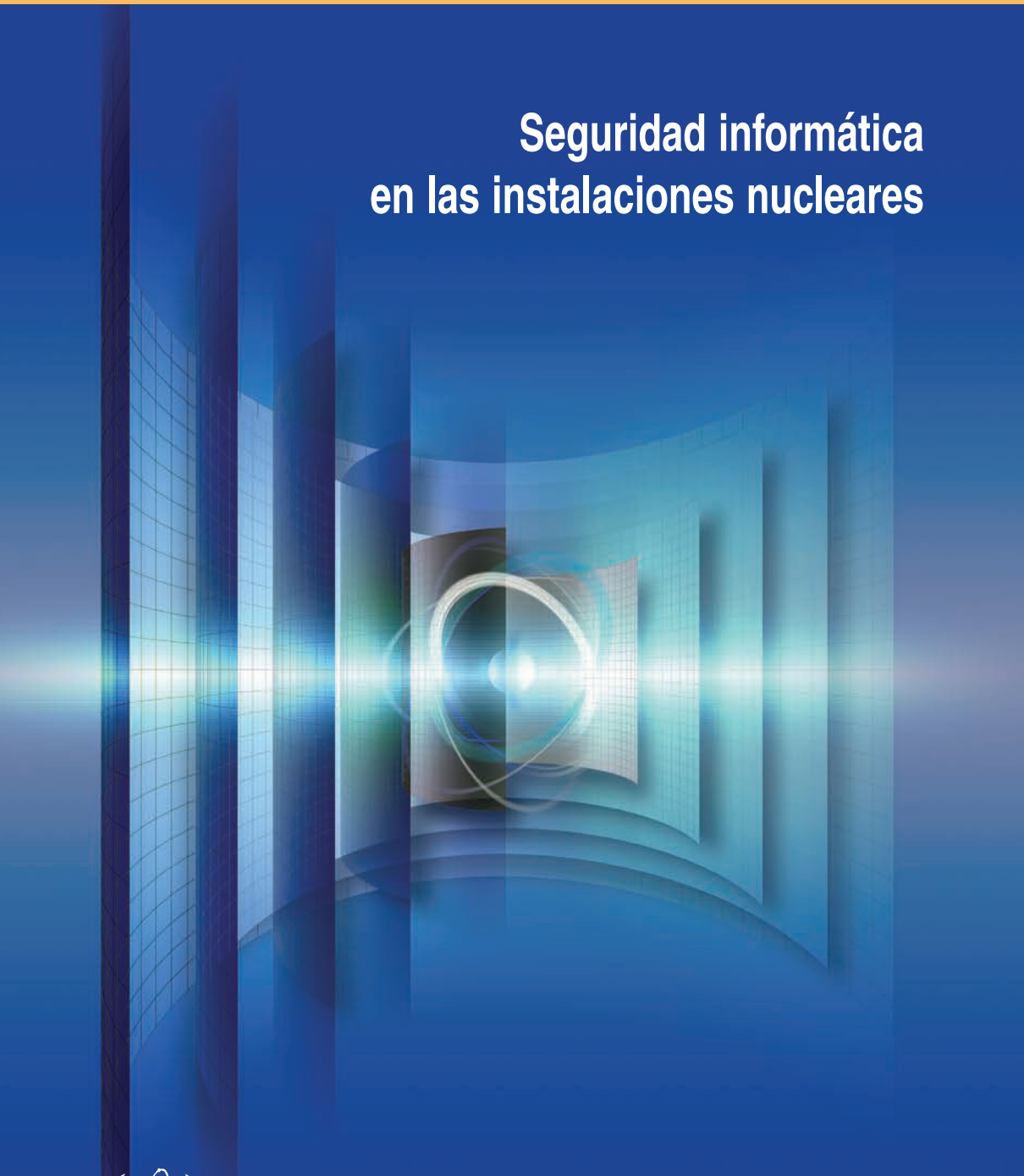
La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

Colección de Seguridad Física Nuclear del OIEA Nº 17

Orientaciones Técnicas
Manual de Referencia

Seguridad informática en las instalaciones nucleares



IAEA
Organismo Internacional de Energía Atómica

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

COLECCIÓN DE SEGURIDAD FÍSICA NUCLEAR DEL OIEA

Las cuestiones de seguridad física nuclear relativas a la prevención y detección de robos, sabotajes, accesos no autorizados y transferencias ilegales u otros actos dolosos relacionados con los materiales nucleares, otras sustancias radiactivas y sus instalaciones conexas, y para dar respuesta a tales actos, se abordan en las publicaciones de la **Colección de Seguridad Física Nuclear del OIEA**. Estas publicaciones son coherentes con los instrumentos internacionales de seguridad física nuclear como la Convención enmendada sobre la protección física de los materiales nucleares, el Código de Conducta sobre la seguridad tecnológica y física de las fuentes radiactivas, las resoluciones 1373 y 1540 del Consejo de Seguridad de las Naciones Unidas, y la Convención Internacional para la supresión de los actos de terrorismo nuclear, y los complementa.

CATEGORÍAS DE LA COLECCIÓN DE SEGURIDAD FÍSICA NUCLEAR DEL OIEA

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

- Las **Nociones Fundamentales de Seguridad Física Nuclear** recoge los objetivos, conceptos y principios de la seguridad física nuclear y constituye la base de las recomendaciones sobre seguridad física.
- Las **Recomendaciones** exponen las prácticas óptimas que deberían adoptar los Estados Miembros al aplicar las Nociones Fundamentales de Seguridad Física Nuclear.
- Las **Guías de Aplicación** exponen con detalle la información que figura en las Recomendaciones en esferas amplias y proponen medidas para su aplicación.
- Las publicaciones de **Orientaciones Técnicas** incluyen: **Manuales de Referencia**, con medidas y/u orientaciones detalladas sobre cómo poner en práctica la información de las Guías de Aplicación en ámbitos o actividades específicos; las **Guías de Capacitación**, que abarcan los programas y/o los manuales para los cursos de capacitación del OIEA en la esfera de la seguridad física nuclear; y las **Guías de Servicio**, que dan orientaciones sobre la realización y el alcance de las misiones de asesoramiento sobre seguridad física nuclear del Organismo

REDACCIÓN Y REVISIÓN

La Secretaría del OIEA recibe la ayuda de expertos internacionales para redactar estas publicaciones. En el caso de las Nociones Fundamentales de Seguridad Física Nuclear, de las Recomendaciones y de las Guías de Aplicación, el OIEA celebra reuniones técnicas de composición abierta para dar a los Estados Miembros interesados y a las organizaciones internacionales competentes la oportunidad de examinar el proyecto de texto. Además, a fin de garantizar un alto grado de análisis y consenso internacionales, la Secretaría presenta los proyectos de texto a todos los Estados Miembros para su examen oficial durante un período de 120 días. De este modo, los Estados Miembros tienen la oportunidad de expresar plenamente sus opiniones antes de que se publique el texto.

Las Orientaciones Técnicas se elaboran en estrecha consulta con expertos internacionales. Aunque no es necesario convocar reuniones técnicas, éstas se pueden celebrar, si se considera necesario, para recabar una amplia gama de opiniones.

En el proceso de redacción y revisión de las publicaciones de la Colección de Seguridad Física Nuclear del OIEA se tienen en cuenta factores de confidencialidad y se reconoce que la seguridad física nuclear va inseparablemente unida a preocupaciones sobre la seguridad física nacional generales y específicas. Un elemento subyacente es que en el contenido técnico de las publicaciones se deben tener en cuenta las normas de seguridad y las actividades de salvaguardias del OIEA.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

SEGURIDAD INFORMÁTICA EN LAS INSTALACIONES NUCLEARES

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

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

AFGANISTÁN, REPÚBLICA ISLÁMICA DEL
ALBANIA
ALEMANIA
ANGOLA
ARABIA SAUDITA
ARGELIA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIYÁN
BAHREIN
BANGLADESH
BELARÚS
BÉLGICA
BELICE
BENIN
BOLIVIA
BOSNIA Y HERZEGOVINA
BOTSWANA
BRASIL
BULGARIA
BURKINA FASO
BURUNDI
CAMBOYA
CAMERÚN
CANADÁ
CHAD
CHILE
CHINA
CHIPRE
COLOMBIA
CONGO
COREA, REPÚBLICA DE
COSTA RICA
CÔTE D'IVOIRE
CROACIA
CUBA
DINAMARCA
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
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, REPÚBLICA ISLÁMICA DE
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
SANTA SEDE
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONA
SINGAPUR
SRI LANKA
SUDÁFRICA
SUDÁN
SUECIA
SUIZA
TAILANDIA
TAYIKISTÁN
TOGO
TRINIDAD Y TABAGO
TÚNEZ
TURQUÍA
UCRANIA
UGANDA
URUGUAY
UZBEKISTÁN
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”.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

COLECCIÓN DE
NORMAS DE SEGURIDAD DEL OIEA Nº 17

SEGURIDAD INFORMÁTICA EN LAS INSTALACIONES NUCLEARES

MANUAL DE REFERENCIA

ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA
VIENA, 2013

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

DERECHOS DE AUTOR

Todas las publicaciones científicas y técnicas del OIEA están protegidas en virtud de la Convención Universal sobre Derecho de Autor aprobada en 1952 (Berna) y revisada en 1972 (París). Desde entonces, la Organización Mundial de la Propiedad Intelectual (Ginebra) ha ampliado la cobertura de los derechos de autor que ahora incluyen la propiedad intelectual de obras electrónicas y virtuales. Para la utilización de textos completos, o parte de ellos, que figuren en publicaciones del OIEA, impresas o en formato electrónico, deberá obtenerse la correspondiente autorización, y por lo general dicha utilización estará sujeta a un acuerdo de pago de regalías. Se aceptan propuestas relativas a reproducción y traducción sin fines comerciales, que se examinarán individualmente. Las solicitudes de información deben dirigirse a la Sección Editorial del OIEA:

Dependencia de Mercadotecnia y Venta
Sección Editorial
Organismo Internacional de Energía Atómica
Centro Internacional de Viena
PO Box 100
1400 Viena (Austria)
fax: +43 1 2600 29302
tel.: +43 1 2600 22417
correo-e: sales.publications@iaea.org
http://www.iaea.org/books

© OIEA, 2013
Impreso por el OIEA en Austria
Junio de 2013
STI/PUB/1527

SEGURIDAD INFORMÁTICA EN LAS
INSTALACIONES NUCLEARES
OIEA, VIENA, 2013
STI/PUB/1527
ISBN 978-92-0-337310-4
ISSN 1816-9317

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

PRÓLOGO

La posibilidad de que se utilicen materiales nucleares u otros materiales radiactivos con fines dolosos no se puede descartar en la actual situación mundial. Los Estados han respondido a este riesgo asumiendo un compromiso colectivo destinado a reforzar la protección y el control de esos materiales y a responder de forma eficaz a sucesos relacionados con la seguridad física nuclear. Asimismo han acordado fortalecer los instrumentos existentes y han establecido nuevos instrumentos jurídicos internacionales para mejorar la seguridad física nuclear en todo el mundo. La seguridad física nuclear es fundamental en la gestión de las tecnologías nucleares y en aplicaciones en las que se utilizan o transportan materiales nucleares u otros materiales radiactivos.

Por conducto de su programa de seguridad física nuclear, el OIEA presta apoyo a los Estados para que establezcan y mantengan un régimen de seguridad física nuclear eficaz. El OIEA ha adoptado un enfoque global de la seguridad física nuclear, en virtud del cual se reconoce que un régimen nacional de seguridad física nuclear eficaz se basa en: la aplicación de instrumentos jurídicos internacionales pertinentes; la protección de la información; la protección física; la contabilidad y el control de los materiales; la detección del tráfico de esos materiales y la respuesta a este; los planes nacionales de respuesta, y las medidas de contingencia. Con su Colección de Seguridad Física Nuclear, el OIEA busca ayudar a los Estados a aplicar y mantener dicho régimen de forma coherente e integrada.

La Colección de Seguridad Física Nuclear del OIEA se compone de las Nociones Fundamentales de Seguridad Física Nuclear, que comprende los objetivos y elementos esenciales del régimen de seguridad física nuclear de un Estado; las Recomendaciones; las Guías de Aplicación, y las Orientaciones Técnicas.

Cada Estado tiene la plena responsabilidad de la seguridad física nuclear, en particular, de prever medidas de seguridad física de materiales nucleares y otros materiales radiactivos, y de instalaciones y actividades conexas; de garantizar la seguridad física de esos materiales durante su utilización, almacenamiento o transporte; de combatir el tráfico ilícito y el desplazamiento involuntario de esos materiales; y de estar preparado para responder a un suceso relacionado con la seguridad física nuclear.

La presente publicación pertenece a la categoría de Orientaciones Técnicas de la Colección de Seguridad Física Nuclear del OIEA y trata la seguridad informática en las instalaciones nucleares. Se basa en la experiencia y las prácticas nacionales, así como en publicaciones de los ámbitos de la seguridad informática y la seguridad física nuclear. Las orientaciones se presentan para su examen por los Estados, las autoridades competentes y los explotadores.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

La preparación de esta publicación de la Colección de Seguridad Física Nuclear del OIEA ha sido posible gracias a las contribuciones de un gran número de expertos de los Estados Miembros. En el amplio proceso de consulta con todos los Estados Miembros se celebraron reuniones de consultores y reuniones técnicas de composición abierta. Seguidamente, el proyecto de documento se hizo circular entre todos los Estados Miembros durante 120 días a fin de recabar nuevas observaciones y propuestas. Las observaciones recibidas de los Estados Miembros se examinaron y tuvieron en cuenta en la versión final de la publicación.

NOTA EDITORIAL

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

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

Las denominaciones concretas de países o territorios empleadas en esta publicación no implican juicio alguno por parte del editor, el OIEA, sobre la condición jurídica de dichos países o territorios, de sus autoridades e instituciones, ni del trazado de sus fronteras.

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

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

ÍNDICE

1. INTRODUCCIÓN 1

1.1. Antecedentes 1
1.2. Objetivo 1
1.2.1. Objetivos de la seguridad física nuclear y de la seguridad informática 1
1.2.2. Ámbito de aplicación 2
1.3. Condiciones específicas de las instalaciones nucleares 3
1.4. Estructura 4
1.5. Metodología 4
1.6. Terminología fundamental 5

PARTE I. GUÍA DE GESTIÓN 7

2. ASPECTOS DE REGLAMENTACIÓN Y GESTIÓN 9

2.1. Aspectos legislativos 9
2.2. Aspectos de reglamentación 10
2.3. Marco de Seguridad física del emplazamiento 12
2.3.1. Política de seguridad informática 13
2.3.2. Sistemas informáticos en las instalaciones nucleares . . 13
2.3.3. Defensa en profundidad 13
2.4. Evaluación del entorno de las amenazas 14

3. SISTEMAS DE GESTIÓN 15

4. CUESTIONES DE ORGANIZACIÓN 17

4.1. Atribuciones y responsabilidades 17
4.1.1. Personal directivo 17
4.1.2. Oficial de seguridad informática 17
4.1.3. Grupo de seguridad informática 19
4.1.4. Otras responsabilidades del personal directivo 19
4.1.5. Responsabilidades individuales 20
4.2. Cultura de seguridad informática 20
4.2.1. Programa de capacitación sobre seguridad informática . 21

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

PARTE II. GUÍA DE APLICACIÓN 23

5. APLICACIÓN DEL PROGRAMA DE SEGURIDAD INFORMÁTICA 25

5.1. Plan y política de seguridad informática 25
5.1.1. Política de seguridad informática 25
5.1.2. Plan de seguridad informática 25
5.1.3. Componentes del CSP 26
5.2. Interacción con otros ámbitos de la seguridad física 27
5.2.1. Seguridad física 27
5.2.2. Seguridad del personal 28
5.3. Análisis y gestión de activos 28
5.4. Clasificación de los sistemas informáticos 29
5.4.1. Importancia para la seguridad tecnológica 30
5.4.2. Sistemas de seguridad física o sistemas conexos 32
5.5. Enfoque graduado a la seguridad informática 32
5.5.1. Niveles de seguridad 33
5.5.2. Zonas 33
5.5.3. Ejemplo de la aplicación de un modelo de niveles de seguridad 34
5.5.4. Separación entre zonas 39

6. AMENAZAS, VULNERABILIDADES Y GESTIÓN DE RIESGOS 40

6.1. Conceptos básicos y relaciones entre ellos 40
6.2. Evaluación y gestión de riesgos 41
6.3. Determinación y caracterización de las amenazas 42
6.3.1. Amenaza base de diseño 43
6.3.2. Perfiles de atacantes 43
6.3.3. Escenarios de ataque 44
6.4. Resultados simplificados de la evaluación de riesgos 48

7. CONSIDERACIONES ESPECIALES RELATIVAS A LAS INSTALACIONES NUCLEARES 49

7.1. Fases de la vida útil y modalidades de funcionamiento de una instalación 50
7.2. Diferencias entre los sistemas de TI y los sistemas de control industrial 50

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

7.3. Demanda de conectividad adicional y consecuencias conexas 52
7.4. Consideraciones relativas a las actualizaciones de los programas informáticos 53
7.5. Diseño seguro y especificaciones relativas a los sistemas informáticos 54
7.6. Procedimiento para el control del acceso de terceros/proveedores 54

REFERENCIAS 57
BIBLIOGRAFÍA 59

ANEXO I: ESCENARIOS DE ATAQUE CONTRA SISTEMAS DE INSTALACIONES NUCLEARES 61

ANEXO II: METODOLOGÍA PARA DETERMINAR LOS REQUISITOS DE SEGURIDAD INFORMÁTICA 65

ANEXO III: FUNCIÓN DEL ERROR HUMANO EN LA SEGURIDAD INFORMÁTICA 70

DEFINICIONES 73

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

1. INTRODUCCIÓN

1.1. ANTECEDENTES

La atención prestada a la seguridad informática se ha incrementado en el último decenio, a medida que han ido saliendo a la luz pruebas claras y recurrentes de las vulnerabilidades de los sistemas informáticos. El aprovechamiento doloso de esas vulnerabilidades se ha observado con una frecuencia y unas repercusiones cada vez mayores. En este escenario de amenazas de complejidad creciente, las posibilidades de ciberterrorismo como medio para atentar contra la infraestructura crítica de un Estado han impulsado a varias autoridades nacionales a preparar defensas y formular nuevas normativas, en las que se establecen requisitos de seguridad informática que afectan a las instalaciones nucleares en múltiples niveles y diversas fases de explotación. Al mismo tiempo, la seguridad de la información propiamente dicha ha evolucionado rápidamente, dando lugar a un copioso conjunto de mejores prácticas internacionales y documentos normativos, entre los que se cuentan los de la serie ISO/IEC 27000 [1 a 5], cuya notoriedad aumenta con velocidad.

Aunque reconoce la validez básica de la serie ISO 27000 y otras normas para distintos sectores y ámbitos de actividad, el OIEA desea centrar la atención en las condiciones específicas relativas a la seguridad informática en las instalaciones nucleares. Por consiguiente, se ha destacado la necesidad de una publicación en la que se reunieran las orientaciones pertinentes y las soluciones adecuadas. La presente publicación recopila los conocimientos y la experiencia de especialistas que han aplicado, ensayado y examinado las orientaciones y las normas en materia de seguridad informática en instalaciones nucleares y otras infraestructuras críticas. En ella se recogen y describen las disposiciones especiales, las mejores prácticas y las enseñanzas extraídas aplicables a la disciplina nuclear, que se sitúan en el contexto de un programa de seguridad coherente con otras orientaciones del OIEA y con otras normas industriales aplicables.

