IAEA BULLETIN
ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA
La publicación emblemática del OIEA | Junio de 2023 | www.iaea.org/es/bulletin

LA SEGURIDAD INFORMÁTICA EN EL MUNDO NUCLEAR

Cómo se elabora un programa de seguridad informática, pág 6

Cómo la inteligencia artificial cambiará la seguridad informática y la seguridad física de la información en el mundo nuclear, pág 14

Una seguridad informática más fuerte para garantizar la seguridad nuclear tecnológica y física, pág 22

BOLETÍN DEL OIEA
es una publicación de la
Oficina de Información
al Público y Comunicación (OPIC)
Organismo Internacional de Energía Atómica
Centro Internacional de Viena
PO Box 100, 1400 Viena (Austria)
Phone: (43-1) 2600-0
iaeabulletin@iaea.org

Directora editorial: Emma Midgley
Diseño y producción: Ritu Kenn

EL BOLETÍN DEL OIEA puede consultarse en línea en
www.iaea.org/es/bulletin

Portada:
(Adobestock.com)

Síganos en:

IAEA

La misión del Organismo Internacional de Energía Atómica es evitar la proliferación de las armas nucleares y ayudar a todos los países, especialmente del mundo en desarrollo, a sacar provecho de los usos de la ciencia y la tecnología nucleares con fines pacíficos y en condiciones de seguridad tecnológica y física.

El OIEA, creado en 1957 como organismo independiente de las Naciones Unidas, es la única organización del sistema de las Naciones Unidas especializada en tecnología nuclear. Por medio de sus laboratorios especializados, únicos en su clase, transfiere conocimientos y competencias técnicas a sus Estados Miembros en ámbitos como la salud humana, la alimentación, el agua, la industria y el medio ambiente.

Además de proporcionar una plataforma mundial para el fortalecimiento de la seguridad física nuclear, el OIEA ha creado la *Colección de Seguridad Física Nuclear,* cuyas publicaciones, que gozan del consenso internacional, ofrecen orientaciones sobre ese tema. La labor del OIEA se centra igualmente en ayudar a reducir al mínimo el riesgo de que los materiales nucleares y otros materiales radiactivos caigan en manos de terroristas y criminales o de que las instalaciones nucleares sean objeto de actos dolosos.

Las normas de seguridad del OIEA proporcionan un sistema de principios fundamentales de seguridad y reflejan un consenso internacional sobre lo que constituye un alto grado de seguridad para proteger a la población y el medio ambiente contra los efectos nocivos de la radiación ionizante. Estas normas han sido elaboradas pensando en que sean aplicables a cualquier tipo de instalación o actividad nuclear destinada a fines pacíficos, así como a las medidas protectoras encaminadas a reducir los riesgos radiológicos existentes.

Mediante su sistema de inspecciones, el OIEA también verifica que los Estados Miembros utilicen los materiales e instalaciones nucleares exclusivamente con fines pacíficos, conforme a los compromisos contraídos en virtud del Tratado sobre la No Proliferación de las Armas Nucleares y otros acuerdos de no proliferación.

La labor del OIEA es polifacética y se lleva adelante, con participación de muy diversos asociados, a escala nacional, regional e internacional. Los programas y presupuestos del OIEA se establecen mediante decisiones de sus órganos rectores: la Junta de Gobernadores, compuesta por 35 miembros, y la Conferencia General, que reúne a todos los Estados Miembros.

El OIEA tiene su Sede en el Centro Internacional de Viena y cuenta con oficinas sobre el terreno y de enlace en Ginebra, Nueva York, Tokio y Toronto. Además, tiene laboratorios científicos en Mónaco, Seibersdorf y Viena. Por otra parte, proporciona apoyo y financiación al Centro Internacional de Física Teórica “Abdus Salam”, en Trieste (Italia).

El papel esencial de la seguridad informática en la seguridad nuclear tecnológica y física

Rafael Mariano Grossi, Director General del OIEA

El ritmo de la innovación digital es asombroso. Tecnologías como la inteligencia artificial (IA) están dando pasos de gigante, incluso en los últimos meses. Estos avances nos ayudarán a mejorar las operaciones controladas digitalmente y las tecnologías de automatización en las instalaciones nucleares, con los posibles beneficios de alcanzar una mayor eficiencia operativa, reducir los costos de mano de obra y lograr una mayor seguridad tecnológica y física.

Los diseños de reactores nucleares avanzados, como los reactores modulares pequeños (SMR) y los microrreactores, ya incluyen planes para utilizar la IA y el aprendizaje automático con el fin de activar funciones innovadoras como la automatización, el control y el mantenimiento de la supervisión a distancia, y las salas de control compartidas. Pero las innovaciones digitales, como la IA y el aprendizaje automático, también suponen una amenaza. Es preciso vigilarlas constantemente para garantizar la integridad de los activos de carácter estratégico y proteger la información en las instalaciones nucleares y radiológicas.

Siempre se han utilizado guardias y verjas para garantizar la protección de las instalaciones nucleares frente a sabotajes o agentes con fines dolosos, pero hoy en día dependemos cada vez más de los sistemas digitales. Los sistemas de instrumentación y control de las instalaciones nucleares se utilizan para aplicaciones clave de seguridad tecnológica y física, lo que mejora la eficacia, pero implica que tengamos que estar especialmente atentos a la protección de estos sistemas informáticos. Países de todo el mundo reconocen el carácter prioritario de esa labor.

El OIEA desempeña un papel único a la hora de fomentar la cooperación entre países y propiciar el intercambio de conocimientos técnicos y prácticas óptimas en el ámbito tecnológico para la adopción de tecnologías en rápido desarrollo. Al mismo tiempo, prestamos asesoramiento a los países sobre cómo reducir al mínimo y mitigar las posibles vulnerabilidades que acompañan y afectan a la seguridad informática. En tan solo los dos últimos años, nuestras actividades globales de asistencia a la seguridad informática han aumentado en más de una cuarta parte, y se han centrado especialmente en apoyar a nivel nacional las normativas e inspecciones de seguridad informática y las actividades en ese ámbito.

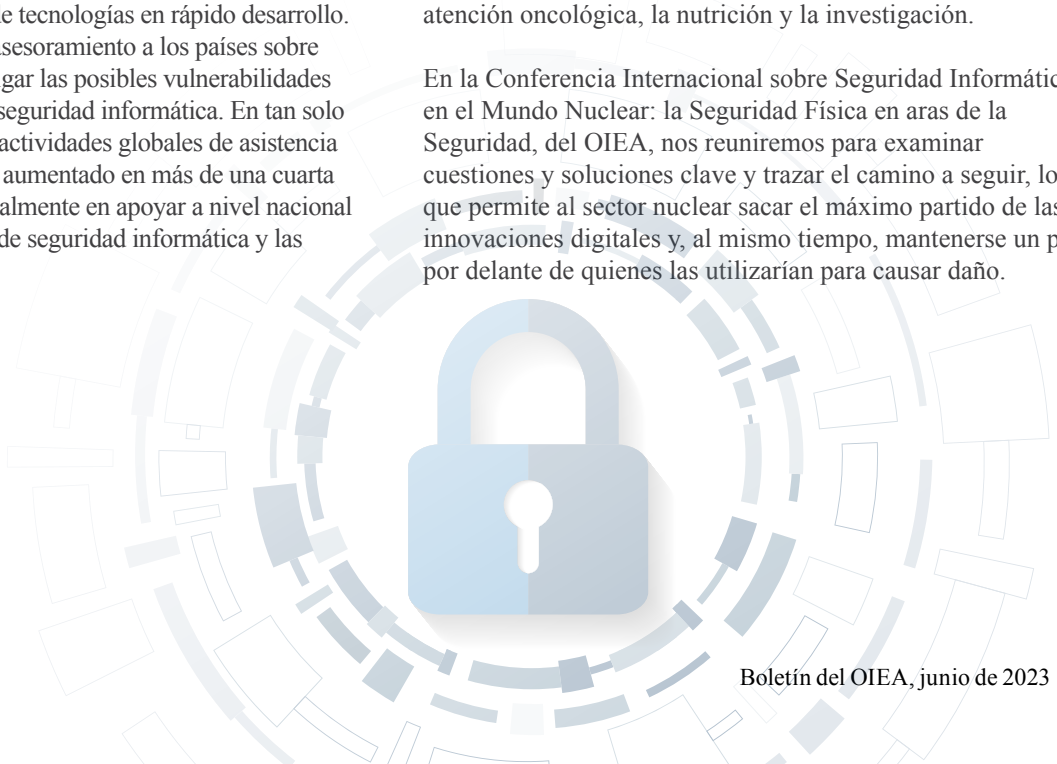
El OIEA ha venido respondiendo a los desafíos de seguridad física nuclear de sus Estados Miembros con una serie de actividades, entre las que se encuentra el suministro de documentos de orientación y la realización de actividades de capacitación que les permitan poner en marcha sólidos programas nacionales de seguridad informática y seguridad física de la información. Estas orientaciones también se utilizan como referencia para evaluar el programa de seguridad informática y seguridad física de la información de un país durante una misión del Servicio Internacional de Asesoramiento sobre Protección Física, conocido como IPPAS.

Además, estamos poniendo en marcha un curso para formar expertos en la redacción de normas de seguridad informática. Próximamente, con el lanzamiento de una plataforma virtual de aprendizaje en línea muchos más países podrán acceder a los cursos de capacitación del OIEA en materia de seguridad informática.

Paralelamente, el OIEA respalda actividades nacionales y regionales de seguridad informática que tienen por objeto sensibilizar sobre la amenaza de los ciberataques y su posible impacto en la seguridad física nuclear. Fomentamos la cooperación entre responsables de la formulación de políticas y expertos internacionales y propiciamos la investigación complementaria.

Las actividades de seguridad informática del OIEA van en aumento ya que los países, incluidos los de ingresos medianos y bajos, recurren cada vez más a la tecnología nuclear para satisfacer sus prioridades, entre ellas la energía limpia, la atención oncológica, la nutrición y la investigación.

En la Conferencia Internacional sobre Seguridad Informática en el Mundo Nuclear: la Seguridad Física en aras de la Seguridad, del OIEA, nos reuniremos para examinar cuestiones y soluciones clave y trazar el camino a seguir, lo que permite al sector nuclear sacar el máximo partido de las innovaciones digitales y, al mismo tiempo, mantenerse un paso por delante de quienes las utilizarían para causar daño.



1 El papel esencial de la seguridad informática en la seguridad nuclear tecnológica y física

4 Hacer frente a las amenazas en materia de seguridad informática
La evolución del programa de asistencia del OIEA

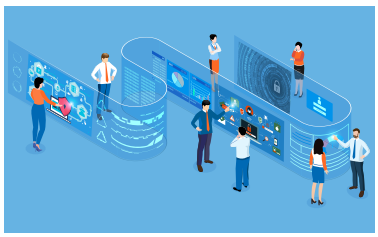
6 Cómo se elabora un programa de seguridad informática

8 Más allá de la protección física
Cómo el Servicio Internacional de Asesoramiento sobre Protección Física (IPPAS) facilita la mejora de la seguridad informática

10 El OIEA brinda asistencia a los países africanos para la elaboración de reglamentos sobre seguridad informática

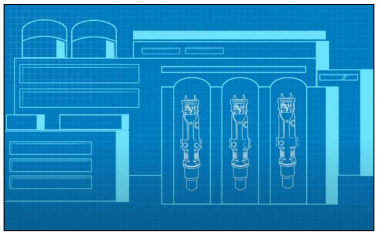
12 Innovación en la capacitación virtual en seguridad informática para instalaciones nucleares y radiológicas

14 Cómo la inteligencia artificial cambiará la seguridad informática y la seguridad física de la información en el mundo nuclear



16 Cómo los ejercicios de seguridad informática ayudan a aumentar la preparación para responder a los ciberataques en la esfera de la seguridad física nuclear

18 Proyectos coordinados de investigación para mejorar las técnicas de detección de anomalías en la seguridad informática



20 Garantizar la seguridad de las tecnologías digitales de la próxima generación de reactores nucleares

22 Una seguridad informática más fuerte para garantizar la seguridad nuclear tecnológica y física

ENTREVISTA

24 Contrarrestar las amenazas en un mundo cada vez más digitalizado

PANORAMA MUNDIAL

26 Cómo la colaboración internacional mantiene al mundo a salvo de las ciberamenazas

— Tighe Smith, IEC

NOTICIAS DEL OIEA

28 Noticias del OIEA

32 Publicaciones

Hacer frente a las amenazas en materia de seguridad informática

La evolución del programa de asistencia del OIEA

Vasiliki Tafili

El cambio a sociedades de redes digitales, en las que las actividades cotidianas están interrelacionadas con la ayuda de sistemas computarizados, inteligencia artificial (IA) y tecnologías digitales, ha repercutido considerablemente en la seguridad nuclear tecnológica y física. No se puede insistir lo suficiente en el papel esencial que desempeñan las tecnologías digitales en el mantenimiento de las funciones de seguridad tecnológica y de seguridad física en las instalaciones dedicadas a la manipulación de material nuclear u otros materiales radiactivos.

"Los sistemas computarizados y las tecnologías digitales son vitales para las instalaciones y las actividades conexas en las que se utilizan materiales nucleares y otros materiales radiactivos", señala Elena Buglova, Directora de la División de Seguridad Física Nuclear del OIEA, que hace hincapié en la necesidad de que todos los países apliquen programas de seguridad informática y mejoren la defensa en profundidad de la seguridad nuclear. "A medida que avanza la tecnología, proteger la confidencialidad, la integridad y la disponibilidad de información y activos de carácter estratégico exige una vigilancia constante para prevenir y mitigar los riesgos, así como un sólido programa de seguridad informática y seguridad física de la información".

La necesidad de hacer frente a las amenazas a la seguridad informática, los ciberataques malintencionados y cualquier vulnerabilidad potencial que puedan introducir las tecnologías digitales, así como la importancia de la seguridad informática para la seguridad nuclear, se determinaron por primera vez en una resolución sobre seguridad física nuclear adoptada por la Conferencia General del OIEA en su quincuagésima quinta reunión ordinaria, en 2011. En ella se tomó conocimiento de los esfuerzos del OIEA "para fomentar la sensibilización a la creciente amenaza de los ataques cibernéticos y sus posibles consecuencias para la seguridad física nuclear". Esta resolución también alentó al OIEA a elaborar documentos de orientación apropiados, celebrar cursos de capacitación y acoger más reuniones de expertos dedicadas específicamente a la ciberseguridad en las instalaciones nucleares a fin de ayudar a los países a protegerse de los ataques cibernéticos.

"En seguimiento de la resolución de la Conferencia General de 2011, las actividades del OIEA se centraron en mejorar las capacidades de seguridad informática a nivel de los Estados y de las instalaciones", expresa la Sra. Buglova, que añade que estas actividades se incluyeron en los Planes de Seguridad Física Nuclear posteriores del OIEA, incluidos los detalles de la realización actual de las actividades de seguridad informática del OIEA que se describen a grandes rasgos en el Plan de Seguridad Física Nuclear para 2022-2025.

