elemento importante de la respuesta a los incidentes de seguridad física informática es la estructura que apoya la comunicación eficaz entre las *entidades explotadoras*, las organizaciones no reguladas, las *autoridades competentes* y las autoridades técnicas.

Esta estructura puede tener varios niveles, según la naturaleza y gravedad del incidente. En la figura 2 se ilustra una posible estructura utilizada por algunos Estados Miembros. El primer nivel de respuesta se produce en el lugar del incidente, por ejemplo en la instalación de una *entidad explotadora*, la oficina de una entidad no regulada o incluso la sede de una *autoridad*

[2] Reproducción por cortesía del Instituto Nacional de Estándares y Tecnología, del Departamento de Comercio de los Estados Unidos. No protegida por derechos de autor en los Estados Unidos de América.

competente. El segundo nivel representa una capacidad nacional, regional o sectorial que presta apoyo técnico para la respuesta a un incidente de seguridad física informática que va más allá de las capacidades del grupo de respuesta, por ejemplo de la autoridad técnica, en el lugar del incidente. Un CERT puede ofrecer esta capacidad. El tercer nivel está dado por las *autoridades competentes* que pueden tener que intervenir según la naturaleza del incidente, como el órgano regulador, los organismos de las fuerzas del orden, los organismos de inteligencia y/u otras entidades.

En las secciones siguientes se describen las responsabilidades correspondientes a estos niveles de respuesta. Aunque se emplea el término '*entidad explotadora*', el mismo nivel de responsabilidad podría aplicarse, según proceda, a entidades no reguladas que tengan responsabilidades en materia de seguridad física nuclear.

Fig. 2. Vías de comunicación entre los niveles de la respuesta a incidentes.

3. POLÍTICA, FUNCIONES Y RESPONSABILIDADES

3.1. PANORAMA GENERAL

Es fundamental que se formule una política, se definan las funciones y responsabilidades y se elaboren procedimientos detallados para responder a los incidentes de seguridad física informática antes de que se produzca un suceso de ese tipo. En la presente sección se ofrecen orientaciones modelo y recomendaciones sobre las políticas, funciones y responsabilidades en los diferentes niveles de la respuesta, que incluyen, entre otros, el Estado (o las organizaciones internacionales), la autoridad técnica, la *autoridad competente* y la *entidad explotadora*.

3.2. POLÍTICAS DE RESPUESTA A INCIDENTES DE SEGURIDAD FÍSICA INFORMÁTICA

Aunque las políticas dependerán en sumo grado de las características específicas de cada organización, la mayoría incluirá los mismos elementos fundamentales, independientemente de que la capacidad de respuesta a los incidentes de seguridad física informática sea interna o esté asignada a otras *autoridades competentes*. En el anexo VIII se describe un ejemplo de una política de este tipo. Sus elementos fundamentales comprenden lo siguiente:

— una declaración del compromiso de la administración;

— los objetivos y el propósito de la política;

— la designación de un coordinador de la respuesta a los incidentes de seguridad física informática;

— el ámbito de aplicación de la política (es decir, a quién y a qué se aplica y en cuáles circunstancias);

— una definición de los incidentes de seguridad física informática y de sus consecuencias en el contexto de la organización;

— la estructura de la organización y la definición de las funciones, las responsabilidades y los niveles de autoridad;

— el orden de prioridad o las categorías de gravedad de los incidentes de seguridad física informática;

— los procesos de presentación de información;

— los requisitos de capacitación y ejercicios;

— un programa de sensibilización;

— la composición del grupo.

3.2.1. Responsabilidades del Estado

Un componente importante de un régimen de seguridad física nuclear es la responsabilidad del Estado de velar por que en todos los niveles orgánicos adecuados (es decir, en la *entidad explotadora*, la *autoridad competente*, la autoridad técnica) existan sistemas y medidas de seguridad física nuclear para detectar y evaluar los *sucesos relacionados con la seguridad física nuclear* y dar aviso de ellos a las *autoridades competentes* que proceda a fin de que puedan ponerse en marcha las medidas de respuesta apropiadas. Esto incluye los incidentes de

seguridad física informática, o las amenazas a ese respecto, que tengan o puedan tener consecuencias para la seguridad física nuclear. Por consiguiente, la responsabilidad del Estado en la respuesta a los incidentes de seguridad física informática puede comprender lo siguiente:

— Establecer legislación sobre la seguridad física de los activos informáticos en las *instalaciones nucleares* y sobre la seguridad física de la información nuclear de carácter estratégico, incluida la tipificación como delito de los ciberataques contra activos nucleares. Esa legislación puede referirse directamente a la seguridad física nuclear o formar parte de un marco de seguridad física más amplio;

— Proporcionar información de interés sobre la amenaza informática a las autoridades y las *entidades explotadoras* pertinentes. (Esta información puede comunicarse directamente o transmitirse por conducto de una *autoridad competente*);

— Establecer un recurso nacional de contingencia para responder, si es necesario, a ciberataques dirigidos contra *materiales nucleares*, *otros materiales radiactivos* o instalaciones o actividades conexas;

— Realizar el análisis de las consecuencias y las operaciones de recuperación que sean necesarias;

— Realizar periódicamente actividades de garantía específica —por ejemplo, ejercicios nacionales de seguridad física nuclear que incluyan escenarios de incidentes de seguridad física informática— para detectar y subsanar todo aspecto o factor que pueda afectar a la capacidad de responder adecuadamente a un incidente de seguridad física informática;

— Especificar y coordinar las actividades de presentación de informes pertinentes para mejorar la gestión de los incidentes de seguridad física informática;

— Desarrollar, utilizar y mantener la amenaza base de diseño (ABD) o la evaluación de la amenaza de modo que incluya un componente referente a la amenaza informática. La ABD o evaluación de la amenaza es un elemento clave del diseño de la capacidad de respuesta informática de la *entidad explotadora* o de otras autoridades. La ABD puede definir además los criterios y los recursos designados para los incidentes de seguridad física informática que entrañen amenazas no previstas en la ABD [7].

3.2.2. Responsabilidades de la autoridad técnica

Una autoridad técnica, como el Grupo de Respuesta a Emergencias Informáticas (CERT), presta servicios parecidos a los del Grupo de Respuesta a Incidentes de Seguridad Física Informática (CSIRT) interno de la *entidad explotadora*, pero por lo general tiene una perspectiva más amplia y recursos o servicios técnicos más extensos.

Se recomienda que la *entidad explotadora* concierte un acuerdo con el CERT (u otras autoridades técnicas pertinentes) para el apoyo en la respuesta a un incidente de seguridad física informática, cuando sea necesario. Este acuerdo, que describirá la relación entre la autoridad técnica y la *entidad explotadora*, podría incluir lo siguiente:

— una definición de las funciones y responsabilidades de las dos organizaciones;

— la especificación de las condiciones en que la *entidad explotadora* solicitará los servicios de la autoridad técnica;

— la especificación de las condiciones en que la autoridad técnica debería comunicar información sobre la amenaza a la *entidad explotadora*;

— información detallada sobre los requisitos de protección y confidencialidad para la información compartida;

— la especificación de las condiciones en que la autoridad técnica comunicaría información de la *entidad explotadora* a otras entidades;

— información detallada sobre la disponibilidad y capacidad de los recursos de la autoridad técnica, y sobre cómo procederá la *entidad explotadora* para solicitar los servicios;

— la especificación de la función y disponibilidad de los servicios de asesoramiento nacionales para la comunicación de nuevas amenazas o vulnerabilidades.

3.2.3. Responsabilidades de la autoridad competente

Las *autoridades competentes*, y específicamente los órganos reguladores, tienen la responsabilidad de establecer los reglamentos y requisitos para la seguridad física nuclear, y los procedimientos correspondientes para evaluar las solicitudes y conceder autorizaciones o licencias. Las responsabilidades específicas que son parte integrante del proceso de manejo de los incidentes de seguridad física informática comprenden lo siguiente:

— La definición de la respuesta esperada de la *entidad explotadora* ante un incidente de seguridad física informática y de los criterios que activarán la facilitación de recursos nacionales en apoyo de la *entidad explotadora*;

— La definición de los requisitos relativos al intercambio, la comunicación y el manejo de la información sobre ciberataques e incidentes;

— La determinación y designación de los componentes de una respuesta a incidentes de seguridad física informática que se incluirán en los planes de contingencia, según proceda. La provisión de orientaciones a la *entidad explotadora* sobre la elaboración de planes de seguridad física informática, incluida la respuesta a incidentes en ese ámbito;

— La realización de evaluaciones y exámenes periódicos de los planes de respuesta a incidentes de seguridad física informática de la *entidad explotadora*;

— La designación de un coordinador de la seguridad física informática que tenga la competencia técnica adecuada para ocuparse de la seguridad física informática y hacer frente a los incidentes en ese ámbito. El coordinador de la seguridad física informática puede trabajar en el órgano regulador nuclear o en otra rama del gobierno; independientemente de dónde se encuentre, debe estar claramente identificado;

— La realización periódica de inspecciones *in situ*.

3.2.4. Responsabilidades de la entidad explotadora

La responsabilidad fundamental de mantener la seguridad tecnológica y física de las operaciones compete a la *entidad explotadora*. Esto incluye la protección de los *materiales nucleares* y *otros materiales radiactivos*. La *entidad explotadora* es la primera línea de defensa en la detección de un ciberataque y en la respuesta inicial. Sus responsabilidades en la respuesta a un incidente de seguridad física informática comprenden lo siguiente:

— El desarrollo y mantenimiento de la seguridad física informática y de la capacidad de responder a los incidentes en ese ámbito para hacer frente a las amenazas previstas en la ABD o en la evaluación de la amenaza;

— La realización de análisis del *riesgo* informático, incluida una evaluación de la vulnerabilidad. Esto puede formar parte de un análisis más amplio del *riesgo* en toda la organización;

— La definición de un conjunto de sistemas y componentes digitales acreditados que cumplan funciones de seguridad tecnológica y física importantes;

— La elaboración de la política de respuesta a incidentes (véase un ejemplo de una política de ese tipo en el anexo VIII) y del plan y los procedimientos para las operaciones de contingencia y de recuperación;

— La designación de un punto de contacto para la seguridad física informática y de un grupo local de respuesta a los incidentes en ese ámbito;

— La caracterización inicial de un incidente de seguridad física informática;

— La notificación de los incidentes, según esté prescrito;

— La provisión de documentación sobre el incidente y la asistencia en el proceso forense;

— La capacitación y realización de ejercicios periódicos para el personal de respuesta a incidentes;

— La interacción con la autoridad técnica (p. ej., el CERT), según sea necesario;

— La comunicación de la información pertinentes sobre los incidentes, según proceda;

— El cumplimiento de los reglamentos o directrices emitidos por la *autoridad competente*.

3.3. GRUPO DE RESPUESTA A INCIDENTES DE SEGURIDAD FÍSICA INFORMÁTICA (CSIRT)

Se recomienda que todas las organizaciones que tengan responsabilidades en materia de seguridad física nuclear y que utilicen computadoras y sistemas informáticos establezcan un Grupo de Respuesta a Incidentes de Seguridad Física Informática (CSIRT). El objetivo es crear una capacidad de respuesta multidisciplinaria para hacer frente a las numerosas facetas y posibles consecuencias de un incidente de esa índole.

Aunque las competencias precisas que deberá tener el grupo dependerán de la naturaleza de la organización, de sus activos informáticos y de los sistemas que puedan resultar afectados, se recomienda que el grupo reúna conocimientos especializados en las siguientes esferas:

— La seguridad física informática y la respuesta a incidentes de seguridad física informática.

  Aunque el campo de la seguridad física informática es extenso, el proceso de respuesta a un incidente en esta esfera requiere determinadas competencias y una capacitación específica para afrontar, analizar y mitigar los sucesos que repercutan en la confidencialidad, integridad y disponibilidad de los sistemas informáticos.

— La arquitectura, el diseño y las operaciones de los sistemas desplegados.

  En la planificación de la respuesta a incidentes de seguridad física informática tiene que participar una persona experimentada en el diseño y la arquitectura de redes, computadoras de mesa y aplicaciones, ya que su conocimiento de los sistemas desplegados permitirá entender cómo vincularlos con el proceso de respuesta a los incidentes de seguridad física.

— La seguridad física nuclear.

  Los *materiales nucleares* y *otros materiales radiactivos*, y las instalaciones y actividades conexas, presentan características, limitaciones y problemas de seguridad especiales. Es importante que estos aspectos se incorporen en el proceso de respuesta a los incidentes informáticos.

— La seguridad tecnológica, según corresponda a la organización.

  El efecto o posible efecto en la seguridad tecnológica es una de las primeras consideraciones que deben evaluarse ante un incidente de seguridad física informática. Esto se aplica especialmente cuando el objetivo del incidente de seguridad física informática pueda ser un robo, acto de sabotaje, acceso no autorizado, transferencia ilegal o cualquier otro *acto doloso* que tenga que ver con *materiales nucleares* y otras sustancias radiactivas y con las instalaciones conexas.

— La comunicación: el intercambio de información interno y externo en relación con el incidente.

  La comunicación es esencial para el éxito de la respuesta a cualquier incidente de seguridad física informática. Esto incluye la comunicación dentro de la organización y con los asociados y otros organismos externos que tengan responsabilidades al respecto.

Obsérvese que la composición del CSIRT puede evolucionar a medida que cambien o se comprendan mejor la naturaleza y el impacto del incidente. El CSIRT puede ser un componente de la respuesta global a una contingencia o emergencia.

3.3.1. Organización del CSIRT

Las computadoras están integradas en casi todas las operaciones de las organizaciones, incluidos los sistemas de gestión empresarial y de la información y, posiblemente, los sistemas de control industrial y de protección física. En esta sección se presenta primero una organización hipotética de respuesta a incidentes de seguridad física informática que abarca todas estas esferas, y a continuación una descripción ilustrativa del flujo de los procesos que puede aplicarse de forma graduada.

Aunque cada organización estructurará sus funciones de respuesta a los incidentes de un modo que se ajuste a las necesidades locales, el siguiente constructo ilustra de manera general la correlación entre los cargos y funciones. En el proceso de respuesta a los incidentes de seguridad física informática se definen siete cargos o funciones centrales. Estos son la dirección de la respuesta al incidente, la coordinación de la respuesta al incidente, el análisis del impacto, la evaluación técnica, el apoyo técnico, las comunicaciones y el apoyo a la respuesta al incidente/enlace con el grupo ampliado. La estructura orgánica y los títulos de los cargos pueden variar, pero es importante que estas funciones se especifiquen y asignen. En la figura 4 se propone una estructura orgánica para estas funciones. Este es solo un ejemplo de una estructura posible de las funciones pertinentes, que idealmente debería basarse en las necesidades específicas de la organización.

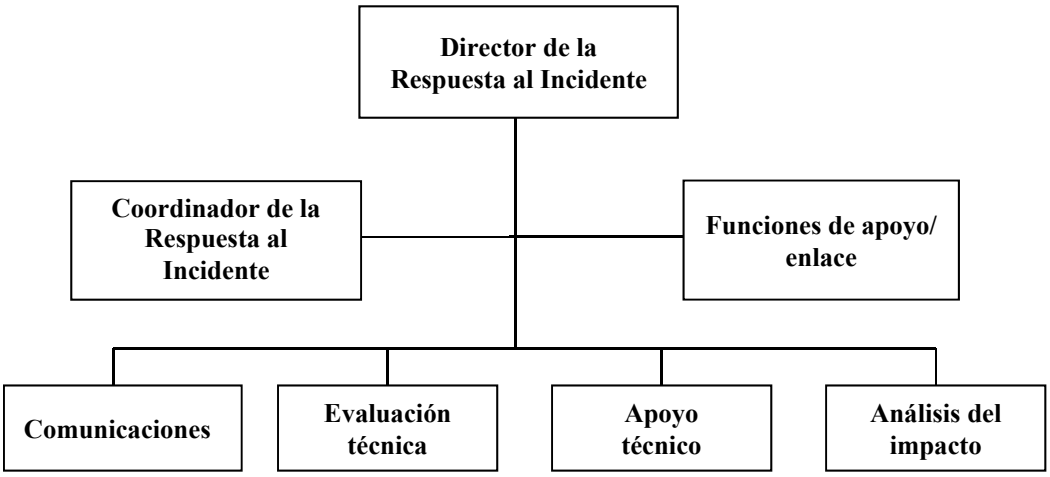

Fig. 3. Estructura orgánica hipotética de un CSIRT.

3.3.2. Director de la Respuesta al Incidente

El Director de la Respuesta al Incidente es un miembro del personal directivo superior que supervisa la respuesta global al incidente de seguridad física informática y asegura el enlace directo con la administración superior. Este cargo no se activa en cada incidente, sino solo cuando la gravedad del suceso requiere la implicación de los niveles más altos de la organización. En estos casos, el Director de la Respuesta al Incidente asume el control de las actividades de respuesta en toda la organización, sustituyendo al Coordinador de la Respuesta al Incidente, que sigue gestionando las actividades en el lugar mismo del incidente.

3.3.3. Coordinador de la Respuesta al Incidente

El Coordinador de la Respuesta al Incidente dirige la respuesta en la escena del incidente, supervisando y gestionando las actividades. En el caso de los incidentes de nivel 0 y 1 (descritos más abajo), el Coordinador de la Respuesta al Incidente puede ser el único coordinador de toda la respuesta. Cuando el incidente escala a niveles más altos, el coordinador transfiere la responsabilidad global de la gestión del incidente al Director de la Respuesta al Incidente, pero mantiene su función de coordinación local.