1.2. OBJETIVO

1.2.1. Objetivos de la seguridad física nuclear y de la seguridad informática

La seguridad física nuclear se refiere a la prevención y detección de actos delictivos o actos intencionales no autorizados que están relacionados con

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

materiales nucleares, otros materiales radiactivos, instalaciones conexas o *actividades conexas,* o que vayan dirigidos contra ellos, y otros actos intencionales que puedan tener, directa o indirectamente, consecuencias perjudiciales para las personas, los bienes, la sociedad o el medio ambiente, así como a la respuesta a esos actos.

La seguridad informática ejerce una función cada vez más vital para la consecución de esos objetivos. Por tanto, en la presente publicación se tratarán la creación y la mejora de programas destinados a proteger las redes y los sistemas informáticos y otros sistemas digitales que sean cruciales para la explotación de las instalaciones en condiciones de seguridad tecnológica y física, y para la prevención de robos, sabotajes y otros actos dolosos.

El alcance de las disposiciones de la presente publicación se ampliará con el fin de abarcar también todos los demás sistemas necesarios para la explotación de las instalaciones, u otros sistemas de apoyo u operacionales cuya modificación o alteración no autorizadas pueda comprometer la seguridad o la capacidad operativa.

En este contexto, los actos dolosos relacionados con los sistemas informáticos y con la seguridad física nuclear se pueden agrupar en las siguientes categorías:

— ataques para reunir información destinada a planificar y ejecutar otros actos dolosos;
— ataques por los que se desactiven o se pongan en peligro los atributos de una o varias computadoras cruciales para la seguridad física o tecnológica de una instalación;
— vulneración de una o varias computadoras, combinada con ataques simultáneos de otro tipo, como intrusión física en lugares blanco.

Los objetivos de la seguridad informática suelen definirse como la protección de los atributos de confidencialidad, integridad y disponibilidad de los datos electrónicos o de los sistemas y procesos informáticos. Esos objetivos de seguridad podrán cumplirse si se detectan y protegen tales atributos de los datos o los sistemas que pueden tener consecuencias negativas para las funciones de seguridad tecnológica y física de las instalaciones nucleares.

1.2.2. Ámbito de aplicación

La finalidad principal de la presente publicación es sensibilizar acerca de la importancia de incorporar la seguridad informática como componente fundamental del plan general de seguridad física de las instalaciones nucleares.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

Además, la publicación aspira a dar orientaciones específicas para las instalaciones nucleares respecto de la aplicación de un programa de seguridad informática. Para ello se presentan sugerencias sobre enfoques, estructuras y procedimientos de aplicación diseñados para las instalaciones nucleares que, en conjunto, son cruciales para alcanzar y mantener el nivel de protección definido en la estrategia de seguridad física de los emplazamientos y para ajustarse a los objetivos nacionales en materia de seguridad física nuclear.

Además, el presente manual de referencia tiene por objeto asesorar sobre la evaluación de los programas existentes, el análisis de los activos digitales críticos y la definición de las medidas apropiadas para reducir los riesgos.

1.3. CONDICIONES ESPECÍFICAS DE LAS INSTALACIONES NUCLEARES

La necesidad de orientaciones relativas a la seguridad informática en las instalaciones nucleares deriva de las condiciones especiales que caracterizan el sector. La lista siguiente no es más que una muestra de esas condiciones, que se examinarán en detalle en la presente publicación:

— las instalaciones nucleares deben atenerse a los requisitos establecidos por los órganos reguladores nacionales que reglamenten directa o indirectamente los sistemas informáticos o establezcan orientaciones sobre ellos.
— es posible que las instalaciones nucleares tengan que protegerse contra otros tipos de amenazas que habitualmente no se tienen en cuenta en otros sectores. Esas amenazas también pueden derivarse del carácter delicado de la industria nuclear.
— las exigencias en materia de seguridad informática de las instalaciones nucleares pueden diferir de las existentes en otros sectores. Las operaciones comerciales habituales solo están sujetas a un número limitado de requisitos. En el caso de las instalaciones nucleares se debe tener en cuenta un conjunto de consideraciones más amplias o completamente distintas que las relativas, por ejemplo, al comercio electrónico, la banca o incluso las aplicaciones militares. En la sección 7 se destacan y explican en detalle estas diferencias.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

1.4. ESTRUCTURA

Las orientaciones de la presente publicación están dirigidas a un público amplio, que incluye a los responsables de formular políticas, los reguladores de la seguridad física nuclear, el personal directivo de las instalaciones, el personal con atribuciones en la esfera de la seguridad física, el personal técnico, los proveedores y los contratistas. Son de aplicación a todas las fases del ciclo de vida de los sistemas de las instalaciones, como el diseño, el desarrollo, las operaciones y el mantenimiento.

La publicación se divide en dos partes:

— la parte I (secciones 2 a 4) está destinada a ayudar al personal directivo a emitir opiniones equilibradas y tomar decisiones fundamentadas en relación con las políticas, el diseño y la gestión de la seguridad informática en las instalaciones. Proporciona orientaciones sobre las disposiciones de reglamentación y gestión de la seguridad informática.
— la parte II (secciones 5 a 7) ofrece orientaciones técnicas y administrativas para la ejecución de un amplio plan de seguridad informática.

1.5. METODOLOGÍA

La metodología básica empleada para aplicar la seguridad informática es similar a las usadas para garantizar la seguridad nuclear tecnológica y física, lo que destaca la necesidad y las ventajas de integrar desde el principio la seguridad informática en los planes generales de seguridad física de las instalaciones.

Los sistemas informáticos se pueden proteger eficazmente si se adaptan las mejores prácticas respecto de los métodos e instrumentos elaborados en la comunidad mundial de la seguridad informática y se tienen en cuenta al mismo tiempo las características específicas del sector nuclear.

El proceso lógico siguiente, que se describe detalladamente en la sección 5, resalta la manera en que una instalación nuclear puede establecer, aplicar, mantener y mejorar la seguridad informática:

— cumplir los requisitos jurídicos y de reglamentación nacionales;
— examinar las orientaciones pertinentes del OIEA y otras directrices internacionales;
— obtener el apoyo del personal directivo superior y suficientes recursos;
— definir un perímetro de seguridad informática;

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

— detectar la interacción entre la seguridad informática y la explotación de la instalación, la seguridad tecnológica nuclear y otros aspectos de la seguridad física del emplazamiento;
— formular una política de seguridad informática;
— evaluar los riesgos;
— seleccionar, diseñar y aplicar medidas de protección en materia de seguridad informática;
— integrar la seguridad informática en el sistema de gestión de la instalación;
— controlar, revisar y mejorar periódicamente el sistema.

La presente publicación examinará con mayor detalle las fases de la metodología de seguridad informática respecto de las que existen disposiciones específicas para las instalaciones nucleares. Otras etapas de esa metodología se podrán poner en práctica haciendo referencia directa a normas nacionales e internacionales vigentes (véanse las referencias al final de la publicación).

1.6. TERMINOLOGÍA FUNDAMENTAL

Dado que los términos expresan conceptos diferentes en distintas comunidades de prácticas, en esta sección se aclara el significado de algunos términos importantes utilizados a lo largo de la presente publicación.

En el contexto que nos ocupa, los términos **computadoras** y **sistemas informáticos** hacen referencia a los dispositivos de computación, comunicación, instrumentación y control que constituyen los elementos funcionales de una instalación nuclear. Esta categoría incluye, además de las computadoras de mesa, los sistemas centrales, los servidores y los dispositivos en red, componentes de menor nivel, como los sistemas incorporados y los PLC (controladores lógicos programables). Básicamente, la presente publicación se refiere a todos los componentes susceptibles de vulneración electrónica.

En toda la publicación, el término **seguridad informática** abarcará la seguridad de todas las computadoras, según la definición anterior, y de todos los sistemas y las redes interconectados constituidos por la suma de los elementos. Los términos **seguridad de la TI** y **ciberseguridad** se consideran sinónimos de seguridad informática a los efectos de esta publicación y no se han utilizado.

La seguridad informática en la definición empleada en esta publicación es un subconjunto de la **seguridad de la información** (definida, por ejemplo, en ISO/IEC 27000 [1]), con la que comparte en gran medida los objetivos, la metodología y la terminología.

Al final de la presente publicación figuran las definiciones de otros términos utilizados.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

Parte I

GUÍA DE GESTIÓN

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

2. ASPECTOS DE REGLAMENTACIÓN Y GESTIÓN

Esta sección destaca los componentes básicos del marco de alto nivel para la seguridad informática en las instalaciones nucleares. En concreto, trata aspectos relacionados con los órganos legislativos y reguladores, así como con la estrategia de gestión y seguridad física de las instalaciones. En la figura 1 se muestra una imagen simplificada de la jerarquía de los instrumentos normativos pertinentes para la creación y aplicación de un programa de seguridad informática en una instalación nuclear.

2.1. ASPECTOS LEGISLATIVOS

Una función clave del Estado consiste en establecer el marco jurídico para la seguridad física nuclear, así como para la seguridad informática en general. De

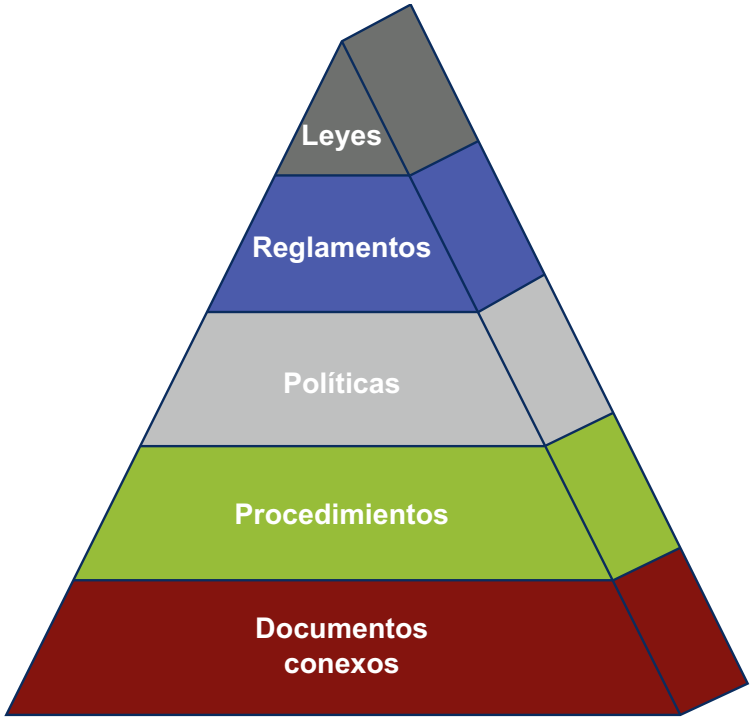


Fig. 1. Instrumentos normativos pertinentes.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

aplicarse adecuadamente, tendrá grandes repercusiones para la seguridad tecnológica y física de las instalaciones nucleares. El ordenamiento jurídico del Estado debe proporcionar, como mínimo, un marco legislativo y de reglamentación que abarque la protección de la información confidencial y se ocupe de cualquier actividad que pueda llevar a atentar contra la seguridad física nuclear.

Por tratarse de cuestiones muy específicas, la seguridad informática quizá requiera disposiciones legislativas especiales que tengan en cuenta el carácter singular de los delitos y modos de operación relacionados con los sistemas informáticos. Los Estados deben analizar en detalle si su legislación en vigor abarca adecuadamente los actos dolosos que puedan perpetrarse con ayuda de las computadoras. Entre otras leyes importantes que pueden influir en la seguridad informática y su aplicación se cuentan las siguientes:

— leyes relativas a delitos informáticos;
— leyes sobre terrorismo;
— leyes sobre la protección de la infraestructura nacional crítica;
— leyes que estipulan la divulgación de información;
— leyes sobre la privacidad y el tratamiento de la información personal.

Es importante que la legislación del Estado se examine y actualice constantemente a fin de incluir disposiciones relativas a actividades delictivas nuevas y emergentes, así como otras posibles amenazas a la seguridad informática.

Dada la índole de las redes informáticas, los adversarios tienen la posibilidad de perpetrar actos dolosos en un Estado desde fuera de sus fronteras físicas, estando así fuera del alcance de su sistema jurídico. En la fecha de elaboración de la presente publicación, el único instrumento jurídico internacional de importancia dedicado a regular la cooperación internacional en materia de delitos informáticos es el Convenio sobre la Ciberdelincuencia, del Consejo de Europa [6].

2.2. ASPECTOS DE REGLAMENTACIÓN

El órgano regulador debe tener en cuenta para sus orientaciones la legislación pertinente y poner a disposición de los explotadores los instrumentos y los medios que les permitan interpretar y aplicar correctamente las obligaciones legales. También puede seleccionar o sugerir guías de referencia adecuadas, como las normas ISO o publicaciones del OIEA.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

Las actividades de los reguladores relacionadas con la seguridad informática deben reconocer explícitamente el objetivo de proteger contra el robo de material nuclear y el sabotaje que puedan entrañar emisiones radiológicas. Por tanto, al elaborar reglamentos sobre seguridad informática también se deben tener en cuenta los reglamentos sobre seguridad nuclear física y tecnológica.

Es recomendable que los órganos reguladores del Estado (en caso de que haya más de uno) colaboren para llegar a una perspectiva armonizada sobre los requisitos necesarios que se deben establecer.

Los órganos reguladores del Estado podrían, como mínimo, formular una declaración de alto nivel sobre los requisitos de reglamentación de la seguridad informática. En otros requisitos normativos más detallados también podrían incluirse disposiciones relativas a los aspectos siguientes:

— Compromiso del personal directivo con la seguridad informática (sección 4).
— Propiedad del programa de seguridad informática, incluido el reparto de las funciones de los oficiales y los grupos de seguridad informática (sección 4).
— Política de seguridad informática, plan de aplicación y plan de ejecución (sección 5), incluidos:
  • la definición del perímetro de seguridad informática;
  • la determinación de riesgos;
  • la estrategia de gestión de riesgos;
  • el programa de capacitación y sensibilización sobre la seguridad informática;
  • la continuidad del plan de operaciones.
— Proceso de auditoría y examen, bien sea interno, externo o realizado por los propios reguladores.

Los requisitos no deben imponer soluciones técnicas detalladas porque pueden quedar obsoletas rápidamente debido a los nuevos avances. En cambio, podrían centrarse en los resultados previstos, ya que estos pueden formularse de manera que sean menos dependientes de la tecnología.

Podría pedirse a las instalaciones que demuestren que se ajustan a los requisitos nacionales de seguridad física mediante un plan general de seguridad física del emplazamiento (SSP) aprobado o un conjunto de documentos equivalente. **Los órganos reguladores del Estado deben publicar los requisitos de seguridad informática como parte de los requisitos del SSP**.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

2.3. MARCO DE SEGURIDAD FÍSICA DEL EMPLAZAMIENTO

La responsabilidad principal de la seguridad física del emplazamiento corresponde a la dirección, específicamente al personal directivo superior, que ha de garantizar el pleno cumplimiento de los requisitos legislativos y de reglamentación mediante la ejecución del SSP.

Todos los ámbitos de la seguridad (a saber, del personal, física, de la información e informática) interactúan y se complementan mutuamente para dar lugar a una postura en materia de seguridad física de la instalación según se haya definido en el SSP (véase la figura 2). Un fallo en uno de los ámbitos de la seguridad física podría tener repercusiones en los demás y plantear la necesidad de imponer requisitos adicionales en relación con los otros aspectos de la seguridad física. La seguridad informática es una disciplina intersectorial que interactúa con todas las demás esferas de la seguridad física de las instalaciones nucleares.

Fig. 2. Relación entre los diferentes ámbitos de la seguridad.

Todo lo dispuesto en la presente publicación debe aplicarse teniendo presente siempre el marco más amplio del plan de seguridad física del emplazamiento. Igualmente, este plan debe elaborarse teniendo en consideración desde un principio la seguridad informática.

También incumbe al personal directivo la responsabilidad de garantizar la coordinación adecuada entre los distintos campos de la seguridad física y la integración de la seguridad informática en el nivel apropiado.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

2.3.1. Política de seguridad informática

La dirección debe ser consciente de que la tecnología informática se utiliza cada vez más para muchas funciones vitales en las instalaciones nucleares. Esta evolución conlleva numerosos beneficios para la seguridad y eficacia operacionales. Sin embargo, a fin de garantizar el funcionamiento correcto de los sistemas informáticos, estos deben disponer de barreras de seguridad adecuadas y equilibradas que otorguen la máxima protección contra actos dolosos sin obstaculizar innecesariamente sus operaciones.

Por consiguiente, todas las instalaciones nucleares deben tener una política de seguridad informática, refrendada y aplicada por el personal directivo de mayor categoría. Esa política especificará los objetivos generales de la instalación en materia de seguridad informática.

La política de seguridad informática debe formar parte de la política general de seguridad física del emplazamiento y se ha de negociar y coordinar con otras responsabilidades pertinentes en materia de seguridad física. Al establecer la política de seguridad informática se deben tener en cuenta también sus repercusiones desde el punto de vista jurídico y de los recursos humanos.

La política de seguridad informática y el plan conexo se examinan con mayor detalle en la sección 5.

2.3.2. Sistemas informáticos en las instalaciones nucleares

Las redes y los sistemas informáticos de apoyo a las operaciones de las instalaciones nucleares comprenden numerosos sistemas de tecnología de la información (TI) con arquitecturas, configuraciones o requisitos de comportamiento no normalizados, tales como sistemas de control industrial especializados, sistemas de control del acceso, sistemas de alarma y seguimiento, y sistemas de información relacionados con la seguridad tecnológica y física y la respuesta a emergencias. Pese a que los sistemas de control industrial especializados han pasado de las aplicaciones estrictamente protegidas por derechos de propiedad a una arquitectura informática más generalizada, aún existen grandes diferencias entre esos sistemas y los de TI normalizados que se han de tener en cuenta al preparar el plan de seguridad física del emplazamiento. En la sección 7 se examinan en detalle las características excepcionales de los sistemas informáticos asociados a las instalaciones nucleares.

2.3.3. Defensa en profundidad

Los requisitos en materia de protección deben reflejar el concepto de múltiples barreras y métodos de protección (estructurales, técnicos, humanos y

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

organizativos) que los adversarios deben superar o evitar para alcanzar sus objetivos.

El principal medio de prevenir y mitigar las consecuencias de la vulneración de la seguridad física es la "defensa en profundidad", que consiste fundamentalmente en la combinación de una serie de niveles de protección consecutivos e independientes que tendrían que fallar o ser vulnerados antes de que un sistema informático se pueda ver comprometido. Si fallara un nivel de protección o una barrera, el nivel o la barrera siguientes cumplirían su función. Correctamente aplicada, la defensa en profundidad garantiza que ningún fallo técnico, humano o de organización pueda, por sí solo, comprometer el sistema informático, y que las combinaciones de fallos que pudieran causar incidentes informáticos sean sumamente improbables. La eficacia independiente de los diferentes niveles de defensa es un elemento necesario de la defensa en profundidad.

2.4. EVALUACIÓN DEL ENTORNO DE LAS AMENAZAS

El entorno de las amenazas para la seguridad informática es un escenario en rápida evolución. Aunque un buen programa de seguridad informática garantiza su propia duración, los controles específicos aplicados contra las amenazas más habituales en la actualidad no garantizan la protección contra las que surjan en el futuro.