¿Cómo ayuda el OIEA a los países a desarrollar o mejorar su seguridad informática?

El establecimiento de un programa de seguridad informática sólido y actualizado es un elemento clave para proteger a los países de los ciberataques en todo tipo de infraestructuras críticas. El OIEA ha sido ágil a la hora de prestar asistencia a los países en todas las fases de desarrollo de los programas nacionales de seguridad informática y seguridad física de la información, asistencia que ha comprendido la facilitación de documentos de orientación y actividades de capacitación.

Cuatro publicaciones de orientaciones de la *Colección de Seguridad Física Nuclear del OIEA* y otras tres publicaciones técnicas ofrecen asesoramiento sobre seguridad informática y seguridad física de la información. Esas orientaciones pueden servir de base para la elaboración de marcos nacionales de seguridad informática, incluidas las estrategias nacionales, así como para los reglamentos y la capacitación en materia de seguridad informática.

Un principio clave de la orientación del OIEA es preservar las funciones críticas en las instalaciones nucleares protegiendo la información y los sistemas computarizados para mantener un entorno seguro desde el punto de vista tecnológico y físico respecto de las instalaciones y los materiales. Esto se logra desarrollando un programa de seguridad informática (véase la página 6), identificando las funciones de seguridad física nuclear, utilizando la gestión del riesgo para determinar las consecuencias potenciales de una seguridad comprometida, definiendo el nivel de seguridad informática necesario para los activos digitales de carácter estratégico y aplicando un enfoque graduado y los conceptos de defensa en profundidad en materia de seguridad informática. Estos elementos deberían diseñarse e implantarse de forma que eviten la puesta en riesgo y ayuden a aumentar la capacidad del explotador para detectar y responder a las intrusiones, así como para mitigar el impacto potencial de los ciberataques.

A solicitud de los países, el OIEA ofrece diversas oportunidades de capacitación a distintos públicos destinatarios, entre los que se encuentran las autoridades competentes, los explotadores, los proveedores y otras entidades que tengan responsabilidades en la puesta en práctica de la seguridad informática. Estos también podrían beneficiarse de los conocimientos especializados del OIEA en la realización de ejercicios de seguridad informática como parte del programa de seguridad física nuclear.

Además, hay cuatro cursos de aprendizaje electrónico sobre seguridad informática gratuitos que están disponibles en árabe, chino, español, francés, inglés y ruso en la Ciberplataforma de

Aprendizaje para la Enseñanza y la Capacitación en Red del OIEA, y se puede acceder a ellos inscribiéndose o a través de una cuenta NUCLEUS. En breve también estará disponible una plataforma de capacitación virtual nueva e innovadora (véase la página 12).

Paralelamente, el OIEA presta apoyo a ejercicios nacionales o regionales de seguridad informática como parte de su labor para concienciar sobre la amenaza de los ciberataques y sus posibles efectos en la seguridad física nuclear. Los ejercicios presentan diferentes escenarios en los que un ataque contra la protección física y los sistemas electrónicos tiene por objetivo directo o indirecto sistemas computarizados y la información de carácter estratégico.

Las actividades de investigación complementan las actividades de seguridad informática del OIEA, principalmente a través del mecanismo consolidado de proyectos coordinados de investigación. En los últimos años se han puesto en marcha proyectos de esta índole para fomentar la labor de la comunidad mundial de investigadores en materia de seguridad informática y seguridad física de la información e incrementar el nivel de preparación para hacer frente a los nuevos desafíos y riesgos (véase la página 18).

¿Qué nos depara el futuro?

El programa de seguridad informática del OIEA para la seguridad física nuclear está en constante evolución. El hecho de que los reactores modulares pequeños y los reactores avanzados dependan de tecnologías avanzadas y sistemas de instrumentación digital, las repercusiones previstas de la IA y la aparición de entornos de aprendizaje virtuales presentan desafíos y ámbitos respecto de los que cabe ampliar el apoyo a los Estados.

“Estamos presenciando una concienciación cada vez mayor de las implicaciones potenciales o reales para la seguridad nuclear tecnológica y física entre países, órganos reguladores, explotadores y otras partes interesadas”, afirma la Sra. Buglova. “Debido al importante crecimiento previsto en el uso de aplicaciones nucleares con fines pacíficos, en concreto los programas nucleoeléctricos, es indispensable considerar la seguridad informática y física de la información como una parte integrante de la seguridad física nuclear”.

Ciberataque

El término “ciberataque” se utiliza para describir un acto doloso con la intención de robar, alterar o destruir un objetivo específico, o impedir el acceso a este, mediante el acceso no autorizado a un sistema computarizado susceptible (o mediante acciones dentro de él). Los ciberataques ponen en peligro la confidencialidad, la integridad o la disponibilidad (o una combinación de estas propiedades) de la información de carácter estratégico dentro de un recurso digital de carácter estratégico, o de ese recurso, y pueden utilizarse para llevar a cabo o facilitar un acto doloso contra una instalación o una actividad u otro acto delictivo o intencional no autorizado que guarde relación con materiales nucleares u otros materiales radiactivos.

Un ciberataque puede llevarse a cabo a través del acceso físico directo a la información o a los recursos de información o a través del acceso electrónico, o mediante una combinación de ambos, y puede ser llevado a cabo directamente por un adversario o por un agente interno (o con su ayuda) influenciado deliberadamente o no por un adversario.

Los ciberataques, una vez detectados, deberían tratarse como incidentes de seguridad informática.

Esta definición está tomada de la publicación *Computer Security for Nuclear Security (Colección de Seguridad Física Nuclear del OIEA* Nº 42-G)

Cómo se elabora un programa de seguridad informática

Vasiliki Tafili y Trent Nelson

Las instalaciones dedicadas a la manipulación de material nuclear u otro material radiactivo, así como a actividades conexas, son infraestructuras críticas que requieren un alto grado de seguridad tecnológica y seguridad física. Con un enfoque exhaustivo y proactivo con respecto a la seguridad informática, las organizaciones pueden proteger los recursos de información de carácter estratégico y los sistemas informáticos de estas instalaciones frente a elementos que pudieran ponerlos en riesgo. El enfoque recomendado por el OIEA en materia de seguridad informática se fundamenta en el establecimiento por los Estados de requisitos relacionados con una estrategia o política nacional, así como en garantías de la confidencialidad y la protección de la información de carácter estratégico y de los sistemas informáticos relacionados con la protección física, la seguridad nuclear y la contabilidad y el control del material nuclear. Estos requisitos también pueden adoptar la forma de reglamentos nacionales en los que se dispongan el desarrollo y la ejecución de un programa de seguridad informática (PSI).

Un PSI es un marco general en que figuran los elementos clave de un plan eficaz para aplicar políticas y procedimientos de seguridad informática que habrán de utilizarse durante toda la vida útil de una instalación nuclear o una instalación con fuentes radiactivas. Tiene por objeto proteger frente a las ciberamenazas los recursos de información de carácter estratégico y los sistemas informáticos críticos para el mantenimiento de las funciones de seguridad tecnológica y seguridad física, a fin de mitigar el impacto de los ciberataques.

Estrategia nacional

Una estrategia de seguridad informática exhaustiva y eficaz requiere un enfoque sistemático que integre diversos elementos, como reglamentos, programas, medidas de protección de la seguridad física y capacidades de respuesta para sostener los regímenes nacionales de seguridad física nuclear.

Reglamentos

En unos reglamentos eficaces se dispone un marco jurídico para proteger los sistemas informáticos de carácter estratégico y se vela por que en las organizaciones haya PSI* establecidos y dotados de los controles adecuados.

Elementos clave del PSI:

Funciones y responsabilidades

Las funciones y responsabilidades organizativas en materia de rendición de cuentas son vitales para una gestión eficaz, especialmente en el caso de la infraestructura crítica. Para inculcar una colaboración y una sinergia eficientes y eficaces en los PSI es preciso que se conozca la jerarquía organizativa y que haya unas líneas claras de autoridad y estructura jerárquica.

Gestión de riesgos, factores de vulnerabilidad y cumplimiento

En el marco de la gestión de riesgos de seguridad informática se evalúan factores de vulnerabilidad y posibles consecuencias de los activos digitales de carácter estratégico y sistemas informáticos, a fin de aplicar controles de seguridad informática empleando un enfoque graduado a modo de defensa frente a los ciberataques. La magnitud de las medidas de seguridad aplicadas debe estar en consonancia con la del riesgo asociado a la información y/o a los sistemas informáticos que son objeto de protección. En función de las consecuencias del factor de vulnerabilidad o amenaza, las organizaciones estarán en condiciones de determinar qué magnitud han de tener las medidas de seguridad para mitigar el riesgo.

Concepción y gestión de la seguridad

El diseño de la seguridad informática es un aspecto crítico de la protección frente a ciberamenazas. Entre los principios fundamentales de diseño figuran un enfoque graduado y la defensa en profundidad, en el marco de lo cual se aplican múltiples capas de controles de seguridad zonificados para prevenir y mitigar los ataques. Asimismo, los requisitos de seguridad deben incorporarse en todo el ciclo de vida de desarrollo del sistema, también por lo que respecta a organizaciones de terceros regidas por políticas y acuerdos claros, para garantizar que las medidas de seguridad sean coherentes y eficaces.

Gestión de recursos digitales

Una seguridad informática eficaz se basa en un proceso sistemático con el que confeccionar una lista exhaustiva de todas las funciones, recursos y sistemas de las instalaciones, incluidos los activos digitales de carácter estratégico esenciales para proteger las operaciones nucleares o para mantener un uso tecnológica y físicamente seguro del material nuclear y otro material radiactivo. Una lista de esa índole también dispone el flujo de datos y las interdependencias importantes para la organización en apoyo de los controles de acceso, las copias de seguridad y otras medidas de seguridad para proteger estos recursos frente a sabotajes o robos.

Procedimientos de seguridad

Las políticas y procedimientos de seguridad física nuclear operacional orientan las medidas destinadas a evitar robos, sabotajes o usos no autorizados de materiales e instalaciones nucleares. Estas políticas garantizan que el acceso a información y activos de carácter estratégico esté estrictamente controlado, y que las personas con acceso sean examinadas y capacitadas de manera adecuada.

Gestión de personal

La probidad, la concienciación y la capacitación son fundamentales para la gestión de personal en la industria nuclear. Deberían realizarse evaluaciones de la probidad para garantizar que el personal es fiable y competente y está exento de cualquier conflicto de intereses que pudiera comprometer la seguridad tecnológica o la seguridad física. A fin de garantizar la seguridad nuclear tecnológica y física, es fundamental mantener un personal cualificado y de confianza.

** La publicación Nº 17-T (Rev. 1) de la* Colección de Seguridad Física Nuclear del OIEA, *titulada* Computer Security Techniques for Nuclear Facilities, *reúne más detalles al respecto.*

Más allá de la protección física

Cómo el Servicio Internacional de Asesoramiento sobre Protección Física (IPPAS) facilita la mejora de la seguridad informática

Vasiliki Tafili

Desde hace casi treinta años los países recurren al Servicio Internacional de Asesoramiento sobre Protección Física (IPPAS) del OIEA para recibir asesoramiento con miras a garantizar la protección física de todo tipo de instalaciones en las que se utilizan materiales nucleares y otros materiales radiactivos, incluidas las centrales nucleares y las unidades de radioterapia de los hospitales. Sin embargo, debido a los avances tecnológicos, los sistemas digitales son actualmente esenciales para las operaciones de estas instalaciones, lo que ha planteado muchos desafíos nuevos en materia de seguridad física nuclear.

En respuesta a la amenaza real de ciberataques contra instalaciones, incluidas las instalaciones nucleares, en 2012 se incorporó al ámbito de acción del IPPAS la seguridad informática y la seguridad física de la información en aras de la protección física. Desde entonces, los países han solicitado cada vez más la inclusión de este módulo en el examen del IPPAS, con el fin de obtener apoyo en la tarea de defenderse de las amenazas a la ciberseguridad.

En cuanto componente central del programa de seguridad física nuclear del OIEA, el IPPAS es un servicio de asesoramiento que examina las prácticas existentes en un país en relación con los instrumentos internacionales pertinentes y las orientaciones del OIEA sobre seguridad física nuclear. Ayuda a los países que lo soliciten a reforzar sus regímenes, sistemas y medidas nacionales de seguridad física nuclear, brindándoles asesoramiento sobre la aplicación de los instrumentos jurídicos internacionales.

"Veintisiete años después de la primera misión IPPAS, el servicio ha evolucionado para hacer frente a los desafíos y necesidades actuales, —indica Heather Looney, Jefa de la Sección de Seguridad Física Nuclear de los Materiales y las Instalaciones de la División de Seguridad Física Nuclear del OIEA—. No se puede garantizar la protección física contra el robo, el sabotaje o el uso no autorizado de materiales nucleares y otros materiales radiactivos si no se cuenta con medidas de seguridad informática. Al invitar a una misión IPPAS los países pueden recibir asesoramiento sobre lo que puede mejorarse y cómo hacerlo", añade.

El IPPAS sigue un enfoque modular y ofrece cinco módulos que abarcan un examen nacional del régimen de seguridad física nuclear para el material nuclear y las instalaciones nucleares; un examen de los sistemas y medidas de seguridad física en las instalaciones nucleares; un examen de la seguridad física del transporte de materiales; un examen de la seguridad física del material radiactivo, las instalaciones y las actividades asociadas, y un examen de la seguridad informática y la seguridad física de la información. Desde la primera misión IPPAS en 1996 hasta la fecha se han realizado 97 misiones, y 22 países han solicitado que se incluya el módulo de seguridad informática y la seguridad física de la información en el examen del IPPAS.

¿Qué debe esperar un país durante la evaluación de la seguridad informática y la seguridad física de la información?

Como primer paso, un grupo de expertos internacionales en seguridad física nuclear del IPPAS analiza cómo se han establecido y gestionado las políticas nacionales relativas a los programas de seguridad informática y la seguridad física de la información. A continuación, el grupo estudiará el marco legislativo y regulador comparando los procedimientos y las prácticas vigentes en el país con las obligaciones especificadas en la Convención sobre la Protección Física de los Materiales Nucleares y su Enmienda de 2005, así como con las orientaciones proporcionadas en las publicaciones pertinentes de la *Colección de Seguridad Física Nuclear del OIEA*. Esto permite determinar si los países cuentan con las políticas y los procedimientos necesarios para lograr una seguridad informática adecuada en las instalaciones nucleares y radiológicas críticas.

A nivel de las instalaciones, con el examen de la seguridad informática se estudiará la gestión de la seguridad informática, el programa de seguridad informática (véase la página 6), los controles del acceso, la arquitectura defensiva de la seguridad informática, así como la detección de sucesos de seguridad informática y la respuesta a estos. El grupo también puede evaluar esferas transversales, como la gestión del riesgo, los enfoques graduados, la cultura de la seguridad física nuclear y la gestión de los recursos humanos.