3.3.4. Función de evaluación técnica

Por lo general, esta función corre a cargo de expertos en la materia que se reúnen según el tipo de suceso o incidente de que se trate. Su tarea es vigilar todas las fuentes conocidas de alertas o notificaciones de amenazas y realizar luego la evaluación técnica para determinar si el incidente se ha manifestado en la organización, colaborando con el Coordinador de la Respuesta al Incidente en la determinación de la progresión inicial del incidente.

3.3.5. Función de análisis del impacto

La función de análisis del impacto consiste en evaluar las consecuencias del incidente para la organización y en determinar si pueden repercutir también en las operaciones de la central o en las operaciones relacionadas con los materiales. El encargado del análisis del impacto trabaja junto con el Director de la Respuesta al Incidente, el Coordinador de la Respuesta al Incidente y los expertos que sean necesarios para reunir suficiente información con el fin de determinar los cursos de acción requeridos para contener y erradicar la amenaza.

3.3.6. Función de comunicación

El encargado de las comunicaciones vela por que los interesados internos y externos estén informados en todo momento del estado del incidente de seguridad física informática. Esto incluye las comunicaciones técnicas sobre las medidas que se hayan de adoptar para ayudar a mitigar el efecto del incidente, las comunicaciones externas, que deben reflejar con exactitud el estado del incidente, y la interacción activa con el grupo ampliado de apoyo al incidente.

3.3.7. Función de apoyo técnico

El apoyo técnico se refiere al conjunto más amplio de recursos informáticos técnicos que pueden ser necesarios en la respuesta. En esta función pueden participar los administradores de sistemas específicos, el personal del servicio de asistencia, los propietarios de sistemas, los ingenieros de instrumentación y control, y los ingenieros de control de procesos. Todos ellos trabajan bajo la dirección del Coordinador de la Respuesta al Incidente y son responsables de aplicar las recomendaciones formuladas por el grupo de evaluación técnica.

3.4. PLAN DE RESPUESTA A INCIDENTES DE SEGURIDAD FÍSICA INFORMÁTICA

El Plan de Respuesta a Incidentes de Seguridad Física Informática y los procedimientos conexos describen específicamente los procesos técnicos, las técnicas, las listas de verificación y los formularios que se utilizarán en la respuesta a un incidente de seguridad física informática. El plan tiene que ser completo y detallado, para que las operaciones de respuesta reflejen las prioridades de la organización. La aplicación de medidas de respuesta normalizadas ayuda a reducir al mínimo los errores, particularmente los que puedan deberse a la rapidez con que hay que actuar y a las condiciones de presión que rigen en la respuesta a un incidente.

Una función principal del Plan de Respuesta a Incidentes de Seguridad Física Informática es velar por la integridad y la rápida recuperación de las funciones de los sistemas esenciales relacionadas con la seguridad tecnológica, la seguridad física, la contabilidad y el control de los materiales, y la preparación para emergencias.

3.4.1. Elementos del Plan de Respuesta a Incidentes de Seguridad Física Informática

Aunque cada plan de respuesta a incidentes de este tipo deberá adaptarse a la estructura y las necesidades de la organización de que se trate, se recomienda incluir los siguientes elementos fundamentales:

— El patrocinio de la administración superior, con inclusión de las aprobaciones, las facultades y los recursos necesarios para ejecutar el plan.

  El compromiso de la administración superior es necesario para contar con los recursos requeridos en la respuesta a un incidente de seguridad física informática y garantizar la adhesión al plan de respuesta en la organización.

— Procedimientos para informar sobre los incidentes de seguridad física informática.

  Se precisan políticas y procedimientos claros para presentar la información sobre el incidente. Ello puede incluir modelos de la información que se debe comunicar y una lista de contactos que esté siempre actualizada.

— Un proceso para decidir cómo y cuándo activar los distintos componentes del plan de respuesta.

La activación del plan de respuesta es una medida que consume muchos recursos y tiempo. Se requieren umbrales claramente definidos que indiquen cuándo activar las distintas partes del plan. Algunos aspectos de este, como los elementos de prevención e investigación, pueden aplicarse a diario, mientras que para otros se necesitan criterios que indiquen cuándo pasar al nivel superior, a fin de que la respuesta al incidente sea mesurada y se base en un enfoque graduado.

— Los requisitos relativos al máximo tiempo de respuesta permitido en la información sobre el incidente, con puntos clave como la notificación inicial, la caracterización técnica y el análisis del impacto inicial.

El CSIRT se compromete a respetar los tiempos máximos establecidos para la detección, la comunicación, la notificación y la caracterización técnica de un incidente. Estas tareas suelen ser difíciles de cumplir cuando la organización se ve enfrentada a un incidente de seguridad física informática que no le es familiar, pero existe la posibilidad de pedir apoyo a otros organismos asociados para entender mejor el tipo de incidente u objeto de que se trata y cumplir los tiempos máximos de respuesta.

— Los detalles sobre la dirección y la organización del CSIRT, con inclusión de las funciones, las responsabilidades y los datos de contacto.

El establecimiento de líneas jerárquicas claras de responsabilidad y rendición de informes es fundamental para velar por que el elemento de respuesta de la organización no esté nunca ausente o a la espera de un recurso que no se haya definido, asignado o proporcionado.

— Las responsabilidades y los procesos de vigilancia para el seguimiento del incidente de seguridad física informática.

Los grupos técnicos definen las responsabilidades y los procesos de vigilancia para el seguimiento de los incidentes de seguridad física informática. También son responsables de garantizar la comunicación con el personal cuyos sistemas o procesos hayan resultado afectados.

— La determinación de los lugares, sistemas, activos e interdependencias esenciales.

El Plan de Respuesta a Incidentes de Seguridad Física Informática debe indicar los *activos digitales de carácter estratégico* y las interdependencias, y señalar también las medidas compensatorias que se aplicarán para proteger esos elementos en caso de que las medidas de seguridad primarias y secundarias resulten comprometidas.

— Una línea clara de progresión en la respuesta, y las autorizaciones necesarias para pasar de un nivel a otro.

La gestión de la progresión es un proceso clave en la respuesta a un incidente de seguridad física informática. Una vez iniciado el proceso de respuesta al incidente, pueden utilizarse los criterios de umbral pertinentes para asegurarse de que la gestión de la respuesta y la participación en ella se estén dando en los niveles adecuados. Los procesos de progresión pueden establecer los criterios que se aplicarán para pasar a un nivel de respuesta superior, las autorizaciones para adoptar decisiones al respecto y las medidas correspondientes.

— Un plan de comunicación claro.

La comunicación del incidente de seguridad física informática tiene múltiples dimensiones, todas ellas de importancia estratégica y táctica. El plan de comunicación de incidentes no se aplica solo a los incidentes de seguridad física informática, pero es importante que en toda respuesta a un incidente de este tipo se consideren las necesidades de comunicación. El plan de comunicación puede tener los siguientes componentes:

- el propósito y objetivo del plan;
- una indicación de la naturaleza de la comunicación prevista en el marco de la respuesta, que describa cómo, qué y con quién se comunicará;
- una especificación de cuándo y con qué frecuencia se comunicará.

Las comunicaciones con la prensa pueden ser necesarias y deseables. Es mejor tener el control del mensaje que se transmite, que estar siempre respondiendo a los mensajes de otros.

— La información de contacto de todas las organizaciones mencionadas en las referencias del Plan de Respuesta a Incidentes de Seguridad Física Informática, incluidas las autoridades técnicas internas y externas y las *autoridades competentes* que proceda.

El Plan de Respuesta a Incidentes de Seguridad Física Informática debe indicar todas las personas, funciones y organizaciones que sean esenciales para la ejecución del plan y proporcionar la información de contacto de todas ellas. En los incidentes de seguridad física informática, el tiempo es un factor crucial para evitar la *vulneración* y garantizar la seguridad tecnológica de las operaciones de la central.

— Los procedimientos y criterios que se han de cumplir para declarar cerrado un incidente de seguridad física informática.

Se requieren directrices claras que indiquen cuándo podrá considerarse terminado un incidente de seguridad física informática.

— Los procedimientos para solicitar recursos adicionales, posiblemente externos (p. ej., de las autoridades técnicas).

Junto con los planes de progresión de la respuesta, se necesitan procedimientos que indiquen cómo conseguir y emplear recursos externos.

— Las necesidades de capacitación del CSIRT.

El CSIRT necesita capacitación periódica para adquirir y mantener sus competencias técnicas y administrativas fundamentales. También puede considerarse la posibilidad de capacitar al grupo para que pueda hacer el mejor uso posible de las prácticas óptimas más recientes del sector en la respuesta a un incidente de seguridad física informática.

— Las necesidades de ejercicios de seguridad física informática y de sistemas de medición para evaluar la eficacia del plan de respuesta.

Además de la capacitación, se necesitan también actividades de garantía específica, como los ejercicios de capacitación y otros métodos de evaluación, junto con sistemas de medición, para evaluar continuamente la eficacia del plan y la preparación del CSIRT.

— Las necesidades de examen periódico del plan y del procedimiento de respuesta.

  Las ciberamenazas son dinámicas. El Plan de Respuesta a Incidentes de Seguridad Física Informática debe examinarse de forma periódica para comprobar que aborde adecuadamente las nuevas amenazas y los nuevos vectores de amenazas. Este examen puede realizarse una vez al año y abarcar el plan completo, o distribuirse a lo largo del año y centrarse cada vez en algunos elementos específicos, para subdividir la tarea y hacerla tal vez más manejable.

— Las lecciones aprendidas.

  La recopilación y el intercambio de las lecciones aprendidas es un componente excelente de la mejora continua.

La confidencialidad del Plan de Respuesta a Incidentes de Seguridad Física Informática y de la información sobre los incidentes debe estudiarse cuidadosamente y manejarse de forma apropiada.

3.5. PROCESOS Y PROCEDIMIENTOS DE LA ENTIDAD EXPLOTADORA

Los procesos y procedimientos de respuesta a incidentes de seguridad física informática de la *entidad explotadora* deben tomar en consideración el entorno operacional, las amenazas potenciales, las vulnerabilidades y la experiencia en incidentes anteriores. Los procedimientos deben también apuntar a reducir al mínimo el impacto en los sistemas que tengan funciones de seguridad tecnológica o física, contabilidad y control de materiales y preparación para emergencias en el ámbito nuclear.

La *entidad explotadora* debe tomar en consideración los escenarios de incidentes posibles (véase el anexo IV) al elaborar los procedimientos de respuesta. Pueden establecerse los procedimientos para hacer frente a situaciones tales como:

— la infección por software maligno, con la correspondiente cuarentena y eliminación;

— la sospecha de infiltración por piratas informáticos;

— los ataques de denegación de servicio (DoS);

— los ataques distribuidos de denegación de servicio (DDoS);

— el aislamiento de un sistema de control respecto de otras redes (si es posible);

— la reconexión de un sistema de control a otras redes;

— la imposibilidad de ver el estado de funcionamiento de un sistema (la pérdida de visualización);

— la imposibilidad de controlar el funcionamiento de un sistema (la pérdida de control);

— los ataques por agentes internos;

— los sondeos en las redes sociales;

— el ataque o la *vulneración* de la cadena de suministro;

— el tráfico de salida de la red no autorizado;

— la rápida reconfiguración a una construcción estable;

— una fuga o pérdida de *información de carácter estratégico*;

— el deterioro de la seguridad tecnológica o de sistemas de seguridad tecnológica especiales.

La lista anterior se basa en los perfiles de ataques conocidos y representa un punto de partida para la elaboración de los procedimientos. Se aconseja que el CSIRT prepare su propio conjunto de procedimientos que responda a su situación. Esos procedimientos deben someterse a un proceso de examen periódico para mantener su aplicabilidad y eficacia.

Además de los procedimientos para hacer frente a determinados tipos de situaciones, se necesitan también procedimientos para respaldar los procesos operacionales que directa o indirectamente apoyen la respuesta a un incidente de seguridad física informática. Estos procedimientos pueden incluirse en orientaciones específicas sobre la respuesta a incidentes, o ser un componente de otros procedimientos operacionales.

— Actualización de las firmas de los sistemas antivirus y de detección de intrusiones.

  La gestión de las amenazas conocidas (software maligno, virus, etc.) requiere un enfoque metódico de la detección de intrusiones y de virus, con múltiples capas de protección (por ejemplo, para la computadora de mesa o para la red) y un plan de actualización de las firmas.

— Procesos de parcheado de seguridad.

  El uso de parches de seguridad puede ser una opción para mitigar las vulnerabilidades conocidas. Durante los incidentes es necesario a veces instalar parches para prevenir la reinfección a través del mismo punto vulnerable.

— Respaldo y recuperación del sistema.

  Como parte del plan de continuidad de las operaciones, deben planificarse respaldos periódicos del sistema y de los datos. Además, deben efectuarse ensayos periódicos de los procesos de recuperación para verificar que en caso de incidente de seguridad física informática los sistemas puedan reconstruirse y recuperarse prontamente, restableciendo las configuraciones correctas conocidas.

— Procesos de contingencia para restringir y/o modificar el control del acceso en apoyo de los procesos de respuesta, análisis e investigación, incluidas la planificación y la configuración de cuentas de usuario de emergencia.

  Durante un incidente de seguridad física informática puede ser necesario restringir el acceso a los sistemas, redes e instalaciones a determinados usuarios solamente, según el alcance de la investigación. Para hacerlo de manera eficiente, tiene que haber medidas técnicas que se puedan aplicar antes de que se produzcan nuevos daños, así como medidas administrativas en virtud de las cuales las personas que adopten la decisión de restringir los recursos tengan claras sus facultadas y cuenten con el respaldo de la administración.

— Confirmación del funcionamiento correcto del sistema (es decir, un procedimiento para verificar que el sistema funciona normalmente).

  La definición del estado normal de un sistema requiere una lista de controles verificables, con sus rangos de valores correspondientes al funcionamiento normal. La puesta a prueba regular de esos controles es una buena manera de entender el funcionamiento del sistema y detectar los comportamientos anómalos. Las pruebas pueden ser realizadas por operadores de seguridad física informática y, periódicamente, por evaluadores independientes.

— Procesos de validación de la integridad de los datos.

  No es suficiente suponer que un sistema que produzca datos estará generando datos que no han sido alterados. Esto es especialmente importante para los SCI de la

instalación que proporcionan datos sobre el funcionamiento físico de procesos y/o componentes. Estos datos pueden verificarse periódicamente para comprender y validar los comportamientos.

— Medidas o sistemas secundarios de respaldo.

En caso de fallo de un sistema o componente, tiene que haber sistemas o medidas definidos para compensar ese fallo, con procesos que permitan la transición de los sistemas que puedan estar afectados a sistemas seguros y posiblemente redundantes. Para ello puede ser necesario restablecer una configuración de construcción segura o pasar a un sistema de respaldo. También pueden requerirse medidas o sistemas compensatorios para mitigar las repercusiones o recuperar la función perdida.

— Manejo de las condiciones de amenaza informática alta (una nueva vulnerabilidad o un exploit aplicable a los sistemas de la instalación).

La respuesta a incidentes incluye el proceso de evaluación y la adaptación para hacer frente a los cambios en las condiciones de la amenaza informática. La nueva vulnerabilidad o los nuevos exploits pueden tratarse mediante el proceso de parcheado de seguridad.

— Procedimientos de recertificación o aceptación del sistema antes del reinicio.

Antes de volver a poner en funcionamiento un componente o un proceso que apoye las funciones de la instalación, puede ser necesario un cierto nivel de recertificación para garantizar la integridad del sistema y comprobar que esté libre de toda *vulneración* y protegido contra el incidente que causó el problema. Además, las condiciones de la licencia pueden exigir un determinado nivel de recertificación.

— Procedimientos especiales en respuesta a un deterioro de la seguridad tecnológica o de sistemas especiales de seguridad tecnológica.

Además de la respuesta normal ante un incidente de seguridad física informática, si el incidente ha repercutido en la seguridad tecnológica o en sistemas especiales de seguridad tecnológica puede ser necesario aplicar procesos adicionales descritos en otros procedimientos. Es importante comprender y definir la interfaz entre esos procedimientos.

— Detección y notificación de las sospechas de incidentes de seguridad física informática.

Aunque puede ser difícil determinar la *vulneración* de una computadora o una operación defectuosa conexa, se necesitan procesos claramente definidos para ayudar al personal a detectar y notificar toda actividad informática sospechosa.

— Recolección de pruebas[3].

Las pruebas digitales son esenciales a muchos niveles: para descubrir los posibles motivos del atacante, la identidad de los perpetradores, el propósito del software maligno, etc. Se requieren procedimientos que indiquen cómo reunir las pruebas y

[3] Recolección de pruebas: la norma internacional ISO/IEC 27037:2012(E) contiene directrices para la realización de actividades específicas de identificación, recopilación, adquisición y preservación de pruebas digitales que puedan tener valor probatorio. Toda persona que intervenga en la respuesta a un incidente de seguridad física informática debe tener clara la fragilidad intrínseca de las pruebas digitales basadas en computadoras, que pueden ser alteradas, manipuladas ilícitamente o destruidas mediante un manejo o un examen incorrectos. Durante la identificación, recopilación, adquisición y preservación de las posibles pruebas digitales es necesario aplicar una metodología aceptable para garantizar la integridad y autenticidad de esos posibles elementos de prueba digitales. Una metodología aceptable para obtener esas pruebas contribuirá a su admisibilidad en las actuaciones judiciales y disciplinarias. En el anexo VI figura más información sobre la recolección de pruebas digitales.

cómo preservar la cadena de custodia de conformidad con los requisitos jurídicos. Estos procedimientos pueden referirse también a efectos ambientales tales como la humedad, la temperatura y el choque a que ha estado expuesto el dispositivo digital, las opciones para el embalaje, y los requisitos aplicables al transporte y el almacenamiento. La recolección y el procesamiento de las pruebas digitales pueden dejarse en manos de las *autoridades competentes*, pero es fundamental que los propietarios de los sistemas y el CSIRT local comprendan y apoyen estos procesos.