La autoridad estatal competente debe emitir periódicamente una evaluación de las amenazas que abarque las amenazas para la seguridad de los sistemas informáticos e información actualizada sobre los vectores de ataques relacionados con la seguridad de los sistemas informáticos empleados en instalaciones nucleares. Una herramienta típica que se utiliza para determinar los niveles de amenazas y como base para el establecimiento de una posición en materia de seguridad física es la amenaza base de diseño (ABD, véase la sección 6.3.1.).

Es vital que las instalaciones realicen de manera activa y permanente evaluaciones de las amenazas y que informen periódicamente al respecto al personal directivo y los responsables de las operaciones.

En la sección 6 figura una descripción detallada, pero no exhaustiva, de los posibles orígenes de los ataques y los mecanismos de ataque conexos de importancia para las instalaciones nucleares, así como de las metodologías empleadas para evaluar y detectar las amenazas.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

3. SISTEMAS DE GESTIÓN

Un sistema de gestión es responsable de establecer políticas y objetivos y de facilitar el logro eficaz y eficiente de dichos objetivos. Los sistemas de gestión son un elemento de apoyo esencial para la cultura de la seguridad física nuclear. En las instalaciones nucleares hay muchas actividades controladas por esos sistemas de gestión que deberían, en principio, integrar elementos relacionados con la seguridad física y tecnológica, la salud, el medio ambiente, la calidad y la economía en una única herramienta de gestión o en un conjunto de sistemas integrados y que se apoyan mutuamente [7, 8].

Es imprescindible examinar los sistemas de gestión para asegurar que sean completos y se atengan a las políticas de seguridad física del emplazamiento. En general, los sistemas de gestión son dinámicos por naturaleza y deben adaptarse a las condiciones cambiantes de la instalación y el entorno; no se pueden aplicar como medida excepcional, sino que es preciso evaluarlos y mejorarlos continuamente. En la figura 3 se muestra el ciclo de vida de los procesos de gestión.

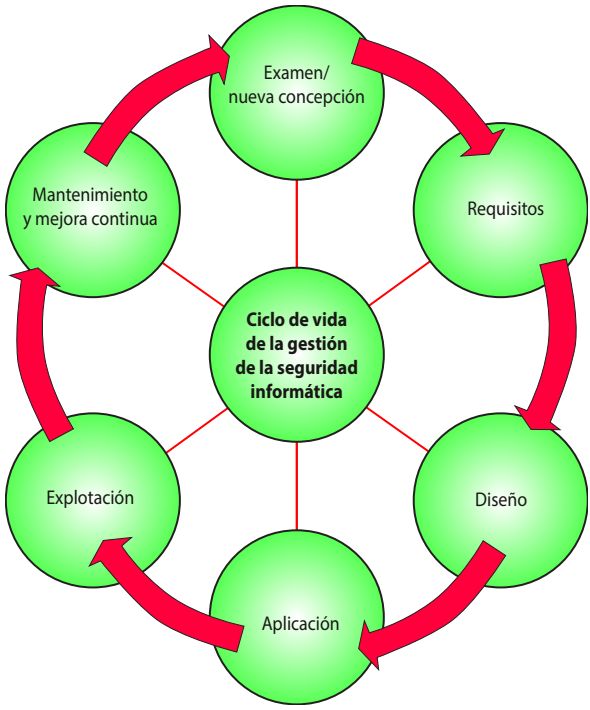


Fig. 3. Ciclo de vida de la gestión de la seguridad.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

El objetivo de la presente sección es complementar las orientaciones existentes relativas a los sistemas de gestión con los detalles necesarios para gestionar la seguridad informática. A continuación se indican los elementos fundamentales que deben examinarse o añadirse a fin de integrar las disposiciones necesarias para la seguridad informática:

— determinación y clasificación de los recursos de información;
— análisis oficial de riesgos;
— cumplimiento de las disposiciones legislativas y reglamentarias;
— requisitos operacionales;
— requisitos relativos a las competencias de personas clave;
— continuidad de las actividades;
— gestión lógica del acceso;
— seguridad durante el ciclo de vida del sistema;
— gestión de la configuración;
— enmienda y aprobación de las medidas de seguridad informática;
— aplicación de las medidas de seguridad informática definidas;
— aceptación de las medidas de seguridad informática aplicadas;
— cumplimiento de las medidas de seguridad informática aprobadas;
— análisis inmediato de incidentes de seguridad informática y notificación adecuada;
— presentación de informes periódicos sobre el cumplimiento;
— exámenes periódicos de las medidas de seguridad aplicadas (auditorías) realizados por partes internas y externas;
— capacitación en materia de sensibilización;
— nuevos riesgos y cambios en los riesgos determinados;
— cambios en los requisitos legislativos y de reglamentación;
— planes de mediano plazo sobre seguridad de la información.

Los procesos indicados deben considerarse actividades continuas que se realizan durante todas las fases del ciclo de vida de los sistemas. Los elementos específicos de la aplicación deben detallarse en el plan de seguridad informática que se describe en la sección 5.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

4. CUESTIONES DE ORGANIZACIÓN

4.1. ATRIBUCIONES Y RESPONSABILIDADES

A continuación se especifican los requisitos mínimos que deben cumplir el personal directivo y el personal especializado para establecer y mantener eficazmente un programa de seguridad informática.

4.1.1. Personal directivo

El personal directivo superior de la instalación se encarga de dar inicio al proceso de seguridad informática mediante el establecimiento de una entidad de apoyo adecuada. A estos efectos, debe:

— asumir la responsabilidad general de todos los aspectos de la seguridad informática;
— definir los objetivos en materia de seguridad de la instalación;
— garantizar el cumplimiento de las leyes y los reglamentos;
— definir el nivel de aceptación de los riesgos para la instalación;
— asignar las responsabilidades de seguridad informática en la entidad;
— garantizar la comunicación adecuada en lo que atañe a los diferentes aspectos de la seguridad física;
— velar por que se establezca una política de seguridad informática aplicable;
— poner a disposición suficientes recursos para la ejecución de un programa de seguridad informática viable;
— velar por que se efectúen verificaciones y actualizaciones periódicas de la política y los procedimientos de seguridad informática;
— garantizar el apoyo a los programas de capacitación y sensibilización.

Generalmente, la responsabilidad del proceso de seguridad informática incumbe en todo momento a los especialistas de la entidad.

4.1.2. Oficial de seguridad informática

La seguridad informática afecta a casi todas las actividades de la instalación. Por eso es importante asignar las funciones de supervisión generales conexas a un órgano bien definido. En la presente publicación se utiliza la denominación “oficial de seguridad informática” (CSO), que en otros casos corresponde a la de “oficial de seguridad de TI” o de “oficial de seguridad de la

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

información", o que puede corresponder a las funciones de varias personas. Independientemente del enfoque empleado, estas funciones deben coordinarse estrechamente en toda la instalación, ser independientes de los departamentos encargados de la ejecución y disponer de mecanismos bien definidos y accesibles de rendición de cuentas al personal directivo superior.

El CSO debe tener conocimientos profundos de la seguridad informática y buenos conocimientos de otros aspectos de la seguridad física de las instalaciones nucleares. Además, debe poseer conocimientos en materia de seguridad tecnológica nuclear y gestión de proyectos, así como la capacidad de integrar en un grupo eficiente a personas que trabajan en diferentes campos.

Entre las responsabilidades típicas de un CSO o equivalente figuran:

— asesorar al personal directivo de la empresa en materia de seguridad informática;
— dirigir el grupo encargado de la seguridad informática;
— coordinar y controlar el avance de las actividades de seguridad informática (como la aplicación de las políticas, las directivas, los procedimientos, las orientaciones y las medidas conexas);
— desempeñar funciones de coordinación con los servicios de seguridad física y otros encargados de la seguridad física y tecnológica a los efectos de la planificación de las medidas de seguridad física y de la respuesta a incidentes conexos;
— determinar los sistemas cruciales para la seguridad informática en una instalación (es decir, los datos de referencia en materia de seguridad informática); debería informarse a los propietarios del equipo de la función que éste desempeña en la seguridad informática;
— realizar evaluaciones periódicas de los riesgos para la seguridad informática;
— realizar inspecciones, verificaciones y exámenes periódicos de los datos de referencia en materia de seguridad informática y presentar informes de situación al personal directivo superior;
— elaborar y ejecutar programas de capacitación y evaluación en materia de seguridad informática;
— preparar y dirigir la respuesta a incidentes en casos de emergencias relacionadas con la seguridad informática, incluida la coordinación con las entidades competentes, tanto internas como externas;
— investigar los incidentes de seguridad informática y adoptar los procedimientos posteriores y las medidas preventivas correspondientes;
— participar en actividades de evaluación de la seguridad física del emplazamiento;

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

— participar en el análisis de las necesidades durante la adquisición o el desarrollo de nuevos sistemas.

4.1.3. Grupo de seguridad informática

Es esencial que el CSO tenga acceso a conocimientos especializados interdisciplinarios adecuados sobre la seguridad informática, la seguridad tecnológica de la instalación y las operaciones de la central, así como sobre la seguridad física y del personal. Se trataría de facilitarle acceso al grupo encargado específicamente de la seguridad informática o acceso a determinados conocimientos especializados dentro de la entidad. El grupo de seguridad informática prestará apoyo al CSO en el desempeño de sus funciones.

4.1.4. Otras responsabilidades del personal directivo

El personal directivo de una entidad debe garantizar, a los distintos niveles y en el marco de sus respectivas esferas de responsabilidad, un grado adecuado de seguridad informática. Entre las responsabilidades típicas figuran:

— dirigir las operaciones con arreglo las orientaciones del plan de seguridad informática del emplazamiento;
— informar sobre los requisitos operacionales al CSO y proporcionarle información relacionada con la seguridad informática, así como resolver posibles conflictos entre los requisitos operacionales, de seguridad física y de seguridad tecnológica;
— poner al CSO al corriente de las condiciones que podrían llevar a modificar las características de la seguridad informática, como cambios de personal, de equipos o de procesos;
— garantizar que el personal reciba capacitación e información suficientes sobre las cuestiones de seguridad informática relacionadas con sus funciones;
— garantizar que las operaciones de los subcontratistas y los proveedores de terceros que trabajan para la dependencia de contratas se ajusten al plan de seguridad física del emplazamiento;
— dar seguimiento a los sucesos de importancia para la seguridad física, monitorizarlos y notificarlos;
— hacer que se apliquen las medidas de seguridad física relativas al personal.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

4.1.5. Responsabilidades individuales

Cada una de las personas que trabajan en una entidad tiene la responsabilidad de aplicar el plan de seguridad informática. Entre las responsabilidades específicas figuran:

— conocer los procedimientos básicos de seguridad informática;
— conocer los procedimientos de seguridad informática específicos del puesto;
— desempeñar las funciones ajustándose a los parámetros de las políticas de seguridad informática;
— notificar al personal directivo cualquier cambio que pueda menoscabar las características de las seguridad informática;
— notificar a la dirección cualquier incidente real o posible que pueda poner en peligro la seguridad informática;
— acudir periódicamente a cursos de capacitación inicial y de perfeccionamiento sobre seguridad física.

4.2. CULTURA DE SEGURIDAD INFORMÁTICA

Una cultura sólida de seguridad informática es un componente esencial de todo plan de seguridad física eficaz. Es importante que el personal directivo garantice la integración plena de la sensibilización a la seguridad informática en la cultura de seguridad física del emplazamiento en general. Las características de la cultura de seguridad física nuclear son las creencias, las actitudes, los comportamientos y los sistemas de gestión que, en su conjunto, dan lugar a un programa de seguridad física nuclear más eficaz. La cultura de seguridad nuclear se cimienta en el reconocimiento, por parte de quienes desempeñan una función en la reglamentación, gestión o explotación de instalaciones o actividades nucleares, o incluso de quienes podrían verse afectados por esas actividades, de que existe una amenaza creíble y de que la seguridad física nuclear es importante. (Para más información sobre la cultura de seguridad física nuclear, véase la ref. [9]). La cultura de seguridad informática es un subconjunto de la cultura de seguridad física general y se basa en la aplicación de las características antes mencionadas a la sensibilización a la seguridad informática.

La experiencia ha demostrado que la mayoría de los incidentes de seguridad informática están relacionados con la actividad humana y que la seguridad de cualquier sistema informático depende en gran medida del comportamiento de todos sus usuarios. En el anexo III se presentan ejemplos de errores humanos que podrían comprometer la seguridad física. La cultura de seguridad informática se

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

establece mediante la recopilación de numerosas actividades destinadas a informar al personal y aumentar la sensibilización a la seguridad informática (por ejemplo, carteles, avisos, debates a nivel del personal directivo, capacitación, ensayos, etc.). Es necesario medir y examinar con cierta periodicidad y mejorar continuamente los atributos de la cultura de seguridad informática. Los indicadores siguientes pueden servir para evaluar la cultura de seguridad informática en una entidad:

— los requisitos de seguridad informática están claramente documentados y el personal los entiende bien;
— existen procesos y protocolos claros y eficaces dentro y fuera de la entidad respecto del funcionamiento de los sistemas informáticos;
— el personal entiende y es consciente de la importancia de ajustarse a los controles previstos en el programa de seguridad informática;
— los sistemas informáticos reciben mantenimiento a fin de garantizar su seguridad y de velar por que funcionen con arreglo a los datos de referencia y los procedimientos en materia de seguridad informática;
— el personal directivo se muestra plenamente comprometido con las iniciativas de seguridad física y las apoya.

4.2.1. Programa de capacitación sobre seguridad informática

Un buen programa de capacitación es una de las piedras angulares de la cultura de la seguridad informática. Es crucial para educar al personal, los contratistas y los proveedores sobre la importancia de respetar los procedimientos de seguridad física y de mantener una cultura de seguridad física.

El programa de sensibilización debería incluir los requisitos siguientes:

— la culminación con éxito de un programa de capacitación y/o sensibilización en materia de seguridad informática debería ser una condición indispensable para el acceso a los sistemas informáticos; la capacitación debería ajustarse a los niveles de seguridad física de los sistemas y a la función de los usuarios prevista;
— debería proporcionarse más capacitación a las personas que desempeñan funciones clave en materia de seguridad física (como el CSO, los integrantes del grupo encargado de la seguridad informática, los directores de proyectos o los administradores de TI) con miras a incrementar sus cualificaciones;
— la capacitación debería repetirse periódicamente en el caso de todo el personal, a fin de incluir los nuevos procedimientos y amenazas;

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

— debería pedirse al personal que demuestre que entiende cuáles son sus responsabilidades en materia de seguridad física.

El programa de capacitación debería incluir elementos de medición para evaluar la sensibilización a la seguridad informática, la eficacia de la capacitación y los procesos de mejora continua o de perfeccionamiento

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

PARTE II

GUÍA DE APLICACIÓN

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

5. APLICACIÓN DEL PROGRAMA DE SEGURIDAD INFORMÁTICA

La presente publicación no establece normas mínimas respecto de los niveles de riesgo aceptables ni un conjunto específico de medidas de mitigación que se puedan utilizar. Cualquier conjunto de normas específicas pasaría a ser rápidamente obsoleto debido a la evolución de los sistemas digitales, la aparición de nuevas amenazas y de nuevos instrumentos de mitigación y la modificación de los requisitos reglamentarios. La parte II de la publicación se centra en la compilación de un conjunto de recomendaciones metodológicas y concretas para apoyar y orientar la aplicación del programa de seguridad informática en las instalaciones nucleares.

Estas recomendaciones no tienen carácter prescriptivo ni definitivo, y deberían utilizarse como orientación; cuando corresponda, podrán adoptarse otras medidas a fin de lograr la defensa en profundidad deseada y otros objetivos fundamentales de la seguridad física nuclear [10–12].

5.1. PLAN Y POLÍTICA DE SEGURIDAD INFORMÁTICA

5.1.1. Política de seguridad informática

Como se indicó en la sección 2.3.1, la política de seguridad informática establece los objetivos de alto nivel en materia de seguridad informática de una entidad. Esta política debe cumplir los requisitos reglamentarios pertinentes. Los requisitos de la política de seguridad informática deberían tenerse en cuenta en documentos de menor importancia, que se utilizarán para aplicar y regular la política. Además, esta política debe ser:

— ejecutable;
— viable;
— verificable.

5.1.2. Plan de seguridad informática

El plan de seguridad informática (CSP) es la aplicación de la política conexa en forma de funciones, responsabilidades y procedimientos institucionales. En él se especifican y detallan los medios para alcanzar los

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

objetivos de seguridad informática en la instalación; el plan forma parte del SSP general (o está vinculado a él).

Este plan debería incluir las principales medidas en relación con la susceptibilidad a vulnerabilidades, las medidas protectoras, el análisis de las consecuencias y las medidas de mitigación que se requieren para establecer y mantener el nivel de riesgo informático aceptable para la instalación nuclear y facilitar el restablecimiento de unas condiciones de funcionamiento seguras.

5.1.3. Componentes del CSP

A la luz de la política de seguridad informática establecida, cada uno de los componentes del plan busca alcanzar sus propias metas y objetivos. En las subsecciones siguientes se proponen el contenido mínimo y desglose del CSP:

a) Organización y responsabilidades:
   1) organigramas;
   2) personas responsables y funciones de notificación;
   3) proceso de examen y aprobación periódicos.

b) Gestión de activos:
   1) lista de todos los sistemas informáticos;
   2) lista de todas las aplicaciones de los sistemas informáticos;
   3) diagrama de la red, con todas las conexiones a sistemas informáticos externos.

c) Evaluación de los riesgos, la vulnerabilidad y el cumplimiento:
   1) examen del plan de seguridad física y periodicidad de las evaluaciones;
   2) autoevaluación (incluidos los procedimientos para la realización de pruebas de penetración);
   3) procedimientos de verificación, y seguimiento y corrección de las deficiencias;
   4) cumplimiento de los requisitos legislativos y de reglamentación.

d) Diseño y gestión de la configuración de la seguridad física de los sistemas:
   1) principios fundamentales de arquitectura y diseño;
   2) requisitos relacionados con los diferentes niveles de seguridad física;
   3) formalización de los requisitos de seguridad informática para suministradores y proveedores;
   4) seguridad física durante el ciclo de vida completo.

e) Procedimientos de seguridad física operacionales:
   1) control del acceso;
   2) seguridad de los datos;
   3) seguridad de las comunicaciones;
   4) seguridad de las plataformas y aplicaciones (por ejemplo, refuerzo);

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

5) vigilancia de los sistemas;
6) mantenimiento de la seguridad informática;
7) manejo de incidentes;
8) continuidad de las actividades;
9) copia de seguridad del sistema.

f) Gestión de personal:
1) verificación de antecedentes;
2) capacitación;
3) cualificación;
4) cese/traslado.

Lo anterior proporciona un marco para el establecimiento del CSP. En este marco se podrían incluir numerosas referencias internacionales, principalmente la norma ISO/IEC 27001 [2], sobre los sistemas de gestión de la seguridad de la información, y la norma ISO/IEC 27002 [3], sobre las recomendaciones para la aplicación.

Si bien la mayoría de los componentes antes enunciados forman parte de los planes de seguridad informática de cualquier empresa o industria, hay ciertas diferencias sutiles en cuanto a su aplicación en las instalaciones nucleares. Estos componentes del CSP se describen más detalladamente en la sección 7; la evaluación de los riesgos, la vulnerabilidad y el cumplimiento se tratan en la sección 6; y el análisis de los activos se detalla en la sección 5.3.