El Japón recibió a una misión IPPAS y su misión de seguimiento en 2015 y 2018 respectivamente. "Para el Japón ha sido una valiosa experiencia examinar el estado actual de las medidas de seguridad informática y promover su mejora a partir de las sugerencias de los examinadores, —declara Hiroyuki Sugawara, Director de Seguridad Física Nuclear Internacional de la División de Seguridad Física Nuclear de

Desde 1996, el Servicio Internacional de Asesoramiento sobre Protección Física (IPPAS) ha ayudado a los países a encontrar maneras de fortalecer la protección de los materiales y las instalaciones nucleares. (Fotografía: OIEA)

la Autoridad de Reglamentación Nuclear (ANR) del Japón—. En respuesta a las conclusiones del IPPAS decidimos reforzar las medidas de seguridad informática y aumentar el número de inspectores con conocimientos especializados en la materia. Además, la ANR incorporó las amenazas a la seguridad informática en su evaluación de las amenazas a nivel nacional y exigió a los titulares de las licencias que adoptaran medidas sólidas de seguridad informática y que mejoraran el contenido de sus planes de seguridad informática incorporando contramedidas para repeler los ciberataques".

Tras una misión IPPAS realizada en 2018, Francia reforzó la visibilidad de la seguridad informática en el marco nacional de seguridad física nuclear. "La misión IPPAS requirió un fuerte compromiso de las distintas partes interesadas, lo que dio a Francia la oportunidad de consolidar su régimen de seguridad física nuclear y estimular su aplicación, —indica Frédéric Boën, Jefe de Proyecto de Seguridad Informática de la Oficina de Seguridad Física Nuclear de la Dirección de Defensa y Seguridad del Ministerio de Transición Energética—. Se aumentó el número de personal especializado en seguridad informática y se establecieron directrices de reglamentación acordes con las normas internacionales y las orientaciones sobre seguridad física nuclear del OIEA".

Desde 2016, el OIEA ha mantenido la Base de Datos sobre Buenas Prácticas del IPPAS para compartir las conclusiones de dichas misiones con la comunidad internacional de la seguridad física nuclear, mejorando así los efectos de la asistencia ofrecida por el OIEA a países de todo el mundo. "El mantenimiento de esta base de datos y la puesta en común de estos ejemplos hacen que los beneficios de las misiones IPPAS transciendan del país anfitrión a la comunidad internacional de expertos en seguridad física nuclear y se multipliquen los efectos de la asistencia ofrecida por el OIEA a sus Estados Miembros", afirma la Sra. Looney.

La mayoría de las buenas prácticas a nivel de los Estados tienen que ver con la gestión de la seguridad física nuclear, sobre la que se apoyan la coordinación y la seguridad informática. Además, existen 40 buenas prácticas relativas a la seguridad informática, tanto a nivel de los Estados como de las instalaciones, a las que pueden acceder los Estados Miembros del OIEA a través de los puntos de contacto designados.

El OIEA sigue brindando apoyo a los países para la mejora de sus regímenes nacionales de seguridad física nuclear, y la demanda de estos para recibir misiones IPPAS en 2023 y en 2024 sigue siendo elevada.

El OIEA brinda asistencia a los países africanos para la elaboración de reglamentos sobre seguridad informática

Andrea Rahandini

En los próximos años se prevé un incremento de la demanda de radioisótopos por parte de África a medida que más países hacen un mayor uso pacífico de la tecnología nuclear. El aumento de las tasas de cáncer ha dado lugar a una mayor demanda en la esfera de la radioterapia, la radiología y la medicina nuclear. El grado en que la industria, la agricultura y la ciencia dependen de las aplicaciones nucleares ha ido a más, y eso ha hecho que se demande una mayor producción de radioisótopos en los reactores de investigación. Estos reactores esenciales funcionan con sistemas informáticos que podrían ser vulnerables a los ciberataques. Al igual que las centrales nucleares, los reactores de investigación son instalaciones nucleares que requieren planes de protección similares para prevenir, mitigar posibles ataques dolosos y para responder a ellos. La protección de todo tipo de instalaciones nucleares frente a posibles ataques de este tipo es un elemento esencial del uso tecnológica y físicamente seguro de la tecnología nuclear en África.

Para contrarrestar estas amenazas, muchos países africanos están aprendiendo de la experiencia de Egipto, Ghana y Nigeria, cada uno de los cuales posee y opera un reactor nuclear de investigación. Con el apoyo del OIEA, estos tres países están elaborando y reforzando sus reglamentos sobre la seguridad informática y aplicando programas para proteger adecuadamente sus instalaciones contra actos informáticos dolosos que podrían repercutir en la seguridad nuclear tecnológica y física de las instalaciones.

"La seguridad informática sigue cobrando importancia a medida que las tecnologías digitales y los sistemas de base informática se integran en la seguridad tecnológica nuclear, la seguridad física nuclear y los aspectos operativos de las instalaciones y operaciones con materiales nucleares y otros materiales radiactivos, —afirma Trent Nelson, Oficial Superior de Seguridad Informática y de la Información de la División de Seguridad Física Nuclear del OIEA—. El OIEA trabaja con los países de África para desarrollar, examinar y mejorar los reglamentos sobre seguridad informática".

En Egipto, el OIEA colabora con la Autoridad Reguladora Nuclear y Radiológica de Egipto (ENRRA) para examinar la normativa vigente sobre seguridad informática y colmar posibles lagunas en los aspectos de reglamentación. En 2022 se organizó un curso nacional de capacitación para aumentar la capacidad de los países de llevar a cabo inspecciones de seguridad informática en instalaciones nucleares. Por medio de las orientaciones sobre seguridad física nuclear del OIEA y las técnicas a disposición de los inspectores, los participantes del curso recibieron los conocimientos y la experiencia práctica necesarios para evaluar mejor la eficacia de la seguridad informática en las instalaciones nucleares y radiológicas.

Nadia M. Nawwar, ingeniera informática de la Instalación de Producción de Radioisótopos (RPF) de la Autoridad de Energía Atómica de Egipto, figuró entre los 22 participantes en el curso. "Aprendí cómo realiza el órgano regulador las inspecciones de seguridad informática y cuáles son las disposiciones de seguridad informática necesarias de que debe disponer el operador —explicó—. Desde que participamos en el curso hemos podido examinar y validar los elementos del reglamento sobre seguridad informática con mayor efectividad. El curso nos ayudó a desarrollar y aplicar un programa de seguridad informática para proteger la información sensible de las instalaciones y los activos digitales de carácter estratégico vulnerables a los ciberataques".

En abril de 2023 el OIEA llevó a cabo una misión de expertos en Ghana con el objetivo de evaluar la actual normativa nacional de seguridad informática y el programa de inspecciones de la Autoridad Reguladora Nuclear de Ghana.

"El desarrollo de la seguridad informática en Ghana planteó varios desafíos, entre ellos la falta de conocimientos técnicos a escala local sobre la materia, la fusión de las cuestiones jurídicas y los conocimientos técnicos, y la forma de gestionar los recursos necesarios —explica Nelson Kodzotse Agbemava, Jefe de Equipo de la Sección de Ciberseguridad Nuclear de esa Autoridad—. Durante el proceso de elaboración del reglamento se solicitó el apoyo de expertos del OIEA y de otros países para garantizar un enfoque completo y sistemático de la seguridad informática".

Asimismo, el OIEA llevó a cabo una misión de expertos en Nigeria en octubre de 2022. "La necesidad de un marco legislativo y regulador eficaz para la seguridad informática fue identificada en 2019 a partir del examen del Plan Integrado de Apoyo a la Seguridad Física Nuclear (INSSP) liderado por el OIEA en el país —dice Ethel Ofoegbu, Oficial Superior de Reglamentación de la Autoridad Reguladora Nuclear de Nigeria (NNRA)—. En consecuencia, el OIEA evaluó el reglamento nacional de seguridad informática, detectó

En agosto de 2023 se pondrá en marcha el Curso de Redacción de Reglamentos sobre Seguridad Informática del OIEA, con el objetivo de ayudar a los países a elaborar sus reglamentos nacionales de seguridad informática

lagunas y proporcionó el asesoramiento necesario. Uno de los resultados fue la elaboración del proyecto de reglamento sobre seguridad informática de Nigeria para instalaciones y actividades nucleares y radiológicas". En la actualidad, Nigeria está examinando el proyecto de reglamento y planificando un curso de capacitación sobre inspecciones informáticas.

Teniendo en cuenta el creciente número de solicitudes de asistencia de los países, el OIEA está elaborando un documento técnico para ayudar a los países a establecer los elementos clave de la reglamentación de la seguridad informática. Asimismo, el OIEA está preparado para ayudar a muchos más países a redactar reglamentos en el ámbito de la seguridad informática cuando se ponga en marcha el Curso de Redacción de Reglamentos sobre Seguridad Informática del OIEA, en agosto de 2023. El objetivo del Curso es ayudar a varios países a elaborar simultáneamente sus reglamentos nacionales específicos de seguridad informática, en lugar de que el OIEA preste asistencia a los países de forma individual. Tras el taller inicial de agosto, el Curso se dictará con carácter semestral en todas las regiones. A través del trabajo conjunto, los participantes tendrán la oportunidad de redactar su estrategia nacional de seguridad informática, que constituye la base reglamentaria de un programa de seguridad informática robusto.

Innovación en la capacitación virtual en seguridad informática para instalaciones nucleares y radiológicas

Anjarika Strohal

Omnipresentes y en constante crecimiento, las tendencias de hoy en la esfera de las tecnologías digitales están cambiando nuestras vidas de manera rápida y considerable. Las infraestructuras críticas actuales, comprendidas las del ámbito de la energía nucleoeléctrica y otros usos pacíficos de la tecnología nuclear, dependen en gran medida de las tecnologías digitales para la fluidez y la fiabilidad de sus operaciones. Es probable que las promesas que encierran las nuevas tecnologías en rápida evolución, como la inteligencia artificial, para resolver problemas y mejorar las operaciones controladas digitalmente contribuyan a mejorar las aplicaciones nucleares. Por ello, hoy en día se utilizan y se tienen en cuenta en los diseños de reactores avanzados.

Lamentablemente, aunque estas tecnologías digitales aportan muchos beneficios, también pueden introducir muchas posibles y desconocidas vulnerabilidades, dada la amenaza omnipresente de intrusiones cibernéticas o ciberataques con fines dolosos contra instalaciones nucleares que podrían explotar estas mismas tecnologías.

El número y el alcance de los ciberataques, cada vez más sofisticados, han creado en la industria nuclear una demanda urgente de capacitación en materia de seguridad informática para instalaciones nucleares y radiológicas. A fin de ayudar a satisfacer esta demanda, el OIEA ha elaborado una serie de cursos de capacitación sobre temas que van desde los aspectos fundamentales de la seguridad informática hasta cuestiones más avanzadas de esa esfera para sistemas de instrumentación y control.

Al impartir estos cursos de capacitación personalizados, sofisticados y complejos, que ofrecen oportunidades de aprendizaje práctico a partir de la experiencia, el OIEA detectó la necesidad de contar con una plataforma en línea sencilla que permitiera normalizar el programa de estudios y posibilitara un uso más amplio y universal por las entidades de capacitación, sin la asistencia presencial del OIEA. Las restricciones a los viajes debido a la pandemia de COVID-19 y el uso generalizado de las tecnologías virtuales pusieron aún más de manifiesto esta necesidad y aceleraron la creación de la plataforma.

La herramienta de capacitación virtual, llamada “Learners”, tiene por objeto ofrecer a la comunidad nuclear cursos de capacitación flexibles y atractivos en materia de seguridad informática, facilitando materiales de capacitación y la adquisición de experiencia mediante ejercicios prácticos realizados en un entorno virtual. Los participantes solo necesitan una computadora y una conexión fiable a Internet para acceder a todos los materiales necesarios para el curso. “Se espera que la nueva plataforma desempeñe un papel fundamental para aumentar el grado de conciencia y mejorar la capacitación en materia de seguridad informática en aras de la seguridad física nuclear, crear una comunidad de expertos más sólida y ayudar a mejorar la seguridad tecnológica y física en las instalaciones nucleares y las relacionadas con material radiactivo”, declara Elena Buglova, Directora de la División de Seguridad Física Nuclear del OIEA.

Capacitación en seguridad informática
y otras actividades

A partir de junio de 2023, el OIEA pondrá la plataforma Learners a disposición de todo el mundo con el fin de mejorar la seguridad informática en las instalaciones nucleares, así como en las instalaciones y las actividades en que se utilizan fuentes radiactivas.

El Instituto Austriaco de Tecnología (AIT), centro colaborador del OIEA en materia de seguridad informática y de seguridad física de la información en aras de la seguridad física nuclear, estableció una alianza con el OIEA para crear la plataforma Learners.

"El entorno de aprendizaje virtual ofrece un inmenso valor para aumentar las capacidades operativas y estratégicas, ya que sirve de apoyo a diversos fines de capacitación —señala Helmut Leopold, Director del Centro de Seguridad Digital Tecnológica y Física del AIT—. Mediante la simulación de entornos reales, la plataforma permite a los participantes adquirir competencias prácticas y experiencia esenciales para una gestión eficaz de la seguridad física nuclear".

Aprender a mejorar la seguridad informática

La plataforma Learners del OIEA se encuentra a disposición de quienes lo soliciten para mejorar la capacitación en materia de seguridad física nuclear. La plataforma está diseñada para que sea fácil de usar por un público internacional y ofrece asistencia multilingüe. Cuenta con diversas prestaciones, como ejercicios guiados, valoraciones inmediatas, integración de presentaciones y soporte multipantalla, gracias a las cuales la plataforma es adaptable y accesible para que la utilicen entidades de capacitación y usuarios directos.

Learners está concebida como una plataforma para desarrollar, ofrecer y utilizar entornos simulados interactivos y se ha creado utilizando tecnologías de código abierto. Los módulos adicionales contemplan enfoques normalizados para las plataformas informáticas, el suministro de infraestructura y de software, que permiten compartir e intercambiar conocimientos fácilmente con los actuales proveedores de capacitación del OIEA y otras organizaciones que tengan la intención de utilizar la plataforma.

Se han creado 12 ejercicios prácticos organizados en seis esferas temáticas basadas en las orientaciones del OIEA sobre seguridad física nuclear centradas en la seguridad informática. "Al utilizar entornos virtualizados representativos de las instalaciones del mundo real, la plataforma Learners refuerza el desarrollo de competencias prácticas y contribuye a un acceso más equitativo a los conocimientos y las destrezas", añade la Sra. Buglova.

La plataforma Learners es una de las facetas de la labor del OIEA encaminada a concienciar, fortalecer la cooperación y prestar apoyo a los Estados para hacer frente a las crecientes amenazas a la ciberseguridad en el sector nuclear. En los últimos cinco años se han ofrecido actividades de capacitación a más de 120 países. Además, el apoyo adaptado mediante misiones de expertos; los cursos de capacitación nacionales, regionales e internacionales; las reuniones técnicas y los seminarios web han fomentado la colaboración activa, el intercambio de conocimientos y el desarrollo de competencias. El OIEA también ayuda a los países a organizar ejercicios de ciberseguridad a gran escala.