En el Plan de Respuesta a Incidentes de Seguridad Física Informática pueden indicarse los representantes de las fuerzas del orden que se habrán de contactar, las condiciones en que es necesario comunicarles que ha ocurrido un incidente de seguridad física informática, cómo hacer esa comunicación, cuáles pruebas deberán recolectarse y el proceso de recolección de pruebas que se deberá utilizar.

4. FASES DE LA RESPUESTA A UN INCIDENTE DE SEGURIDAD FÍSICA INFORMÁTICA

4.1. PANORAMA GENERAL

En la presente sección se describen las distintas fases de la respuesta a un incidente de seguridad física informática y las tareas y responsabilidades asignadas a la *entidad explotadora*, la *autoridad competente* y la autoridad técnica. En el caso de muchas de esas tareas, la responsabilidad es compartida y recae en más de una de estas entidades.

El proceso de respuesta consta de cuatro fases interdependientes: la preparación; la detección y el análisis; la contención, erradicación y recuperación; y la actividad posterior al incidente. Con frecuencia, múltiples grupos trabajarán en los diferentes aspectos de la respuesta. La colaboración y el flujo de la información entre estos grupos, y de una fase a la siguiente, son esenciales para la rápida resolución del incidente y la pronta recuperación.

4.2. PREPARACIÓN

La fase de preparación comprende las funciones clave de la planificación, a saber, el establecimiento de una política que sirva de base para elaborar los procesos operacionales y defina claramente las funciones y responsabilidades de todas las partes involucradas en el proceso de respuesta al incidente; la redacción e implementación de procedimientos para aplicar las medidas de política; y la identificación de los activos. Es importante que los criterios para los incidentes de seguridad física informática estén claramente definidos, al igual que los requisitos aplicables a la respuesta correspondiente. También es esencial que la administración superior haya dado su acuerdo a esas funciones de planificación y respuesta.

Asimismo, durante la fase de preparación se alienta al CSIRT o a los CSIRT a que participen en ejercicios de seguridad física, tanto por separado como junto con otros grupos de primeros actuantes y de respuesta a emergencias. Estos ejercicios pueden consistir en debates y análisis de posibles escenarios de *vulneración*, evaluaciones del *riesgo* y el impacto, actividades para asegurarse de que el personal conozca las otras funciones de respuesta a un incidente, y el orden de prioridad de las actividades de recuperación. Los ejercicios son a la vez una actividad de garantía específica y un medio para detectar cualquier deficiencia en las actividades de respuesta.

El cuadro que figura a continuación contiene una lista de las tareas correspondientes a la fase de preparación del proceso de respuesta a un incidente de seguridad física informática. Cada tarea estará asignada a una o varias de las organizaciones siguientes: la *entidad explotadora* (EE), la *autoridad competente* (AC) o la autoridad técnica (AT).

CUADRO 1. TAREAS DE LA FASE DE PREPARACIÓN

	Tarea	EE	AC	AT	Observaciones
1.	Establecer la política de respuesta a incidentes de seguridad física informática, incluidas las funciones y responsabilidades.	X	X	X	Las funciones y responsabilidades deben incluir la relación entre las organizaciones. La AC debe tener una política de respuesta a los incidentes de seguridad física informática.
2.	Designar el Grupo de Respuesta a Incidentes de Seguridad Física Informática (CSIRT).	X	X		La EE y la AC deben designar el grupo de conformidad con las funciones y responsabilidades establecidas.

	Tarea	EE	AC	AT	Observaciones
3.	Desarrollar los procedimientos de respuesta a un incidente de seguridad física informática.	X	X	X	Es aconsejable que los procedimientos incluyan los requisitos y criterios de comunicación para las actividades en que participen distintas organizaciones.
4.	Determinar los *activos digitales de carácter estratégico*.	X			Conocer estos activos, su configuración, su arquitectura y el flujo de datos es esencial para la respuesta y la recuperación.
5.	Determinar el *riesgo* y definir las prioridades de la respuesta.	X			La EE tiene la responsabilidad de determinar el *riesgo* y definir las prioridades de la respuesta, recurriendo a expertos, cuando sea necesario.
6.	Determinar las capacidades necesarias y las posibles lagunas en la respuesta a un incidente de seguridad física informática.	X			La EE tiene la responsabilidad de determinar las capacidades necesarias, así como cualquier laguna en la arquitectura o el plan de seguridad física informática que pudiera obstaculizar o impedir una respuesta adecuada.
7.	Determinar las herramientas que se utilizarán en la respuesta a un incidente de seguridad física informática y garantizar su disponibilidad.	X		X	La AT puede proporcionar una lista de las herramientas que recomienda para apoyar las capacidades de defensa informática y la preparación de artefactos para su procesamiento por la AT. Se recomienda que la EE indique y, si es posible, cualifique[4] las herramientas que se emplearán en el proceso de respuesta a un incidente de seguridad física informática. Las herramientas pueden respaldar la recopilación de información sobre el incidente y el análisis de este.
8.	Velar por que el CSIRT disponga de información exacta y actualizada sobre la arquitectura, el diagrama de flujo de los datos y la configuración.	X			La EE es responsable de la exactitud de todos los diagramas de la arquitectura, incluidos el flujo de datos y los datos sobre la configuración.
9.	Velar por que el CSIRT realice ejercicios de seguridad física (tanto por separado como junto con otros grupos de respuesta a emergencias).	X	X	X	Es conveniente que la EE realice simulacros y ejercicios de respuesta a emergencias (con la participación periódica de la AC y la AT) para validar los procedimientos de respuesta, incluidos los requisitos relativos a la comunicación entre las organizaciones.
10.	Examinar y analizar los posibles escenarios de *vulneración* que sean compatibles con la evaluación de la amenaza o la amenaza base de diseño.	X	X	X	Se aconseja que la EE, la AC y la AT repitan periódicamente esta tarea para cerciorarse de que se han incorporado los nuevos vectores de amenazas y actualizado los escenarios de *vulneración*.
11.	Definir los criterios para la notificación de los incidentes de seguridad física informática.		X	X	La AC y la AT deben determinar los criterios y umbrales de los incidentes de seguridad física informática que activarán los requisitos de notificación, y definir los casos en que se recomiende la consulta externa.

[4] Es decir, certifique que satisfacen los requisitos de cualificación del equipo o el software en las condiciones en que pueden tener que cumplir sus funciones de seguridad tecnológica y física. El equipo cualificado que contiene programas informáticos es equipo que se ha sometido a ensayos para verificar que no generará efectos adversos en los sistemas en que se ponga en servicio o en uso.

	Tarea	EE	AC	AT	Observaciones
12.	Definir y aplicar métodos de detección automáticos y manuales.	X	X	X	La AC y la AT proporcionarán orientaciones sobre los métodos de detección como parte de las buenas prácticas. La EE determinará cuáles de ellos será indispensable aplicar, en función de las características específicas de la infraestructura y los *activos digitales de carácter estratégico* de su instalación.
13.	Realizar exámenes y evaluaciones periódicos del Plan de Respuesta a Incidentes de Seguridad Física Informática de la *entidad explotadora*.	X	X		Tanto la EE como la AC tienen que llevar a cabo actividades de evaluación relacionadas con la respuesta a incidentes de seguridad física informática.

4.3. DETECCIÓN Y ANÁLISIS

Durante la fase de detección y análisis, el CSIRT se encarga de determinar la caracterización técnica del incidente. Como parte de las actividades de detección, debe velarse por que exista una infraestructura de monitorización de datos adecuada para respaldar la detección, recolección y preservación de la información que se relacione con incidentes reales o potenciales. El CSIRT podrá utilizar un entorno de prueba y evaluación para analizar el incidente, a fin de no perturbar los sistemas operacionales o dañar las posibles pruebas forenses.

Una de las partes más difícil de la fase de detección y análisis es determinar cuáles sucesos habrán de rastrearse en el proceso de respuesta a un incidente de seguridad física informática. En el anexo I de este documento figuran dos listas de indicadores de incidentes de seguridad física informática, y en el anexo IV se presentan escenarios de incidentes que aportan el contexto de esos indicadores.

Las actividades de análisis pueden realizarse a muchos niveles distintos e ir más allá de la labor del grupo de respuesta inicial a un incidente de seguridad física informática y de la caracterización técnica inicial del incidente. Algunos aspectos del análisis pueden requerir mucho tiempo y esfuerzo. Las prioridades del análisis podrían ser:

1. Determinar las posibles repercusiones del incidente en la seguridad tecnológica, la seguridad física y la preparación para emergencias, así como las medidas necesarias para poner la organización o instalación en un estado seguro.

2. Determinar el alcance del incidente para poner en marcha una respuesta adecuada.

3. Determinar el daño que puede causar el incidente en lo que respecta a la posible pérdida de información, los daños físicos a la instalación y la percepción pública.

4. Determinar la naturaleza del incidente en lo que respecta a la intención del atacante y a la amenaza existente.

5. Determinar la causa raíz del incidente y los esfuerzos necesarios para prevenir o mitigar su repetición en el futuro.

6. Identificar la fuente del ataque y el atacante, y elaborar un perfil de este.

En la sección 4 figuran más orientaciones sobre los tipos de análisis que pueden ser necesarios en un incidente. El anexo II de este documento contiene una guía para el análisis de los incidentes, y el anexo VI ofrece un panorama general del proceso de recolección de pruebas forenses para apoyar el análisis de un incidente de seguridad física informática. Esta

información respaldará la respuesta colectiva del CSIRT, del personal directivo de la organización y de todas las partes externas interesadas.

En el cuadro siguiente se enumeran las tareas correspondientes a la fase de detección y análisis del proceso de respuesta a un incidente de seguridad física informática que respaldan la creación de una caracterización técnica y la evaluación del daño causado por el incidente. Cada tarea estará asignada a una o varias de las organizaciones siguientes: la *entidad explotadora* (EE), la *autoridad competente* (AC) o la autoridad técnica (AT).

CUADRO 2. TAREAS DE DETECCIÓN Y ANÁLISIS

	Tarea	EE	AC	AT	Observaciones
1.	Notificar los incidentes de seguridad física informática o las actividades sospechosas.	X	X		La AC puede establecer requisitos específicos de notificación de los sucesos informáticos. En ellos pueden detallarse los sucesos concretos que la EE deberá notificar.
2.	Velar por la adecuada monitorización de los datos.	X	X		La EE tiene la responsabilidad de velar por la adecuada monitorización de los datos, y la AC es responsable de supervisar el cumplimiento de esta obligación por la EE.
3.	Construir un entorno de prueba y evaluación adecuado.	X		X	La EE tiene la responsabilidad de construir un entorno de prueba y evaluación adecuado, teniendo en cuenta las orientaciones de la AT, cuando corresponda.
4.	Recoger y preservar la información.	X		X	La EE tiene la responsabilidad de recoger y preservar la información, teniendo en cuenta las orientaciones de la AT, cuando corresponda.
5.	Analizar la ciberamenaza y actualizar la evaluación de la amenaza.	X	X	X	La EE tiene la responsabilidad de actualizar y/o reanalizar las evaluaciones de la amenaza, teniendo en cuenta las orientaciones de la AT y la AC, cuando corresponda.
6.	Determinar las posibles repercusiones en la seguridad tecnológica, la seguridad física y la preparación para emergencias, así como las medidas inmediatas necesarias para poner la instalación en un estado tecnológica y físicamente seguro.	X			La EE tiene la responsabilidad de determinar las posibles repercusiones de un incidente de seguridad física informática en la seguridad tecnológica, la seguridad física y la preparación para emergencias.
7.	Determinar cuáles organizaciones participarán en la respuesta.	X	X	X	La determinación de las entidades que serán informadas o a las que se hará participar en la respuesta a un incidente de seguridad física informática requiere a veces una decisión colectiva de la EE, la AC y la AT.
8.	Determinar la causa raíz (que puede ser un proceso en curso) y las medidas compensatorias.	X		X	Se aconseja que la EE realice un análisis de la causa raíz, con el apoyo de la AT, cuando sea el caso.
9.	Determinar los límites de la infección y las vías de propagación.	X		X	La EE debe determinar los límites de la infección y la propagación, con el apoyo de la AT, cuando sea el caso.
10.	Evaluar la *vulneración* de sistemas similares.	X		X	La EE debe evaluar si están comprometidos otros sistemas similares, con el apoyo de la AT, cuando sea el caso.

	Tarea	EE	AC	AT	Observaciones
11.	Evaluar la *vulneración* de otras instalaciones.		X	X	Si una instalación está afectada, muchas otras podrían también estar comprometidas. Tras un incidente de seguridad física informática, la AC y la AT deben trabajar con otras instalaciones para determinar si están infectadas o comprometidas.
12.	Elaborar una estrategia de mitigación.	X		X	La EE debe elaborar una estrategia de mitigación para el incidente de seguridad física informática, teniendo en cuenta las orientaciones de la AT, cuando corresponda.

4.4. MITIGACIÓN (CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN)

Dado el carácter cíclico y continuo del proceso de respuesta a incidentes de seguridad física informática, las actividades de mitigación también deben ser continuas e irse adaptando a medida que se reúne y analiza más información durante la fase de detección y análisis. Los objetivos de la mitigación son: 1) contener el incidente de seguridad física informática, 2) erradicar todo software maligno de los sistemas afectados, y 3) recuperar la función del sistema, lo que puede requerir otras medidas compensatorias. Incluso si los componentes o sistemas comprometidos no cumplen una función de seguridad física o tecnológica fundamental, deberán ser controlados y declarados conformes para evitar la propagación del ataque a un componente o sistema que sí cumpla una función de seguridad tecnológica o física de importancia crítica.

Al planificar una estrategia de contención, es importante tener en cuenta que durante la investigación de un incidente se puede determinar que hay una serie de componentes comprometidos. Si uno de ellos cumple una función de seguridad tecnológica o física fundamental para la organización —por ejemplo, porque contribuye a la protección de *activos digitales de carácter estratégico* o al comportamiento seguro de la instalación o de los *materiales nucleares* u *otros materiales radiactivos*— será necesario aplicar medidas para que no se interrumpa la protección, hasta que el componente pueda volver a funcionar. Tales medidas podrían incluir la sustitución de un servicio por otro igual (como un cortafuego de respaldo), el aislamiento de componentes, sistemas y arquitecturas de seguridad tecnológica, o una solución temporal, como un guardia de seguridad que proteja el acceso a una parte de la instalación, por ejemplo si el sistema de control digital del acceso no está disponible. Lo que debe recuperarse es la función, no necesariamente el propio sistema informático.

Los tres pasos de la mitigación —la contención, la erradicación y la recuperación— se pueden ilustrar, por ejemplo, para el caso de que se descubra un software maligno en un sistema. El primer paso sería neutralizar la posibilidad de propagación por medio de vectores de infección ya existentes o nuevos. Lo siguiente sería determinar si es necesario desplegar medidas adicionales, como herramientas de vigilancia de la seguridad física o firmas actualizadas para las herramientas existentes, a fin de proteger y defender los sistemas contra la reinfección. Por último, se puede realizar una reconstrucción del sistema, reinstalando el sistema operativo y el software conexo a partir de una copia fiable y recuperando luego los datos del sistema a partir de los respaldos correctos de que se disponga. En el caso de los sistemas de control industrial, este paso podría incluir también la instalación de nuevo equipo. Una vez reconstruido el sistema, puede ser necesario realizar pruebas de aceptación para verificar su funcionamiento e integridad.

En el cuadro que figura a continuación se enumeran las tareas correspondientes a la fase de mitigación del proceso de respuesta a un incidente de seguridad física informática que respaldan la restauración de las funciones y los sistemas necesarios (y que pueden requerir el

uso de medidas compensatorias). Cada tarea estará asignada a una o varias de las organizaciones siguientes: la *entidad explotadora* (EE), la *autoridad competente* (AC) o la autoridad técnica (AT).

CUADRO 3. TAREAS DE MITIGACIÓN

	Tarea	EE	AC	AT	Observaciones
1.	Velar por que la instalación (y/o el sistema) se ponga en un estado tecnológica y físicamente seguro.	X			La EE debe adoptar las medidas adecuadas para poner el sistema, los sistemas o la instalación en un estado tecnológica y físicamente seguro.
2.	Neutralizar la propagación y los nuevos vectores de infección (p. ej., aplicando medidas compensatorias).	X		X	La EE tiene la responsabilidad de neutralizar la propagación y los nuevos vectores de infección que pueda haber, con la asistencia de la AT, cuando corresponda.
3.	Llevar a cabo la reconstrucción del sistema y la recuperación a partir de un respaldo.	X	X	X	La EE es responsable de reconstruir el sistema, de conformidad con las directrices para la seguridad física establecidas por la AC y en consulta con la AT, para evitar la reinfección del sistema.
4.	Instalar nuevo equipo.	X	X		Algunos incidentes de seguridad informática pueden conducir a una situación en que sea preferible sustituir el equipo en lugar de recuperarlo. La EE puede tener que instalar nuevo equipo, respetando las orientaciones de la AC sobre la instalación de sistemas y su acreditación.
5.	Vigilar el proceso de mitigación.	X	X		Durante la mitigación, es aconsejable que la EE vigile el proceso para comprobar su eficacia. De igual modo, la AC puede exigir actualizaciones periódicas del proceso de mitigación y su eficacia.
6.	Vigilar que no haya reinfección.	X		X	La EE tiene la responsabilidad de vigilar el entorno para comprobar que no haya reinfección, recurriendo a las competencias técnicas de la AT cuando proceda.