5.2. INTERACCIÓN CON OTROS ÁMBITOS DE LA SEGURIDAD FÍSICA

Como se indica en la sección 2.3, el CSP debería aplicarse y mantenerse en el marco del plan general de protección de la instalación. El plan de seguridad informática específico de la instalación debería formularse en estrecha consulta con especialistas en protección física, seguridad tecnológica, operaciones y TI. El CSP debe examinarse y actualizarse periódicamente para reflejar los sucesos habidos en cualquier ámbito de la seguridad física y la experiencia operacional extraída del sistema de seguridad física del emplazamiento.

5.2.1. Seguridad física

El plan de seguridad física y el CSP deberían complementarse mutuamente. En el caso de los activos informatizados existen requisitos para el control del acceso físico e, igualmente, el hecho de que un sistema electrónico se vea comprometido puede llevar a la degradación o pérdida de ciertas funciones de protección física. Los escenarios de ataque bien podrían incluir la coordinación

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

de ataques tanto electrónicos como físicos. Los grupos encargados del plan de seguridad física y el CSP deberían mantenerse mutuamente informados y coordinar sus esfuerzos para asegurar la coherencia entre ambos planes durante el proceso de su elaboración y examen.

5.2.2. Seguridad del personal

Además de la sensibilización y capacitación, hay otros aspectos de la seguridad física (generalmente abordados en el marco de la seguridad del personal) que son esenciales para establecer una seguridad informática coherente. Las disposiciones necesarias para definir un nivel apropiado de verificación de antecedentes, compromisos de confidencialidad y procedimientos en materia de rescisión de contratos, y para determinar las competencias requeridas para los cargos, deberían coordinarse entre los responsables de la seguridad informática y del personal. En particular, en el caso del personal con responsabilidades clave en materia de seguridad física (administradores de sistemas o miembros del grupo encargado de la seguridad física) quizá sea necesario establecer un nivel más elevado de verificación de antecedentes.

5.3. ANÁLISIS Y GESTIÓN DE ACTIVOS

La interacción entre los sistemas informáticos de las instalaciones nucleares podría afectar la seguridad física de maneras nada obvias. Por consiguiente, es importante que en el plan de seguridad física se **especifiquen todos los activos** y se incluya un **inventario más completo de los que son cruciales para las funciones de seguridad física y tecnológica de la instalación**. El inventario podría incluir datos, sistemas informáticos, sus interfaces y sus propietarios.

La metodología siguiente atiende a esas necesidades:

a) debería recopilarse información relativa a los sistemas informáticos existentes a fin de crear una lista de todos los activos;
b) deberían delinearse las interconexiones entre los activos especificados;
c) debería determinarse y evaluarse la importancia de esos activos para las funciones de seguridad tecnológica y para los sistemas de seguridad tecnológica, los sistemas conexos y los sistemas de seguridad física especificados.

Es fundamental concluir cada fase antes de pasar a la siguiente.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

Un análisis integral de los sistemas informáticos de una instalación nuclear incluye:

— las funciones/tareas y modalidades de funcionamiento de todos los sistemas informatizados existentes;
— la determinación de las interconexiones pertinentes, incluidas las fuentes de alimentación;
— el análisis del flujo de datos para determinar qué se comunica con qué, cómo y por qué motivo;
— los procedimientos que inician la comunicación, la frecuencia de las comunicaciones y los protocolos;
— la ubicación de los sistemas y el equipo informatizados;
— el análisis de los grupos de usuarios;
— la propiedad (de los datos y de los sistemas informatizados);
— el correspondiente nivel de seguridad física (véase la sección 5.5, enfoque graduado).

Se supone que gran parte de la información necesaria para el análisis ya está disponible, pero que aún debe recopilarse y organizarse. Entre las fuentes de información pertinente figuran las especificaciones de los sistemas y la documentación conexa.

5.4. CLASIFICACIÓN DE LOS SISTEMAS INFORMÁTICOS

Como se define en la sección 1.6, en el contexto de la presente publicación, los términos computadora y sistemas informáticos hacen referencia a los dispositivos de computación, comunicación, instrumentación y detección que constituyen los elementos funcionales de una instalación nuclear. Las funciones informáticas que más atención requieren son los procesos de control y de datos relacionados con la seguridad tecnológica y física. Otras funciones informáticas pueden ser motivo de preocupación desde el punto de vista del apoyo que se les presta, de los efectos secundarios o indirectos que podrían comprometer la seguridad física o de la productividad de la central en general.

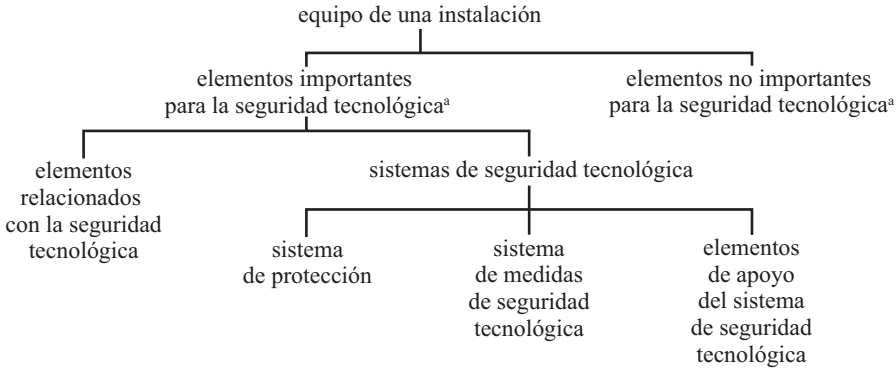
A continuación figura una lista no exhaustiva de los sistemas informáticos que pueden encontrarse en las instalaciones nucleares y que guardan relación con los objetivos de esta orientación. Se clasifican por separado según su importancia para la seguridad tecnológica y para la seguridad física. Ambas clasificaciones deberían tenerse en cuenta al definir el nivel adecuado de seguridad física que se aplicará (sección 5.5) y en el análisis de la evaluación del riesgo (sección 6.2).

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

Cabe señalar igualmente que algunas funciones se solapan claramente en el caso tanto de la seguridad tecnológica como de la física.

5.4.1. Importancia para la seguridad tecnológica

En las normas de seguridad del OIEA (p.ej., refs. [13–15]) el equipo de una instalación nuclear se clasifica según su función, como se muestra en la figura 4.



[a] En este contexto, un "elemento" es una estructura, un sistema o un componente.

Fig. 4. Equipo de una instalación según la función de seguridad tecnológica

Sistemas relacionados con el equipo de una instalación

— Sistemas importantes para la seguridad tecnológica

• Sistemas de seguridad tecnológica

— Sistemas de protección: sistemas de instrumentación y control (I y C) que se usan para las medidas de protección del reactor y la central activadas automáticamente.
— Sistemas de medidas de seguridad tecnológica: sistemas de I y C que ejecutan medidas de seguridad tecnológica, activadas por los sistemas de protección y manualmente.
— Elementos de apoyo del sistema de seguridad tecnológica: I y C para los sistemas de suministro eléctrico de emergencia.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

- Sistemas relacionados con la seguridad tecnológica

  — Sistemas de control del proceso: Sistemas de I y C para el control de la central.
  — I y C de la sala de control, incluidos los sistemas de alarma.
  — Sistemas informáticos de procesos que recopilan y preparan información para la sala de control.
  — Sistemas de I y C para la manipulación y el almacenamiento del combustible.
  — Sistemas de protección contra incendios.
  — Sistemas de control del acceso.
  — Infraestructura de comunicación de datos y por voz.

— Sistemas no importantes para la seguridad tecnológica

- Sistemas de control de funciones no importantes para la seguridad tecnológica (p.j., la desmineralización)

También se deberían tener en cuenta los sistemas informáticos que no necesariamente están relacionados con el equipo de una instalación pero que pueden tener, no obstante, un impacto en la seguridad tecnológica.

Sistemas no relacionados con el equipo de una instalación

— Ofimática

- Sistemas de autorización y orden de trabajo: sistemas que permiten coordinar las actividades laborales a fin de crear un entorno de trabajo adecuado.
- Sistemas de ingeniería y mantenimiento: sistemas que se ocupan de los detalles relacionados con la explotación, el mantenimiento y el apoyo técnico de la central.
- Sistemas de gestión de la configuración: sistemas destinados al seguimiento de la configuración de la central, incluidos los modelos, las versiones y las piezas instaladas en la instalación nuclear.
- Sistemas de gestión de documentos: sistemas utilizados para almacenar y recuperar información sobre la central, como planos o actas de reuniones.
- Intranet: sistema que permite acceder a toda la documentación de la central, tanto técnica como administrativa, al personal autorizado. Normalmente ese acceso es de lectura únicamente.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

— Conectividad externa

- Correo electrónico: sistema que se utiliza para transmitir información a partes externas.
- Sitio web público: sistema que se utiliza para facilitar información sobre la instalación a los usuarios de Internet.
- Acceso remoto/acceso de terceros: sistemas que permiten el acceso desde el exterior, controlado estrictamente, a ciertas funciones internas de un emplazamiento.

5.4.2. Sistemas de seguridad física o sistemas conexos

En el caso de los sistemas de seguridad física aún no existe una clasificación comparable a la establecida para los sistemas de seguridad tecnológica. Sin embargo, la clasificación de ese tipo sistemas de la instalación debería ser una parte importante del análisis de los activos. La lista siguiente podría ser de ayuda para dicha clasificación:

— Sistemas de control del acceso físico: sistemas utilizados para garantizar que solo las personas autorizadas accedan a las zonas de un emplazamiento sobre la base de la función que desempeñen;
— Infraestructura de comunicación de datos y por voz;
— Base de datos de autorizaciones en relación con la seguridad: sirve para asegurar que las personas tengan la autorización apropiada para acceder a una zona del emplazamiento o a información que se conserva en su interior;
— Sistemas de vigilancia y control de alarmas de seguridad: se utilizan para controlar todas las alarmas de seguridad del emplazamiento y ayudar a evaluarlas;
— Componentes de seguridad de las computadoras y la red;
— Sistemas de contabilidad y control nucleares.

5.5. ENFOQUE GRADUADO A LA SEGURIDAD INFORMÁTICA

La seguridad de los sistemas informáticos debería basarse en un enfoque graduado, consistente en aplicar medidas de seguridad proporcionales a las posibles consecuencias de un ataque. Una forma práctica de aplicar ese enfoque es clasificar los sistemas informáticos por *zonas* y aplicar principios de protección graduada a cada zona según el *nivel* de seguridad requerido en ella. La clasificación de los sistemas informáticos en distintos niveles y zonas debería realizarse en función de su importancia para la seguridad tecnológica y física

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

(véase la sección 5.4). No obstante, **convendría que el proceso de evaluación del riesgo pudiera incorporarse e influir en el enfoque graduado**.

5.5.1. Niveles de seguridad

Los niveles de seguridad son una abstracción que define el grado de protección requerido por los diversos sistemas informáticos de una instalación. En cada nivel del enfoque graduado se requerirá diferentes medidas protectoras para poder satisfacer los requisitos de seguridad pertinentes. Algunas medidas protectoras se aplican a todos los sistemas informáticos en todos los niveles, mientras que otras son propias de determinado(s) nivel(es).

El modelo de niveles de seguridad facilita la asignación de medidas protectoras a varios sistemas informáticos en función de la clasificación del sistema (asignándolo a un nivel) y la definición del conjunto de medidas protectoras apropiadas para ese nivel.

Los niveles y las medidas protectoras correspondientes deberían documentarse adecuadamente en el CSP.

5.5.2. Zonas

Las zonas son un concepto lógico y físico para agrupar los sistemas informáticos con fines de administración, comunicación y aplicación de medidas protectoras. El modelo de zonas permite agrupar las computadoras de igual o similar importancia para la explotación de la central en condiciones de seguridad tecnológica y física a los efectos de la administración y aplicación de medidas protectoras.

El empleo de un modelo de zonas debería ajustarse a las directrices siguientes:

— cada zona comprende sistemas cuya importancia para la seguridad física y tecnológica de la instalación es igual o comparable;
— los sistemas pertenecientes a una misma zona requieren medidas protectoras similares;
— los distintos sistemas informáticos de una zona crean un espacio fiable de comunicación interna dentro de esa zona;
— en los límites de una zona se requieren mecanismos de separación respecto del flujo de datos sobre la base de las políticas específicas de cada zona;
— las zonas pueden dividirse en subzonas para mejorar la configuración.

Dado que las zonas constan de sistemas de importancia igual o comparable para la seguridad tecnológica y física de la instalación, cada una puede ser

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

asignada a un nivel, el cual indica las medidas protectoras aplicables a todos los sistemas informáticos de esa zona. Sin embargo, la relación entre las zonas y los niveles no es unívoca; un nivel puede tener asignadas múltiples zonas cuando todas ellas requieren el mismo grado de protección. Las zonas son agrupaciones lógicas y físicas de sistemas informáticos, mientras que los niveles representan el grado de protección necesario.

El modelo de zonas debería documentarse adecuadamente en el CSP, con una descripción general de todos los sistemas informáticos, todas las líneas de comunicación pertinentes, todos los cruces entre zonas y todas las conexiones externas.

5.5.3. Ejemplo de la aplicación de un modelo de niveles de seguridad

A continuación se presenta un ejemplo de las medidas de seguridad aplicadas a distintos niveles. Se trata simplemente de una de las posibles aplicaciones del enfoque graduado; la elección exacta de los niveles y sus respectivas medidas de seguridad debería ajustarse al entorno considerado, las características específicas de la instalación y el análisis específico de los riesgos para la seguridad.

En este caso:

— Las medidas genéricas deberían aplicarse a todos los sistemas informáticos.
— Los niveles de seguridad abarcan desde el nivel 5 (protección mínima requerida) hasta el nivel 1 (protección máxima requerida), como se muestra en la figura 5.
— Las medidas correspondientes a los distintos niveles no son acumulativas (por lo que pueden repetirse).

Nivel genérico

Las siguientes medidas genéricas deberían aplicarse a los sistemas y los niveles correspondientes:

— se definen políticas y prácticas para cada nivel.
— se redactan procedimientos operacionales de seguridad física y todos los usuarios los leen.
— el personal con autorización para acceder al sistema debe contar con las cualificaciones y experiencia adecuadas, así como con la autorización de seguridad necesaria.
— los usuarios obtienen acceso solamente a las funciones de los sistemas que necesitan para llevar a cabo sus tareas.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

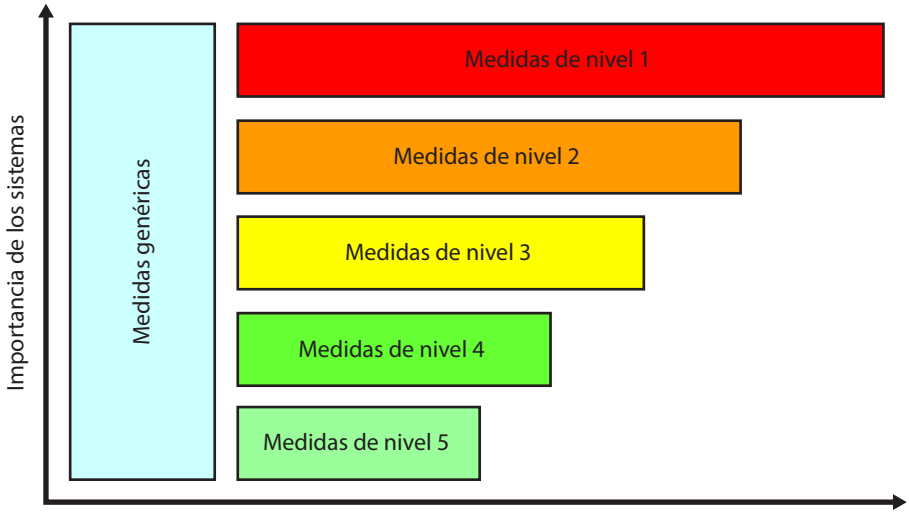


Fig. 5. Nivel de seguridad/alcance de las medidas.

— existen mecanismos apropiados para el control del acceso y la autentificación del usuario.
— existen sistemas o procedimientos de detección de anomalías.
— se supervisan las vulnerabilidades de las aplicaciones y los sistemas, y se adoptan las medidas apropiadas.
— periódicamente se realizan evaluaciones de las vulnerabilidades de los sistemas.
— los medios removibles deberían controlarse con arreglo a los procedimientos operacionales de seguridad física.
— los componentes de seguridad de las computadoras y la red deberían someterse a medidas de mantenimiento estrictas.
— los componentes de seguridad de las computadoras y la red (como servicios de acceso de seguridad, sistemas de detección de intrusiones, sistemas de prevención de intrusiones y servidores de red privada virtual [VPN][1]) son objeto de estrictas medidas de registro y supervisión.
— existen procedimientos apropiados en materia de copias de seguridad y recuperación de datos.

[1] Una red privada virtual (VPN) es una red creada con medios de comunicación públicos para conectar nodos, dotada de mecanismos de criptografía y otros instrumentos de seguridad que permiten garantizar que solo los usuarios autorizados puedan acceder a ella e impedir que los datos sean interceptados.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

— el acceso físico a los componentes y sistemas es restringido y depende de las funciones de estos.

Nivel 1

Además de las medidas genéricas, las medidas protectoras de nivel 1 deberían aplicarse en el caso de sistemas tales como los de protección, que son vitales para la instalación y requieren el nivel más elevado de seguridad. Se podría tratar, entre otras, de las siguientes medidas:

— no debería autorizarse la entrada en sistemas del nivel 1 de ningún tipo de flujo de datos en red (por ejemplo, acuse de recibo, señalización) procedentes de sistemas clasificados en niveles de seguridad menores. Solo deberían permitirse las comunicaciones hacia el exterior. Cabe señalar que esta comunicación en un solo sentido no garantiza intrínsecamente la fiabilidad e integridad (cabría tener en cuenta las redundancias/correcciones de errores). Cabe señalar también que esto excluye cualquier tipo de protocolos de intercambio (entre ellos el TCP/IP[2]), incluso con instrucciones de conexión controladas. se recomienda firmemente no hacer excepciones, pero si se hacen, convendría estudiar cada caso y refrendarlo con una justificación completa y un análisis de los riesgos para la seguridad.[3]
— las medidas destinadas a garantizar la integridad y disponibilidad de los sistemas forma parte normalmente de justificación de la seguridad tecnológica.
— no se permite el acceso remoto con fines de mantenimiento.
— el acceso físico a los sistemas está estrictamente controlado.
— el número de personas con acceso a los sistemas se mantiene en un mínimo absoluto.
— toda modificación aprobada de los sistemas informáticos está sujeta a la regla de la actuación por pareja.
— todas las actividades deberían registrarse y supervisarse.
— todos los datos introducidos en los sistemas son aprobados y verificados caso por caso.

[2] Protocolo de control de transmisión/protocolo de Internet — protocolos de transmisión de datos.

[3] Algunos Estados Miembros son de la firme opinión de que no debería hacerse excepción alguna.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

— todas las modificaciones, comprendidos el mantenimiento de equipo informático, las actualizaciones y las modificaciones de programas informáticos, se someten a estrictos procedimientos organizativos y administrativos.