Un centro de capacitación práctica y demostraciones

De cara al futuro, es fundamental seguir invirtiendo en este tipo de iniciativas de creación de capacidad para garantizar los más altos niveles de seguridad física nuclear en todo el mundo. El moderno Centro de Capacitación y Demostración en materia de Seguridad Física Nuclear del OIEA abrirá sus puertas en el segundo semestre de 2023 a fin de ayudar a fortalecer la capacidad de los países para hacer frente al terrorismo nuclear mediante experiencias de capacitación práctica. Los innovadores cursos de capacitación ofrecidos en el Centro abarcarán temas relacionados con la seguridad informática e incluirán escenarios de ciberataques que podrían tener como objetivo instalaciones nucleares o instalaciones y actividades en las que se utilizan fuentes radiactivas.

Eventos por región

Cómo la inteligencia artificial cambiará la seguridad informática y la seguridad física de la información en el mundo nuclear

Mitchell Hewes

Las tecnologías de inteligencia artificial (IA) y aprendizaje automático podrían tal vez revolucionar el mundo y dar paso a un progreso y una innovación sin precedentes al transformar la forma en que creamos, consumimos y utilizamos la información. Las tecnologías de IA, conforme se vuelvan cada vez más sofisticadas, transformarán las industrias, racionalizarán los procesos e incluso podrán influir en nuestra manera de vivir. El sector nuclear no es la excepción, y cabe esperar que los beneficios de la IA se reflejen en muchos procesos y operaciones de las instalaciones nucleares y radiológicas.

Al mismo tiempo, el rápido avance de la IA también conlleva múltiples riesgos. Los agentes con fines dolosos pueden utilizar la IA para perpetrar ataques más avanzados y selectivos o explotarla para poner en riesgo la integridad de las redes, los sistemas y la información de carácter estratégico de las instalaciones nucleares y radiológicas.

Beneficios para la seguridad informática y la seguridad física de la información

El OIEA se prepara para las transformaciones que traerá consigo la IA fomentando la cooperación internacional en este ámbito a fin de garantizar que todos los países puedan beneficiarse de las oportunidades y, al mismo tiempo, prepararse para mitigar los riesgos. A través de mecanismos como reuniones técnicas y proyectos coordinados de investigación (PCI), el OIEA apoya el desarrollo, la difusión y la aplicación de técnicas de IA, así como las contramedidas y la defensa contra agentes con fines dolosos.

Tal vez la ventaja más significativa de la IA en el ámbito de la seguridad informática y la seguridad física de la información sea la menor dependencia de la intervención y el análisis humanos. Los sistemas basados en la IA pueden funcionar ininterrumpidamente para monitorizar las redes y los sistemas en busca de amenazas. Al automatizar estas tareas, los profesionales de la seguridad física nuclear tienen tiempo para centrarse en tareas más estratégicas y responder con mayor eficiencia a los incidentes cuando ocurren.

“Las capacidades de aprendizaje adaptativo de la IA pueden aprovecharse para mejorar la seguridad informática y la seguridad física de la información, ya que detectan con rapidez las amenazas y proporcionan automáticamente a los expertos humanos la información que necesitan para coordinar las actividades de respuesta, —afirma Fan Zhang, Profesora Adjunta del Instituto de Tecnología de Georgia en los Estados Unidos de América, que participó en un PCI de apoyo a la investigación para reforzar la seguridad informática—. No sustituirá la mano de obra, sino que creará recursos y conocimientos que harán de la detección y la respuesta tempranas en el ámbito de la seguridad informática objetivos realistas”.

Gracias a los algoritmos avanzados de aprendizaje automático, la IA también puede ayudar a las instalaciones nucleares y radiológicas a reforzar sus defensas contra los ciberataques mediante la detección de anomalías en los datos de los sistemas informáticos. Los sistemas de seguridad física asistidos por IA pueden monitorizar y analizar constantemente grandes cantidades de datos para determinar si se produce alguna actividad anómala en el funcionamiento normal de las instalaciones. Mediante los ciberataques se pueden introducir datos falsos para engañar con fines dolosos a los operadores de las instalaciones nucleares. En este caso, los sistemas asistidos por IA se pueden aprovechar para alertar a los responsables de una central nuclear de la más mínima variación en el funcionamiento normal. Al proporcionar un mayor conocimiento de la situación, la IA también permite detectar de forma temprana las acciones delictivas e impulsa la respuesta necesaria en caso de incidentes.

Desafíos que han de afrontarse

Los beneficios que ofrece la IA en las instalaciones nucleares y radiológicas dependen en gran medida de cómo se haya preparado el sistema de IA. La IA es tan inteligente como los datos de entrenamiento con los que trabaja y puede ser manipulada para ofrecer lecturas y resultados falsos si no dispone de los datos de entrada correctos, lo que sigue siendo un obstáculo importante para su uso en la esfera de la seguridad física nuclear. Incluso con los avances recientes en la tecnología de la IA, no es viable utilizarla como sustituto de un ser humano. La protección física, la contabilidad y el control de materiales nucleares y las mediciones directas —actividades esenciales para garantizar la seguridad física nuclear— requieren la intervención humana.

Otro desafío que presenta la IA en relación con la seguridad física nuclear es comprender cómo y por qué un modelo de IA ha tomado determinada decisión o ha hecho una predicción concreta. “La transparencia y la explicabilidad, que implica que las personas pueden entender la lógica que fundamenta las decisiones o las predicciones de la IA, son algunos de los problemas más importantes de los modelos de IA. A menudo no es fácil comprender cómo estos modelos llegan a

sus conclusiones, lo que dificulta confiar en sus resultados y garantizar la integridad de estos —señala Scott Purvis, Jefe de la Sección de Gestión de la Información de la División de Seguridad Física Nuclear del OIEA—. Ello se vuelve sumamente problemático cuando estos modelos sustituyen a los sensores que proporcionan mediciones directas y a la experiencia humana adquirida con las características singulares de cada instalación. Resulta poco factible ofrecer garantía alguna de la integridad del sistema sin un conocimiento avanzado previo exhaustivo de los algoritmos de IA para reconocer cómo y por qué se toman las decisiones".

Las orientaciones del OIEA sobre seguridad informática en aras de la seguridad física nuclear comprenden prácticas óptimas relativas a los sistemas de control humanos que sirven de guía a las instalaciones a la hora de determinar qué procesos pueden automatizarse mediante la IA y cuáles deben seguir contando con supervisión humana, al menos hasta que se conozcan los riesgos de esta tecnología en rápido desarrollo. También constituyen un recurso esencial que puede permitir a los países poner en marcha importantes medidas de seguridad informática para detectar y prevenir los ciberataques, así como para responder a ellos.

Además, el OIEA elaboró un PCI de apoyo a la investigación para reforzar la seguridad informática. Titulado "Mejora del análisis de incidentes de seguridad informática en instalaciones nucleares", el PCI reunió a representantes de 13 países con el fin de trabajar en la mejora de las capacidades de seguridad informática en instalaciones nucleares, incluidas las técnicas de IA, para detectar anomalías que indiquen ciberataques selectivos.

La carrera por adoptar tecnologías de IA

La IA ha demostrado su potencial para beneficiar a las personas que utilizan la tecnología nuclear con fines pacíficos. A medida que aumenta su uso para mejorar los procesos y las operaciones en las instalaciones nucleares y radiológicas, también debe aumentar la concienciación sobre los riesgos asociados a su adopción generalizada. Las organizaciones deben mantener un programa de seguridad informática robusto para garantizar la seguridad física nuclear mientras se benefician de la IA.

Para ello es necesario un cambio de paradigma fundamental en la forma de entender la confianza y el carácter estratégico. Hay que tener en cuenta todos los posibles puntos de fallo de un sistema, incluso los que no están relacionados con su diseño. Los agentes con fines dolosos pueden aprovechar la IA para crear programas maliciosos más sofisticados, automatizar ciberataques, explotar sesgos y vulnerabilidades de los modelos o eludir las medidas de seguridad física imitando el comportamiento de los usuarios legítimos. Esta "carrera de armamentos" entre defensores y detractores exigirá innovación y adaptación constantes.

La IA también puede ayudar a las instalaciones nucleares y radiológicas a reforzar sus defensas contra los ciberataques mediante la detección de anomalías en los datos de los sistemas informáticos. (Imagen: AdobeStock)

Un mayor uso de la tecnología de la IA para mejorar las medidas de seguridad informática en las instalaciones nucleares podría ofrecer importantes beneficios, entre ellos, una detección de amenazas optimizada, medidas de seguridad proactivas, una menor dependencia de la intervención humana y una mejor respuesta a los incidentes. Si aprovechan los beneficios de la IA y, al mismo tiempo, hacen frente a sus riesgos, las organizaciones pueden mejorar de manera considerable su seguridad informática ante la evolución de las ciberamenazas.

Cómo los ejercicios de seguridad informática ayudan a aumentar la preparación para responder a los ciberataques en la esfera de la seguridad física nuclear

Emma Midgley

Históricamente, las instalaciones nucleares se han concentrado en asegurar su material nuclear frente a ataques dolosos a través de medidas de protección física como armas de fuego, guardias y verjas. Estas medidas resultan efectivas aún hoy para amurallar las instalaciones nucleares, impidiendo el robo de material nuclear u otros materiales radiactivos, el sabotaje o el acceso no autorizado a los sistemas de control. Sin embargo, en las últimas décadas, la amenaza de los ciberataques se ha intensificado, en un mundo que tiende cada vez más a la digitalización. Cualquier país, incluso los que cuentan con los programas de investigación y energía nucleoeléctrica más avanzados, puede ser vulnerable a un ataque. Se ha hecho necesario elaborar marcos nacionales de seguridad informática y de respuesta contra las ciberamenazas a las instalaciones nucleares. Mediante ejercicios a gran escala, el OIEA brinda asistencia a los países para mejorar su protección contra los ciberataques y los ayuda a mejorar sus estrategias de detección y respuesta a los ciberataques contra las instalaciones nucleares.

El OIEA ha desarrollado ejercicios de seguridad informática para centrales nucleares e instalaciones radiológicas que se han llevado a cabo a escala nacional en todo el mundo. Estos ejercicios permiten a los países practicar y preparar su respuesta ante el peor de los escenarios posibles de vulneración de la ciberseguridad en una instalación nuclear. Los escenarios teóricos permiten determinar los puntos débiles de las políticas, los procedimientos y los procesos, e identificar las lagunas que deben colmarse mediante técnicas de mitigación, creación de capacidades y/o cambios organizativos. Además de ayudar a los Estados en la realización de ejercicios a gran escala para poner a prueba la seguridad informática en las instalaciones nucleares, las orientaciones del OIEA sobre seguridad física nuclear centradas en la seguridad informática también constituyen un recurso esencial que puede permitir a los países poner en marcha importantes medidas de seguridad informática para detectar, prevenir y responder a los ciberataques.

“Es fundamental desarrollar políticas, funciones y responsabilidades definidas y procedimientos detallados de respuesta a los incidentes de seguridad informática antes de que se produzca un incidente —afirma Trent Nelson, Oficial Superior de Seguridad Informática y de la Información de la División de Seguridad Física Nuclear del OIEA—. Esta es la esfera en la que el OIEA puede ayudar en muchos aspectos que van desde ejercicios y orientación, hasta compartir prácticas y procedimientos óptimos para garantizar una comunicación eficaz y una sólida protección de la seguridad”.

La vulnerabilidad de las instalaciones nucleares frente a los ciberataques se debe a varios factores, como las personas, la complejidad de la cadena de suministro y la información delicada compartida entre las múltiples partes interesadas que utilizan los sistemas informáticos que sustentan las funciones nucleares.

“Pensemos en un ataque en el que se compromete a un proveedor y se falsifica una orden de trabajo, haciendo que un técnico de confianza con acceso autorizado lleve a cabo una acción que sea ligeramente incorrecta —dice Trent Nelson—. Esta es una de las muchas formas que agentes con fines dolosos podrían encontrar para burlar los sistemas de seguridad”.

Un elemento importante para reducir el impacto que un ciberataque podría tener es la sensibilización y la comunicación efectiva entre las partes interesadas, ya que cualquiera de estos grupos, o de los individuos que forman parte de ellos, puede ser objeto de un ataque por parte de agentes dolosos. En la defensa de las instalaciones nucleares hay cuatro actores claves: el órgano regulador; el explotador de la instalación; las organizaciones de apoyo técnico (equipos de respuesta a incidentes de seguridad informática (CSIRT) y/o centros de operaciones para la seguridad informática); y las organizaciones externas, como proveedores y organizaciones de apoyo. La realización de ejercicios es una buena manera de poner a prueba las comunicaciones, la presentación de informes y las notificaciones entre las partes interesadas, así como de verificar y validar la seguridad tecnológica y la seguridad física de las estructuras organizativas.

Un elemento importante para reducir el impacto que un ciberataque podría tener es la sensibilización y la comunicación efectiva entre las partes interesadas.
(Imagen: AdobeStock)

Aunque en un escenario ideal a los ciberatacantes les resultaría imposible penetrar en los sistemas de seguridad informática de las instalaciones nucleares, la naturaleza cambiante de los agentes con fines dolosos, y la falibilidad de la naturaleza humana, hacen que sea casi imposible predecir cómo se desarrollará el próximo ataque a gran escala. Por lo tanto, la detección oportuna de los ataques es clave. En un ejercicio realizado recientemente en Eslovenia, un ciberataque teórico ayudó a verificar y validar las capacidades de detección y respuesta para defenderse de los ciberataques.

"La seguridad informática no es un proyecto ni un proceso, sino un viaje de por vida que requiere un esfuerzo, una atención y una práctica continuos —declara Samo Tomažič, Jefe de la División de Ciberseguridad de la Administración Eslovena de Seguridad Nuclear—. Ejercicios como el realizado en Eslovenia permiten a todas las entidades pertinentes del sector nuclear evaluar la solidez de sus planes de respuesta a incidentes en caso de ser objeto de un ciberataque".

En caso de incidente grave de seguridad informática que pudiera contribuir a un suceso de seguridad nuclear tecnológica o física, se debería contar con la ayuda de un CSIRT, además de con las partes interesadas habituales de una instalación nuclear. Un incidente de este tipo podría ocasionar, por ejemplo, el quebrantamiento de políticas o procedimientos de seguridad; efectos sobre los activos o sistemas digitales sensibles; o la pérdida de información sensible, así como del control de funciones críticas para la seguridad nuclear.

En este caso, una vez que se identifica un incidente de seguridad informática o se detecta que esta ha sido comprometida, el CSIRT trabaja con las partes interesadas de la instalación para investigar el incidente, recopilar datos forenses, analizar qué ocurrió y dónde, y prestar asistencia para contener y erradicar la intrusión a fin de ayudar a los explotadores a volver a poner en línea la instalación nuclear. Al final de la respuesta, se reúnen pruebas de informática forense para ayudar en cualquier investigación penal sobre el ataque y garantizar un intercambio de información eficaz con miras a seguir reforzando las medidas de seguridad informática en la instalación nuclear en el futuro.