Si un entorno está infectado, el CSIRT y el perito forense tienen por lo menos dos responsabilidades:

— Confeccionar una lista de las acciones observables que caracterizan a la cepa de software maligno de que se trate, como los cambios en el sistema de archivos, las modificaciones de los registros, las balizas y los eventos de registro; esta información puede añadirse luego a los conjuntos de reglas alimentados por esos sensores.

— Confeccionar una lista de las firmas de software maligno que pueda actualizarse en los programas antivirus maestro y cliente y en el sensor de límite.

4.5. ACTIVIDAD POSTERIOR AL INCIDENTE

La última fase de la respuesta son las actividades posteriores al incidente. El objetivo es aplicar medidas para evitar la repetición de ese tipo de incidente de seguridad física informática en el futuro, o para detectarlo rápidamente y reducir al mínimo sus efectos, si se produce. Esta fase puede incluir la determinación de las lecciones aprendidas, para su uso interno y posiblemente para darlas a conocer a la comunidad más amplia que trabaja en la respuesta a incidentes de seguridad física informática, a fin de contribuir a evitar que un

ataque similar tenga éxito en otro lugar. Las principales conclusiones pueden conducir finalmente a la aplicación de nuevas medidas de seguridad física para prevenir la reinfección, y a la actualización de los perfiles de las amenazas dentro de las evaluaciones de la ciberamenaza. Otras actividades son la evaluación de la eficacia del plan de seguridad física informática y la determinación de la capacitación necesaria para subsanar las deficiencias en el desempeño. Esto puede comprender también una evaluación de los recursos que se requirieron para hacer frente al incidente en cuestión.

En el cuadro que figura a continuación se enumeran las tareas correspondientes a la fase de la actividad posterior al incidente del proceso de respuesta a un incidente de seguridad física informática que respaldan la aplicación de medidas para prevenir la repetición del incidente, incluidas la determinación de las lecciones aprendidas y la aplicación de nuevas medidas de seguridad física para evitar esa repetición. Cada tarea estará asignada a una o varias de las organizaciones siguientes: la *entidad explotadora* (EE), la *autoridad competente* (AC) o la autoridad técnica (AT).

CUADRO 4. TAREAS POSTERIORES AL INCIDENTE

	Tarea	EE	AC	AT	Observaciones
1.	Elaborar las lecciones aprendidas.	X	X	X	En la medida en que hayan participado en la respuesta, la EE, la AC y la AT tienen la responsabilidad de extraer las lecciones aprendidas de cada incidente de seguridad física informática.
2.	Potenciar las medidas de seguridad física para prevenir la reinfección.	X	X	X	La EE tiene la responsabilidad de potenciar las medidas de seguridad física; la AT podrá ser consultada, cuando sea necesario y adecuado, y la AC puede tener que aprobar las nuevas medidas de seguridad física, cuando así esté prescrito.
3.	Actualizar la evaluación de la amenaza.	X	X	X	La EE actualizará la evaluación de la amenaza sobre la base del análisis posterior al incidente; la AT podrá ser consultada, cuando corresponda.
4.	Evaluar la eficacia del plan de seguridad física informática.	X	X		Se aconseja que la EE evalúe la eficacia de su plan de seguridad física informática, y rinda informe de ello a la AC, cuando corresponda.
5.	Realizar actividades de capacitación y ejercicios para subsanar las deficiencias en el desempeño.	X	X	X	La capacitación y los ejercicios para subsanar las deficiencias en el desempeño pueden diseñarse de modo que incluyan a la EE, la AC y/o la AT, en función de la naturaleza de la deficiencia y de los factores de que dependa.
6.	Presentar los informes posteriores al incidente que correspondan.	X	X	X	La EE, la AC y la AT pueden tener sus propios requisitos de presentación de informes.
7.	Realizar una evaluación de los recursos asignados.	X		X	La EE podrá realizar una evaluación con el fin de determinar los recursos que fueron necesarios para hacer frente al incidente de seguridad física informática, solicitando la orientación de la AT, cuando sea el caso.
8.	Compartir las lecciones aprendidas con la comunidad más amplia.	X	X	X	La EE, la AC y la AT tal vez deseen compartir las lecciones aprendidas con la comunidad más amplia de expertos en el mismo campo. Esto puede hacerse por medio de un único documento, pero todas las partes que hayan intervenido en la respuesta al incidente de seguridad física informática tienen que poder contribuir a la elaboración de las enseñanzas extraídas según corresponda.

4.6. COMUNICACIÓN DE INFORMACIÓN

Durante el proceso de respuesta a un incidente de seguridad física informática puede haber varias situaciones o fases en que sea necesario comunicar información a distintos organismos, no solo cuando se inicie la respuesta al incidente sino también durante el resto del proceso. El objetivo de ello es que toda persona que necesite tener conocimiento de un incidente de seguridad física informática sea informada oportunamente, teniendo presente que en ciertos tipos de incidentes los actuantes tendrán probablemente mucho que hacer. La determinación de la frecuencia de esos informes y del grado de detalle requerido es a menudo un reto para las organizaciones.

En el cuadro que figura a continuación se enumeran las tareas que deben realizarse en la fase de comunicación de información del proceso de respuesta a un incidente de seguridad física informática para velar por que los organismos pertinentes estén debidamente informados de todo incidente que se considere grave o crítico. Cada tarea estará asignada a una o varias de las organizaciones siguientes: la *entidad explotadora* (EE), la *autoridad competente* (AC) o la autoridad técnica (AT).

CUADRO 5. TAREAS DE COMUNICACIÓN DE INFORMACIÓN

	Tarea	EE	AC	AT	Observaciones
1.	Especificar normas para toda la organización sobre los límites de tiempo dentro de los cuales los administradores de sistemas y otros funcionarios deberán informar de los incidentes de seguridad física informática anómalos al CSIRT.	X	X		Estas directrices especificarán los criterios para la comunicación de los incidentes y el plazo que se tendrá para hacerla. Puede haber requisitos a este respecto para las comunicaciones iniciadas por la EE y por la AC.
2.	Especificar los mecanismos que se utilizarán para informar sobre la respuesta a un incidente, y el tipo de información que deberá incluirse en la notificación.	X	X	X	Es importante establecer el mecanismo y el formato de las notificaciones antes de que ocurran incidentes de seguridad física informática.
3.	Determinar en qué situaciones un incidente de seguridad física informática requerirá la notificación de la AT, de conformidad con los requisitos jurídicos o reglamentarios.	X	X	X	La EE debe saber cuándo está obligada por la AC a informar de un incidente de seguridad física informática a la AT.
4.	Reunir y mantener la información de contacto que se utilizará para comunicar los incidentes de seguridad física informática.	X	X	X	Es importante que haya puntos de contacto entre la EE, la AC y la AT para los incidentes de seguridad física informática y su notificación.
5.	Proporcionar retroinformación y sensibilizar a los funcionarios y al personal del emplazamiento con respecto a la prevención y la respuesta a incidentes futuros.	X			Es importante que los funcionarios y el personal del emplazamiento reciban periódicamente una capacitación de sensibilización sobre la seguridad física que incluya una estructura y claros criterios para las notificaciones.

5. ANÁLISIS DE LOS INCIDENTES DE SEGURIDAD FÍSICA INFORMÁTICA

5.1. PANORAMA GENERAL

El análisis de un incidente de seguridad física informática es una actividad que se lleva a cabo a lo largo de todas las fases de la respuesta y que tiene diferentes objetivos y requiere distintos tipos de competencias. Además de las repercusiones en la seguridad física, el análisis incluye la evaluación técnica del incidente y de los múltiples niveles de impacto en las operaciones y en la seguridad tecnológica. Ciertos análisis están supeditados a otros, pero algunos se pueden realizar simultáneamente. Los tipos de análisis posibles incluyen, entre otros:

— El análisis del impacto: ¿cuál es el impacto ambiental, político, económico, financiero y social del incidente?

— El análisis de la seguridad tecnológica: ¿Cuáles son las repercusiones en la seguridad tecnológica nuclear y en las funciones de seguridad tecnológica del personal? ¿Se requieren medidas inmediatas para evitar que se llegue a condiciones de accidente o para poner la instalación en un estado seguro? ¿Podría la progresión del incidente aumentar su gravedad?

— La caracterización técnica: ¿Cuáles son el tipo y la naturaleza del ataque? ¿Cuán eficaz es el perfil de seguridad física vigente contra ese tipo de ataque? ¿Está protegida la instalación contra la progresión del incidente? En otras palabras, ¿son suficientes las medidas de seguridad física vigentes para impedir un aumento del nivel de gravedad del incidente?

— El análisis de la amenaza: este es el análisis del incidente en términos de la modificación de la amenaza. ¿Es el incidente un indicador de actividades agresivas por parte de un nuevo adversario? ¿Indican el *blanco*, las herramientas y la táctica una nueva capacidad o iniciativa por parte de un adversario? Por consiguiente, ¿tiene la organización que actualizar su posición de seguridad física con respecto a la amenaza?

Estos análisis ayudarán al personal directivo y a los grupos de respuesta a caracterizar el incidente (según las categorías de gravedad que se exponen a continuación) y a establecer las prioridades adecuadas para la respuesta (es decir, la gestión de la progresión).

5.2. CATEGORIZACIÓN DE LA GRAVEDAD

El concepto de las categorías de gravedad ayuda a comunicar y notificar los incidentes de seguridad física informática sospechosos. La evaluación de un incidente de seguridad física informática y su asignación a una categoría de gravedad ofrecen un medio de expresar el impacto real o potencial de un incidente. Aunque los incidentes de seguridad física informática pueden categorizarse de muchas maneras diferentes —por tipo, manifestación, etc.— su asignación a una categoría de gravedad se centra específicamente en el impacto.

Todavía no existe un consenso internacional afianzado para la asignación de los incidentes de seguridad física informática a categorías de gravedad en función de la seguridad física nuclear, pero el cuadro siguiente proporciona un ejemplo de un esquema de categorización posible. Este esquema puede adaptarse a las distintas organizaciones y tiene por objeto ayudar a establecer las prioridades entre las actividades y los recursos de respuesta. Se recomienda que los Estados Miembros elijan un esquema de categorización apropiado que corresponda a sus necesidades.

Las categorías de gravedad van de la categoría 0 (funcionamiento normal) a la categoría V, que representa el impacto más grave.

CUADRO 6. DESCRIPCIÓN GENERAL DE LAS CATEGORÍAS DE GRAVEDAD

Categoría de gravedad	Descripción
V	Incidentes de seguridad física informática que dan lugar a una o más de las situaciones siguientes: — un suceso relacionado con la seguridad tecnológica nuclear; — el robo de *materiales nucleares* u *otros materiales radiactivos*; — un acto de sabotaje de instalaciones con *materiales nucleares* u *otros materiales radiactivos* que acarree daños materiales/consecuencias importantes.
IV	Incidentes de seguridad física informática que dan lugar a una o más de las situaciones siguientes: — la ejecución/activación de sistemas de seguridad tecnológica (p. ej., una parada automática), procedimientos de seguridad tecnológica (p. ej., una parada iniciada por un operador), y/o procedimientos de emergencia; — la pérdida o *vulneración* de las funciones del sistema de protección física; — la pérdida o *vulneración* de las funciones de control y contabilidad de los *materiales nucleares*; — la pérdida o *vulneración* de información nuclear de carácter estratégico que pueda repercutir gravemente en la seguridad nuclear tecnológica y física y posiblemente favorecer un suceso de la categoría V.
III	Incidentes de seguridad física informática que incluyen: — indicadores de la actividad de un agresor en sistemas internos; — indicadores de posibles actividades de reconocimiento; — ataques no específicos con un impacto mínimo; — la pérdida o *vulneración* de información nuclear de carácter estratégico que pueda repercutir moderadamente en la seguridad nuclear tecnológica y física.
II	Existencia en otro lugar de un exploit o actividad que podría repercutir en la seguridad nuclear tecnológica o física. No se detecta ningún efecto inmediato.
I	Detección de una vulnerabilidad de la seguridad física informática que podría repercutir en la seguridad nuclear tecnológica o física.
0	Funcionamiento normal.

Las categorías de gravedad III a V comprenden indicaciones de que se ha producido un ciberataque real a los sistemas internos.

Obsérvese que las categorías de gravedad se relacionan con el impacto, y no con el propio ataque o vector de intrusión, y que el cuadro anterior y la descripción que sigue se dan solo a título de ejemplo, para ayudar a las organizaciones a informar sobre la respuesta a un incidente de seguridad física informática y a determinar las prioridades en ella.

5.2.1. Categorías de gravedad V y IV

Los incidentes de seguridad física informática de la categoría V son los que dan lugar a graves violaciones de la seguridad nuclear física y/o tecnológica. Los ataques de categoría V suelen tener consecuencias materiales.

Los incidentes de seguridad física informática de la categoría IV son los que pueden plantear una amenaza inmediata y grave para los objetivos de seguridad nuclear tecnológica y física. Estos incidentes producen una degradación de la seguridad física, la seguridad tecnológica o los sistemas operacionales, pero no conducen a la inhabilitación completa de estos sistemas para cumplir sus funciones de seguridad tecnológica o física.

Las actividades que se enumeran a continuación [9] pueden contribuir a generar accidentes de las categorías V y IV:

— La *vulneración*/intrusión de un sistema. Todos los casos intencionales o no intencionales de *vulneración* de un sistema o de intrusión en él por personas no autorizadas, con inclusión de la *vulneración* a nivel del usuario, la *vulneración* a nivel del administrador, y los casos en que los usuarios sobrepasan sus privilegios.

— Los códigos malignos. Todos los casos de infección, o de intentos persistentes de infección, por un código maligno —como los virus, los caballos de Troya o los gusanos informáticos— que plantean una amenaza para los sistemas o sus funciones.

— La denegación de servicio. La denegación (o el intento persistente de denegación) intencional o no intencional de un servicio que afecta a un sistema o priva de acceso a grandes segmentos de una red, o que amenaza con hacerlo.

— Las actividades no planificadas. Toda actividad no planificada que repercuta negativamente en uno o varios *activos digitales de carácter estratégico* o en las funciones conexas de seguridad nuclear tecnológica o física o en los servicios de emergencia.

— Los usos no autorizados. Toda actividad que repercuta negativamente en el funcionamiento normal, de fondo, de un *activo digital de carácter estratégico* o un sistema conexo y/o que no pueda considerarse relacionada con una unidad operativa o una misión de la administración superior. Son usos no autorizados, entre otros, el escaneo de puertos que degrada excesivamente el funcionamiento; la suplantación de identidad en el Protocolo de Internet (IP); el reconocimiento de redes; la vigilancia; la *vulneración* de servidores; o las actividades ilegales.

— La *vulneración* de la información. Toda divulgación no autorizada de información sobre la seguridad física nuclear que eluda los controles y transmita esa información a entidades que no la necesitan para cumplir una función oficial en la organización.

5.2.2. Categoría de gravedad III

Los incidentes de seguridad física informática de la categoría III plantean una amenaza potencial a largo plazo para los intereses de la seguridad física informática o degradan la eficacia global de la posición de la organización en materia de seguridad física informática. Como ejemplos cabe citar:

— Los intentos de intrusión. Un intento significativo y/o persistente de intrusión distinto de la actividad diaria o del nivel del fondo y que puede dar lugar a un acceso no autorizado (*vulneración*) si el sistema no está debidamente protegido.

— La actividad de reconocimiento. Las sondas y los escaneos persistentes de vigilancia y mapeo de recursos que sobresalen de la actividad diaria o el nivel de fondo y representan una actividad destinada a reunir información sobre las vulnerabilidades de una red o a cartografiar los recursos de red y los servicios disponibles. Los parámetros para la recopilación y notificación de datos sobre los escaneos y las sondas de reconocimiento deben documentarse.

5.2.3. Categoría de gravedad II

Los incidentes de seguridad física de la categoría II son exploits o actividades que han ocurrido en otro lugar y que podrían tener repercusiones similares en la seguridad física de la *instalación nuclear*. Como ejemplos de este tipo de incidentes cabe mencionar:

— La infección por software maligno en otra *instalación nuclear*. Si se detecta una infección por programas malignos en otra *instalación nuclear* y el *blanco* de esos programas es un sistema que también existe en la propia instalación, la situación deberá tratarse como un incidente de seguridad física informática de categoría II.

— La exfiltración de información sobre la arquitectura de red de otra *instalación nuclear*. Si se han robado los planos de la arquitectura de red de una *instalación nuclear* que tiene elementos de diseño de carácter estratégico iguales a los de la propia instalación, la situación deberá tratarse como un incidente de seguridad física informática de categoría II.

5.2.4. Categoría de gravedad I

Los incidentes de seguridad física informática de la categoría I son los casos en que se detecta una vulnerabilidad de la seguridad física informática que podría repercutir en la seguridad nuclear física o tecnológica. En general, se tratará de sucesos que corresponden al espectro de los tipos de incidentes y sucesos posibles, pero que aún no han sido atribuidos a un ataque activo.

5.2.5. Relación de las categorías de gravedad con los niveles de seguridad física

En la publicación Nº 17 de la *Colección de Seguridad Física Nuclear del OIEA*, titulada *Seguridad informática en las instalaciones nucleares* [3] se examina la asignación de niveles de seguridad física informática a zonas de equipos sobre la base de un enfoque graduado de la protección. El objetivo es proteger todos los sistemas informáticos de la instalación que puedan ser objeto de *actos dolosos* con arreglo al nivel de seguridad física informática que se les haya asignado. Por lo tanto, la asignación de los sistemas informáticos a los diferentes niveles de seguridad física informática se basa en su importancia para la seguridad tecnológica y física. Si se aplica este enfoque, las categorías de gravedad de los incidentes de seguridad física informática pueden vincularse con los niveles de seguridad física de los sistemas informáticos.