Nivel 2

Además de las medidas genéricas, las medidas protectoras de nivel 2 deberían aplicarse en el caso de sistemas tales como los de control operacional, que requieren un nivel elevado de seguridad. Se podría tratar, entre otras, de las siguientes medidas:

— entre los sistemas de nivel 2 y los de nivel 3 solo es posible mantener un flujo de datos en red en una dirección, a saber, hacia el exterior. Solo los mensajes de acuse de recibo necesarios o los mensajes de señales controlados se pueden aceptar en la dirección opuesta (hacia el interior) (p.ej., en relación con el TCP/IP).
— el acceso para mantenimiento a distancia podría permitirse según cada caso y durante un período de trabajo definido. En los casos en que se autorice ese acceso, deberán adoptarse medidas protectoras estrictas y los usuarios deberán respetar una política de seguridad definida (por contrato).
— el número de personas a las que se otorgará acceso a los sistemas se mantendrá al mínimo y se hará una clara distinción entre los usuarios y el personal administrativo.
— las conexiones físicas a los sistemas deberían controlarse estrictamente.
— se han adoptado todas las medidas razonables para garantizar la integridad y disponibilidad de los sistemas.
— la evaluación de las vulnerabilidades relacionadas con las acciones en los sistemas podría generar inestabilidad en la central o en los procesos, por lo que solamente debería efectuarse utilizando bancos de prueba, sistemas no esenciales y durante las pruebas de aceptación en fábrica o durante paradas prolongadas previstas.

Nivel 3

Además de las medidas genéricas, las medidas protectoras de nivel 3 deberían aplicarse en el caso de los sistemas de supervisión en tiempo real no necesarios para las operaciones, tales como los sistemas de supervisión de procesos en tiempo real de una sala de control, clasificados en el nivel medio por las diversas amenazas cibernéticas que enfrentan. Se podría tratar, entre otras, de las siguientes medidas protectoras:

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

— el acceso a Internet desde sistemas de nivel 3 no está permitido.
— el registro y las pistas de auditoría de los recursos clave se encuentran bajo supervisión.
— se establecen servicios de acceso de seguridad para proteger los sistemas de este nivel del tráfico no controlado desde los sistemas de nivel 4 y para permitir únicamente un número limitado de actividades específicas.
— deberían controlarse las conexiones físicas a los sistemas.
— el acceso con fines de mantenimiento a distancia solo está autorizado en ciertos casos, a condición de que se controle estrictamente; la computadora remota y su usuario deben respetar una política de seguridad definida y especificada por contrato.
— las funciones de los sistemas a disposición de los usuarios se controlan mediante mecanismos de control del acceso y en función de las necesidades. Toda excepción a este respecto tendrá que analizarse minuciosamente, pero convendría recurrir a otras medidas de protección (como el acceso físico).

Nivel 4

Además de las medidas genéricas, las medidas de nivel 4 deberían aplicarse en el caso de los sistemas de gestión de datos técnicos empleados para las actividades de mantenimiento o de gestión de las operaciones relacionadas con los componentes o sistemas requeridos por las especificaciones técnicas de las operaciones (p.ej., permiso de trabajo, orden de trabajo, etiquetado, gestión de documentación), clasificados en el nivel moderado por las diversas amenazas cibernéticas que enfrentan. Entre las medidas de nivel 4 se incluyen las siguientes:

— solo los usuarios aprobados y cualificados están autorizados a efectuar modificaciones en los sistemas.
— se puede otorgar a los usuarios acceso a Internet desde los sistemas de nivel 4 a condición de que se apliquen medidas protectoras adecuadas.
— se establecen servicios de acceso de seguridad para proteger los sistemas de este nivel del tráfico no controlado desde redes externas de una empresa o instalación y para permitir que se realicen determinadas actividades que están controladas.
— deberían controlarse las conexiones físicas a los sistemas.
— el acceso con fines de mantenimiento a distancia está autorizado y controlado; la computadora remota y su usuario deben respetar una política de seguridad definida, especificada por contrato y controlada.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

— las funciones de los sistemas que están a disposición de los usuarios se controlan mediante mecanismos de control del acceso. Toda excepción a este respecto tendrá que analizarse minuciosamente, pero convendría recurrir a otras medidas de protección.
— el acceso a distancia desde el exterior está autorizado para los usuarios aprobados, siempre que se apliquen los mecanismos de control del acceso apropiados.

Nivel 5

Las medidas de nivel 5 deberían aplicarse en el caso de los sistemas que no tienen importancia directa a efectos del control técnico o el funcionamiento, como los sistemas ofimáticos clasificados en el nivel bajo por las diversas amenazas cibernéticas que enfrentan. Entre las medidas de nivel 5 se incluyen las siguientes:

— solo los usuarios aprobados y cualificados están autorizados a efectuar modificaciones en los sistemas.
— el acceso a Internet desde los sistemas de nivel 5 está autorizado a condición de que se apliquen medidas protectoras adecuadas.
— el acceso a distancia desde el exterior está autorizado para los usuarios aprobados, siempre que se apliquen los controles apropiados.

5.5.4. Separación entre zonas

Los límites entre las zonas requieren mecanismos de separación respecto del flujo de datos a fin de impedir el acceso no autorizado de una zona que no requiere tanta protección a otra que requiere mayor protección, así como y la propagación de errores entre ellas.

Las medidas técnicas y administrativas necesarias para garantizar la separación entre zonas deberán ajustarse a los requisitos específicos de los niveles de protección. No debería existir ninguna interconexión directa entre varias zonas.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

6. AMENAZAS, VULNERABILIDADES Y GESTIÓN DE RIESGOS

En la sección 6.1 se exponen los conceptos básicos que se emplean en el marco de la gestión de riesgos para sistemas informáticos. La gestión de riesgos es importante en todas las fases del ciclo de vida de los sistemas de la instalación, entre ellas las de diseño, desarrollo, funcionamiento y mantenimiento. La sección 6.2 ofrece una visión general de las etapas que debe comprender una metodología amplia de gestión de riesgos, mientras que las secciones 6.3 y 6.4 se centran en las etapas de la metodología en que deben tenerse en cuenta las características específicas de la industria nuclear.

6.1. CONCEPTOS BÁSICOS Y RELACIONES ENTRE ELLOS

En el contexto de la seguridad informática, el riesgo es la posibilidad de que una amenaza determinada aproveche las vulnerabilidades de un activo o grupo de activos y cause así daños a la instalación. Se mide combinando la probabilidad de que se produzca un suceso y la gravedad de sus consecuencias.

La figura 6 es un diagrama que muestra las múltiples interconexiones entre los conceptos de amenaza, vulnerabilidad y riesgo [16].

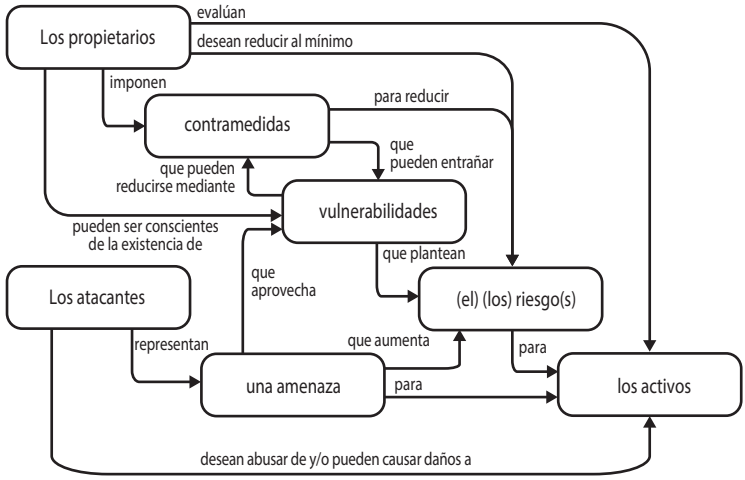


Fig. 6. Conceptos de seguridad física y relaciones entre ellos (adaptada de la norma ISO 13335-1 2004 [16]).

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

6.2. EVALUACIÓN Y GESTIÓN DE RIESGOS

La evaluación de riesgos es una herramienta importante para determinar las esferas a las que conviene dedicar recursos y esfuerzos al tratar la cuestión de las vulnerabilidades y la probabilidad de que se puedan aprovechar.

Se trata de un proceso por el que se definen y documentan determinadas combinaciones de amenazas, vulnerabilidades y repercusiones, y por el que se crean controles de protección apropiados. La evaluación de las amenazas y vulnerabilidades sirve de base para la elaboración de las contramedidas requeridas para prevenir o mitigar las consecuencias de ataques contra sistemas informáticos.

Entre las etapas básicas de una metodología de evaluación y gestión de riesgos figuran:

— la definición del perímetro y del contexto;
— la determinación y caracterización de las amenazas;
— la evaluación de las vulnerabilidades;
— la elaboración de escenarios de ataque;
— el análisis de las probabilidades de que se puedan aprovechar con éxito las vulnerabilidades;
— la evaluación del nivel de riesgo; y
— la definición de contramedidas.

A fin de analizar y evaluar los riesgos de forma sistemática y coherente, se debe seguir un proceso bien definido que pueda ajustarse a las normas existentes. En la actualidad, hay numerosas metodologías y herramientas de evaluación o gestión de riesgos plenamente desarrolladas que pueden estructurar ese proceso de manera eficiente y que, por lo tanto, han logrado una amplia aceptación. La mayoría de ellas se basan en conceptos comunes y en la lógica. La norma internacional vigente en la materia es la ISO/IEC 27005 — Information Security Risk Management [4]. En el anexo II se presenta otro ejemplo concreto de metodología. Las autoridades de cada país pueden exigir que se aplique una metodología o política específica de evaluación de riesgos, y las instalaciones pueden tener además las suyas propias.

La Agencia Europea de Seguridad de las Redes y de la Información (ENISA) ha realizado un interesante estudio de los métodos y herramientas de evaluación de riesgos, al que ha dedicado una página web especial [17].

La necesidad de evaluar los sistemas, el alcance de la evaluación y la frecuencia con que se actualizan los análisis de riesgos dependen de la importancia de la función de seguridad tecnológica y física de cada sistema. Además, debe considerarse la posibilidad de realizar un nuevo análisis o al menos

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

un estudio cuando se produzcan modificaciones en el sistema, por ejemplo, a raíz de la implantación de nuevos equipos, programas informáticos o procedimientos, o de un cambio importante en las competencias del operador. Por lo general, el número de amenazas y vulnerabilidades posibles aumenta cuando los sistemas autónomos pasan a ser sistemas interconectados.

En los casos en que no sea viable realizar un análisis de los riesgos en función de amenazas concretas, se recomienda el uso de mejores prácticas y buenos principios de ingeniería.

6.3. DETERMINACIÓN Y CARACTERIZACIÓN DE LAS AMENAZAS

La figura 7 pone de relieve la tendencia constante a la creciente sofisticación de los ataques y los pocos conocimientos que se necesitan para emprenderlos. Los programas de seguridad informática deberían tratar de mantener un nivel de evaluación que abarque una gama muy amplia de escenarios de ataque posibles.

En los grandes eventos de piratas informáticos se suelen encontrar publicaciones sobre la vulnerabilidad de los sistemas de control del sector industrial. El hecho de que esas publicaciones presentan generalmente una visión desfasada de las competencias e intereses reales más actuales de los piratas

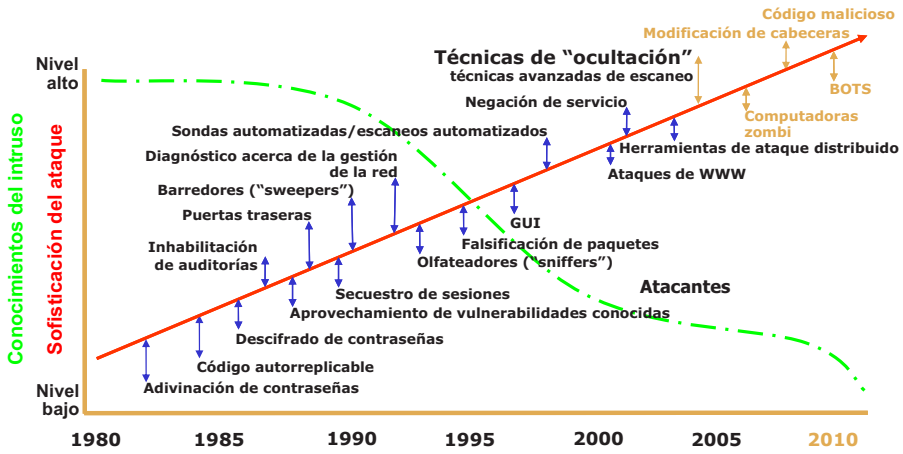


Fig. 7. La complejidad de las amenazas crece a medida que aumenta el número de atacantes.[4]

[4] LIPSON, H.F., Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, Special Report CMS/SEI-2002-SR-009 (2000) 10.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

también debería tenerse en cuenta en las actividades de sensibilización. Además, los grupos de respuesta a emergencias informáticas nacionales han comenzado recientemente a publicar material sobre las vulnerabilidades de los programas informáticos de ICS, lo que ha permitido fomentar su difusión entre la opinión pública y la comunidad de seguridad informática, y centrar la atención en dichas soluciones y deficiencias de los productos.

Así pues, tras determinar el apoyo y los recursos adecuados requeridos, las primeras medidas en el establecimiento de un programa de seguridad informática deberían centrarse en la comprensión de las posibles amenazas, sobre la base de perfiles de atacantes y escenarios de ataque creíbles. En un primer momento, podría crearse una matriz de perfiles de atacantes que comprenda una serie de atacantes, motivaciones y posibles objetivos creíbles. Esta matriz podría utilizarse luego para crear escenarios de ataque verosímiles; en las subsecciones siguientes se examina en mayor detalle este proceso.

6.3.1. Amenaza base de diseño

Una herramienta importante comúnmente utilizada para determinar los niveles de amenaza y como base para establecer las características de la seguridad física es la amenaza base de diseño (ABD). La ABD es una descripción de los atributos y las características de los posibles adversarios (internos y/o externos). La ABD se deriva de información de inteligencia creíble, pero no pretende ser una descripción de las amenazas que imperan en la vida real. Basada en el entorno de amenazas del momento, la ABD representa la mayor amenaza razonable contra la que una instalación debería prever mecanismos de defensa. Los Estados utilizan las ABD en sus sistemas de reglamentación para determinar una asignación adecuada de recursos a la protección de los materiales y las instalaciones nucleares contra acciones hostiles. (Para más información sobre la ABD, véase la ref. [18].)

Convendría estudiar la posibilidad de incorporar en esos escenarios amenazas de ataques aislados con/contra sistemas informáticos o amenazas de ataques coordinados que entrañen el uso de sistemas informáticos.

6.3.2. Perfiles de atacantes

En los cuadros 1 y 2 se ilustra un conjunto de posibles perfiles de atacantes. El cuadro 1 se centra en las amenazas internas/de agentes internos (véase también la ref. [19] en relación con la amenaza de agentes internos), mientras que en el cuadro 2 se determinan algunas amenazas externas posibles. Los cuadros vinculan los tipos generales de atacantes a los recursos de que disponen, la duración de los ataques, las herramientas que probablemente utilizan y las

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

motivaciones de los atacantes. Los perfiles deben adaptarse a cada instalación. Por lo tanto, se requiere un proceso adecuado de recopilación de información de inteligencia para garantizar la exhaustividad y pertinencia de la matriz de atacantes.

6.3.3. Escenarios de ataque

Al crear escenarios de ataque, se pueden barajar diversas posibilidades. La instalación nuclear puede ser atacada con el objetivo de:

— preparar por etapas un ataque coordinado que se perpetrará posteriormente para sabotear la central y/o retirar material nuclear;
— poner en peligro la seguridad de las personas o del medio ambiente;
— emprender un ataque contra otra instalación;
— sembrar confusión y miedo;
— obtener un beneficio económico para un grupo de delincuentes;
— generar inestabilidades importantes en el mercado y beneficios para determinados agentes del mercado.

En función de los objetivos o propósitos de los ataques, los atacantes intentarán aprovechar las distintas vulnerabilidades de los sistemas. Estos ataques pueden conducir a:

— el acceso no autorizado a información (pérdida de confidencialidad);
— la interceptación y modificación de información, programas o equipo informáticos, etc. (pérdida de integridad);
— el bloqueo de las líneas de transmisión de datos y/o la parada de los sistemas (pérdida de disponibilidad);
— la intrusión no autorizada en los sistemas de comunicación de datos o las computadoras (pérdida de fiabilidad).

Todos estos aspectos pueden tener consecuencias y repercusiones importantes en el funcionamiento de los sistemas informáticos, lo que puede comprometer directa o indirectamente la seguridad tecnológica y física de la instalación. Al crear escenarios de ataque, habría que tener en cuenta las tendencias tecnológicas y la facilidad de acceso a las tecnologías de ataque. En el anexo I se exponen algunos escenarios de ataques ficticios pero realistas, a una instalación nuclear.

CUADRO 1. AMENAZAS INTERNAS

Atacante	Recursos	Duración	Herramientas	Motivación
Agente infiltrado	"Ingeniería social" facilitada. Acceso a los sistemas a cierto nivel. Documentación y conocimientos especializados disponibles sobre los sistemas.	Variable, pero generalmente no puede dedicar muchas horas.	Acceso existente, conocimiento de la programación y la arquitectura de los sistemas: — Posible conocimiento de contraseñas existentes; — Posibilidad de introducir puertas traseras y/o troyanos creados con fines específicos; — Posible apoyo de expertos externos.	Robo de información interna, secretos de tecnología o información personal. Beneficio económico (venta de información a la competencia). Chantaje.
Empleado/usuario descontento	Recursos medios/importantes. Acceso a los sistemas a cierto nivel. Documentación sobre los sistemas y conocimientos especializados disponibles sobre determinados sistemas internos y operacionales.	Variable, pero generalmente no puede dedicar muchas horas.	Acceso existente, conocimiento de la programación y la arquitectura de los sistemas. Posible conocimiento de contraseñas existentes. Capacidad para introducir herramientas o *scripts* no profesionales (a veces más elaborados si el empleado/usuario descontento posee conocimientos informáticos específicos).	Venganza, perturbación, caos. Robo de información interna. Poner en situación embarazosa al empleador/a otro empleado. Degradar la imagen pública o minar la confianza del público.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

CUADRO 2. AMENAZAS EXTERNAS

Atacante	Recursos	Duración	Herramientas	Motivación
Pirata informático aficionado	Aptitudes diversas, pero generalmente limitadas. Aparte de la información pública, poco conocimiento de los sistemas.	Mucho tiempo, no tiene mucha paciencia.	*Scripts* y herramientas generalmente disponibles. Posibilidad de desarrollar sus propias herramientas.	Diversión, prestigio. Objetivo de oportunidad. Aprovechamiento de las vulnerabilidades que estén "al alcance de la mano".
Opositor activo a la energía nucleoeléctrica	Recursos limitados, pero puede recibir apoyo financiero por conductos secretos. Acceso a herramientas de la comunidad cibernética. Aparte de la información pública, poco conocimiento de los sistemas.	Los objetivos de los ataques pueden ser determinados eventos de los que ya se tenía conocimiento (p.ej. celebraciones, elecciones). Mucho tiempo, paciencia y motivación.	Conocimientos informáticos disponibles. Posible apoyo de la comunidad de piratas informáticos. "Ingeniería social".	Convicción de salvar el mundo. Influencia en la opinión pública sobre determinadas cuestiones. Obstaculización de operaciones internas.
Antiguo empleado/ usuario descontento	Recursos limitados si no forma parte de un grupo más grande. Puede poseer aún documentación sobre los sistemas. Puede utilizar una antigua vía de acceso no administrada. Posibles vínculos con personal de la instalación.	Variable y según el grupo al que el atacante esté asociado.	Posible conocimiento de contraseñas existentes. Puede utilizar una antigua vía de acceso no administrada. Puede haber creado puertas traseras de acceso a los sistemas cuando todavía era empleado. "Ingeniería social".	Venganza, perturbación, caos. Robo de información interna. Poner en situación embarazosa al empleador/a otro empleado. Degradar la imagen pública o minar la confianza del público.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

CUADRO 2. AMENAZAS EXTERNAS (cont.)