En el ejercicio de Eslovenia, la detección de ciberataques fue esencial para poder responder a este incidente de seguridad teórico y probar y validar los procedimientos de respuesta a incidentes. Estos ejercicios sirven para poner a prueba la relación entre seguridad tecnológica, seguridad física y preparación para emergencias, y refuerzan los regímenes de seguridad física nuclear mediante la determinación de posibles puntos débiles y el desarrollo de los cambios necesarios para mejorar su preparación global ante posibles amenazas a la ciberseguridad. Además, estos ejercicios brindan la oportunidad de poner a prueba los canales de comunicación nacionales e internacionales para las notificaciones y la presentación de informes. En general, la realización periódica de ejercicios de seguridad informática es un aspecto importante del mantenimiento de la seguridad física de las instalaciones nucleares.

Proyectos coordinados de investigación para mejorar las técnicas de detección de anomalías en la seguridad informática

Rodney Busquim e Silva y Andrea Rahandini

La detección de anomalías en el funcionamiento de los sistemas informáticos que controlan funciones críticas de seguridad tecnológica y de seguridad física requiere amplios conocimientos especializados, y las medidas necesarias deben probarse, analizarse y ajustarse para que sean eficaces.

"La detección de anomalías desempeña un papel importante en la evaluación temprana de posibles amenazas contra los sistemas computarizados de instalaciones nucleares y radiológicas —afirma Scott Purvis, Jefe de la Sección de Gestión de la Información de la División de Seguridad Física Nuclear del OIEA—. Las técnicas de detección de anomalías suelen utilizan aplicaciones de la inteligencia artificial, como el aprendizaje automático, métodos basados en la estadística o los conocimientos y demás tecnologías". Estas tecnologías se utilizan para detectar desviaciones de las comunicaciones de red previstas o mediciones de procesos que pueden ser el primer indicio de que un intruso saltó las defensas de un sistema informático, y pueden detectar ciberataques en tiempo real.

Además, son importantes porque un agente con fines dolosos altamente capacitado puede introducir programas maliciosos que pongan en riesgo las funciones de seguridad tecnológica o de seguridad física de un sistema digital a la vez que falsifica los datos de sensores y los indicadores que se envían a un operador. Esto significa que el operador puede no saber que se está produciendo una actividad dolosa y, en un principio, reaccionará teniendo en consideración lo que se muestra en la sala de control, por lo que posiblemente tomaría una medida incorrecta. Solo mediante la detección automatizada de las más mínimas anomalías en un ciberataque de este tipo podría informarse correctamente a un operador.

Para abordar esta importante esfera de trabajo y otros desafíos relacionados con la seguridad informática, el OIEA puso en marcha un proyecto coordinado de investigación (PCI) específico en 2016.

La investigación y el desarrollo por medio de los PCI son una parte fundamental de las actividades del OIEA en materia de seguridad informática para la seguridad física nuclear. Estos proyectos producen un conjunto de investigaciones y conclusiones prácticas que complementan las iniciativas en curso del OIEA para fortalecer las capacidades de los países en materia de prevención, detección, respuesta y recuperación tras incidentes de seguridad informática que puedan afectar directa o indirectamente la seguridad nuclear tecnológica y física de instalaciones nucleares y radiológicas.

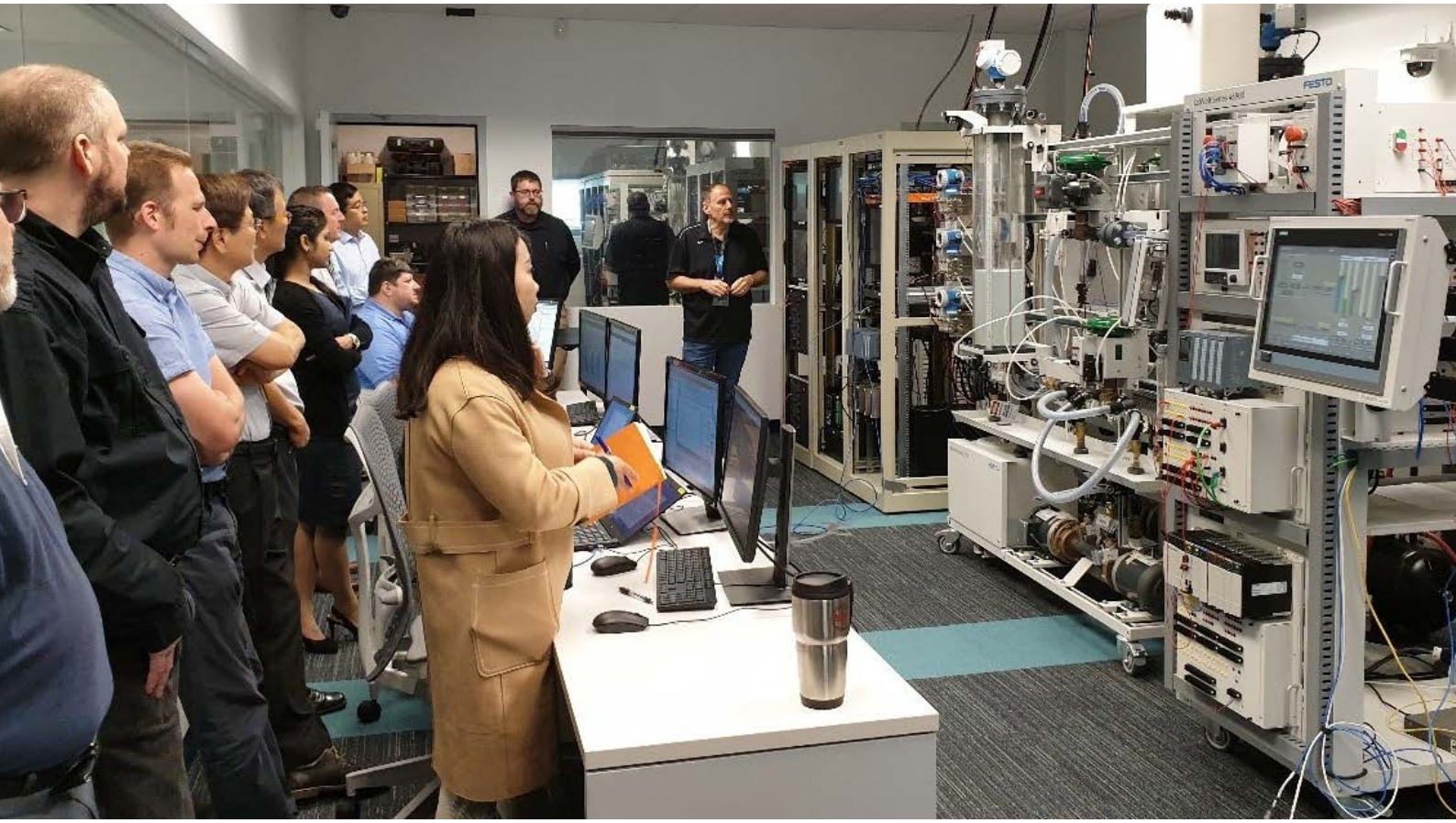
"Los adversarios son cada vez más sofisticados, y sus capacidades cibernéticas suponen desafíos cada vez mayores a la hora de desarrollar herramientas de detección de anomalías —dice el Sr. Purvis—. Para desarrollar técnicas de detección de anomalías es necesario acceder a datos de red y procesos de planta realistas y físicamente coherentes a fin de entrenar y probar los modelos de detección".

El escenario de ciberataques para crear capacidad

El PCI de 2016, titulado "Mejora del análisis de incidentes de seguridad informática en instalaciones nucleares", arrojó resultados importantes, por ejemplo, permitió seguir investigando herramientas y técnicas específicas que antes no se podían investigar sin el riesgo de exponer información sensible procedente de instalaciones nucleares y radiológicas.

El grupo del PCI, integrado por investigadores de 13 países y 17 organizaciones, creó una instalación ficticia, denominada Central Nuclear Asherah, y la Universidad de São Paulo creó un simulador (ANS) a partir de dicha instalación. Desarrollaron en conjunto escenarios realistas de ciberataque dentro de una instalación nuclear. Estos escenarios de ciberataque han permitido explorar y evaluar la eficacia de las medidas de seguridad informática y también las posibles consecuencias operativas de que un recurso digital se vea comprometido. Asimismo, el grupo trabajó en la obtención y el análisis de datos y en la elaboración y la puesta a prueba de técnicas para detectar ciberataques.

"Hemos desarrollado y utilizado el simulador ANS para generar un repositorio de datos a efectos de entrenar nuestros modelos de aprendizaje automático y evaluar su eficacia. El PCI del OIEA reunió a asociados internacionales para llevar a cabo investigaciones y creó nuevos conocimientos en este ámbito —expresa Ricardo Marques, profesor de la Escuela Politécnica de la Universidad de São Paulo (Brasil)—. La cooperación entre los participantes del PCI fue esencial para validar la labor realizada".



La Universidad de São Paulo desarrolló un simulador basado en una instalación ficticia denominada Central Nuclear Asherah.
(Fotografía: OIEA)

Los resultados prácticos del PCI también se han utilizado para la enseñanza y la capacitación continuas de un gran número de estudiantes de posgrado e investigadores de diversas disciplinas. Esto ha contribuido aún más a la investigación y los esfuerzos realizados con el objetivo de mejorar constantemente la seguridad informática en instalaciones nucleares y radiológicas.

"Parte de mi investigación como estudiante de doctorado se ha llevado a cabo utilizando el ANS y su interfaz persona-máquina, una interfaz que permite al usuario observar el simulador y comunicarse con él y que fue desarrollada en el marco del PCI del OIEA —cuenta Si Wen, estudiante de doctorado de la Universidad de Tsinghua (China)—. Llevé a cabo una investigación sobre técnicas de detección de anomalías, y el ANS fue clave para generar los datos necesarios para entrenar y evaluar un algoritmo de detección creado para centrales nucleares. Sin la colaboración entre todos los institutos participantes y las herramientas desarrolladas por el grupo del PCI, sería imposible llevar adelante mi investigación doctoral sobre la seguridad informática de los sistemas digitales de las centrales nucleares", agrega.

Los resultados prácticos del PCI —el ANS, las herramientas y las orientaciones— están a disposición de los institutos de investigación interesados de todo el mundo. Pueden conseguirse presentando al OIEA, a través de la autoridad nacional competente, un formulario de solicitud, que se encuentra disponible en el Portal de Información sobre Seguridad Física Nuclear (NUSEC) del OIEA.

Más recientemente, en 2023, el OIEA puso en marcha un nuevo PCI sobre la mejora de la seguridad informática para los sistemas de detección de radiaciones a fin de investigar metodologías y técnicas que mejoren la seguridad informática de los equipos de detección de radiación. Los proyectos de investigación previstos en el marco del nuevo PCI, con 12 organizaciones participantes (entre ellas, laboratorios nacionales, universidades e institutos nacionales de investigación) de 11 países, abordarán el uso de tecnologías digitales emergentes, como la computación en la nube, y seguirán estudiando y desarrollando técnicas innovadoras de detección de anomalías.

Garantizar la seguridad de las tecnologías digitales de la próxima generación de reactores nucleares

Joanne Liou

Aunque todas las innovaciones traen consigo potenciales beneficios que podrían transformar las industrias, también conllevan potenciales riesgos. En el ámbito nuclear, los reactores nucleares avanzados, incluidos los reactores modulares pequeños (SMR), están incorporando tecnologías innovadoras, sobre todo digitales, que aportan soluciones novedosas.

Existe un creciente interés por los SMR. Estos reactores nucleares avanzados tienen una capacidad de potencia limitada, generalmente de hasta 300 MW(e) por unidad, lo que representa cerca de un tercio de la capacidad de generación de los reactores nucleares de potencia tradicionales. No obstante, el uso de tecnología digital de vanguardia en estos nuevos reactores plantea nuevos desafíos en materia de seguridad nuclear tecnológica y física. En todo el mundo hay más de 80 diseños y conceptos de SMR que se encuentran en diferentes fases de desarrollo.

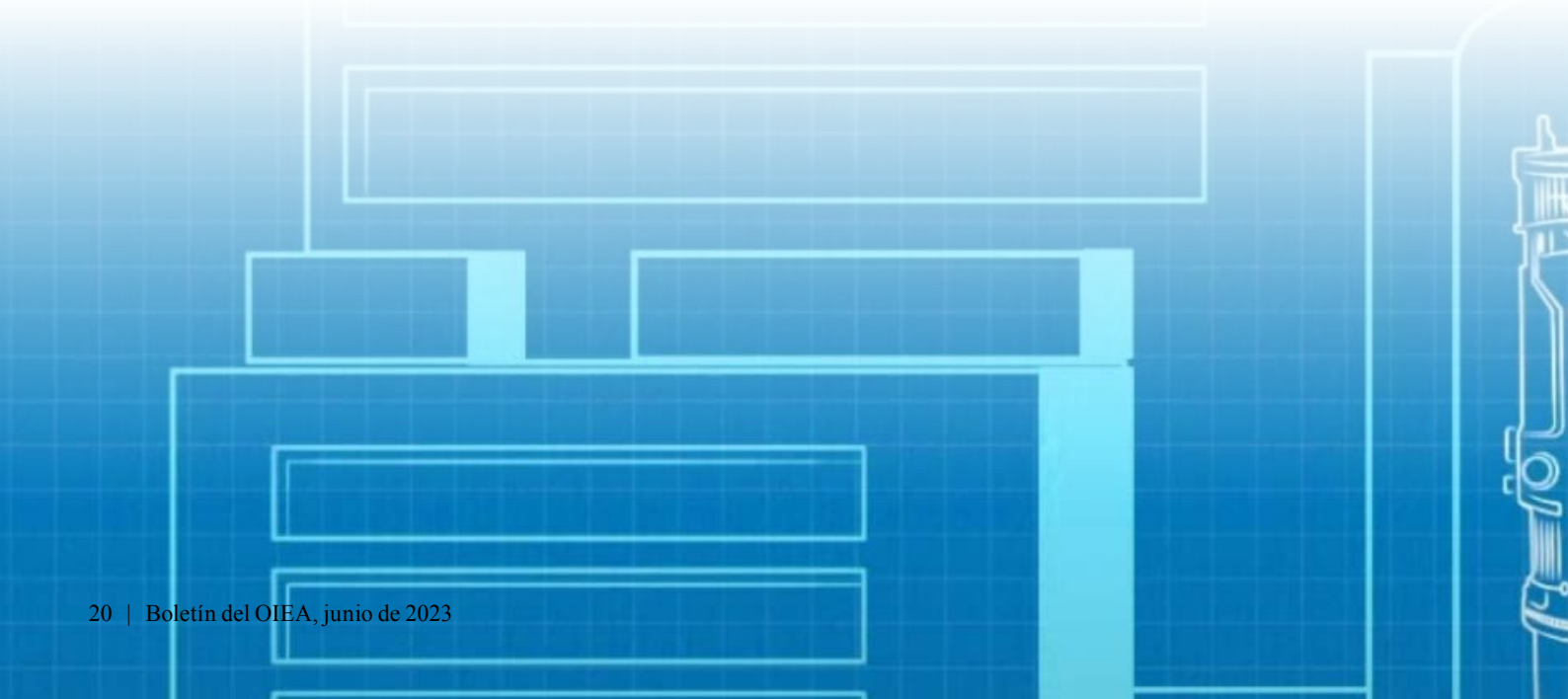
"Uno de los desafíos para el despliegue de SMR es de qué manera acelerar el desarrollo de la tecnología que utilizan y demostrar su nivel de preparación y, al mismo tiempo, mantener el cumplimiento de las normas de la seguridad nuclear tecnológica y física —declara Rodney Busquim e Silva, Oficial de Seguridad de la Tecnología de la Información del OIEA—. Esto reafirma la necesidad de considerar y mantener soluciones de instrumentación y control digitales y de seguridad informática durante el ciclo de vida de los SMR".