La categoría de gravedad de un incidente depende de las consecuencias (directas o indirectas) que pueda tener. Estas consecuencias pueden inferirse del nivel de seguridad física informática asignado al sistema. Por lo tanto, el vínculo entre los niveles de seguridad física informática y las categorías de gravedad proporciona una forma ‘intuitiva’ y rápida de determinar la posible

repercusión o consecuencia de un incidente. De este modo, la asignación de niveles de seguridad física informática puede ayudar a expresar la gravedad de los incidentes.

Esta correlación ofrece un punto de partida para la respuesta inicial. En el análisis del incidente de seguridad física informática deberá examinarse si el incidente debe ser elevado a una categoría de gravedad superior.

En el cuadro 7 se presenta un ejemplo de este enfoque.

CUADRO 7. RELACIÓN DE LOS NIVELES DE SEGURIDAD FÍSICA INFORMÁTICA CON LAS CATEGORÍAS DE GRAVEDAD

Nivel de seguridad física informática	Descripción del nivel de seguridad física	Categoría de gravedad máxima
1	Sistemas de importancia vital para la instalación y que requieren el máximo nivel de seguridad física. Los incidentes que afectan a estos sistemas pueden conducir directamente a una violación de un objetivo de seguridad nuclear física o tecnológica.	V
2	Sistemas que requieren un nivel alto de seguridad física. Los incidentes que afectan a estos sistemas pueden conducir indirectamente, pero no de forma directa, a una violación de un objetivo de seguridad nuclear física o tecnológica (una de las funciones de protección sigue disponible).	IV
3	Sistemas de supervisión en tiempo real que no se requieren para las operaciones y que tienen un nivel de gravedad mediano respecto de diversas ciberamenazas. Los incidentes que afectan a estos sistemas pueden utilizarse para preparar una violación de un objetivo de seguridad nuclear física o tecnológica.	III
4	Sistemas de gestión de datos técnicos utilizados para gestionar las actividades de mantenimiento o explotación relacionadas con componentes o sistemas prescritos en la especificación técnica y que tienen un nivel de gravedad mediano respecto de diversas ciberamenazas. Los incidentes que afectan a estos sistemas pueden utilizarse para preparar una violación de un objetivo de seguridad nuclear física o tecnológica.	III
5	Sistemas que no son directamente importantes para fines operacionales o de control técnico. Los incidentes que afectan a estos sistemas pueden utilizarse para apoyar el reconocimiento de las actividades futuras de los adversarios.	III

5.3. CONSECUENCIAS DE LOS INCIDENTES DE SEGURIDAD FÍSICA INFORMÁTICA PARA LA SEGURIDAD TECNOLÓGICA

La seguridad nuclear física y la seguridad nuclear tecnológica tienen en común el objetivo de proteger a las personas, los bienes, la sociedad y el medio ambiente. Las medidas de seguridad física y las medidas de seguridad tecnológica deben diseñarse de manera integrada para aprovechar las sinergias y velar por que las medidas de seguridad física no comprometan la seguridad tecnológica y viceversa [1]. La seguridad física informática tiene repercusiones tanto en la seguridad nuclear tecnológica como en la seguridad nuclear física.

Los incidentes de seguridad física informática (es decir, los ciberataques) pueden dar lugar a sucesos relacionados con la seguridad tecnológica nuclear. Se ha demostrado que los ciberataques son capaces de modificar las funciones de los sistemas de control de una *instalación nuclear* para producir daños materiales; el ataque con el programa maligno Stuxnet fue un ejemplo de ello.

Una instalación que contenga un reactor nuclear (ya sea de potencia o de investigación) puede encontrarse en varios estados diferentes, como se ilustra en la figura 3. Un ciberataque podría, en teoría, poner el sistema en una condición no analizada que se aparte del funcionamiento normal. Los ciberataques pueden modificar la lógica, la configuración o los puntos de tarado de un sistema operativo o engañar al operador e inducirlo a realizar acciones incorrectas. Los resultados de estos ataques pueden dejar a la instalación en un estado que no se haya tomado en consideración en el análisis de la base de diseño y que pueda conducir a condiciones de accidente.

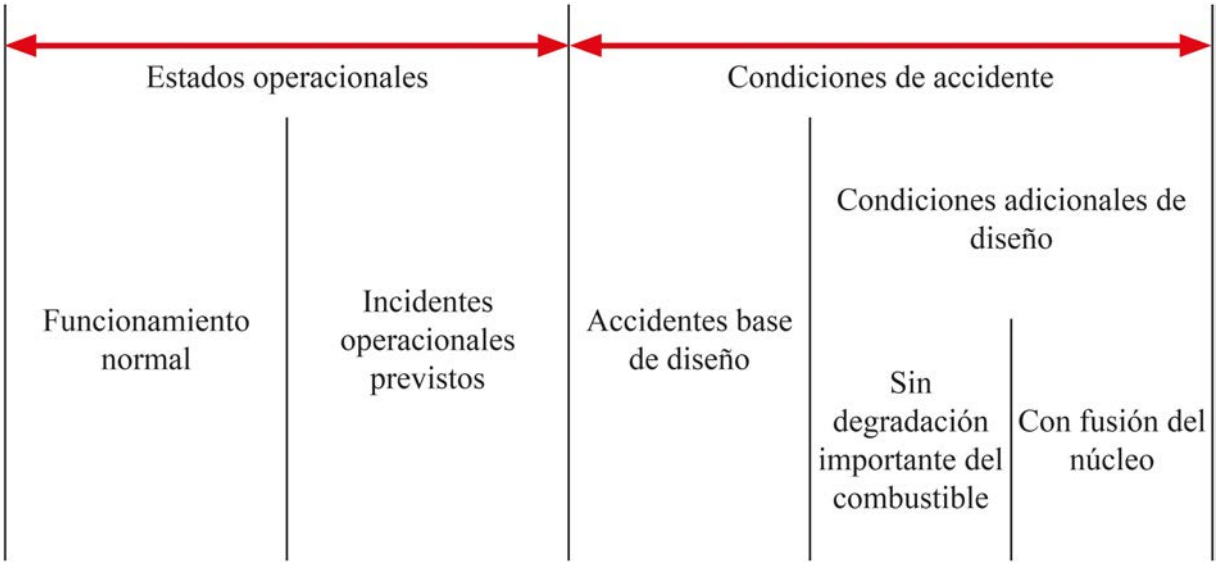

Fig. 4. Estados de una instalación (estados del reactor) [10].

En el Glosario de seguridad del OIEA [10], las condiciones de accidente se definen como "alteraciones del funcionamiento normal más graves que los incidentes operacionales previstos, incluidos los accidentes base de diseño y los accidentes muy graves".

Los procedimientos de operación de emergencia (POE) se elaboran normalmente para el caso de que fallen funciones del sistema de I+C, pero también pueden tener que ocuparse del mal

funcionamiento de un sistema que se deba a un software maligno o a una *vulneración* de un sistema informático. El objetivo principal de los POE es proteger a las personas, la sociedad y el medio ambiente contra los daños derivados de peligros radiológicos. La respuesta al suceso nuclear y la información sobre el suceso deben ceñirse a las orientaciones nacionales e internacionales aprobadas. Secundariamente, los POE pueden ocuparse de aspectos de la respuesta a incidentes de seguridad física informática tales como la recopilación de información y el análisis del incidente.

En el párrafo 4.1 de la Guía de Seguridad NS-G-2.11 [11] de la *Colección de Normas de Seguridad del OIEA* se señala que "[l]a experiencia operacional de la instalación se evaluará de manera sistemática. Los sucesos anormales con consecuencias importantes para la seguridad se investigarán para determinar sus causas directas y básicas." En el mundo de hoy, esas investigaciones deben tomar en consideración la posibilidad de un ciberataque.

Los incidentes de seguridad física informática pueden ser también sucesos de seguridad tecnológica notificables. Como ejemplos de posibles sucesos de seguridad tecnológica notificables cabe mencionar:

- Una parada de la instalación que sea dictada por los límites y condiciones operacionales;
- Un funcionamiento o una condición que estén prohibidos por los límites y condiciones operacionales;
- Cualquier suceso o condición anómala que conduzca a una degradación grave de la condición de la *instalación nuclear*, incluidas sus principales barreras de seguridad tecnológica;
- Cualquier suceso o condición anómala que conduzca al accionamiento manual o automático del sistema de protección del reactor o de dispositivos de seguridad tecnológica;
- Cualquier suceso en que una única causa o condición o una secuencia de eventos conduzca a una pérdida importante de operabilidad de un sistema de seguridad tecnológica;
- Cualquier problema o defecto en el análisis de la seguridad tecnológica, el diseño, la fabricación o la explotación que conduzca o sea capaz de conducir a una condición de explotación no analizada anteriormente o que pueda sobrepasar las condiciones de la base de diseño;
- Cualquier suceso importante relacionado con la seguridad tecnológica que tenga lugar durante una parada o una recarga de combustible (p. ej., la caída de un conjunto combustible);
- Cualquier suceso nuclear que cause muertes o heridas graves entre los miembros del personal del emplazamiento.

La mencionada publicación NS-G-2.11, que se titula *Un sistema de retroinformación sobre la experiencia derivada de sucesos ocurridos en establecimientos nucleares* [10], también contiene una descripción de estos sucesos, con los requisitos de notificación e investigación prescritos.

Aunque el examen se ha centrado en las *instalaciones nucleares*, las mismas consideraciones pueden ser válidas para la seguridad tecnológica de otras instalaciones en que haya *materiales nucleares* y *otros materiales radiactivos*.

5.4. PÉRDIDA O VULNERACIÓN DE INFORMACIÓN DE CARÁCTER ESTRATÉGICO

Los incidentes de seguridad física informática pueden dar lugar a una *vulneración* o pérdida de *información de carácter estratégico*. En el contexto de la seguridad física nuclear, se entiende por *información de carácter estratégico* aquella cuya divulgación (o modificación, alteración, destrucción o denegación de uso) no autorizada podría comprometer la seguridad física nuclear. En la publicación NSS-23-G [6] se ofrecen orientaciones más detalladas sobre la identificación, protección y gestión de la información nuclear. Esa publicación [6] es una guía de aplicación para la investigación de incidentes de seguridad física de la información.

Un incidente de seguridad física informática de esta naturaleza puede extrañar:

- la pérdida o el robo de equipo informático o de soportes portátiles (como un lápiz de memoria USB, un DVD, etc.);
- la pérdida o el robo de un teléfono móvil;
- el acceso no autorizado a una computadora o una red;
- la *vulneración* de una contraseña o un control del acceso;
- software maligno o hardware que extraigan información, como los programas de captura de teclado, de captura de paquetes de red o de captura de pantalla, o los dispositivos de captura de imágenes.

Aunque parte del análisis técnico se centrará en la mecánica del incidente, también deberá evaluarse su impacto. A este respecto, pueden considerarse los siguientes aspectos:

- ¿Quién puede tener la información?
- ¿Fue el robo de información un acto delictivo específico o al azar?
- ¿Está disponible esa información en una fuente de libre acceso?
- ¿Es la información solo en parte de carácter estratégico, o lo es en su totalidad?
- ¿Cuándo se perdió o vulneró la información?
- ¿Cuál es la sensibilidad al factor tiempo de la información perdida?
- ¿Cómo podría utilizarse la información con intenciones dolosas? ¿Cuál es el impacto potencial?
- ¿Qué medidas pueden mitigar el uso o el impacto de esa información?
- ¿Quién más posee la información y puede tener que ser advertido de su *vulneración*?

La sensibilidad de la información vulnerada o perdida puede dictar los requisitos y plazos de notificación de su pérdida o *vulneración* a las *autoridades competentes*. Incluso si la información no se relaciona directamente con la seguridad física nuclear, su naturaleza puede hacer que el incidente deba regirse por los requisitos de notificación de la legislación nacional; un ejemplo sería la pérdida de expedientes médicos o de otra información personal identificable.

5.5. ANÁLISIS DE LA AMENAZA

El análisis de la amenaza es un proceso continuo en el que la información de inteligencia y la información procedente de las fuerzas del orden y de las fuentes de libre acceso se combina con el conocimiento de las prioridades y vulnerabilidades de una organización para generar una evaluación de la amenaza a que está expuesta la organización. El análisis de la amenaza

puede también describir las motivaciones, intenciones y capacidades relacionadas con esas amenazas. Un incidente de seguridad física informática puede ser una indicación de una acción o un cambio de táctica del adversario, o de *actos dolosos* que se van a ejecutar o ya se están ejecutando, y tiene que ser evaluado a la luz de esas posibilidades. El objetivo es determinar si el incidente permite identificar a un agente nuevo o en fase de cambio en lo que respecta a la táctica utilizada, la capacidad y la intención.

El análisis debe responder, entre otras, a las siguientes preguntas:

— ¿Indica el incidente de seguridad física informática los objetivos específicos o la intención, a corto o largo plazo, del atacante?

— Dentro del ciclo del ataque, ¿a cuál etapa de este corresponde el incidente (el reconocimiento, la explotación, la eliminación de pruebas, etc.)?

— ¿Puede el ataque ser atribuido a un agente conocido? En caso afirmativo, ¿indica algún cambio de táctica o de capacidad en ese agente?

— ¿Puede el incidente o ataque ser vinculado a ataques parecidos cometidos anteriormente?

— ¿Se trata de un ataque específico o de un ataque al azar?

— ¿Cuánto ha durado el ataque?

— A juzgar por la naturaleza del ataque y por la información que se pueda haber obtenido, ¿cuál es el probable *blanco* siguiente?

— ¿Qué medidas se necesitan para identificar al atacante y remontarse al origen del ataque?

5.6. CARACTERIZACIÓN TÉCNICA

La caracterización técnica de un ataque proporciona una definición concisa de sus características operacionales indicativas, su posible objetivo y sus efectos. El registro de esta información en un formato estructurado apoya el análisis, la determinación de tendencias y el intercambio de información. Una posible caracterización técnica de un incidente de seguridad física informática incluiría un conjunto compuesto por los descriptores que se enumeran a continuación. Este listado no pretende ser exhaustivo; el propósito es ilustrar las principales características de un ataque que se pueden determinar y registrar.

— Impacto: {confidencialidad, integridad y disponibilidad}

— Alcance del impacto: {una o múltiples organizaciones, impacto nacional o internacional}

— Clases: {red, política, configuración, plataforma, SCI, dispositivo}

— Agente: {interno, externo}

— Categoría de gravedad: {funcionamiento defectuoso, degradación de los servicios, pérdida de confianza, uso indebido}

— Motivación: {intencional o no intencional}

— Método de *vulneración*: {robo de datos personales, página web infectada, dispositivo USB, agente interno, terceros, etc.}

En el anexo VII figuran ejemplos de incidentes con sus caracterizaciones técnicas.

5.7. NIVELES DE PROGRESIÓN

La respuesta no será la misma para todos los incidentes de seguridad física informática y tendrá que ser acorde con el impacto real o potencial del incidente en la organización. En esta sección se presenta el concepto de los niveles de progresión. En muchos sentidos, este concepto es similar al de las categorías de gravedad, pero los niveles de progresión se refieren al grado de participación o de respuesta ante un determinado incidente. Un incidente de seguridad física informática puede evolucionar en el sentido de que aumenten la cantidad y el tipo de recursos que se necesiten para una respuesta adecuada. En el cuadro que figura a continuación se establecen algunos niveles de progresión hipotéticos y los posibles perfiles de respuesta.

CUADRO 8. POSIBLES PERFILES DE RESPUESTA PARA DIFERENTES NIVELES DE PROGRESIÓN

Nivel de progresión	Descripción	Funciones implicadas
0	Funcionamiento normal. Grupos de ingenieros vigilan las alertas de seguridad física y los indicadores de incidentes de diversas fuentes.	• Evaluación técnica
1	Descubrimiento del incidente. Se ha descubierto un incidente o amenaza de seguridad física informática. Determinar las medidas de defensa que se deben adoptar. Si es necesario, informar a los empleados de las medidas requeridas.	• Evaluación técnica • Coordinación de la respuesta al incidente • Función de comunicación • Función de análisis del impacto • Función de apoyo técnico
2	Manifestación del incidente. Se ha manifestado un incidente o amenaza de seguridad física informática. Determinar el curso de acción para la contención y erradicación. Si es necesario, informar a los empleados de las medidas requeridas.	• Dirección de la respuesta al incidente • Coordinación de la respuesta al incidente • Función de evaluación técnica • Función de apoyo técnico • Función de comunicación • Función de análisis del impacto
3	Suceso importante. El incidente o amenaza de seguridad física informática es de amplio alcance o tiene consecuencias importantes. Determinar el curso de acción para la contención y erradicación. Informar a los empleados. Prepararse para iniciar una actuación judicial.	• Dirección de la respuesta al incidente • Coordinación de la respuesta al incidente • Función de evaluación técnica • Función de apoyo técnico • Función de comunicación • Función de apoyo a la respuesta al incidente • Función de análisis del impacto

En las secciones siguientes se examinan con más detalle las funciones correspondientes a los diferentes niveles de progresión.