Atacante	Recursos	Duración	Herramientas	Motivación
Delincuencia organizada	Recursos importantes. Empleo de conocimientos cibernéticos especializados.	Variable, pero casi siempre de corta duración.	*Scripts*, herramientas propias. Puede contratar a un "pirata informático a sueldo". Puede contratar a un antiguo empleado/un empleado en funciones. "Ingeniería social".	Chantaje. Robo de material nuclear. Extorsión (beneficio económico). Aprovechamiento de los temores del sector en el plano financiero y de la imagen. Venta de información (técnica, interna o personal).
Estado nación	Recursos importantes y conocimientos especializados. Actividades de recopilación de información de inteligencia. Posible capacitación/experiencia operacional en relación con los sistemas.	Variable.	Grupos de expertos en cibernética capacitados. Herramientas sofisticadas. Puede contratar a un antiguo empleado/un empleado en funciones. "Ingeniería social".	Recopilación de información de inteligencia. Creación de puntos de acceso para acciones futuras. Robo de tecnología.
Terrorista	Aptitudes diversas. Posible capacitación/experiencia operacional en relación con los sistemas.	Mucho tiempo, mucha paciencia.	*Scripts*, herramientas propias. Puede contratar a un "pirata informático a sueldo". Puede contratar a un antiguo empleado/un empleado en funciones. "Ingeniería social".	Recopilación de información de inteligencia. Creación de puntos de acceso para acciones futuras. Caos. Venganza. Impacto en la opinión pública (miedo).

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

6.4. RESULTADOS SIMPLIFICADOS DE LA EVALUACIÓN DE RIESGOS

En el cuadro 3 se ofrecen, a título ilustrativo únicamente, ejemplos de los sistemas que pueden encontrarse en una instalación nuclear. También se determina el posible impacto del éxito de un ataque en dichos sistemas, así como el correspondiente impacto en la instalación, y se presentan ejemplos genéricos de contramedidas apropiadas.

CUADRO 3. SISTEMAS TÍPICOS DE LAS INSTALACIONES NUCLEARES

Sistema	Impacto en la seguridad informática	Posible impacto en la instalación	Contramedidas propuestas
Sistema de protección del reactor	Pérdida de integridad de los programas informáticos/datos críticos para la seguridad tecnológica. Pérdida de disponibilidad de la función.	CRÍTICO Seguridad tecnológica de la central, comprometida; emisión radiactiva.	Medidas de seguridad física de nivel 1
Sistema de control de procesos	Pérdida de integridad de los programas informáticos/datos de control. Pérdida de disponibilidad de la función.	GRANDE Funcionamiento de la central comprometido.	Medidas de seguridad física de nivel 2
Sistema de autorización y orden de trabajo	Pérdida de integridad de los datos y de disponibilidad del sistema.	MEDIO Actuación errónea con respecto a los componentes. Alteraciones en el funcionamiento y mantenimiento normales.	Medidas de seguridad física de nivel 4

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

CUADRO 3. SISTEMAS TÍPICOS DE LAS INSTALACIONES NUCLEARES

Sistema	Impacto en la seguridad informática	Posible impacto en la instalación	Contramedidas propuestas
Sistema de control del acceso físico	Pérdida de disponibilidad y de integridad de los sistemas de acceso al emplazamiento. Pérdida de confidencialidad de los datos de acceso al emplazamiento.	GRANDE Acceso otorgado a personas no autorizadas. Las personas autorizadas no pueden tener acceso a las zonas requeridas.	Medidas de seguridad física de nivel 2
Sistema de gestión de documentos	Pérdida de confidencialidad, disponibilidad e integridad de los datos.	MEDIO Información utilizada para planificar ataques más graves.	Medidas de seguridad física de nivel 4
Correo electrónico	Pérdida de confidencialidad, de integridad y de disponibilidad.	REDUCIDO Cargas administrativas. Las operaciones cotidianas son más difíciles.	Medidas de seguridad física de nivel 5

La noción de probabilidad, fundamental para la evaluación de riesgos, no se tiene en cuenta en este cuadro. La probabilidad de éxito de los ataques, así como sus posibles consecuencias, dependen del contexto y la instalación que se tomen en consideración. Además, debería realizarse una evaluación más minuciosa de los requisitos de confidencialidad, integridad y disponibilidad respecto de cada sistema que se tenga en cuenta en la evaluación de riesgos.

7. CONSIDERACIONES ESPECIALES RELATIVAS A LAS INSTALACIONES NUCLEARES

Dado el carácter singular de la industria nuclear, la seguridad informática en el caso de las instalaciones nucleares debe abordar problemas que se añaden a los

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

que se plantean en el caso de las redes de TI de empresas o incluso en el de sistemas de control de procesos similares ajenos al sector nuclear. En las secciones siguientes se describen algunos de los problemas inherentes al sector nuclear.

7.1. FASES DE LA VIDA ÚTIL Y MODALIDADES DE FUNCIONAMIENTO DE UNA INSTALACIÓN

Las instalaciones nucleares presentan una amplia gama de diseños y características operacionales. Las fases de la vida útil de estas instalaciones y sus modalidades de funcionamiento son múltiples, e incluyen:

— El diseño, la construcción y la puesta en servicio.
— El funcionamiento normal:
  • Funcionamiento en régimen de potencia;
  • Puesta en marcha de la central;
  • Parada en caliente;
  • Parada en frío;
  • Recarga de combustible y mantenimiento.
— La clausura.

Estas fases de la vida útil y modalidades de funcionamiento múltiples pueden requerir distintos sistemas y entornos operacionales. Por ejemplo, los períodos de mantenimiento intenso suelen entrañar la sustitución, la modificación y el ensayo de equipo, o pueden requerir la contratación de personal suplementario y el acceso de terceros/subcontratistas. Esta diversidad se debería tener en cuenta en el CSP. En particular, la diversidad de fases de la vida útil podría exigir revisiones exhaustivas del CSP.

7.2. DIFERENCIAS ENTRE LOS SISTEMAS DE TI Y LOS SISTEMAS DE CONTROL INDUSTRIAL

Los sistemas informáticos y las arquitecturas de red de apoyo a las operaciones de las centrales nucleares no son sistemas informáticos normalizados desde el punto de vista de los requisitos de arquitectura, configuración o comportamiento. Estos sistemas pueden clasificarse como sistemas de control industrial (ICS) especializados. Pese a que los ICS han pasado de las aplicaciones estrictamente protegidas por derechos de propiedad a arquitecturas informáticas

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

más generalizadas, siguen existiendo marcadas diferencias entre los ICS y los sistemas de TI normalizados que se han de tener en cuenta en cualquier CSP.

En el cuadro 4, basado en un documento del NIST [20], se exponen las principales diferencias entre los ICS y los sistemas de TI clásicos.

CUADRO 4. DIFERENCIAS ENTRE LOS SISTEMAS DE TI Y LOS ICS [20]

Categoría	**Sistema de tecnología de la información**	**Sistema de control industrial**
Requisitos de comportamiento	Tiempo no real La respuesta debe ser coherente Se exige un rendimiento específico elevado Una gran demora y fluctuación pueden ser aceptables	Tiempo real El factor temporal de la respuesta es crucial Un rendimiento específico modesto es aceptable Una gran demora y/o fluctuación es un problema grave
Requisitos de disponibilidad	Respuestas como la reinicialización son aceptables Dependiendo de los requisitos operacionales del sistema, a menudo se pueden tolerar deficiencias en la disponibilidad	Respuestas como la reinicialización pueden no ser aceptables en vista de los requisitos de disponibilidad de los procesos Las paradas deben planificarse y programarse con días/semanas de antelación Para lograr una alta disponibilidad de los sistemas, se requieren ensayos exhaustivos previos a su utilización
Requisitos de gestión de riesgos	La confidencialidad e integridad de los datos son vitales La tolerancia a los fallos es menos importante; los tiempos de inactividad pasajeros no entrañan un gran riesgo El principal impacto en este contexto sería una demora de las operaciones internas	La seguridad de las personas es primordial, seguida de la protección del proceso La tolerancia a los fallos es esencial; ni siquiera los tiempos de inactividad pasajeros son aceptables El principal impacto en este contexto sería el incumplimiento de disposiciones reglamentarias, la pérdida de vidas, de equipo o de productividad
Atención centrada en la seguridad de la arquitectura	La atención se centra principalmente en la protección de los activos de TI y la información que se almacena en ellos o se transmite entre ellos El servidor central podría requerir más protección	El objetivo primordial es proteger los clientes periféricos (p.ej., dispositivos de campo como controladores de proceso) La protección del servidor central sigue siendo importante
Consecuencias imprevistas	Las soluciones de seguridad se conciben en torno a los sistemas de TI típicos	Los instrumentos de seguridad deben someterse a prueba para asegurar que no pongan en peligro el funcionamiento normal del ICS
Crítica con respecto al tiempo	Interacción menos crítica en caso de emergencia Puede aplicarse, en la medida necesaria, un control del acceso muy restringido	La respuesta a las interacciones humanas y de otra índole en caso de emergencias es crítica El acceso al ICS, aunque debería estar estrictamente controlado, no debería obstaculizar la interacción hombre-máquina

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

CUADRO 4. DIFERENCIAS ENTRE LOS SISTEMAS DE TI Y LOS ICS [20] (cont.)

Categoría	Sistema de tecnología de la información	Sistema de control industrial
Funcionamiento del sistema	Los sistemas están diseñados para ser utilizados con sistemas operativos típicos Las actualizaciones se realizan fácilmente gracias a instrumentos de instalación automatizada	Sistemas operativos diferentes y personalizados, a menudo sin capacidades de seguridad Las modificaciones de programas informáticos deben ser efectuadas con cuidado, normalmente por los proveedores de programas informáticos, debido a los algoritmos de control especializados y quizá a los programas y equipo informáticos de que se trate
Limitaciones de recursos	Los sistemas cuentan con recursos específicos suficientes para apoyar la introducción de aplicaciones de terceros, tales como soluciones de seguridad	Los sistemas están diseñados para apoyar el proceso industrial previsto; la memoria y los recursos informáticos destinados a apoyar la introducción de una tecnología de seguridad son muy reducidos
Comunicaciones	Protocolos de comunicación normalizados Principalmente redes cableadas con algunas capacidades inalámbricas localizadas Prácticas típicas de creación de redes de TI	Numerosos protocolos de comunicación protegidos por derechos de propiedad y normalizados Varios tipos de medios de comunicación utilizados, en particular redes cableadas e inalámbricas (radio y satélite) Las redes son complejas y a veces requieren los conocimientos especializados de ingenieros de control de procesor
Gestión de los cambios	Los cambios de programas informáticos se efectúan de manera oportuna siguiendo buenas políticas y procedimientos de seguridad. Suele tratarse de procedimientos automatizados.	Los nuevos programas informáticos deben ser objeto de ensayos exhaustivos y utilizarse progresivamente en todo el sistema para asegurar que se mantenga la integridad del sistema de control. A menudo, las paradas del ICS deben planificarse y programarse con días/semanas de antelación.
Apoyo controlado	Tiene en cuenta diversos tipos de apoyo	Los servicios de apoyo suelen prestarse por intermedio de un solo proveedor
Vida útil de los componentes	Vida útil del orden de 3 a 5 años	Vida útil del orden de 15 a 20 años
Acceso a los componentes	Normalmente, los componentes se encuentran en un lugar de acceso fácil	Los componentes pueden estar aislados y en lugares remotos, y puede que sea necesario realizar un gran esfuerzo físico para acceder a ellos

7.3. DEMANDA DE CONECTIVIDAD ADICIONAL Y CONSECUENCIAS CONEXAS

Un motivo de preocupación cada vez mayor con respecto a los ICS es el creciente deseo de establecer interconectividad entre los sistemas de empresas y de ingeniería y los sistemas operativos. Habida cuenta del deseo de las sedes de las empresas, los planificadores y los ingenieros de acceder en tiempo real a los

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

datos de una central, se están creando puentes entre las redes de control bien delimitadas que manejan la central y las redes de datos sin límites utilizadas para facilitar el acceso corporativo. Esos puentes pueden constituir un medio de intrusión en las redes.

Otra característica singular desde el punto de vista de la arquitectura es la existencia de centros de operaciones de emergencia situados lejos de la instalación. Estos centros ofrecen una alternativa para las actividades de monitorización y las operaciones de emergencia a distancia relacionadas con la central en caso de que un incidente inutilice la instalación principal. Los requisitos relacionados con la vigilancia/el mantenimiento de algunos elementos del control de la central plantean la necesidad de establecer un flujo de datos por algún medio de comunicación. Este medio podría utilizarse para poner en peligro el sistema principal y acceder a él. Además, la necesidad de duplicar las funciones obliga a mantener requisitos de seguridad homogéneos en dos sistemas. De no mantenerse uno de los sistemas, se abriría una vía para la intrusión y la piratería.

La necesidad de realizar actividades de análisis, mantenimiento o actualizaciones a distancia también puede dar lugar a vulnerabilidades similares. Antes de atender a cualquier demanda de conectividad adicional, debe efectuarse un análisis minucioso de los riesgos.

7.4. CONSIDERACIONES RELATIVAS A LAS ACTUALIZACIONES DE LOS PROGRAMAS INFORMÁTICOS

Muchos de los reglamentos actuales relacionados con la validación o certificación de equipo de las centrales nucleares se han elaborado teniendo en cuenta equipo analógico, que no queda obsoleto rápidamente. En cambio, los planes y las mejores prácticas de seguridad de la TI prevén actualizaciones y correcciones periódicas de los programas informáticos y componentes digitales, ya que estos últimos quedan obsoletos con mayor rapidez.

Por lo tanto, es importante tener en cuenta el problema que plantean las correcciones y actualizaciones de los programas informáticos en los sistemas digitales de control o monitorización nuclear. En el peor de los casos, cada modificación o revisión de un programa informático podría considerarse como un cambio en el sistema y dar lugar a una validación específica del sistema o incluso a la renovación de la certificación de algunos sistemas críticos. Se trata de un proceso engorroso que puede llevar a un retraso en la aplicación de las correcciones o a la decisión deliberada de aplazar la actualización de los programas informáticos. Para limitar esos efectos, debería hacerse una distinción entre las actividades de mantenimiento corriente, que no necesitan esos procesos,

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

y las modificaciones de los sistemas, que requieren certificaciones o ensayos nuevos de los sistemas críticos. En todos los casos, cualquier modificación en los sistemas de seguridad tecnológica o conexos y en los de seguridad física debe efectuarse de conformidad con los procedimientos acordados.

7.5. DISEÑO SEGURO Y ESPECIFICACIONES RELATIVAS A LOS SISTEMAS INFORMÁTICOS

En las etapas iniciales de diseño y desarrollo de muchos de los sistemas e instrumentos actuales de control de procesos y control industrial, no se concedió importancia a la seguridad informática. La tendencia reciente a la conectividad de los sistemas y procesos, la integración de sistemas informáticos comerciales y la proliferación de las actividades informáticas con fines dolosos (como la piratería informática) han impulsado la necesidad de considerar la seguridad informática como uno de los requisitos básicos en la adquisición de equipo nuevo.

En consecuencia, deberían formalizarse los requisitos de seguridad en el contexto de la negociación de contratos con los suministradores. El documento ISO sobre los criterios comunes (ISO 15408) [21] podría servir para formalizar tales requisitos. Otro ejemplo es el esfuerzo de definir un lenguaje de adquisición para sistemas de control [22], del Departamento de Seguridad Interna Nacional de los Estados Unidos, que ha publicado orientaciones y recomendaciones sobre la definición de los requisitos de seguridad cibernética y el establecimiento de un lenguaje específico en materia de adquisiciones de sistemas de control.

7.6. PROCEDIMIENTO PARA EL CONTROL DEL ACCESO DE TERCEROS/PROVEEDORES

Es fundamental tener en cuenta el nivel de seguridad con respecto a terceros y proveedores, por lo que es primordial que el departamento de seguridad colabore estrechamente con el departamento encargado de los contratos, a fin de garantizar que en cada contrato se incorporen las disposiciones relativas a la seguridad.

Las entidades del sector nuclear suelen adjudicar los contratos a entidades externas; algunos de esos contratos prevén que las empresas subcontratistas deben mantener, en sus propios locales, información o activos protegidos. A menos que los procesos de adjudicación y gestión ulterior del contrato se ajusten a normas estrictas, la información y los activos protegidos podrían verse en peligro o ser revelados sin autorización.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

Habida cuenta de todo lo anterior, es importante que el personal directivo responsable de cada instalación/entidad del sector nuclear mantenga una estrecha relación laboral con la empresa subcontratista a fin de garantizar que a lo largo de la elaboración y ejecución del contrato, y en el momento de la entrega final, se aborden los aspectos de seguridad fundamentales.

De estimarse necesario, convendría realizar controles y verificaciones para asegurar que el sistema de gestión de la empresa subcontratista se ocupe adecuadamente de las cuestiones relativas a la seguridad, y que las prácticas y medidas de la entidad estén en conformidad con ese sistema.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

REFERENCIAS

[1] COMISIÓN ELECTROTÉCNICA INTERNACIONAL, Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary, ISO/IEC 27000:2009, ISO, Ginebra (2009).

[2] COMISIÓN ELECTROTÉCNICA INTERNACIONAL, Information Technology — Information Security Management Systems — Requirements, ISO/IEC 27001:2005, ISO, Ginebra (2005).

[3] COMISIÓN ELECTROTÉCNICA INTERNACIONAL, Information Technology — Code of Practice for Information Security Management, ISO/IEC 27002:2005, ISO, Ginebra (2005).

[4] COMISIÓN ELECTROTÉCNICA INTERNACIONAL, Information Technology — Security Techniques — Information Security Risk Management, ISO/IEC 27005:2008, ISO, Ginebra (2008).

[5] COMISIÓN ELECTROTÉCNICA INTERNACIONAL, Information Technology — Security Techniques — Requirements for Bodies Providing Audit and Certification of Information Security Management Systems, ISO/IEC 27006:2007, ISO, Ginebra (2007).

[6] CONSEJO DE EUROPA, Convenio sobre cibercriminalidad, ETS Nº 185, COE, Estrasburgo (2001).

[7] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Sistema de gestión de instalaciones y actividades, Colección de Normas de Seguridad del OIEA Nº GS-R-3, OIEA, Viena (2002).

[8] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Application of the Management System for Facilities and Activities, Colección de Normas de Seguridad del OIEA Nº GS-G-3.1, OIEA, Viena (2006).

[9] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Nuclear Security Culture, Colección de Seguridad Física Nuclear del OIEA Nº 7, OIEA, Viena (2008).

[10] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Objetivos y principios fundamentales en materia de protección física, documento GOV/2001/41, OIEA, Viena (2001).

[11] Protección física de los materiales y las instalaciones nucleares, INFCIRC/225/Rev.4, OIEA, Viena (1999).

[12] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Orientaciones y sugerencias para la aplicación del documento INFCIRC/225/Rev.4, Protección Física de los Materiales y las Instalaciones Nucleares, IAEA-TECDOC-967 (Rev.1), OIEA, Viena (2002).

[13] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, Colección de Normas de Seguridad del OIEA Nº NS-G-1.3, OIEA, Viena (2002).

[14] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Software for Computer Based Systems Important to Safety in Nuclear Power Plants, Colección de Normas de Seguridad del OIEA Nº NS-G-1.1, OIEA, Viena (2000).

[15] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Glosario de Seguridad Tecnológica del OIEA – Terminología empleada en seguridad tecnológica nuclear y protección radiológica, Edición de 2007, OIEA, Viena (2008).