Soluciones y desafíos informáticos

Los innovadores diseños de los SMR se basan en sistemas de instrumentación y control digitales que hacen posibles sus características innovadoras. El hecho de que cada vez se necesiten más tecnologías digitales para la automatización, el control de supervisión y el mantenimiento a distancia, junto con otras características novedosas, pone de relieve la necesidad de soluciones informáticas.

Algunos SMR están diseñados para el despliegue de la energía nucleoeléctrica en zonas aisladas y con un número reducido de personal sobre el terreno, lo que puede hacer necesaria la monitorización a distancia constante y fiable. Dado el diseño de los sistemas de instrumentación y control digitales, la aplicación de medidas de seguridad informática debería ser un requisito previo para una comunicación segura entre el emplazamiento del SMR y un centro de apoyo. "De la necesidad de intercambiar información pueden surgir vías susceptibles de ser explotadas por ciberdelincuentes, por lo que se deben aplicar consideraciones de ciberseguridad robustas a la infraestructura de comunicación —señala Mike St. John-Green, experto en seguridad informática que reside en el Reino Unido—. Es preciso proteger la confidencialidad, la disponibilidad y la integridad de la información en las operaciones a distancia para garantizar el funcionamiento seguro y fiable de los SMR y la infraestructura conexa".

La inteligencia artificial (IA) y el aprendizaje automático también apoyan las operaciones de los SMR. La IA comprende las tecnologías que producen sistemas capaces de rastrear problemas complejos, mientras que las tecnologías de aprendizaje automático "aprenden" cómo realizar una tarea concreta sobre la base de los datos disponibles. Al combinar simulaciones digitales de instalaciones nucleares y sistemas de vigilancia y control con sistemas de IA, la industria nuclear busca optimizar funciones complejas, lo que podría aumentar la eficiencia operacional. Sin embargo, estas ventajas llevan aparejada la posibilidad de ciberataques. Por ejemplo, los algoritmos de software de los que se sirven la IA y el aprendizaje automático dependen de bases de datos que



podrían ser objeto de manipulación para provocar errores en el proceso de toma de decisiones de la IA.

"Estos sistemas pueden ser objeto de inyección de código, por ejemplo, que consiste en alimentarlos intencionadamente con datos corruptos durante el proceso de desarrollo, distribución o instalación del software. El desafío general radica en cómo infundir suficiente transparencia a los algoritmos de IA y aprendizaje automático. El uso aceptable de la IA y el aprendizaje automático debe estar claramente definido con unos niveles de riesgo aceptables", afirma Si Wen, estudiante de doctorado de la Universidad de Tsinghua de China.

Seguridad física desde el diseño

Los expertos coinciden en que la seguridad informática de las instalaciones nucleares debe tenerse en cuenta desde buen principio. Esta lógica proactiva, denominada "seguridad física desde el diseño", se inspira en las prácticas óptimas y las lecciones extraídas de la experiencia del pasado y recoge el concepto de "incorporación en el diseño" que también se aplica en los ámbitos de la seguridad tecnológica nuclear, las salvaguardias y la clausura de instalaciones.

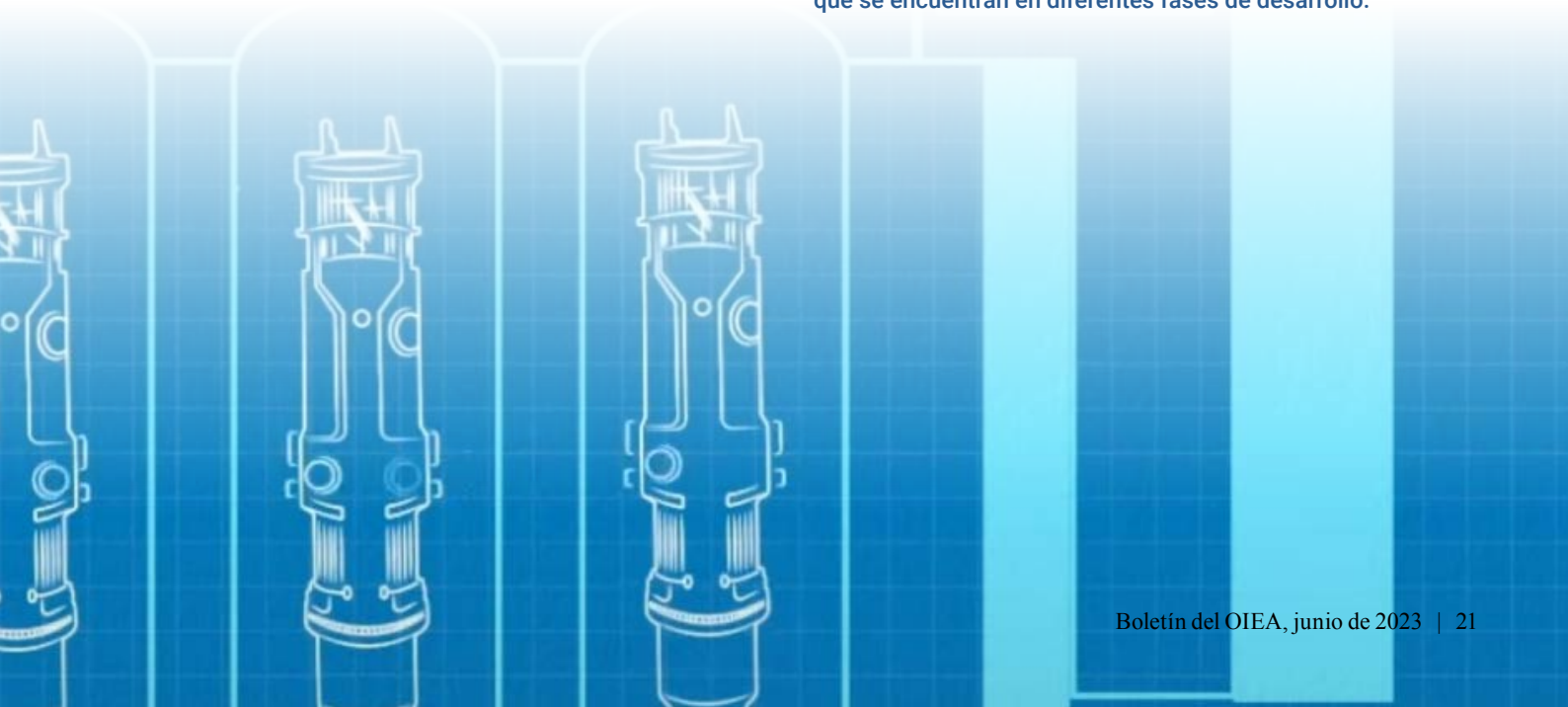
La seguridad informática desde el diseño tiene como objetivo reducir los riesgos para la seguridad física en su origen mediante un enfoque que contemple la seguridad física sistemática y constante a lo largo de todas las fases de la vida útil de la instalación o el proceso. "Las medidas de seguridad informática deben tomarse en cuenta y mantenerse durante todo el ciclo de vida de los SMR, desde el diseño hasta la clausura, pasando por la operación —afirma el Sr. Busquim e Silva—. Si piensan en la seguridad física, incluida la ciberseguridad, desde buen principio, los creadores de instalaciones pueden tomar decisiones relativas al diseño que las hagan más seguras desde el punto de vista tecnológico y físico, eficientes y eficaces en función del costo".

La función del OIEA

El OIEA conecta expertos, de organizaciones nucleares y de otra índole, con el objetivo de examinar y detectar los problemas y los desafíos relacionados con la seguridad informática que plantean las características tecnológicas y operacionales de los SMR. Por ejemplo, en febrero de 2022, el OIEA celebró una reunión técnica sobre sistemas de instrumentación y control y seguridad informática para SMR con el fin de promover la cooperación y facilitar el intercambio de información entre expertos internacionales. Los participantes coincidieron en la necesidad de armonizar los enfoques y los reglamentos nacionales para lograr la viabilidad del mercado internacional de los SMR. "En lo que respecta a los SMR normalizados, las soluciones de instrumentación y control abren un ámbito técnico completamente nuevo. La creciente automatización necesaria para los nuevos modos de operación y el amplio uso de sistemas digitales exigen medidas de seguridad informática y soluciones de ingeniería desde el nivel del diseño para garantizar un funcionamiento tecnológica y físicamente seguro de la central", señala Jorge Casanova de la Autoridad Regulatoria Nuclear de la Argentina, quien asistió a la reunión.

Además, en marzo de 2023, el OIEA organizó un taller para seguir estudiando la creación de capacidades técnicas relacionadas con la seguridad informática y la instrumentación y el control para SMR. Asimismo, el OIEA tiene previsto iniciar un proyecto coordinado de investigación sobre el tema en 2024.

En todo el mundo hay más de 80 diseños y conceptos de SMR que se encuentran en diferentes fases de desarrollo.



Una seguridad informática más fuerte para garantizar la seguridad nuclear tecnológica y física

Lydie Evrard
Directora General Adjunta y Jefa del Departamento de Seguridad Nuclear Tecnológica y Física

La seguridad tecnológica nuclear y la seguridad física nuclear tienen el mismo objetivo y la misma visión: proteger a las personas, a las sociedades y al medio ambiente de los posibles efectos nocivos de la radiación ionizante. Aunque las actividades que abordan la seguridad tecnológica nuclear y la seguridad física nuclear son diferentes, es fundamental establecer un enfoque bien coordinado de gestión de la interrelación entre esas dos esferas. Es importante garantizar que se pongan en práctica medidas pertinentes de manera que se aprovechen las oportunidades para la mejora mutua, sin comprometer ni la seguridad tecnológica ni la seguridad física.

Bien se sabe que en las instalaciones nucleares y radiológicas se precisan medidas y sistemas de seguridad física para proteger los equipos, sistemas y dispositivos, que normalmente tienen por objeto mantener la seguridad tecnológica, de un acto deliberado de sabotaje que pudiera provocar una emisión con consecuencias radiológicas. Por lo general, en los antiguos diseños y aplicaciones, los sistemas de seguridad debían protegerse únicamente con medidas de protección física. Sin embargo, las tendencias tecnológicas actuales, crecientes y omnipresentes están ampliando considerablemente el papel de los sistemas digitales en la eficiencia de las operaciones en las instalaciones nucleares y radiológicas, particularmente, en relación con los responsables de importantes funciones de las instalaciones, como los sistemas de instrumentación y control, entre ellos, los que se utilizan para fines de seguridad tecnológica y seguridad física.

La seguridad de estos sistemas requiere una vigilancia estricta a fin de detectar las vulnerabilidades e impedir el acceso no autorizado a los sistemas de control digital que puedan poner en riesgo las funciones de seguridad tecnológica o de seguridad física. En este sentido, la seguridad informática está cobrando cada vez mayor importancia respecto de la interacción entre la seguridad tecnológica y la seguridad física, y se está abordando como parte de otras esferas fundamentales como la infraestructura de reglamentación; las disposiciones técnicas del diseño y la construcción de establecimientos nucleares; los controles de acceso a estos establecimientos; la clasificación de las fuentes radiactivas; la gestión de fuentes radiactivas y el material radiactivo, incluido el combustible gastado y los productos de los desechos radiactivos; la detección y la recuperación de fuentes huérfanas y los planes de respuesta a emergencias y de contingencia.

A nivel nacional, los encargados de la formulación de políticas deben considerar conjuntamente la seguridad física nuclear y la seguridad tecnológica nuclear a la hora de elaborar el reglamento sobre seguridad informática. La asignación clara de responsabilidades, el liderazgo y la gestión del riesgo son la base de la interrelación entre la seguridad tecnológica y la seguridad física y tienen la misma importancia de cara a la implementación de medidas eficaces en materia de seguridad informática. A la vez, la seguridad informática es un desafío intrínseco a nivel mundial.

En este contexto, se reconoce ampliamente la importancia de la cooperación internacional y el papel central del OIEA. La interrelación entre la seguridad tecnológica nuclear y la seguridad física nuclear se pone de relieve en las normas de seguridad y en las orientaciones sobre seguridad física nuclear del OIEA. Desde hace aproximadamente un decenio, el OIEA ha estado desarrollando y ofreciendo a los países un conjunto exhaustivo de medios de asistencia en el ámbito técnico de la seguridad física de la información y de la seguridad informática, prestándoles apoyo en la adopción de medidas eficaces contra los ciberataques que podrían afectar la seguridad física nuclear. Además, el OIEA brinda apoyo en el establecimiento de sinergias entre los sistemas y las medidas de seguridad tecnológica nuclear y seguridad física nuclear al objeto de garantizar que las medidas adoptadas en los dos ámbitos se complementen en lugar de contraponerse.

De cara al futuro, los avances tecnológicos continuarán aumentando la importancia de contar con una seguridad informática sólida en relación con la seguridad nuclear tecnológica y física a nivel de los Estados y de las instalaciones. Las tecnologías en rápida evolución, como la inteligencia artificial, son prometedoras en lo que se refiere a la resolución de algunos problemas y a la mejora de las operaciones controladas digitalmente y, al mismo tiempo, plantean nuevos desafíos que hay que afrontar. De manera similar, las tecnologías inalámbricas y de automatización se están considerando y utilizando en la actualidad en diseños de reactores nucleares avanzados, como los reactores modulares pequeños y los microrreactores. Dado que las ciberamenazas evolucionan constante y rápidamente, el apoyo del OIEA a las necesidades de los Estados Miembros para fortalecer la seguridad informática en aras de la seguridad nuclear tecnológica y física deber ser ágil para mantenerse al corriente de todas las nuevas oportunidades y desafíos de estas nuevas tecnologías con el fin de proporcionar normas, prácticas óptimas, capacitación y directrices más eficientes. Esto es a lo que apunta continuamente el Departamento de Seguridad Nuclear del OIEA.

Contrarrestar las amenazas en un mundo cada vez más digitalizado

Wolfgang Picot

En mayo de 2022, el Instituto Austríaco de Tecnología (AIT) pasó a ser el primer centro colaborador del OIEA en seguridad informática y seguridad física de la información en aras de la seguridad física nuclear. El AIT presta apoyo a cursos y ejercicios internacionales y regionales de capacitación en el ámbito de la seguridad informática para instalaciones y actividades nucleares, desarrolla módulos de demostración técnica para crear más conciencia acerca de las ciberamenazas, y contribuye a la elaboración de materiales de capacitación para el nuevo Centro de Capacitación y Demostración en materia de Seguridad Física Nuclear, ubicado en Seibersdorf.