5.8. FLUJO DEL PROCESO Y PROGRESIÓN

5.8.1. Nivel de progresión 0

El nivel 0 representa el funcionamiento normal de la instalación u organización. Esta es la fase proactiva de la respuesta a incidentes, que requiere diligencia y la investigación de las amenazas potenciales, las posibles vulnerabilidades y los nuevos vectores de ataque. El objetivo es adoptar medidas proactivas para velar por que, en caso de ataque, este se detecte prontamente y se faciliten la correcta caracterización de la gravedad y la debida respuesta. Las actividades del nivel 0 comprenden:

— la vigilancia continua del sistema informático;

— la vigilancia de las alertas y los avisos externos sobre nuevas vulnerabilidades y amenazas.

5.8.2. Nivel de progresión 1

El nivel 1 representa la fase en que se detecta por primera vez una indicación de algún nivel de *vulneración* o actividad dolosa en los sistemas informáticos. La indicación inicial puede ser simplemente un comportamiento anómalo de un determinado componente o sistema. En esta fase puede no haber todavía ningún efecto adverso. Los esfuerzos iniciales se centrarán en investigar la naturaleza de la indicación y su posible repercusión, y si se trata efectivamente de un ataque o si la indicación se debió a otros factores, como errores de configuración o un fallo en el entorno de control. En ambos casos, se determina la causa raíz y se adoptan medidas para prevenir la repetición de un incidente similar en el futuro. Las actividades del nivel 1 comprenden:

— el examen y la recopilación de información sobre el incidente;

— el registro y rastreo de la anomalía;

— el triaje;

— la determinación de si el suceso se puede o no clasificar como un incidente de seguridad física informática.

Si el suceso se clasifica como un incidente de seguridad física informática, debe darse aviso al Coordinador de la Respuesta al Incidente. El Coordinador decidirá la composición de los grupos de análisis técnico y de apoyo técnico y, con ayuda del personal del grupo de comunicación, comenzará a notificar el incidente a todos los empleados. Esta notificación tiene por objeto proporcionar a los empleados información y orientaciones para que reduzcan su exposición inmediata a la amenaza. Mientras el personal de apoyo técnico responde al incidente, el Coordinador de la Respuesta al Incidente trabajará con el personal de análisis del impacto para determinar el efecto global del incidente y si necesario elevarlo al nivel 2.

Funciones de evaluación técnica:

— Determinar las medidas de defensa inicial requeridas;

— Notificar al Coordinador de la Respuesta al Incidente;

— Si se requiere una acción por parte de los empleados, como la actualización de los archivos antivirus, dar aviso de ello a la parte u organización responsable.

Funciones del Coordinador de la Respuesta al Incidente:

— Recibir y rastrear todas las amenazas potenciales que se notifiquen;

— Determinar la composición del grupo de evaluación técnica;

— Alertar a las organizaciones internas y a las organizaciones de apoyo pertinentes de la amenaza potencial y de las medidas defensivas que sea necesario adoptar;

— Alertar al Director de la Respuesta al Incidente de la amenaza potencial;

— Alertar al grupo de comunicación, si se requiere una notificación interna o externa;

— Elevar la respuesta al incidente al nivel 2, si se recibe un informe que indique que la amenaza se ha manifestado;

— Iniciar un registro cronológico de los sucesos.

Funciones de comunicación:

— Si se requiere una acción por parte de los empleados, dar aviso de ello a los empleados.

5.8.3. Nivel de progresión 2

Una vez que el Coordinador de la Respuesta al Incidente y el personal de análisis del impacto han decidido elevar el incidente al nivel 2, el Director de la Respuesta al Incidente interviene y asume la responsabilidad global del incidente.

El nivel 2 comienza con un incidente de nivel 1 que se eleva al nivel 2 como resultado de la aparición de uno o varios efectos adversos. Además de la participación del miembro del CSIRT en la respuesta inicial, las condiciones del impacto pueden requerir la consulta con el proveedor del sistema o con personal de seguridad física. En muchos casos, el grupo de comunicación deberá encargarse de que se efectúen todas las notificaciones adecuadas. Las actividades del nivel 2 comprenden:

— el análisis (investigación forense, recolección de pruebas, recomendaciones para la mitigación);

— la puesta en marcha de procedimientos operacionales para emergencias de seguridad tecnológica, cuando haya una pérdida de una función de seguridad tecnológica (ya sea real o percibida);

— el suministro de información a la *entidad explotadora* de la instalación;

— la mitigación y recuperación (con el procedimiento operacional normalizado o con un procedimiento *ad hoc*);

— la evaluación del daño;

— la documentación y la cadena de custodia;

— la evaluación de las medidas adoptadas.

Las actividades de los grupos son parecidas a las del nivel 1, pero incluirán también una mayor integración de las diferentes *autoridades competentes* y autoridades técnicas, y pueden comprender asimismo actividades paralelas para una respuesta de seguridad tecnológica o de emergencia.

Funciones del Director de la Respuesta al Incidente:

— Dirigir las actividades de respuesta al incidente;

— Proporcionar información sobre el estado del incidente y asesoramiento al personal directivo de la organización;

— Elevar el incidente al nivel 3, si procede;

— Determinar cuándo se ha mitigado el *riesgo* hasta un nivel aceptable.

Funciones de evaluación técnica:

— Determinar el mejor curso de acción para contener el incidente;

— Dar aviso al equipo de apoyo técnico de las medidas que sea necesario adoptar;

— Informar sobre las medidas adoptadas y sobre la situación al Coordinador de la Respuesta al Incidente.

Funciones del Coordinador de la Respuesta al Incidente:

— Notificar al Director de la Respuesta al Incidente de la manifestación de la amenaza;

— Alertar al grupo de apoyo a la respuesta de que se ha producido un incidente;

— Alertar al grupo ampliado;

— Recibir el informe de la situación presentado por el grupo de evaluación técnica e informar al Director de la Respuesta al Incidente.

Funciones de comunicación:

— Informar a la organización en nombre del Director de la Respuesta al Incidente;

— Informar a los empleados de la organización sobre cualquier medida que deban adoptar conforme a lo que haya determinado el grupo de evaluación técnica y ordenado el Director de la Respuesta al Incidente.

Funciones de apoyo técnico:

— Adoptar las medidas que haya determinado el grupo de evaluación técnica;

— Informar al Coordinador de la Respuesta al Incidente sobre las medidas adoptadas, el número de empleados involucrados, etc., para que incluya esos datos en el registro cronológico.

5.8.4. Nivel de progresión 3

El nivel 3 puede no tener un impacto inmediatamente observable fuera de la instalación local, pero difiere del nivel 2 en que impone la necesidad de ponerse en contacto con la autoridad técnica (p. ej., con el CERT) para recabar asesoramiento técnico adicional. Esto ocurrirá a menudo cuando el mecanismo de ataque no esté descrito en el cuerpo conocido de boletines de seguridad física informática publicados, como en el caso de la manifestación inicial o del 'día cero' de un software maligno fuera de los entornos controlados. La autoridad técnica no solo ayudará en la caracterización técnica y la resolución del incidente, sino que también será responsable de velar por que tenga lugar la comunicación internacional, de gobierno a gobierno, necesaria para evitar la propagación a mayor escala.

Un incidente de nivel 3 tiene efectos inmediatos y generalizados que rebasan la esfera de control de la *entidad explotadora* de la instalación o central. No solo intervendrán las autoridades técnicas, para hacer frente a esos efectos, sino también funcionarios gubernamentales y agentes del orden, para intentar determinar la atribución del ataque con

vistas a una posible acción judicial. Además, puede ser necesario pedir la asistencia de organizaciones de gestión de emergencias, si se produce una emisión accidental de radiación, una amenaza a *materiales nucleares* especiales o cualquier otro suceso significativo que tenga ramificaciones de seguridad tecnológica o física. Las actividades del nivel 3 comprenden:

— la gestión y adopción de decisiones a nivel de la autoridad técnica;

— posiblemente, la gestión y adopción de decisiones a nivel nacional;

— la investigación criminal;

— la comunicación internacional.

Las actividades de los grupos son parecidas a las del nivel 2, pero incluirán una mayor integración entre las diferentes *autoridades competentes* y autoridades técnicas, y pueden comprender también actividades paralelas para la respuesta de seguridad tecnológica y de emergencia.

Funciones del Director de la Respuesta al Incidente:

— Dirigir las actividades de respuesta al incidente;

— Proporcionar informes del estado del incidente y asesoramiento al personal directivo de la organización;

— Determinar cuándo se ha mitigado el *riesgo* hasta un nivel aceptable.

Funciones de evaluación técnica:

— Seguir monitorizando todas las fuentes conocidas de alertas, buscando nueva información o medidas que se puedan adoptar para eliminar la amenaza;

— Seguir informando sobre la situación al Coordinador de la Respuesta al Incidente, para que incluya esa información en el registro cronológico de los sucesos;

— Vigilar la eficacia de las medidas adoptadas y modificarlas, si es necesario;

— Proporcionar información actualizada al Director de la Respuesta al Incidente sobre la eficacia de las medidas adoptadas y los avances en la eliminación de la amenaza.

Funciones del Coordinador de la Respuesta al Incidente:

— Prestar asistencia al Director de la Respuesta al Incidente en la ejecución de la respuesta;

— Llevar el registro cronológico de los sucesos;

— Registrar con números secuenciales los mensajes sobre la situación que se coloquen en el repositorio de la dirección del accidente a fin de que sean fácilmente accesibles para todo el personal que necesite información corriente sobre la situación.

Funciones de comunicación:

— Informar a los empleados de la organización siguiendo las instrucciones del Director de la Respuesta al Incidente.

Funciones de apoyo técnico:

— Proseguir las acciones para erradicar la amenaza que hayan decidido el Director de la Respuesta al Incidente y el equipo de evaluación técnica;

— Continuar informando al Coordinador de la Respuesta al Incidente sobre las medidas adoptadas, el personal involucrado, etc., para que incluya esa información en el registro cronológico.

Funciones de apoyo:

— Ponerse en contacto con las autoridades locales, si se considera adecuado;

— Si se pide la intervención de las autoridades locales, adoptar disposiciones para que puedan entrar al centro de mando;

— Velar por que se reúna toda la información necesaria para respaldar una acción judicial o restitución financiera.

5.8.5. Actividad posterior al incidente

Una vez terminadas las actividades de respuesta a un incidente de seguridad física informática, es importante aprovechar el conocimiento sobre el incidente para introducir mejoras en los procesos y en la seguridad física. Las medidas que se recomienda aplicar después del incidente comprenden lo siguiente:

Funciones del Director de la Respuesta al Incidente:

— Preparar un informe para la Dirección Ejecutiva que incluya:

  — una estimación del daño/impacto;

  — las medidas adoptadas durante el incidente (sin detalles técnicos);

  — las medidas de seguimiento necesarias para eliminar o mitigar la vulnerabilidad;

  — las políticas o procedimientos que requieren actualización;

  — las medidas adoptadas para reducir al mínimo las pérdidas o la exposición negativa;

  — el registro cronológico y los registros de auditorías de sistemas que existan.

— Documentar las lecciones aprendidas y las recomendaciones para evitar la repetición del incidente, modificando el Plan de Respuesta a Incidentes de Seguridad Física Informática según corresponda.

Funciones de apoyo:

— Jurídico y financiero: trabajar con las autoridades locales que corresponda, si el incidente fue causado por una fuente externa;

— De recursos humanos y de seguridad física: trabajar con la administración para determinar las medidas disciplinarias necesarias, si el incidente se debió a una fuente interna.

REFERENCIAS

[1] ORGANISMO INTERNACIONAL DE ENERGIA ATOMICA, *Nociones Fundamentales de Seguridad Física Nuclear*, *Objetivo y elementos esenciales del régimen de seguridad física nuclear de un Estado*, *Colección de Seguridad Física Nuclear del OIEA* Nº 20, OIEA, Viena, 2014.

[2] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Recomendaciones de Seguridad Física Nuclear sobre la Protección Física de los Materiales y las Instalaciones Nucleares (INFCIRC/225/Rev.5)*, *Colección de Seguridad Física Nuclear del OIEA* Nº 13, OIEA, Viena, 2012.

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

[4] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Guide to Industrial Control Systems (ICS) Security, Special Publication 800–82, USA (2011).

[5] CONSEJO DE EUROPA, *Convenio sobre la Ciberdelincuencia*, Budapest, 2001. Disponible en línea en: https://rm.coe.int/16802fa41c

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).

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

[8] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Computer Security Incident Handling Guide, Special Publication 800–61 Revision 2, USA (2012).

[9] UNITED STATES DEPARTMENT OF ENERGY, Environmental Management Consolidated Business Center (EMCBC), Subject: Cyber Security Incident Response, IP-240-04, Rev. 2, USA (2010)

[10] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Glosario de seguridad tecnológica del OIEA*, *Edición de 2007*, Viena, 2007.

[11] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, *Un sistema de retroinformación sobre la experiencia derivada de sucesos ocurridos en establecimientos nucleares*, *Colección de Normas de Seguridad del OIEA* Nº NS-G-2.11, Viena, 2012.

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).

Activos digitales de carácter estratégico. Sistemas informáticos que cumplen funciones importantes para la seguridad nuclear tecnológica o física o para la contabilidad y el control de los *materiales nucleares*.

Acto doloso. Acto o intento de retirada no autorizada o de sabotaje. [2]

Amenaza para la seguridad física nuclear. Persona o grupo de personas con la motivación, la intención y la capacidad de cometer actos delictivos o actos intencionales no autorizados que entrañen o tengan por *blanco materiales nucleares*, *otros materiales radiactivos* o las instalaciones o actividades conexas, u otros actos que, según haya determinado el Estado, puedan menoscabar la seguridad física nuclear.

Autoridad competente. Organización o institución gubernamental que ha sido designada por un Estado para desempeñar una o varias funciones de seguridad física nuclear. [1]

Las autoridades competentes pueden ser órganos reguladores, organismos de las fuerzas del orden, organismos de control de aduanas y de fronteras, organismos de inteligencia y de seguridad, organismos sanitarios, etc.

Blanco. *Material nuclear* u *otro material radiactivo*, instalación o actividad relacionada con esos materiales, u otro lugar u objeto que pueda ser utilizado en una *amenaza para la seguridad física nuclear*, por ejemplo un gran evento público, un lugar estratégico, o información y activos de información de carácter estratégico.

Entidad explotadora. Persona, organización o entidad gubernamental con licencia o autorización para explotar una instalación o para realizar una actividad conexa.

Gestión del riesgo. Proceso destinado a reducir el *riesgo* a un nivel aceptable, y a limitar el daño derivado de la *vulneración* de la información.

Información de carácter estratégico. Información, en cualquiera de sus formas, incluidos los programas informáticos, cuya divulgación, modificación, alteración, destrucción o denegación de uso no autorizada podría comprometer la seguridad física nuclear. [1]

Instalación nuclear. Instalación (incluidos los edificios y el equipo conexos) en que se producen, procesan, utilizan, manipulan o almacenan *materiales nucleares* o en que se realiza su disposición final, y para la que se requiere una autorización o licencia.

Material nuclear. Cualquier material que sea un material fisionable especial o un material básico, según las definiciones que figuran en el artículo XX del Estatuto del OIEA. [1]

Material radiactivo. Todo material que, en virtud de lo dispuesto en la legislación o la reglamentación nacional o por un órgano regulador, está sometido a control reglamentario a causa de su radiactividad. [3]

Otro material radiactivo. Todo *material radiactivo* que no sea un *material nuclear*. [1, 3]

Riesgo. Posibilidad de que una determinada amenaza aproveche las vulnerabilidades de un activo o grupo de activos y, de ese modo, cause un daño a la organización. Se determina combinando la probabilidad de que un suceso ocurra con la gravedad de las consecuencias que acarrearía. [5]

Suceso relacionado con la seguridad física nuclear. Suceso con consecuencias potenciales o reales para la seguridad física nuclear a las que hay hacer frente.

Vulneración. Violación de la confidencialidad, pérdida de la integridad o pérdida de la disponibilidad, accidentales o deliberadas, de un activo de información.

ANEXO I

INDICADORES DE INCIDENTES

El proceso de respuesta a un incidente de seguridad física informática comienza con la detección e investigación de sucesos e incidentes que indiquen una posible amenaza o *vulneración*. Los indicadores de esos incidentes no se limitan a la esfera técnica y pueden incluir el análisis del flujo de trabajo de los procesos y la interacción con el personal en toda la instalación.

A continuación figuran dos listas de indicadores de incidentes. La primera se confeccionó en la consultoría multinacional del OIEA sobre la respuesta a incidentes de seguridad física informática. La segunda se ha tomado de la publicación del NIST 800-82, titulada *Guide to Industrial Control System (ICS) Security* [I-1].

Indicadores de incidentes de seguridad física informática:

— tráfico de red anómalo — exfiltración de datos;

— modificación no programada del entorno;

— comportamiento errático — mayor latencia de red, ciclos adicionales de la CPU en la estación de trabajo del ingeniero o la consola del operador, etc.;

— conectividad no documentada en la red inalámbrica;

— tráfico conectado directamente a la LAN corporativa;

— acceso aumentado a través de sistemas de seguridad física;

— manipulación física de componentes;

— intentos fallidos de inicios de sesión;

— discrepancias entre el estado indicado en la consola y el estado real;

— resúmenes codificados del sistema para versiones de software válidas que no se corresponden con los valores registrados;

— irregularidades en los registros consolidados;

— intentos ilícitos de acceder a información estratégica controlada;

— robo de documentos de diseño técnico o de registros del personal de la instalación, aumento de las sondas externas referentes a las operaciones nucleares, los proveedores y la construcción de la planta, los subcontratistas, etc. (es decir, cualquier cosa que pueda ayudar al agresor a conseguir una ventaja).