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

[16] COMISIÓN ELECTROTÉCNICA INTERNACIONAL, Information Technology — Security Techniques — Management of Information and Communications Technology Security — Part 1: Concepts and Models for Information and Communications Technology Security Management, ISO/IEC 13335-1:2004, ISO, Ginebra (2004).

[17] AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN, Inventory of Risk Management/Risk Assessment Methods and Tools, http://www.enisa.europa.eu/act/rm/cr/risk-management-inventory/rm-ra-tools.

[18] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Development, Use and Maintenance of the Design Basis Threat, Colección de Seguridad Física Nuclear del OIEA Nº 10, OIEA, Viena (2009).

[19] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Preventive and Protective Measures Against Insider Threats, Colección de Seguridad Física Nuclear del OIEA Nº 8, OIEA, Viena (2008).

[20] STOUFFER, K. A., FALCO, J. A., SCARFONE, K., Guide to Industrial Control Systems (ICS) Security — Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC), Rep. NIST SP-800-82, National Intitute of Standards and Technology, Chicago (2011).

[21] COMISIÓN ELECTROTÉCNICA INTERNACIONAL, Information Technology — Security Techniques — Evaluation Criteria for IT Security, ISO/IEC 15408:2008, ISO, Ginebra (2008).

[22] DEPARTAMENTO DE SEGURIDAD INTERNACIONAL DE LOS ESTADOS UNIDOS, Cyber Security Procurement Language for Control Systems, septiembre (2009), http://www.us-cert.gov/control_systems/pdf/FINAL-Procurement_Language_Rev4_ 100809.pdf

[23] COMISIÓN ELECTROTÉCNICA INTERNACIONAL, Risk Management — Vocabulary, ISO/IEC Guide 73:2009, ISO/IEC, Ginebra (2009).

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

BIBLIOGRAFÍA

INSTITUTO NACIONAL DE NORMALIZACIÓN DE LOS ESTADOS UNIDOS, SOCIEDAD INTERNACIONAL DE AUTOMATIZACIÓN, Security Technologies for Industrial Automation and Control System, ANSI/ISA-TR99.00.01-2007, ANSI, Washington DC, (2007).

MINISTERIO FEDERAL DEL INTERIOR, National Plan for Information Infrastructure Protection, BMI, Berlín (2005).

ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Objetivos y principios fundamentales en materia de protección física, documento GOV/2001/41, OIEA, Viena (2001).

SOCIEDAD INTERNACIONAL DE AUTOMATIZACIÓN, Integrating Electronic Security into the Manufacturing and Control Systems Environment, Instrumentation, Systems and Automation Society, ISA-TR99.00.02-2004, ISA, Research Triangle Park, NC (2004).

INSTITUTO DE SEGURIDAD NUCLEAR DE COREA, Cyber Security of Digital Instrumentation and Control Systems in Nuclear Facilities, KINS/GT-N09-DR, KINS, Seúl (2007).

CENTRO DE COORDINACIÓN DE LA SEGURIDAD DE LA INFRAESTRUCTURA NACIONAL, Good Practice Guide: Process Control and SCADA Security, Version 2.0, NISCC, Noviembre (2006).

INSTITUTO DE ENERGÍA NUCLEAR, Cyber Security Plan for Nuclear Power Reactors, NEI 08-09 (Rev. 5), NEI, Washington DC (2010).

COMISIÓN REGULADORA NUCLEAR, Cyber Security Programs for Nuclear Facilities, Regulatory Guide 5.71, NRC, Rockville, MD (2010).

ORGANIZACIÓN DE COOPERACIÓN Y DESARROLLO ECONÓMICOS, Directrices de la OCDE para la seguridad de sistemas y redes de información: Hacia una cultura de seguridad, OCDE, París (2004).

ORGANIZACIÓN DE COOPERACIÓN Y DESARROLLO ECONÓMICOS, Implementation Plan for the OECD Guidelines for the Security of Information Systems and Network: Towards a Culture of Security, DSTI/ICCP/REG(2003)5/REV1, OCDE, París (2003).

ORGANIZACIÓN DE COOPERACIÓN Y DESARROLLO ECONÓMICOS, The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries, DSTI/ICCP/REG (2005)1/FINAL, OCDE, París (2005).

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

Anexo I

ESCENARIOS DE ATAQUE CONTRA SISTEMAS DE INSTALACIONES NUCLEARES

Como se describe en la sección 6.3, la índole y la forma de los ataques informáticos, contra los que es imprescindible protegerse, pueden variar significativamente. Aunque los ataques pueden adoptar diversas formas, las consecuencias de alto nivel incluyen las siguientes:

— acceso no autorizado a información o la interceptación de datos (pérdida de confidencialidad);
— modificación no autorizada de información, programas o equipo informáticos, etc. (pérdida de integridad);
— bloqueo de las líneas de transmisión de datos o la parada de los sistemas (pérdida de disponibilidad).

Al elaborar las medidas de prevención contra ataques informáticos, es muy importante comprender la índole de los ataques y las posibles vías que pueden usar los atacantes para obtener la información pertinente y el acceso a los sistemas informáticos objetivo. **Los que se indican a continuación son meros ejemplos destinados a alentar a los lectores a que, cuando comprendan mejor las amenazas, reflexionen sobre su organización o sistema y, de ser necesario, corrijan su posición en materia de seguridad física.** Aunque los ataques indicados son ficticios, se refieren a escenarios verosímiles basados en ataques similares perpetrados en otros sectores. Reflexionar sobre ellos es una buena manera de garantizar que el plan de seguridad física aborda la dinámica del cambiante entorno de amenazas.

Un ataque informático bien orquestado consta de varias fases, entre ellas:

— selección del objetivo;
— reconocimiento;
— acceso a los sistemas o vulneración de los mismos;
— ejecución del ataque;
— eliminación de huellas para negar la culpabilidad.

Las subsecciones siguientes describen tres escenarios ficticios de ataques informáticos. El primero de ellos, entre cuyos objetivos está el acopio de información, podría aplicarse como preludio de los otros dos.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

Escenario I — Recopilación de información en apoyo de un acto doloso

Objetivo del ataque — obtener acceso físico a zonas controladas (de acceso limitado) de la instalación en apoyo de ataques posteriores.

Está dirigido contra la persona que administra las tarjetas de acceso y asigna los privilegios de acceso. El acceso físico a zonas restringidas entrañaría un peligro para la computadora del administrador de las tarjetas como para el sistema del código de acceso. El atacante simula ser un subcontratista que va a entregar piezas de equipo.

Entre los posibles objetivos de las actividades de acopio de información en apoyo del ataque figuran:

— información sobre el personal para posibles actos de extorsión o "ingeniería social";
— documentación sobre el diseño del sistema de control del acceso;
— políticas o planes de ingeniería de los sistemas de seguridad física u otras zonas importantes de la central;
— calendarios de las operaciones — horarios de la central, rutinas diarias, quién trabaja, cuándo trabaja, quién está de vacaciones o cuándo se producen ciertos cambios;
— lista de proveedores y cuándo trabajan en el equipo;
— inventario de equipos y piezas;
— contraseñas y medidas de control del acceso;
— medidas administrativas y técnicas de control del acceso;
— información sobre los desarrolladores de programas informáticos y los proyectos en curso;
— arquitectura de la red;
— arquitectura de las telecomunicaciones.

Entre los posibles métodos para recopilar esta información cabe citar:

— "ingeniería social";
— búsquedas en la web con fines de información pública;
— búsquedas en la basura;
— ataque de escaneo, ataque a redes inalámbricas;

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

— ataques por correo electrónico — *phishing*[1] para acceder a la red, programas de captura de teclado;
— instalación de programas informáticos o dispositivos en máquinas anfitrionas mediante discos, memorias USB o CD.
— escuchas para averiguar contraseñas o códigos de acceso (vigilancia manual, de audio o de vídeo).

El ataque puede consistir en:

— obtener un código y una tarjeta (con banda magnética) de acceso;
— robar o duplicar una tarjeta de acceso;
— acceder a la máquina para crear una tarjeta nueva;
— crear una nueva entrada para un empleado;
— asumir la identidad de un empleado cesado recientemente;
— otorgar el nivel de acceso deseado.

Una vez obtenidos la tarjeta y los códigos, el atacante usa la información adquirida sobre la actividad organizativa para entrar en la instalación haciéndose pasar por alguien que entrega piezas de equipo.

Escenario II — Ataque destinado a desactivar o vulnerar uno o varios sistemas informáticos

Objetivo del ataque — sabotear una central nuclear e impedir que se vuelva a poner en funcionamiento de inmediato.

En este ejemplo, durante una parada, un subcontratista realiza ensayos del sistema de control de agua de alimentación. El contratista instala un punto de acceso a distancia para monitorizar y ensayar el sistema desde su oficina. Una vez terminada la tarea, el contratista deja instalado el punto de acceso por error.

El atacante ha recopilado información sobre la central en la que se identifica al subcontratista como antiguo trabajador de la central y principal blanco para obtener la información requerida. Lleva a cabo un ataque de *phishing* por correo electrónico contra la oficina del subcontratista e introduce un programa furtivo (*root kit*) en el sistema, que otorga controles administrativos. Así, el atacante consigue acceder a la red informática de los contratistas y descubre los planes de ensayo de la central y también el puerto de acceso a distancia que no ha sido desactivado.

[1] *Phishing* hace referencia a intentos de adquirir de manera fraudulenta información de carácter estratégico, como nombres de usuarios, contraseñas y datos de tarjetas de crédito, simulándose una entidad fiable en una comunicación electrónica.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

Con esta información, el atacante puede llevar a cabo un ataque de denegación de servicio (*DoS*)[2] contra el sistema de control de agua de alimentación inundando la red de comunicaciones hasta causar un fallo del sistema, diseñado para procesar únicamente una cantidad mínima de comunicaciones.

Cuando el atacante ha obtenido el acceso, analizado la red y detectado el protocolo de comunicaciones, lanza el ataque. Como resultado de ello, el sistema de control de agua de alimentación ya no responde y se produce una parada de emergencia manual de la central. Resulta imposible determinar de inmediato la causa de fallo del sistema de control de agua de alimentación y la central permanece parada para llevar a cabo la investigación.

Escenario III — Vulneración del sistema informático como herramienta para un ataque coordinado

Objetivo del ataque — robo de material nuclear durante su transporte entre dos instalaciones de almacenamiento. Se realizará un ataque informático para modificar el inventario y el sistema de seguimiento a fin de ocultar la pérdida del material robado.

El reconocimiento y la recopilación de información de inteligencia permiten detectar el proceso de marcado y seguimiento de los envíos de material radiactivo entre instalaciones de almacenamiento. Esto incluye las etiquetas RFID[3] colocadas en los distintos artículos en que se describe el componente y se detalla el contenido.

El plan de ataque incluye ayuda desde el interior para retirar el material en ruta. Las fases del ataque comprenden:

— la interceptación del transporte en ruta;
— la retirada de una pequeña cantidad del material radiactivo transportado;
— la reprogramación del chip RFID para que refleje la cantidad real restante;
— la modificación del sistema de seguimiento del inventario para reflejar el transporte de la nueva cantidad e indicar la cantidad robada aún almacenada en la instalación de salida.

El ataque informático se centra en acceder por red a la base de datos del inventario y modificar el registro de inventario y traslado.

[2] La denegación de servicio (DoS) consiste en impedir el acceso autorizado a un recurso del sistema o demorar las operaciones y funciones del sistema.

[3] Identificación por radiofrecuencia: tecnología empleada para la identificación y el seguimiento mediante ondas de radio.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

Anexo II

METODOLOGÍA PARA DETERMINAR LOS REQUISITOS DE SEGURIDAD INFORMÁTICA

El proceso de determinación, control, eliminación o reducción al mínimo de las amenazas que pueden afectar la seguridad informática de una instalación nuclear debería ponerse en marcha de manera sistemática y coherente, de conformidad con las normas en vigor. El presente anexo ofrece una visión más detallada de una metodología específica. El que se haya optado por esta metodología entre las muchas existentes no implica su aprobación por el OIEA y debería considerarse únicamente como un ejemplo detallado. Para una introducción genérica de la evaluación del riesgo, consúltese la sección 6.1.

En general, para comprender las amenazas y vulnerabilidades de un sistema informatizado concreto, primero es necesario analizarlo desde el punto de vista funcional y técnico, y detectar los factores pertinentes de confiabilidad que es necesario mantener. A continuación se deben determinar y analizar los riesgos asociados a esos factores.

En los párrafos siguientes se ofrece una visión general de EBIOS. "EBIOS" es un acrónimo francés que significa *expresión de las necesidades e identificación de los objetivos de seguridad* (expression des besoins et identification des objectifs de sécurité). Ha sido diseñado por la Oficina Central de Seguridad de la Información de Francia (DCSSI, Direction Centrale de la Sécurité des Systèmes d'Information).[1]

EBIOS proporciona un enfoque oficial para evaluar y tratar los riesgos en el ámbito de la seguridad de los sistemas de información comprendidas las herramientas de apoyo para las autoridades contratantes, la redacción de documentos y la sensibilización.

Aquí se dan solamente los principios básicos del enfoque, adaptados a partir de la documentación disponible en el sitio web de apoyo de la DCSSI.

Principios del método EBIOS

Estudio del contexto y definición del perímetro

[1] Métodos para lograr la seguridad de los sistemas de información: http://www.ssi.gouv.fr/site_rubrique113.html.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

El primer paso consiste en definir el contexto técnico, institucional y reglamentario del estudio. En particular, un sistema de información se basa en los **elementos esenciales**, las funciones y la información que constituyen el valor añadido del dicho sistema para la organización.

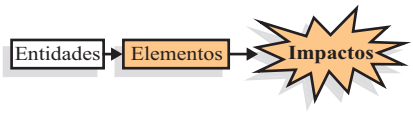
Por ejemplo, un sistema de monitorización del sistema de refrigeración de una central se basa en diversos datos, como medidas, parámetros y resultados de cálculos, así como en varias funciones que permiten realizar esos cálculos.

Los elementos esenciales están vinculados a un conjunto de **entidades** de distintos tipos: equipos y programas informáticos, redes, organizaciones, recursos humanos y emplazamientos.

Tomemos como ejemplo un parámetro utilizado para activar una bomba concreta del sistema de refrigeración. Está vinculado a las computadoras que realizan la monitorización, el programa informático de procesamiento, los operadores, el estado de las fuentes frías, el estado de la central, los reglamentos aplicables, etc.

Producto: meta del estudio (contexto + elementos + entidades).

Expresión de sensibilidades



Para garantizar que las actividades se realizan correctamente, es necesario expresar la **sensibilidad** de cada elemento esencial.

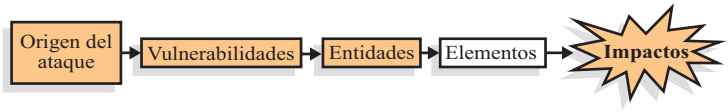
Esta expresión se basa en varios **criterios de seguridad física** tales como disponibilidad, integridad y confidencialidad. Si no se tiene en cuenta esa sensibilidad, se producirá un **impacto** en la organización, que puede adoptar varias formas, como incumplimientos de la seguridad física nuclear, problemas de seguridad tecnológica, funcionamiento incorrecto de las actividades, pérdida de la confianza de los clientes o pérdidas financieras.

Volviendo al ejemplo del parámetro de activación de la bomba del sistema de refrigeración de la central, el requisito de disponibilidad e integridad en relación con esta información debería tener una prioridad elevada a fin de evitar cualquier impacto perjudicial sobre el material, el entorno o el personal, pero también a los efectos de la disponibilidad de la central.

Producto: sensibilidades.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

Estudio de la amenaza



Toda organización está expuesta a diversos agentes de amenazas por su entorno natural, su cultura, su imagen, su ámbito de actividad, etc. Estos agentes pueden clasificarse por tipo (natural, humano o ambiental) y por causa (accidental o deliberada).

El agente puede usar diversos **métodos de ataque**, que es necesario identificar. Un método de ataque se caracteriza por los atributos de la seguridad física (como disponibilidad, integridad o confidencialidad) que puede violar y por los agentes de amenazas probables.

Volviendo al ejemplo, una central nuclear debe tener en cuenta gran número de agentes de amenazas, como se explica en la sección 6.3:

— espionaje/ladrones de tecnología;
— empleado/usuario descontento (interno o externo);
— pirata informático aficionado;
— ciberactivista;
— delincuencia organizada;
— estado nación;
— terrorista,

así como gran número de métodos de ataque:

— escuchas;
— inundación con comunicaciones/denegación de servicio;
— programa informático trampa/puerta trasera;
— ataques para obtener nombres de usuario/contraseñas (fuerza bruta, diccionario, etc.).

Cada entidad tiene **vulnerabilidades** que los agentes de amenazas pueden aprovechar si emplean los métodos de ataque pertinentes. Así pues, podemos resaltar varias vulnerabilidades relacionadas con el sistema de refrigeración de una central nuclear:

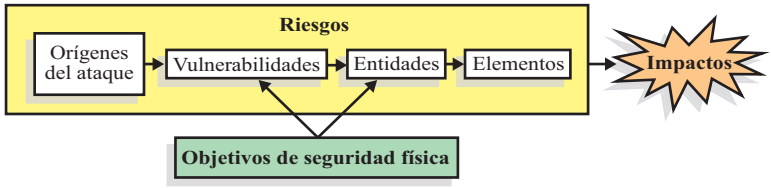
— posible existencia de funciones ocultas introducidas durante la fase de diseño y desarrollo (programas informáticos);
— el uso de equipos no evaluados (equipos informáticos);

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

— la posibilidad de crear o modificar los comandos de los sistemas en línea (redes);
— la red, que puede usarse para alterar el programa informático de recursos del sistema (redes);
— la intrusión en la instalación mediante vías de acceso indirectas (locales);
— el incumplimiento de las instrucciones por los operadores (personal);
— la ausencia de medidas de seguridad física durante las fases de diseño, instalación y funcionamiento (organización).

Producto: formulación de las amenazas (incluidos los escenarios).

Expresión de los objetivos de seguridad física



Ahora hay que determinar la manera en que los agentes de amenazas y sus métodos de ataque pueden afectar a los elementos esenciales: este es el **riesgo**.

El riesgo representa los posibles daños. Se desprende del hecho de que un agente de amenaza puede afectar a los elementos esenciales al utilizar un método de ataque concreto para aprovechar las vulnerabilidades de las entidades de las que dependen esos elementos.

En el ejemplo, existe el riesgo de vulneración de información sensible por un programa informático trampa como resultado de la posibilidad de crear o modificar los comandos del sistema vinculados a la red, lo que podría tener un impacto en el material, el entorno, la seguridad del personal, la disponibilidad de la central y la confianza pública.

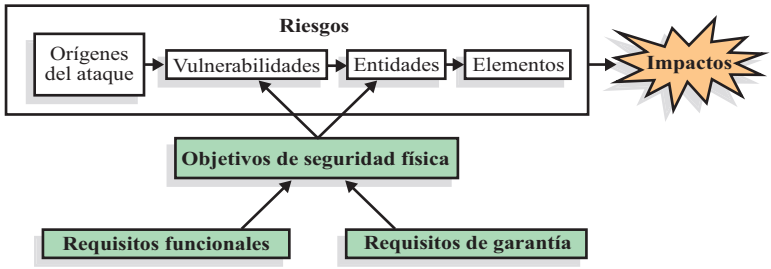
Los **objetivos de seguridad física** consisten principalmente en hacer frente a las vulnerabilidades de las entidades que plantean todos los riesgos retenidos. Lógicamente, no merece la pena proteger lo que no está expuesto a ningún riesgo. Sin embargo, a medida que aumenta la posibilidad de riesgo, también debe aumentar la firmeza de los objetivos de seguridad física. Por lo tanto, esos objetivos representan un conjunto de especificaciones perfectamente adaptado.