Hablamos con el Director del Centro de Seguridad Tecnológica y Física del AIT, Helmut Leopold, para comprender mejor en qué consiste esta cooperación.

P: ¿Cuáles son, en general, los riesgos y amenazas emergentes en materia de seguridad informática?

R: Hoy en día muchos dispositivos digitales modernos se construyen pensando en redes más extensas.

Muchos de ellos necesitan acceso a Internet para funcionar. Todo desarrollo de software entraña posibles errores que pueden dar lugar a vulnerabilidades. El número de amenazas contra la seguridad física que afectan al funcionamiento de los sistemas de tecnologías de la información (TI) aumenta a la luz de la escasa protección de las interfaces y la irresponsabilidad de los usuarios. Los atacantes se aprovechan de las vulnerabilidades de los sistemas digitales para lograr el acceso.

El desarrollo de métodos y herramientas de ataque discurre en paralelo al de los procesos de innovación digital. En Internet se encuentran fácilmente programas informáticos para piratas informáticos, lo que facilita los ataques, incluso para atacantes menos competentes. Nos enfrentamos a un diverso ecosistema de ciberataques impulsado por la delincuencia organizada, el espionaje económico e industrial y el terrorismo cibernético.

Así pues, hoy en día, usuarios, empresas y autoridades se ven amenazados por un amplio espectro de ciberataques que, acompañados de campañas específicas de desinformación, pueden afectar la infraestructura digital de Estados enteros, sacudiendo así los cimientos de nuestras sociedades.

P: ¿La industria nuclear se enfrenta a los mismos desafíos?

R: Los negocios y los distintos consumidores utilizan principalmente tecnologías de la información (TI) basadas en datos y orientadas a la comunicación. Por el contrario, las instalaciones de producción y las infraestructuras críticas emplean la llamada tecnología operativa (TO) que monitoriza y controla los comportamientos y los resultados prácticos de procesos de producción definidos. Tradicionalmente, la TO ha estado mucho menos interconectada que la TI, pero los avances tecnológicos han acercado a estos dos campos, haciendo que el *software* y los dispositivos de TO se conecten, cada vez más, a redes de mayor amplitud.

Este desarrollo resulta problemático, pues hay menor conciencia acerca de la ciberseguridad en el campo de la TO que en el de la TI.

Por ello, estas nuevas amenazas para la seguridad física de las TI se vuelven pertinentes para la TO de producción industrial e infraestructura crítica. Asimismo, esta cuestión es cada vez más importante para la industria nuclear, que tradicionalmente tenía un enfoque conservador y mantenía aislados los sistemas de control.

P: ¿Qué actividades lleva adelante el AIT con el fin de mejorar la ciberseguridad en el ámbito de la seguridad física nuclear?

R: El programa de investigación del AIT examina cómo escenarios de amenazas cambiantes podrían repercutir en los sistemas de TO, y tiene por objeto desarrollar conocimientos técnicos y nuevas soluciones para aumentar la resiliencia de las infraestructuras críticas frente a los ciberataques. Este trabajo constituye la base para el desarrollo de nuevas normas mundiales de seguridad física, procedimientos de certificación para elementos críticos del sistema y nuevas arquitecturas del sistema que incorporen medidas sólidas de ciberseguridad en los sistemas de TO desde la etapa inicial del diseño.

El AIT ofrece asimismo una enseñanza y capacitación integrales como preparación frente a ataques contra la ciberseguridad. En simulaciones complejas de sistemas informáticos “virtualizados”, denominadas “cyber ranges”, los usuarios, los desarrolladores de sistemas, el personal de operación y los representantes gubernamentales reaccionan ante escenarios realistas de ciberataques. Esta clase de simulación es fundamental para garantizar que los sistemas de TI y TO son resilientes y pueden repeler eficazmente las ciberamenazas.

P: ¿Qué ventajas plantea el entorno de aprendizaje virtual desarrollado por el AIT y el OIEA?

R: La experiencia práctica es el proceso de aprendizaje más eficaz. El AIT y el OIEA desarrollaron un "cyber range" que ofrece la posibilidad de crear "gemelos digitales" de las infraestructuras digitales críticas existentes, en el que, además, se imparte capacitación en escenarios de aplicación muy realistas.

En él, los usuarios gubernamentales y de la industria pueden evaluar y someter a prueba la eficacia de los mecanismos de protección y los procesos institucionales u operacionales.

Las experiencias del "cyber range" respaldan la creación de capacidades de defensa sostenibles, tanto para las organizaciones públicas como privadas.

P: Además de la capacitación virtual, ¿de qué manera promueve el AIT la seguridad física nuclear con su trabajo y sus conocimientos especializados?

R: Podemos ayudar en la defensa frente a atacantes, por ejemplo, desarrollando software para monitorizar dispositivos perimetrales que suelen conectar las redes internas de las organizaciones a Internet. Antes de causar daños, los atacantes suelen servirse de estos dispositivos como puntos de entrada al sistema.

Aplicamos nuestra experiencia en detección de anomalías para entrenar el software de análisis que monitoriza los dispositivos perimetrales de uso común en un determinado tipo de instalación nuclear.

Ese software puede activar una alarma o adoptar contramedidas si un dispositivo actúa de forma extraña. Así, los operadores pueden detectar y desalentar prontamente los ciberataques antes de que estos puedan causar perjuicios significativos.

P: Hace un año, el AIT fue designado primer centro colaborador del OIEA en seguridad informática al servicio de la seguridad física nuclear, y sigue siendo el único centro de este tipo a día de hoy. ¿Qué significa esto para la labor del AIT?

R: Estamos sumamente orgullosos de haber sido designados centro colaborador, y seguimos brindando apoyo para impartir un curso regional de capacitación sobre seguridad informática aplicada a los sistemas de instrumentación y control en el sector nuclear. El curso se dictó dos veces en 2022, y algunos de los resultados prácticos de nuestro proyecto conjunto se emplearon para desarrollar una plataforma de aprendizaje virtual.

Asimismo, hemos participado en actividades relacionadas con la seguridad informática en el desarrollo de reactores modulares pequeños.

En la actualidad prestamos asistencia al OIEA para la preparación de la Conferencia Internacional sobre Seguridad Informática en el Mundo Nuclear: la Seguridad Física en aras de la Seguridad, que tendrá lugar en 2023 y en la que ofreceremos demostraciones de nuestra plataforma de capacitación virtual, presidiremos mesas redondas y presentaremos artículos relacionados con nuestra investigación en el sector, entre otras cosas.

P: ¿Cómo colabora el AIT con el Centro de Capacitación y Demostración en materia de Seguridad Física Nuclear?

R: Hemos estado trabajando codo a codo con nuestros colegas del OIEA para desarrollar módulos de capacitación, demostraciones y ejercicios para el Centro de Capacitación y Demostración en materia de Seguridad Física Nuclear. Incorporamos módulos sobre seguridad informática en los cursos de capacitación relacionados con la protección física de materiales nucleares y otros materiales radiactivos, así como aquellos vinculados a la detección y respuesta en relación con materiales nucleares y otros materiales radiactivos no sometidos a control reglamentario. Este arreglo tiene por objeto reforzar el concepto de que la seguridad informática es un elemento integral e indisociable de la seguridad física nuclear.

Cómo la colaboración internacional mantiene al mundo a salvo de las ciberamenazas

Tighe Smith es el Coordinador de la norma IEC SC45A WGA9. Ha sido designado por un comité para dirigir el grupo de trabajo A9 de la Comisión Electrotécnica Internacional (IEC), dedicado a la ciberseguridad.

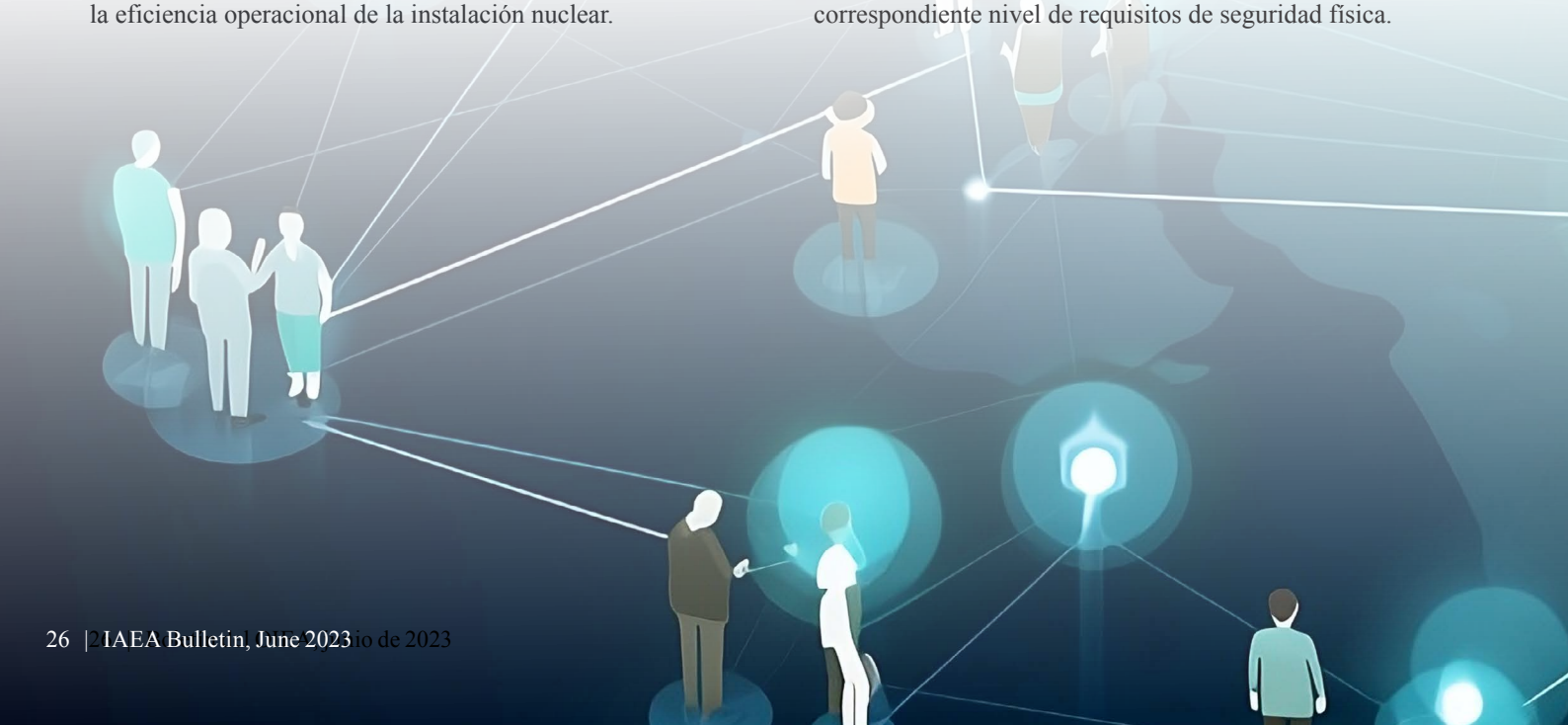
La IEC es una organización mundial sin fines de lucro que elabora normas internacionales para el diseño, la construcción y la operación de equipos eléctricos, incluidos los utilizados en las centrales nucleares. Fundada en 1906, la IEC reúne a más de 170 países y ha publicado 10 000 normas internacionales IEC.

La industria nuclear se enfrenta a un desafío importante a la hora de mantener la seguridad informática, debido al uso generalizado de dispositivos digitales. Esta tendencia se observa claramente en la vida cotidiana, donde los frigoríficos inteligentes, la iluminación y otros dispositivos controlados a distancia a través de la computación en la nube se han convertido en algo habitual. Muchos sistemas de las instalaciones nucleares que antes no tenían componentes digitales hoy en día los llevan incorporados. Su potencia computacional, su naturaleza reprogramable y su capacidad de interconexión aportan una eficiencia sin igual en apoyo de las operaciones y la seguridad nuclear tecnológica y física.

Los reactores modulares pequeños y otros nuevos diseños de reactores se están desarrollando en un mundo en que prima lo digital, con un uso de los sistemas informáticos aún más extendido que en diseños anteriores. Estos reactores pueden estar concebidos para funcionar a distancia o incluso de forma autónoma, utilizando una infraestructura de red informática para comunicarse con un operador central. Gracias a este planteamiento los operadores y los sistemas automatizados pueden analizar grandes volúmenes de datos e incrementar así la eficiencia operacional de la instalación nuclear.

Sin embargo, esta modernización digital de la industria nuclear trae consigo más desafíos, ya que, sin una seguridad informática adecuada, los puntos débiles o vulnerabilidades podrían ser explotados por agentes con fines dolosos en ataques contra una de estas instalaciones.

A fin de hacer frente a los desafíos que plantea la rápida evolución de la tecnología digital en las instalaciones nucleares, y dada la necesidad de contribuir a la armonización de los enfoques que aplican los distintos países e instalaciones, la Comisión Electrotécnica Internacional (IEC) ha adoptado un enfoque basado en las consecuencias y el conocimiento de los riesgos que se ajusta a las orientaciones sobre seguridad informática y seguridad física de la información de la *Colección de Seguridad Física Nuclear del OIEA*. En lugar de un enfoque prescriptivo, recomendamos un enfoque graduado, que permita a las organizaciones determinar el nivel de control necesario para un producto o proceso en función de las posibles consecuencias de un ciberataque. Por ejemplo, el primer paso en un programa de seguridad informática es examinar las funciones de la instalación nuclear, evaluar sus efectos en la seguridad tecnológica y física y determinar el correspondiente nivel de requisitos de seguridad física.



Prevención, detección y mitigación

Dado que predecir cómo evolucionarán los ciberataques en el futuro es todo un reto, la IEC ha colaborado estrechamente con el OIEA y ha elaborado normas que recomiendan que los programas de seguridad informática de las instalaciones nucleares se centren en la detección, la respuesta y la recuperación, además de la prevención. Incluso si los elementos de un ciberataque logran su objetivo, debería disponerse de mecanismos que permitan restablecer las funciones necesarias y asegurar su correcto desempeño para garantizar que la seguridad tecnológica y física no se vean comprometidas.