Indicadores de incidentes de seguridad física informática recogidos en la publicación del NIST 800-82:

— tráfico de red excepcionalmente intenso;

— falta de espacio en el disco, o reducción considerable del espacio libre;

— utilización excepcionalmente alta de la CPU;

— creación de nuevas cuentas de usuario;

— uso o intento de uso de cuentas de administrador;

— cuentas bloqueadas;

— archivos de registro vaciados;
— archivos de registro llenos con un número excepcionalmente alto de sucesos;
— alertas de programas antivirus o de sistemas de detección de intrusiones;
— programas antivirus y otros controles de seguridad física desactivados;
— cambios imprevistos en parches;
— máquinas o dispositivos de campo inteligentes conectados;
— solicitudes de información sobre el sistema (intentos de ingeniería social);
— cambios imprevistos en los ajustes de configuración;
— parada imprevista del sistema;
— mensajes de error o interrupción en una web, una base datos o un servidor de aplicaciones;
— acceso excepcionalmente lento a las computadoras de la red;
— nombres de archivos con caracteres inhabituales, o archivos y carpetas nuevos o no previstos;
— cambios en la configuración de auditoría;
— gran número de correos electrónicos rebotados con contenido sospechoso;
— desviación inhabitual de los flujos de tráfico típicos de la red;
— comportamiento errático del equipo de SCI, especialmente si más de un dispositivo presenta ese comportamiento;
— toda invalidación evidente de sistemas de seguridad, de respaldo o de recuperación frente a fallos;
— equipo, servidores, o tráfico de red con picos de alta utilización, cuando el propio proceso operacional es constante y previsible;
— tráfico desconocido o inhabitual desde una red corporativa u otra red externa hacia la red de sistemas de control;
— extracciones o instalaciones forzadas de firmware desconocido o no previsto.

REFERENCIA

[I-1] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, “Guide to Industrial Control System (ICS) Security (Final Public Draft)”, Special Publication 800–82, USA (2008), pp 6–19.

ANEXO II

GUÍA PARA EL ANÁLISIS DE INCIDENTES

En el presente anexo se describen las categorías de información sobre los incidentes que se pueden utilizar para evaluar y medir los atributos de una amenaza. Un incidente de seguridad física informática puede ser la manifestación de un *acto doloso*. En muchos casos, no es fácil entender el motivo de ese acto, ni quién lo cometió. El análisis del incidente en lo que respecta a los agentes de la amenaza es importante porque ayuda a determinar no solo el motivo, sino también los cambios en las características de la amenaza, la táctica y las posibles actividades ulteriores.

La información que sigue se ha elaborado a partir de la orientación contenida en la publicación *Cyber Threat Metrics* [II-1].

Características del incidente

— ¿Qué tipo de incidente se produjo (p. ej., desfiguración de un sitio web, denegación de servicio, acceso no autorizado, reconocimiento/sondeo)?

— Si lo causó un software maligno (p. ej., un virus o un troyano), ¿cuál era su propósito?

- el mando y control
- el acceso remoto
- la exfiltración de datos
- la manipulación de datos
- la vigilancia de actividades

Características del sistema atacado

— ¿Cuál era el nivel de protección física del *blanco?*:

- alto — plenamente protegido con control del acceso, vigilancia de archivos, parches actualizados, etc.
- moderado — con cierto grado de protección
- bajo — con medidas de protección muy limitadas

Cronograma

— ¿Cuál es la fecha de la actividad inicial relacionada con el incidente?

— ¿Cuál es la fecha más reciente de actividad relacionada con el incidente?

— ¿En qué fecha se detectó el incidente?

Actividad encubierta

— ¿Cómo se detectó la actividad relacionada con el incidente?

- vigilancia de la red
- una aplicación de vigilancia (p. ej., un sistema de detección de intrusiones o un programa antivirus)
- un administrador del sistema
- un usuario del sistema

— Las actividades detectadas, ¿se relacionaron inmediatamente con el incidente o se descartaron como falsas alarmas?

— ¿Se modificaron o suprimieron registros de sucesos o sellos de tiempo para confundir la actividad relacionada con el incidente?

— ¿Se utilizaron herramientas de borrado de archivos/discos en el incidente?

— ¿Correspondieron las actividades del incidente a la etapa de reconocimiento, de sondeo, de ejecución o de explotación del ataque?

Vector del ataque

— ¿Se facilitó el incidente mediante:

- phishing?
- ingeniería social (distinta del phishing)?
- acceso remoto (p. ej., por VPN o módem)?
- acceso interno?

— Si el ataque fue facilitado por cualquier tipo de ingeniería social, incluido el phishing, ¿se trató de un ataque individual, con un blanco específico, o de un ataque amplio y de carácter general?

Sofisticación del ataque

— ¿Hubo más de un sistema informático afectado por el incidente?

— ¿Hubo múltiples accesos a la red interna durante el incidente?

— ¿Fueron las actividades relacionadas con el incidente novedosas de alguna forma (es decir, se trató de un ataque de día cero) o comunes (realizadas con conjuntos de programas fáciles de adquirir)?

Firma antivirus

— ¿Existe una firma antivirus (de cualquier proveedor) para el software maligno utilizado en el incidente?

— En caso afirmativo, ¿existía esa firma y estaba ampliamente disponible en la fecha de la actividad inicial?

— Interacción física:

- ¿hubo accesos físicos al sistema como parte del incidente?
- ¿se facilitó el incidente mediante la introducción de un medio físico (p. ej., una memoria USB, un CD, un hardware)?
- ¿tuvo el incidente algún efecto físico, en el mundo real?

Ocultación

— ¿Estaba alguna parte del software maligno cifrada o empaquetada?

— ¿Hubo alguna inyección de una actividad, función o secuencia de comandos en otra con fines dolosos?

Vulneración de datos

— ¿Hubo alguna *vulneración* de datos (p. ej., por manipulación, exposición o supresión) en relación con el incidente? En caso afirmativo,

- ¿qué tipo de datos resultaron comprometidos (p. ej., información solo para uso oficial, información personal identificable, información sensible no clasificada o información nuclear controlada no clasificada)?
- ¿repercutió la *vulneración* de los datos en el funcionamiento o la misión del sistema?

— ¿Hubo una exfiltración de datos como parte del incidente? En caso afirmativo,

- ¿qué tipo de datos fueron exfiltrados (p. ej., resúmenes codificados de contraseñas, información personal identificable, información solo para uso oficial, información controlada no clasificada, información protegida por patentes, militar, de seguridad)?
- ¿hubo múltiples exfiltraciones de datos?
- ¿hubo datos cifrados en el proceso de exfiltración?

Atribución

— ¿Es posible atribuir con certeza las actividades relacionadas con el incidente a un agente específico?

— ¿Ha reivindicado algún grupo o persona la responsabilidad del incidente?

— En caso afirmativo, ¿lo hizo mediante una declaración pública o privada? ¿Se trató de una declaración de carácter general, específica o limitada?

— ¿Ha emitido algún grupo o persona una declaración de amenaza específica contra la organización que sufrió el incidente?

— ¿Se utilizaron puntos intermedios? En caso afirmativo, ¿cuántos?

— ¿Dónde se originó el ataque?

REFERENCIA

[II-1] Mateski, M., et al., Cyber Threat Metrics, Sandia Report SAND2012–2427, March 2012.

ANEXO III

CONSIDERACIONES ESPECIALES PARA LOS SISTEMAS DE CONTROL INDUSTRIAL

Los sistemas de control industrial representan entornos operativos singulares que pueden requerir atención especial en la respuesta a un incidente de seguridad física informática. A continuación se enumeran algunas consideraciones que podrían tenerse en cuenta en la planificación y la respuesta.

— Un ataque informático puede tener consecuencias físicas en el entorno operativo;

— La respuesta debe centrarse en primer lugar en mantener la seguridad tecnológica y prevenir las consecuencias radiológicas inaceptables;

— La respuesta a un incidente de seguridad física informática puede ser solo una parte de una actividad de respuesta más amplia a ataques que se relacionen con la seguridad tecnológica o con el acceso no autorizado a *materiales nucleares*;

— El diseño y las modificaciones de los sistemas de control de la instalación deben incluir consideraciones específicas relativas a la seguridad física informática;

— Hay múltiples modos de funcionamiento disponibles para facilitar la colocación de una central nuclear en una condición segura después de un ciberataque;

— Los sistemas de control industrial dependen a menudo de una infraestructura secundaria fundamental, que también debe tomarse en consideración en relación con un ciberataque. Los ataques a estos sistemas e infraestructuras secundarios pueden tener, en muchos casos, una repercusión directa en las funciones primarias;

— La respuesta a un incidente de seguridad física informática puede requerir una capacitación específica sobre el entorno de la instalación o de las operaciones;

— El Grupo de Respuesta a Incidentes de Seguridad Física Informática debe incluir a ingenieros de sistemas, y disponer de herramientas previamente aprobadas (ensayadas para determinar su impacto operacional) y procesos aceptables;

— La seguridad física informática debe considerarse en relación con el plan global de seguridad física del emplazamiento;

— Los ejercicios de seguridad tecnológica y física de la instalación deben incluir escenarios de seguridad física informática;

— La seguridad física informática debe integrarse en la cultura operacional y de seguridad tecnológica de la central; para ello se requiere una fusión de la seguridad física, las redes, los servidores de la empresa, las computadoras, las operaciones de la central, etc.;

— Debe evaluarse el impacto que pueden tener las medidas de respuesta informática relacionadas con *activos digitales de carácter estratégico* en la continuidad de las actividades;

— Es fundamental que todos los actuantes estén validados mediante credenciales previamente aprobadas y controles de los antecedentes;

— El grupo de respuesta debe incluir a ingenieros de sistemas, ingenieros de I+C e informáticos.

ANEXO IV

ESCENARIOS DE INCIDENTES

Para mejorar la capacidad de respuesta a incidentes de seguridad física informática no basta tener un conocimiento cabal de la tecnología básica y de cómo se utiliza para detectar incidentes; también es útil conocer el contexto del incidente en el escenario de un ataque. A menudo es difícil entender los incidentes fuera del contexto del ataque. ¿Por qué dejó de funcionar un determinado componente del sistema de control y sin embargo no se produjo un fallo? ¿Qué son esos paquetes de datos aparentemente inocuos que tratan de escapar de la red todos los días a las 13.00 horas? Por este motivo, presentamos a continuación varios escenarios de incidentes de seguridad física informática que ayudarán a poner los incidentes de ese tipo en un contexto.

IV-1. POSIBLES ESCENARIOS DE INCIDENTES

Hay muchos escenarios de incidentes que podrían afectar a una instalación. Los métodos por los que se podría comprometer de distintas formas el funcionamiento de los sistemas comprenden lo siguiente:

— Una perturbación causada por el retraso o el bloqueo del flujo de información en la red corporativa o la red de control;

— Cambios no autorizados en las instrucciones programadas en PLC, unidades terminales remotas, sistemas de control distribuido o controladores SCADA, cambios en los umbrales de las alarmas o comandos no autorizados enviados al equipo de control, que puedan producir daños en el equipo (si se superan las tolerancias) o paradas prematuras de los procesos (como el cierre prematuro de las líneas de transmisión) y causar un incidente ambiental o incluso desactivar el equipo de control;

— Información falsa enviada a operadores nucleares autorizados ya sea para encubrir cambios no autorizados o para inducirlos a poner en marcha medidas inadecuadas;

— Una modificación del software o los ajustes de configuración de un *activo digital de carácter estratégico* que produzca resultados imprevisibles;

— La interferencia con el funcionamiento de sistemas de seguridad tecnológica;

— Un software maligno (p. ej., un virus, gusano informático o caballo de Troya) introducido en el sistema que contiene *activos digitales de carácter estratégico*;

— Una modificación de la versión electrónica o impresa de los procedimientos o las instrucciones de trabajo para causar daños a productos, al equipo o al personal;

— Una injerencia física en sistemas de control situados en emplazamientos remotos automatizados que no se puedan monitorizar físicamente. Con una injerencia física en esos sistemas, los adversarios podrían establecer una conexión fiable con una red de control de la instalación que contenga *activos digitales de carácter estratégico*.

IV-2. POSIBLES VECTORES DE ATAQUES

Los vectores de ataques pueden ser, entre otros:

— Una computadora portátil infectada que se utilice para el mantenimiento y la configuración de componentes de sistemas de control conectados al sistema;

— Medios extraíbles y dispositivos móviles que interactúen con *activos digitales de carácter estratégico*;

— Un subcontratista que realice actividades de mantenimiento e infecte sistemas a distancia a través de su sistema remoto;

— Conexiones inalámbricas ilícitas a sistemas o a *activos digitales de carácter estratégico*;

— La pérdida de control del acceso del personal de mantenimiento de terceras empresas presente en el emplazamiento que tenga acceso no acompañado a componentes de I+C. Estos conjuntos de datos pueden encontrarse en los sistemas corporativos y no en los propios sistemas técnicos y, por lo tanto, estar más fácilmente al alcance de un activista interno;

— Una *vulneración* de conexiones de datos remotas utilizadas para la monitorización constante del emplazamiento;

— La pérdida de control del acceso y de la rendición de cuentas respecto de piezas electrónicas y componentes para la reparación;

— La falta de una cultura de la seguridad física en lo que respecta a la introducción de programas malignos y el reconocimiento y la respuesta ante una *vulneración* informática;

— El uso no autorizado de cuentas ocultas de proveedores conocidos o de contraseñas introducidas en el código fuente.

ANEXO V

INFORMACIÓN SOBRE LOS INCIDENTES

Cuando se informa sobre un incidente de seguridad física informática, es importante indicar las características pertinentes de la *vulneración* y las circunstancias que rodearon el descubrimiento del incidente. En la presente sección se enumeran los detalles que se recopilan normalmente en el proceso de respuesta a un incidente de seguridad física informática. Esta información se aplica a las investigaciones tanto internas como externas. Es importante que en la comunicación de la información se sigan protocolos específicos, que indiquen con exactitud la información que se debe comunicar, quién está autorizado a hacerlo, y a quién y en qué circunstancias se puede comunicar esa información. No toda la información se aplicará a cada incidente.

Categoría	Ejemplo
Clasificación del informe del incidente.	De carácter estratégico, clasificado, etc.
Nombre de la organización.	
Persona de contacto para el incidente (nombre, teléfono, dirección de correo electrónico).	
Ubicación física de la computadora/red afectada.	
Nivel de clasificación del sistema comprometido.	Clasificado, no clasificado, secreto, de carácter estratégico.
Fecha del incidente.	
Hora del incidente (incluida la zona horaria).	
Descripción de la infraestructura crítica afectada.	
Tipo de incidente y categoría del impacto.	Intrusión: impacto moderado. Denegación de servicio: impacto alto.
Direcciones IP (Protocolo de Internet) y nombres de dominios afectados.	
Direcciones IP y nombres de dominios del origen del ataque.	
Sistema operativo de la computadora o las computadoras afectadas.	
Funciones de la computadora o las computadoras afectadas.	
Número de computadoras afectadas.	
Método sospechado de intrusión/ataque.	
Autores sospechosos y/o posible motivación del ataque.	

Categoría	Ejemplo
Pruebas de una suplantación de identidad.	
Software de aplicación afectado.	
Descripción de la infraestructura de seguridad física existente cuando se produjo el incidente.	
¿Produjo la intrusión o el incidente una pérdida de información o su modificación?	
Si se trató de información privada sobre el personal, ¿se ha dado aviso de ello a las organizaciones y personas afectadas?	
Pruebas del daño sufrido por el sistema o los sistemas afectados, incluido el nivel/alcance del acceso no autorizado.	
Descripción de las tácticas, técnicas y procedimientos (TTP) del adversario observados.	
¿Cuáles vulnerabilidades se explotaron, si se aplica?	
Descripción de las medidas de investigación y los esfuerzos de mitigación.	
Última vez que se modificaron o encendieron los sistemas afectados.	
Evaluación del impacto del incidente.	
Programa antivirus: versión y actualización más reciente.	
Metodología utilizada para la identificación de incidentes.	Sistema de detección de intrusiones, análisis de los registros de auditoría, administradores de sistemas.

ANEXO VI

RECOLECCIÓN DE PRUEBAS

En la respuesta a un incidente es necesario tomar en consideración la recolección de pruebas para el análisis posterior y para la investigación por las fuerzas del orden. "La computación o informática forense es el proceso que permite identificar, preservar, analizar y presentar las pruebas digitales de un modo que sea aceptable en una acción judicial." [VI-1]

VI-1. REGLAS DE LA INVESTIGACIÓN FORENSE

Cuando se realizan exámenes forenses de sistemas informáticos, hay algunas reglas que se deben respetar en la investigación. [VI-2]

Someter el original a la mínima manipulación posible

Esta puede considerarse la regla más importante de la informática forense. Siempre que sea posible, deberán hacerse copias de las pruebas y utilizar los duplicados para el examen. Cuando así se haga, la copia deberá ser una reproducción exacta del original y habrá de autenticarse, para evitar que se pueda poner en duda la integridad de la prueba.

Documentar todo cambio

En algunas circunstancias, la alteración de las pruebas es inevitable. Por ejemplo, el arranque o la parada de un dispositivo pueden introducir cambios en la memoria y/o en los archivos temporales. Cuando así sea, deberán documentarse la naturaleza, el alcance y el motivo de los cambios efectuados.

Cumplir los principios probatorios

Los principios probatorios son las reglas que deben seguir los investigadores al manipular y examinar las pruebas para que los elementos probatorios recogidos sean aceptables en una actuación judicial.

No excederse de los propios conocimientos

Si una investigación sobrepasa el nivel de conocimientos y pericia de la persona que la efectúa, debe ser interrumpida. Quien se encuentre en esta situación deberá pedir asistencia a una persona más experimentada, por ejemplo a un investigador especializado, o, si el tiempo lo permite, obtener más capacitación para mejorar sus propios conocimientos y habilidades. Es aconsejable no proseguir el examen, porque se puede comprometer el resultado del caso.