Uno de los objetivos de seguridad física de la central nuclear del ejemplo es proteger la creación y modificación de los comandos del sistema vinculados a la red en relación con el sistema de refrigeración.

Producto: objetivos de seguridad física.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

Determinación de los requisitos de seguridad



A continuación, el grupo encargado de aplicar el enfoque debe elaborar las especificaciones exactas de las funciones de seguridad física requeridas, tras lo cual debe demostrar que los objetivos de seguridad física están plenamente abarcados por estos **requisitos funcionales**.

En el ejemplo, los requisitos funcionales para proteger la creación y modificación de los comandos del sistema vinculados a la red podrían incluir:

— una serie de autopruebas ejecutadas por el sistema a intervalos regulares durante el funcionamiento normal para demostrar que funciona correctamente;
— control del acceso físico y lógico.

Por último, el equipo responsable debe especificar los **requisitos de garantía** que permiten alcanzar, y ulteriormente demostrar, el nivel de confianza requerido.

Uno de los requisitos de garantía podría ser que el creador del sistema debe efectuar un análisis de resistencia de las funciones de seguridad física del sistema al nivel de resistencia requerido.

Producto: requisitos funcionales y de garantía.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

Anexo III

FUNCIÓN DEL ERROR HUMANO EN LA SEGURIDAD INFORMÁTICA

En el presente anexo se examinan las cuestiones relacionadas con la actuación humana en la esfera de la seguridad informática; concretamente, se analiza la manera en que la actuación humana puede afectar a la capacidad de la organización para resistir a un ataque, reconocerlo, recuperar datos o servicios esenciales y adaptarse para hacer frente a nuevas amenazas. La investigación continúa impulsando el desarrollo de soluciones técnicas tales como programas informáticos para la monitorización de la seguridad física, programas de detección o prevención de intrusiones, sistemas de autentificación más eficaces y métodos de cifrado más resistentes, pero con mucha frecuencia no se tiene en cuenta el elemento humano como causa y como medida preventiva en materia de seguridad informática.

Múltiples informes han señalado los errores humanos como causa principal de la infracción de las normas de seguridad informática. Según estimaciones recientes, el número de errores humanos relacionados con esas infracciones oscila entre el 60 % y el 80 %. La mayoría de estos errores podrían haberse prevenido con una mayor inversión en sensibilización y más diligencia en el funcionamiento y la supervisión.

La supervivencia de los sistemas y las operaciones es uno de los objetivos de un programa de seguridad informática e incluye los siguientes elementos:

— resistencia del sistema a los ataques;
— reconocimiento del ataque y evaluación del daño;
— recuperación de los servicios esenciales y de la totalidad de los servicios;
— adaptación y evolución del sistema como defensa contra ataques futuros.

El cuadro III-1 ofrece ejemplos de esos elementos en un intento de clasificar los tipos habituales de errores humanos en los procesos y las aplicaciones. Los errores humanos son cometidos tanto por los administradores como por los usuarios de los sistemas. Esta lista no pretende ser exhaustiva, sino que está destinada a ilustrar el nivel de interacción humana asociado con la ejecución de estos sistemas y procesos.

Aunque el cuadro se centra en los aspectos negativos de la actuación humana, también cabe señalar sus impactos positivos. Aunque a veces es el eslabón más débil de la cadena, el operador humano o el empleado puede ser la barrera que impide el fallo o la vulneración del sistema. La tecnología nunca será una solución completa y los empleados son uno de los niveles de una estrategia

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

de defensa en profundidad destinada a garantizar la seguridad y supervivencia del sistema. Las encuestas muestran constantemente que el principal problema de seguridad es la falta de sensibilización y de capacitación adecuadas en materia de seguridad informática.

Cuadro III-1. ERRORES HUMANOS COMUNES

Proceso/aplicación	Errores humanos comunes
Resistencia a los ataques	
Restricción del acceso (administración del sistema)	—Permisos de archivo inadecuados. —Servicios innecesarios abiertos. —Puertos vulnerables abiertos. —Acceso físico otorgado. —Protectores de pantalla con contraseña no utilizados. —Parches del sistema no instalados. —Desconocimiento de lo que implica instalar un parche. — Descarga o instalación de programas informáticos malintencionados o corruptos.
Creación/uso de contraseñas	—Contraseñas anotadas. —Contraseñas poco seguras. —Uso de contraseñas predeterminadas. —Contraseñas divulgadas. —No utilización de contraseñas. — Uso de una misma contraseña para sistemas seguros y no seguros.
Reconocimiento del ataque y del daño	
Sistemas de detección de intrusiones	—Configuración inadecuada (conjunto de reglas) —No actualización del sistema. —Falta de vigilancia en la revisión de los registros.
Auditoría de registros	—Falta de diligencia en la revisión de los registros. — Tendencias a lo largo de múltiples períodos de registro no examinadas.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

Cuadro III-1. ERRORES HUMANOS COMUNES

Proceso/aplicación	Errores humanos comunes
Recuperación del sistema	
Copia de seguridad y restauración	—Copias de seguridad no hechas. —Copias de seguridad no hechas oportunamente. —Configuración inadecuada. —Daños físicos a los medios de las copias de seguridad. —Eliminación accidental de datos. —Almacenamiento de los medios de las copias de seguridad en un lugar inseguro o no protegido. —Uso de medios defectuosos. —Etiquetado erróneo de los medios. —Destrucción física de los medios. —Procedimientos de restauración no sometidos a ensayo. —Copias múltiples de información crucial del sistema no hechas. —Medios de las copias de seguridad no almacenados fuera de la instalación.
Adaptación a nuevas amenazas	
Procedimientos de la empresa	—Desconocimiento de la política de la empresa. —Incumplimiento de la política de la empresa. —Inexistencia de una política de la empresa en materia de recuperación. —Utilización de una política no actualizada. —No verificación de la política/los procedimientos. —No aplicación de la política.

Para poder utilizar plenamente a los empleados como activo en la seguridad informática y la supervivencia del sistema, es necesario que cumplan las siguientes condiciones:

— deben entender perfectamente la importancia de su función dentro del plan general de seguridad informática;
— deben contar con los conocimientos y las aptitudes necesarios en materia de seguridad informática para cumplir sus responsabilidades;
— deben comprender que una cultura de seguridad eficaz comienza por ellos.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

DEFINICIONES

Para los fines de la presente publicación, los términos que figuran a continuación se utilizan con los significados aquí indicados. Estas definiciones pueden diferir del uso que tengan en otros campos. Algunas definiciones están tomadas de otras publicaciones del OIEA, aunque algunos términos se utilizan aquí en el contexto específico de la seguridad informática. Otras proceden de normas internacionales (p.ej., de las referencias [1, 15, 23] de la presente publicación).

amenaza. Posible causa de un incidente no deseado que puede causar daños a un sistema u organización (ISO).
Nota: En otras publicaciones de la Colección de Seguridad Física Nuclear del OIEA, "amenaza" se suele definir como "persona o grupo de personas con motivación, intención y capacidad para cometer un acto doloso". Sin embargo, en la presente publicación el término se emplea en el contexto de la seguridad informática, en el que una amenaza no es necesariamente una persona o un grupo de personas.

ataque. Intento de destruir, exponer, alterar, desactivar o robar un activo, obtener acceso no autorizado al mismo, o hacer uso de él sin autorización (ISO).

autenticación. Garantía de que una característica declarada de una entidad es correcta (ISO).

confidencialidad. Propiedad por la que la información no se revela o pone a disposición de personas, entidades o procesos no autorizados (ISO).

contramedida. Medida adoptada para contrarrestar una amenaza, o para eliminar o reducir vulnerabilidades.

control del acceso. Asegurar que el acceso a los activos se autoriza y limita sobre la base de requisitos institucionales y de seguridad física (ISO).

defensa en profundidad. Combinación de niveles sucesivos de sistemas y medidas para la protección de blancos contra amenazas para la seguridad física nuclear.

disponibilidad. Propiedad de estar accesible y ser utilizable a petición de una entidad autorizada (ISO).

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

evaluación del riesgo. Proceso general de detección, estimación, análisis y evaluación sistemáticos del riesgo.

incidente de seguridad informática. Suceso que pone en peligro, real o potencialmente la confidencialidad, integridad o disponibilidad de un sistema de información basado en una computadora, en red o digital, o de la información procesada, almacenada o transmitida por dicho sistema, o bien que constituye una violación o un riesgo inminente de violación de las políticas o los procedimientos de seguridad, o de las políticas sobre usos aceptables.

ingeniería social. Forma no técnica de recopilación de información o ataque que depende de la interacción humana para manipular a las personas para que violen involuntariamente los procedimientos de seguridad, como por ejemplo, mediante la revelación de información o la realización de otras acciones que afectan a la seguridad.

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

integridad. Propiedad de proteger los activos para que sean exactos y completos (ISO).

necesidad de conocer. Principio según el cual los usuarios, procesos y sistemas reciben acceso solamente a la información, las capacidades y los activos que son necesarios a fin de ejecutar las funciones para las que están autorizados.

perímetro de seguridad informática. Frontera lógica en torno a una red a la que están conectados los activos críticos y a la que el acceso es controlado.

política de seguridad informática. Conjunto de directrices, reglamentos, normas y prácticas que prescriben la manera en que una organización administra y protege las computadoras y los sistemas informáticos.

riesgo. Posibilidad de que una amenaza determinada aproveche las vulnerabilidades de un activo o grupo de activos y, de ese modo, cause daño a la organización. Se mide en función de la combinación de las probabilidades de que se produzca un suceso y la gravedad de sus consecuencias.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

seguridad de la información. Mantenimiento de la confidencialidad, la integridad y la disponibilidad de la información.
Nota: También puede referirse a otras propiedades, como la autenticidad, la rendición de cuentas, el no repudio y la fiabilidad (ISO).

seguridad informática. Aspecto concreto de la seguridad de la información relacionado con las redes y los sistemas informáticos y los sistemas digitales.

vulnerabilidad. Deficiencia de un activo o control que puede ser aprovechada por una amenaza (ISO).

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

IAEA
Organismo Internacional de Energía Atómica

Lugares donde se pueden encargar publicaciones del OIEA

En los siguientes países se pueden adquirir publicaciones del OIEA de los proveedores que figuran a continuación, o en las principales librerías locales. El pago se puede efectuar en moneda local o con bonos de la UNESCO.

ALEMANIA
UNO-Verlag, Vertriebs- und Verlags GmbH, Am Hofgarten 10, D-53113 Bonn
Teléfono: + 49 228 94 90 20 • Fax: +49 228 94 90 20 ó +49 228 94 90 222
Correo-e: bestellung@uno-verlag.de • Sitio web: http://www.uno-verlag.de

AUSTRALIA
DA Information Services, 648 Whitehorse Road, MITCHAM 3132
Teléfono: +61 3 9210 7777 • Fax: +61 3 9210 7788
Correo-e: service@dadirect.com.au • Sitio web: http://www.dadirect.com.au

BÉLGICA
Jean de Lannoy, avenue du Roi 202, B-1190 Bruselas
Teléfono: +32 2 538 43 08 • Fax: +32 2 538 08 41
Correo-e: jean.de.lannoy@infoboard.be • Sitio web: http://www.jean-de-lannoy.be

CANADÁ
Bernan Associates, 4501 Forbes Blvd, Suite 200, Lanham, MD 20706-4346, EE.UU.
Teléfono: 1-800-865-3457 • Fax: 1-800-865-3450
Correo-e: customercare@bernan.com • Sitio web: http://www.bernan.com

Renouf Publishing Company Ltd., 1-5369 Canotek Rd., Ottawa, Ontario, K1J 9J3
Teléfono: +613 745 2665 • Fax: +613 745 7660
Correo-e: order.dept@renoufbooks.com • Sitio web: http://www.renoufbooks.com

CHINA
Publicaciones del OIEA en chino: China Nuclear Energy Industry Corporation, Sección de Traducción
P.O. Box 2103, Beijing

ESLOVENIA
Cankarjeva Zalozba d.d., Kopitarjeva 2, SI-1512 Ljubljana
Teléfono: +386 1 432 31 44 • Fax: +386 1 230 14 35
Correo-e: import.books@cankarjeva-z.si • Sitio web: http://www.cankarjeva-z.si/uvoz

ESPAÑA
Díaz de Santos, S.A., c/ Juan Bravo, 3A, E-28006 Madrid
Teléfono: +34 91 781 94 80 • Fax: +34 91 575 55 63
Correo-e: compras@diazdesantos.es, carmela@diazdesantos.es, barcelona@diazdesantos.es, julio@diazdesantos.es
Sitio web: http://www.diazdesantos.es

ESTADOS UNIDOS DE AMÉRICA
Bernan Associates, 4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4346, EE.UU.
Teléfono: 1-800-865-3457 • Fax: 1-800-865-3450
Correo-e: customercare@bernan.com • Sitio web: http://www.bernan.com

Renouf Publishing Company Ltd., 812 Proctor Ave., Ogdensburg, NY, 13669, EE.UU.
Teléfono: +888 551 7470 (gratuito) • Fax: +888 568 8546 (gratuito)
Correo-e: order.dept@renoufbooks.com • Sitio web: http://www.renoufbooks.com

FINLANDIA
Akateeminen Kirjakauppa, P.O. BOX 128 (Keskuskatu 1), FIN-00101 Helsinki
Teléfono: +358 9 121 41 • Fax: +358 9 121 4450
Correo-e: akatilaus@akateeminen.com • Sitio web: http://www.akateeminen.com

FRANCIA
Form-Edit, 5, rue Janssen, P.O. Box 25, F-75921 París Cedex 19
Teléfono: +33 1 42 01 49 49 • Fax: +33 1 42 01 90 90
Correo-e: formedit@formedit.fr • Sitio web: http://www. formedit.fr

Lavoisier SAS, 145 rue de Provigny, 94236 Cachan Cedex
Teléfono: + 33 1 47 40 67 02 • Fax +33 1 47 40 67 02
Correo-e: romuald.verrier@lavoisier.fr • Sitio web: http://www.lavoisier.fr

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

HUNGRÍA
Librotrade Ltd., Book Import, P.O. Box 126, H-1656 Budapest
Teléfono: +36 1 257 7777 • Fax: +36 1 257 7472 • Correo-e: books@librotrade.hu

INDIA
Allied Publishers Group, 1st Floor, Dubash House, 15, J. N. Heredia Marg, Ballard Estate, Mumbai 400 001
Teléfono: +91 22 22617926/27 • Fax: +91 22 22617928
Correo-e: alliedpl@vsnl.com • Sitio web: http://www.alliedpublishers.com

Bookwell, 2/72, Nirankari Colony, Delhi 110009
Teléfono: +91 11 23268786, +91 11 23257264 • Fax: +91 11 23281315
Correo-e: bookwell@vsnl.net

ITALIA
Libreria Scientifica Dott. Lucio di Biasio "AEIOU", Via Coronelli 6, I-20146 Milán
Teléfono: +39 02 48 95 45 52 ó 48 95 45 62 • Fax: +39 02 48 95 45 48
Correo-e: info@libreriaaeiou.eu • Sitio web: www.libreriaaeiou.eu

JAPÓN
Maruzen Company Ltd, 1-9-18, Kaigan, Minato-ku, Tokyo, 105-0022
Teléfono: +81 3 6367 6079 • Fax: +81 3 6367 6207
Correo-e: journal@maruzen.co.jp • Sitio web: http://www.maruzen.co.jp

NACIONES UNIDAS
Dept. I004, Room DC2-0853, First Avenue at 46th Street, Nueva York, N.Y. 10017, EE.UU.
Teléfono (Naciones Unidas): +800 253-9646 ó +212 963-8302 • Fax: +212 963 -3489
Correo-e: publications@un.org • Sitio web: http://www.un.org

NUEVA ZELANDIA
DA Information Services, 648 Whitehorse Road, MITCHAM 3132, Australia
Teléfono: +61 3 9210 7777 • Fax: +61 3 9210 7788
Correo-e: service@dadirect.com.au • Sitio web: http://www.dadirect.com.au

PAÍSES BAJOS
De Lindeboom Internationale Publicaties B.V., M.A. de Ruyterstraat 20A, NL-7482 BZ Haaksbergen
Teléfono: +31 (0) 53 5740004 • Fax: +31 (0) 53 5729296
Correo-e: books@delindeboom.com • Sitio web: http://www.delindeboom.com

Martinus Nijhoff International, Koraalrood 50, P.O. Box 1853, 2700 CZ Zoetermeer
Teléfono: +31 793 684 400 • Fax: +31 793 615 698
Correo-e: info@nijhoff.nl • Sitio web: http://www.nijhoff.nl

Swets and Zeitlinger b.v., P.O. Box 830, 2160 SZ Lisse
Teléfono: +31 252 435 111 • Fax: +31 252 415 888
Correo-e: infoho@swets.nl • Sitio web: http://www.swets.nl

REINO UNIDO
The Stationery Office Ltd, International Sales Agency, P.O. Box 29, Norwich, NR3 1 GN
Teléfono (pedidos) +44 870 600 5552 • (información): +44 207 873 8372 • Fax: +44 207 873 8203
Correo-e (pedidos): book.orders@tso.co.uk • (información): book.enquiries@tso.co.uk • Sitio web: http://www.tso.co.uk

Pedidos en línea
DELTA Int. Book Wholesalers Ltd., 39 Alexandra Road, Addlestone, Surrey, KT15 2PQ
Correo-e: info@profbooks.com • Sitio web: http://www.profbooks.com

Libros relacionados con el medio ambiente
Earthprint Ltd., P.O. Box 119, Stevenage SG1 4TP
Teléfono: +44 1438748111 • Fax: +44 1438748844
Correo-e: orders@earthprint.com • Sitio web: http://www.earthprint.com

REPÚBLICA CHECA
Suweco CZ, S.R.O., Klecakova 347, 180 21 Praga 9
Teléfono: +420 26603 5364 • Fax: +420 28482 1646
Correo-e: nakup@suweco.cz • Sitio web: http://www.suweco.cz

REPÚBLICA DE COREA
KINS Inc., Information Business Dept. Samho Bldg. 2nd Floor, 275-1 Yang Jae-dong SeoCho-G, Seúl 137-130
Teléfono: +02 589 1740 • Fax: +02 589 1746 • Sitio web: http://www.kins.re.kr

Los pedidos y las solicitudes de información también se pueden dirigir directamente a:

Dependencia de Mercadotecnia y Venta, Organismo Internacional de Energía Atómica
Centro Internacional de Viena, P.O. Box 100, 1400 Viena, Austria
Teléfono: +43 1 2600 22529 (ó 22530) • Fax: +43 1 2600 29302
Correo-e: sales.publications@iaea.org • Sitio web: http://www.iaea.org/books

12-12793

La publicación No. 17-T (Rev. 1) sustituye a la presente publicación.

La presente publicación busca crear conciencia sobre la importancia de incorporar la seguridad informática como parte fundamental del plan general de seguridad física de las instalaciones nucleares. Además, tiene por objeto proporcionar orientaciones para las instalaciones nucleares sobre la aplicación de un programa de seguridad informática, así como prestar asesoramiento sobre la evaluación de los programas existentes, la determinación de los activos digitales críticos y la definición de las medidas apropiadas para reducir los riesgos.

ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA
VIENA
ISBN 978–92–0–337310–4
ISSN 1816–9317