VI-2. RECOLECCIÓN DE PRUEBAS

Matthew Braid, en su artículo de AusCERT titulado *Collecting Electronic Evidence After a System Compromise* [VI-3], ha compilado una lista de cinco principios probatorios que se deben cumplir para que las pruebas sean útiles y los ha explicado de una manera fácil de entender. Su explicación de los principios probatorios es la siguiente:

Admisibilidad

Este es el principio más básico — las pruebas tienen que poderse utilizar en un tribunal u otra instancia. El incumplimiento de este principio es equivalente a no haber recogido la prueba, pero tiene un costo más alto.

Autenticación

Si la prueba no se puede vincular claramente al incidente, no se podrá probar nada. Es necesario poder demostrar que existe una relación pertinente entre la prueba y el incidente.

Exhaustividad

A menudo no es suficiente recoger pruebas que den una sola perspectiva del incidente. No solo es necesario reunir pruebas que puedan ayudar a demostrar la actuación del atacante sino que, para cumplir el requisito de la exhaustividad, los investigadores deben examinar y evaluar también todas las demás pruebas disponibles y retener aquellas que contradigan o de alguna otra forma socaven la fiabilidad de las pruebas posiblemente inculpatorias contra el sospechoso. De igual modo, es esencial reunir pruebas que eliminen a otras personas sospechosas. Por ejemplo, si se puede demostrar que el atacante estaba conectado al sistema en el momento del incidente, deberá demostrarse también quiénes más lo estaban y por qué se piensa que no tuvieron que ver con el incidente. Esta es la que se denomina prueba exculpatoria, y es una parte importante de la demostración de una hipótesis.

Fiabilidad

Los procedimientos de recolección y análisis de las pruebas no deben sembrar dudas sobre la autenticidad y veracidad de estas.

Credibilidad

Las pruebas que se presenten deben ser claras, fáciles de entender y dignas de fe para el jurado. De nada sirve presentar un volcado de memoria en formato binario si el jurado no tiene idea de lo que significa. Del mismo modo, si se presenta una versión formateada que un jurado puede entender fácilmente, debe poder demostrarse su relación con el original en formato binario, de lo contrario el jurado no tendrá cómo saber que no se trata de información falsa.

Además de estas orientaciones, en la recolección de pruebas conviene asimismo:

- Llevar un registro continuo de la actividad para poder hacer el seguimiento de todas las medidas adoptadas durante el incidente;
- Velar por que los elementos importantes para la investigación tengan el debido sello de tiempo, y por que el dispositivo que dé la hora funcione correctamente y esté sincronizado con los otros recursos de la red;
- Identificar a todas las personas que hayan tenido acceso a la información;
- Preservar los volcados de red y los volcados de memoria (si es posible) durante el incidente;
- Determinar si el sistema comprometido debe aislarse o mantenerse en funcionamiento hasta que se pueda realizar el examen forense. Esto dependerá de la naturaleza del sistema en cuestión;

— Determinar antes de que ocurra un incidente las pruebas que se habrán de recoger. Se recomienda que este aspecto se coordine con el organismo correspondiente de las fuerzas del orden;

— Reunir los registros y la información sobre el funcionamiento antes y después del incidente de seguridad física, para analizarlos más a fondo.

El CERT del Departamento de Seguridad Nacional de los Estados Unidos encargado de los sistemas de control industrial ha publicado una guía de dos páginas sobre la preparación para el análisis de incidentes informáticos. [VI-4] La guía incluye detalles sobre el establecimiento de capacidades de análisis de sistemas, la preparación operacional y la importancia del registro y la preservación de los datos forenses. Entre otras cosas, se recomienda:

— Tomar notas detalladas de lo que se observe, con las fechas y las horas, las medidas de mitigación adoptadas o no adoptadas, la indicación de si el registro de la actividad del dispositivo estaba activado o inactivado y los nombres de máquina del equipo que se sospeche que pueda estar comprometido. En general, mucha información es mejor que poca;

— Cuando sea posible, capturar los datos del sistema en funcionamiento (es decir, las conexiones de red y los procesos abiertos en ese momento) antes de desconectar una máquina comprometida de la red;

— Capturar imágenes forenses de la memoria del sistema y del disco duro antes de apagar el sistema;

— No ejecutar ningún programa antivirus 'a posteriori', porque el escaneo del antivirus modifica las fechas de archivos de importancia crítica e impide descubrir y analizar los posibles archivos malignos y los cronogramas;

— No hacer ningún cambio en el sistema operativo o en el hardware, tampoco actualizaciones o parches, ya que con ello se sobrescribiría información importante sobre el posible programa maligno.

REFERENCIAS

[1] McKemmish, Rodney. "What is Forensic Computing", Australian Institute of Criminology: Trends and Issues in Crime and Criminal Justice, June 1999. Available online at: <http://aic.gov.au/documents/9/C/A/%7B9CA41AE8-EADB-4BBF-9894-64E0DF87BDF7%7Dti118.pdf>

[2] Ryder, Karen. "Computer Forensics — We've Had an Incident, Who Do We Get to Investigate?". SANS Institute InfoSec Reading Room, 2002. Available online at: <http://www.sans.org/reading-room/whitepapers/incident/computer-forensics-weve-incident-investigate-652>

[3] Braid, Matthew. "Collecting Electronic Evidence After a System Compromise", 2001, Available online at: < https://www.auscert.org.au/download.html?f=22>

[4] United States Department of Homeland Security, "Preparing for Cyber Incident Analysis", 2008. Available online at: <https://ics-cert.us-cert.gov/sites/default/files/DHS_CyberSecurity_CSSP-Incident_Handling-v10.pdf>

ANEXO VII

EJEMPLOS DE CARACTERIZACIONES TÉCNICAS

En el presente anexo se dan ejemplos de caracterizaciones técnicas que pueden servir de referencia al realizar el análisis del entorno para apoyar la elaboración de un plan de respuesta a incidentes de seguridad física informática. Cada ejemplo comprende una descripción y las características de un conjunto propuesto de categorías que incluyen el impacto, el alcance del impacto, las clases, el agente, el nivel de gravedad, la motivación y el método de *vulneración*.

VII-1. EJEMPLO 1

El CERT envía una advertencia indicadora de que se ha observado una nueva muestra de software maligno en el laboratorio y de que, entre sus numerosas firmas, los sistemas infectados apuntan a una determinada dirección de Internet. La célula de respuesta a amenazas da aviso al grupo encargado de la red de la necesidad de actualizar los filtros de auditoría y los sensores de la red para buscar posibles conexiones con esa dirección externa. Más tarde, ese mismo día, se activan múltiples alertas y se determina que tres sistemas están infectados. Todos ellos forman parte del grupo de finanzas de una red separada de todas las operaciones de la central. Tras un análisis más a fondo, se escanean los datos de red capturados y se descubre un fichero adjunto a diez correos electrónicos que corresponde al resumen codificado de la carga útil del software maligno. El centro de operaciones de seguridad física crea la siguiente caracterización técnica de la amenaza:

Impacto:	Confidencialidad e integridad
Alcance del impacto:	Una sola organización
Clases:	Red, política, configuración y plataforma
Agente:	Externo
Nivel de gravedad:	Tipo 2 — pérdida de confianza (de los sistemas financieros, no de la parte operacional de la instalación, por el momento).
Motivación:	Intencional (dada la alerta emitida por el CERT)
Método de vulneración:	Phishing personalizado.

VII-2. EJEMPLO 2

Un tablero de control de un sistema informático experimenta un fallo crítico repentino. Los operadores de la central observan inmediatamente que un elemento crítico del equipo se desconecta e inicia el proceso de conexión de los servicios de respaldo. El operador a cargo de ese elemento del equipo conecta la computadora portátil de mantenimiento al sistema de control y descarga los archivos de registro y el volcado del sistema que está disponible. Mientras analiza los registros de auditoría, traspasa el volcado del sistema a la AT, que tiene la capacidad necesaria para analizar el archivo. Durante el análisis del archivo, el operador del sistema observa en el archivo de registro una serie de mensajes que indican un aumento constante de la temperatura interna del dispositivo, hasta que falla el tablero de control. Algunos minutos más tarde, la AT llama y señala que encontró un proceso residente en la memoria en el momento en que se produjo el fallo del sistema que podría estar vinculado a un ataque a un SCADA conocido. El centro de operaciones de seguridad física crea la siguiente caracterización técnica de la amenaza:

Impacto:	Integridad y disponibilidad
Alcance del impacto:	Una sola organización (con posibilidad de impacto nacional si no se restaura la plena capacidad del servicio crítico).
Clases:	SCI, dispositivo
Agente:	Desconocido a la fecha
Nivel de gravedad:	Tipo 1 — Degradación de los servicios y pérdida de confianza*
Motivación:	Intencional
Método de vulneración:	Desconocido a la fecha.

* En el supuesto de que no se trate de un suceso doloso. Si se piensa que los fallos fueron dolosos, actualícese como corresponda.

VII-3. EJEMPLO 3

El centro de operaciones de seguridad física informática comienza a recibir alrededor de una llamada por hora de usuarios que señalan que han recibido una llamada de una persona que se presentó como el administrador de seguridad y les pidió su contraseña para poder proceder al mantenimiento del sistema y a la verificación de las cuentas. El grupo de seguridad física envía inmediatamente un correo electrónico a todos los usuarios para recordarles que no deben nunca dar su contraseña a nadie. Ningún usuario declara que dio su contraseña.

Impacto:	Integridad
Alcance del impacto:	Una sola organización (con posibilidad de que sean múltiples, si un usuario de más de una instalación reutiliza su contraseña).
Clases:	Política
Agente:	Probablemente externo, pero aún no es seguro
Nivel de gravedad:	Tipo 3 — Actividad de un agresor detectada
Motivación:	Intencional
Método de vulneración:	Ninguna vulneración detectada hasta el momento.

ANEXO VIII

EJEMPLO DE UNA POLÍTICA DE RESPUESTA A INCIDENTES DE SEGURIDAD FÍSICA INFORMÁTICA

{Este anexo proporciona a las organizaciones un modelo para elaborar su política de respuesta a incidentes de seguridad física informática. Las organizaciones que lo utilicen deberán adaptar la política a sus necesidades específicas. El texto que figura entre corchetes [ ] debe adaptarse a la organización de que se trate, mientras que el texto entre llaves { } es información explicativa que se debe suprimir.}

I. Objetivos y propósito de la política

El mantenimiento de la seguridad nuclear tecnológica y física contra las posibles amenazas es una de las máximas prioridades operacionales en ***[nombre de la organización]***. En el mundo de hoy, es indispensable tener en cuenta la amenaza de ataques informáticos.

Somos conscientes de que la seguridad tecnológica y física en ***[nombre de la organización]*** depende, en parte, de la existencia de un programa de seguridad física informática completo basado en la defensa en profundidad. Todos nuestros empleados son componentes esenciales de ese programa.

[Nombre de la organización] tiene que ser capaz de responder a un incidente de seguridad física informática de un modo que no comprometa la seguridad nuclear tecnológica y física. Esto comprende la protección de la información y los activos de información de carácter estratégico.

La presente política de respuesta a incidentes de seguridad física informática tiene por objeto establecer un enfoque sistemático y bien definido para adoptar las medidas adecuadas cuando se detecte un ataque informático o se registre una violación de la política de seguridad física informática.

Esta política y los procedimientos conexos constituyen el Plan de Respuesta a Incidentes de Seguridad Física Informática, que establece las prioridades de la organización, los procesos técnicos, las técnicas, las listas de verificación y los formularios específicos que se utilizarán en la respuesta a un incidente. Una de las funciones principales del Plan de Respuesta a Incidentes de Seguridad Física Informática es garantizar la integridad y la rápida restauración y recuperación de las funciones de los sistemas esenciales relacionadas con la seguridad tecnológica, la seguridad física, la contabilidad y el control de los materiales y la preparación para emergencias.

II. Ámbito de aplicación de la política

La presente política se aplica a todos los empleados, que son responsables de proteger la información y los sistemas informáticos en ***[nombre de la organización]*** y de notificar los comportamientos e incidentes sospechosos. Si un empleado detecta un incidente o un comportamiento posiblemente sospechoso, debe, en primer lugar, adoptar medidas para establecer una situación tecnológica y físicamente segura y, en segundo lugar, dar aviso de ello al Oficial de Seguridad Física Informática o al funcionario superior designado al efecto. Los procedimientos operacionales pueden definir los requisitos y procesos para responder a un incidente informático que afecte a determinados sistemas, como los de ingeniería o de seguridad física.

III. Incidentes de seguridad física informática

Un incidente de seguridad física informática es un suceso que afecta o puede afectar a los sistemas informáticos o redes de computadoras. También puede ser un acto que viole una política de seguridad física informática explícita o implícita.

Son ejemplos de incidentes de este tipo:

- los intentos (logrados o fallidos) de obtener acceso no autorizado a un sistema o a sus datos
- una perturbación no deseada o una denegación de servicio
- el uso no autorizado de un sistema para el procesamiento o almacenamiento de datos
- los cambios en las características del hardware, el firmware o el software que se realizan sin el conocimiento, una instrucción o el consentimiento del propietario.

IV. Grupo de Respuesta a Incidentes de Seguridad Física Informática (CSIRT)

[Nombre de la organización] ha establecido un Grupo de Respuesta a Incidentes de Seguridad Física Informática (CSIRT). El CSIRT es un componente de intervención organizada que presta los servicios de respuesta en caso de incidente de seguridad física informática. Este grupo se compone de un conjunto predeterminado de personas que abarcan una variedad de competencias y tienen actividades y facultades de respuesta asignadas para toda la duración del incidente. Aunque el establecimiento de un estado tecnológica y físicamente seguro durante un incidente de seguridad física informática es responsabilidad de cada empleado, el CSIRT decidirá y dirigirá los procesos que se consideren necesarios para contener, mitigar o resolver los problemas que susciten preocupación.

El CSIRT actúa bajo la dirección del Oficial de Seguridad Física Informática. El CSIRT consta de un núcleo de especialistas en diferentes disciplinas. A ellos podrán sumarse otros especialistas, en función de la naturaleza del incidente y de sus posibles consecuencias.

Los miembros del núcleo del CSIRT son:

- El Oficial de Seguridad Física Informática
- [el ingeniero de redes]
- [el representante del departamento de ingeniería]
- [el administrador del sistema de seguridad física]
- [el representante de comunicaciones]
- [el ingeniero de seguridad tecnológica]

{Obsérvese que algunas de estas personas pueden ser expertos subcontratados que aporten determinadas competencias técnicas que no existan en la fuerza de trabajo.}

Las responsabilidades del CSIRT comprenden, entre otras cosas:

- el establecimiento de un registro del incidente y la consignación en él de toda la información pertinente a medida que avanza la actividad de respuesta;
- la determinación de la naturaleza y el alcance del incidente;
- la determinación del impacto posible del incidente;
- la realización de las notificaciones internas y externas necesarias;

— la elevación de la respuesta al incidente al nivel de la Dirección Ejecutiva, si es el caso;

— la recomendación de una respuesta y la adopción de las medidas que decida la Dirección Ejecutiva;

— los contactos con departamentos adicionales y su integración en la respuesta, si procede;

— la vigilancia de los progresos de la respuesta;

— la recolección de las pruebas para las fuerzas del orden, según proceda;

— la documentación de un resumen del incidente y de las medidas de restauración adoptadas;

— el estudio/la aplicación de medidas de mitigación para la defensa contra futuros ataques;

— la realización de actividades de capacitación sobre la respuesta a incidentes;

— la realización de ejercicios periódicos de respuesta a incidentes.

V. Comunicación

Durante un incidente de seguridad física informática, la comunicación es un elemento clave de una respuesta coordinada. Esto incluye requisitos de notificación internos y, posiblemente, externos. Como parte de los procedimientos de respuesta a un incidente de seguridad física informática, el Oficial de Seguridad Física Informática deberá elaborar un plan de comunicaciones que abarque los informes requeridos y los criterios de información que se aplicarán.

El CSIRT es responsable también de la comunicación del incidente, lo que supone velar por que se transfiera la información adecuada a la administración superior, los agentes de las fuerzas del orden, el órgano regulador, etc. El plan de comunicación indicará los puntos de contacto adecuados de las autoridades competentes y las autoridades técnicas pertinentes, y la información para comunicar con ellos.

VI. Requisitos de capacitación y ejercicios

Uno de los elementos más cruciales tanto de la prevención como de la respuesta ante un incidente de seguridad física informática son las personas que trabajan en ***[nombre de la organización]***.

Un componente clave de la presente política de respuesta a incidentes de seguridad física informática es el establecimiento de un programa de sensibilización sobre la seguridad física informática. Al acceder por primera vez a los sistemas informáticos, y periódicamente después de ese acceso inicial, todos los empleados recibirán capacitación en la prevención y el reconocimiento de incidentes de seguridad física informática, y en la respuesta a ellos. Esta capacitación se adaptará a las necesidades específicas de cada departamento.

El personal técnico recibirá la capacitación adicional que sea necesaria para respaldar la prevención, la respuesta, el análisis y la mitigación de los incidentes de seguridad física informática.

[Nombre de la organización] realizará ejercicios de capacitación periódicos para ensayar el proceso de respuesta a incidentes. Estos ejercicios se centrarán no solo en los procedimientos técnicos sino en todo el proceso de respuesta, incluidos los requisitos de comunicación con la autoridad competente y con las autoridades técnicas.

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

18-00939S

Organismo Internacional de Energía Atómica
Viena
ISBN 978-92-0-306717-1