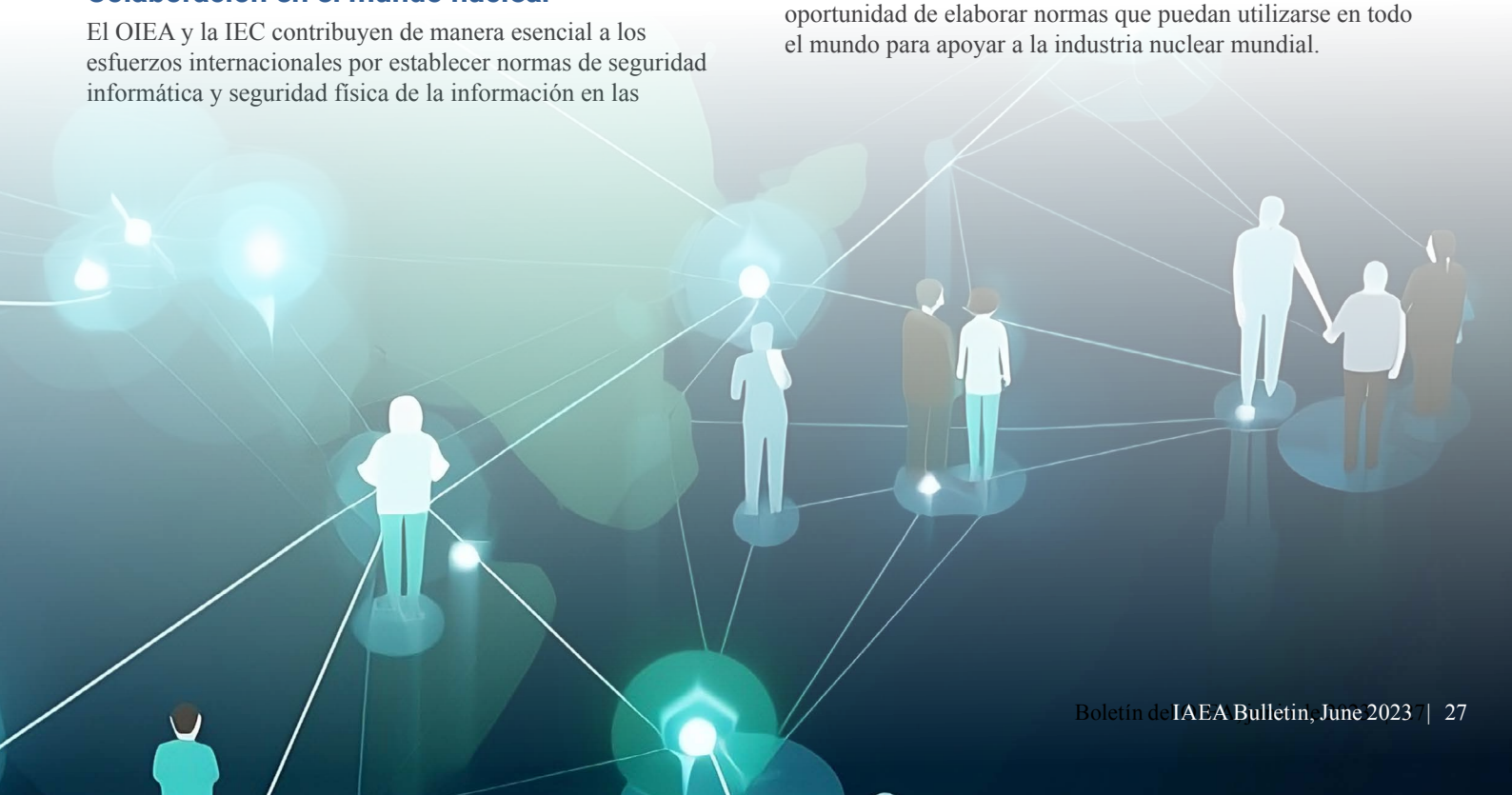
La rápida digitalización de nuestro mundo, sumada a la expansión de la inteligencia artificial y el aprendizaje automático, puede hacer que la seguridad informática en las instalaciones nucleares parezca una cuestión abrumadora. La colaboración internacional es crucial para que estas instalaciones sigan funcionando en condiciones tecnológica y físicamente seguras a pesar de esos desafíos. Desde hace más de medio siglo, el OIEA, la comunidad internacional y la industria nuclear colaboran en la labor de normalización para contribuir a la seguridad tecnológica y física de la tecnología nuclear con fines pacíficos. En un contexto en que cuestiones mundiales como el cambio climático y la seguridad energética se están volviendo más acuciantes, muchos países buscan en la tecnología nuclear nueva e innovadora una forma de generar energía con bajas emisiones de carbono, con lo que la normalización es aún más importante para mantener la seguridad tecnológica y física de las instalaciones nucleares.

Colaboración en el mundo nuclear

El OIEA y la IEC contribuyen de manera esencial a los esfuerzos internacionales por establecer normas de seguridad informática y seguridad física de la información en las instalaciones nucleares. El OIEA elabora publicaciones de orientación en el marco de la *Colección de Seguridad Física Nuclear* mediante consenso internacional, en las que se exponen conceptos y normas para garantizar la seguridad informática y seguridad física de la información como elementos fundamentales para alcanzar los objetivos de seguridad física nuclear. En la *Colección de Seguridad Física Nuclear* se ofrecen orientaciones sobre la organización de los recursos de los Estados y la formulación de reglamentos y conceptos de la industria para aplicar un enfoque de ingeniería con base cibernética en las instalaciones nucleares.

Como organización internacional de normalización que promueve prácticas óptimas y el intercambio de conocimientos, la IEC colabora estrechamente con el OIEA. En el marco del memorando de entendimiento entre la IEC y el OIEA, científicos y expertos que trabajan con la IEC elaboran normas e informes técnicos sobre la aplicación de las orientaciones del OIEA a través de requisitos programáticos y de ingeniería concretos. Estos requisitos pueden ser de utilidad para el diseño y la creación de sistemas digitales en la actualidad y en el futuro, que pueden certificarse si se ajustan a los modelos reguladores en consonancia con las orientaciones del OIEA. De esta manera, los expertos que representan la experiencia de la industria nuclear en la aplicación de las normas IEC pueden apoyar la elaboración de futuras versiones de las orientaciones del OIEA.

Los científicos y los expertos contribuyen a la labor de la IEC de forma voluntaria, y siempre serán bienvenidos quienes deseen sumarse a ella. La comunidad de expertos en seguridad informática del ámbito nuclear es relativamente pequeña, incluso a escala mundial. Al colaborar con la IEC se tiene la oportunidad de elaborar normas que puedan utilizarse en todo el mundo para apoyar a la industria nuclear mundial.



Código de Conducta del OIEA

20 años de avances en la seguridad tecnológica y la seguridad física de las fuentes radiactivas

Oradores del evento paralelo "La Igualdad de Género y la Inclusión, y el Código de Conducta sobre Seguridad Tecnológica y Física de las Fuentes Radiactivas: 20 Años de Avances". (Fotografía: W. Wawrzuta/OIEA)

En mayo de 2023, más de 270 expertos jurídicos y técnicos procedentes de 128 países y de 4 organizaciones internacionales se reunieron en Viena (Austria) para examinar los avances logrados en la seguridad tecnológica y la seguridad física de las fuentes radiactivas y para abordar esferas que requieren mejoras.

Las fuentes radiactivas desempeñan una función indispensable en muchos ámbitos. En la medicina, ayudan a tratar el cáncer. En la agricultura, permiten que los científicos desarrollen variedades de cultivos mejoradas que se adapten al cambio climático y aborden la seguridad alimentaria. En el arte y la arqueología, ayudan a conservar un patrimonio cultural de incalculable valor. No obstante, estas fuentes deben manipularse con las debidas medidas de seguridad tecnológica y física.

Para ayudar a los países a enfrentar los riesgos y proteger a las personas y al medio ambiente frente a la exposición accidental a la radiación o frente a actos intencionados no autorizados en los que se utilicen fuentes radiactivas, el OIEA elaboró el Código de Conducta sobre Seguridad Tecnológica y Física de las Fuentes Radiactivas, que la Junta de Gobernadores del OIEA aprobó en 2003 y que este año conmemora su 20º aniversario.

"Han transcurrido 20 años desde la aprobación del Código de Conducta y estamos logrando avances constantes en la mejora de la seguridad tecnológica y física de las fuentes radiactivas en todo el mundo —declaró el Director General del OIEA, Rafael Mariano Grossi, en la sesión inaugural de la Reunión de Composición Abierta de Expertos Técnicos y Jurídicos para Intercambiar Información sobre la Aplicación por los Estados del Código de Conducta sobre la Seguridad Tecnológica y Física de las Fuentes Radiactivas—. No obstante, se debe seguir trabajando para conseguir un compromiso político aún mayor y poner en común prácticas óptimas mundiales para la gestión sostenible y tecnológica y físicamente segura de estas fuentes."

La reunión, con una duración de cinco días, sirvió como plataforma para que expertos de todo el mundo intercambiaran información sobre prácticas de aplicación nacionales del Código de Conducta y sus dos documentos complementarios, Directrices y Orientaciones. Esas reuniones se celebran cada tres años y permiten que los países pongan en común sus experiencias, intercambien lecciones aprendidas y señalen los desafíos actuales y futuros en la aplicación del Código.

Durante la semana, los participantes profundizaron en diversos temas, como la evolución de la seguridad nuclear tecnológica y física, los aspectos jurídicos, la cooperación internacional, el desarrollo futuro y el impacto del Código de Conducta. En los debates se trataron los desafíos y las prioridades relacionados con el establecimiento del marco regulador adecuado para la seguridad tecnológica y física de las fuentes radiactivas, la gestión de su ciclo de vida, los reglamentos sobre su importación y exportación y el modo en que se deberían gestionar estas fuentes cuando se las declare en desuso. Ante todo, la reunión ofreció a los participantes la posibilidad de poner en común sus respectivos enfoques para aplicar eficazmente las disposiciones del Código de Conducta.

Orientación esencial para un futuro tecnológica y físicamente seguro

Uno de los participantes en el evento de inauguración, el Copresidente de la reunión, Ramzi Jammal, Vicepresidente Ejecutivo y Director de Operaciones Reglamentarias de la Comisión Canadiense de Seguridad Nuclear (CCSN), hizo hincapié en que la aplicación del Código de Conducta es fundamental para garantizar la protección del medio ambiente, el público y los trabajadores. "Nuestro objetivo último es garantizar la seguridad tecnológica y física en general de las fuentes radiactivas durante todo su ciclo de vida, a fin de evitar la exposición accidental a la radiación e impedir la utilización de fuentes radiactivas con fines dolosos. Se trata de un esfuerzo colaborativo y continuo."

Durante la presentación de una sesión especial sobre la historia del Código, Theresa Clark, Directora Adjunta de División en la Comisión Reguladora Nuclear de los Estados Unidos, también se dirigió a los asistentes en calidad de Copresidenta: "Para reflexionar sobre estos veinte años y celebrar esta andadura, queríamos lograr un conocimiento común sobre la trayectoria del Código desde el punto de vista jurídico y técnico, de modo que podamos intercambiar experiencias y prácticas óptimas y aprender los unos de los otros con miras a mejorar la aplicación del Código en todo el mundo."

En el Código de Conducta se explica con detalle de qué manera los países pueden garantizar la seguridad tecnológica y física de las fuentes radiactivas desde su producción inicial hasta su disposición final definitiva. Contiene consideraciones internacionales y ofrece recomendaciones sobre la formulación, la armonización y la aplicación de políticas, leyes y reglamentos nacionales, así como sobre la cooperación entre países. Si bien se trata de un documento jurídicamente no vinculante, desde su aprobación por la Junta de Gobernadores en 2003, 146 Estados han expresado su apoyo político a la aplicación de las disposiciones del Código.

El Código de Conducta está complementado por dos documentos de Directrices y Orientaciones. Las Directrices sobre la Importación y Exportación de Fuentes Radiactivas tratan de las funciones y responsabilidades para garantizar la importación y la exportación tecnológica y físicamente seguras de fuentes radiactivas. En las Orientaciones sobre la Gestión de las Fuentes Radiactivas en Desuso se proporciona orientación sobre la gestión de las fuentes en desuso y se delimitan las opciones sobre la gestión del final del ciclo de vida, como el reciclaje y la reutilización, el almacenamiento a largo plazo y la disposición final, y la devolución al suministrador. Estas Orientaciones también alientan a establecer una política y una estrategia nacionales para la gestión de las fuentes en desuso.

"El Código de Conducta y sus Directrices y Orientaciones aportan beneficios tangibles a la seguridad radiológica y la seguridad física nuclear a escala nacional e internacional, puesto que permiten un aprovechamiento pleno de las fuentes radiactivas para lograr un futuro sostenible," concluyó la Copresidenta Aayda Ahmed Al Shehhi, Directora de Seguridad Radiológica en la Autoridad Federal de Reglamentación Nuclear (FANR) de los Emiratos Árabes Unidos.

El OIEA trabaja y colabora estrechamente con los países para garantizar la gestión armonizada y tecnológica y físicamente segura de las fuentes radiactivas. Les brinda apoyo en la labor de implementar los principios del Código y ofrece una amplia asistencia en la elaboración de estrategias y planes de acción para aplicarlo; en la mejora de la concesión de licencias, la inspección, la ejecución y los sistemas de gestión; y en el fortalecimiento de la capacidad de los organismos reguladores nacionales en consonancia con las normas de seguridad del OIEA, la orientación sobre seguridad física nuclear y prácticas óptimas internacionales.

Fortalecimiento de la diversidad y la inclusión en el ámbito nuclear

Paralelamente a la reunión, la CCSN celebró un evento paralelo titulado "La Igualdad de Género y la Inclusión, y el Código de Conducta sobre Seguridad Tecnológica y Física de las Fuentes Radiactivas: 20 Años de Avances." Este evento, que reunió a 120 participantes, tenía por objeto analizar las formas de promover y fortalecer la participación femenina en el ámbito nuclear —incluidas las esferas de la seguridad nuclear tecnológica y la seguridad nuclear física— y proporcionar igualdad de oportunidades a todas las personas, con independencia de su género.

"Contar con una amplia representación en la mesa contribuye a aumentar la actitud vigilante, que a su vez conduce a fortalecer la cultura de la seguridad en la organización. La igualdad de género no es exclusivamente un problema que atañe a la mujer, sino que se trata de una cuestión que afecta a la sociedad y que debemos abordar todos", señaló Rumina Velshi, Presidenta y Directora Ejecutiva de la CCSN, quien añadió que, debido a la creciente demanda de recursos humanos, será fundamental garantizar que las mujeres dispongan de más oportunidades en el ámbito nuclear.

"La seguridad nuclear tecnológica y física se basa en mantener una actitud vigilante y de aprendizaje, estar abiertos a la retroinformación constructiva y tener la capacidad de combinar distintos puntos de vista y movilizar distintos conocimientos especializados. La diversidad, incluida la diversidad de género, es un verdadero activo en este sentido. Somos más fuertes y más eficientes cuando incorporamos la diversidad y alentamos a nuestro personal a que exprese su opinión," declaró durante el evento Lydie Evrard, Directora General Adjunta del OIEA y Jefa del Departamento de Seguridad Nuclear Tecnológica y Física.

Por su parte, Margaret Doane, Directora General Adjunta del OIEA y Jefa del Departamento de Administración, señaló que "mejorar la participación de las mujeres y de personas de distinta procedencia en sectores relacionados con el ámbito nuclear es fundamental para cualquier organización." Asimismo, puso de manifiesto las iniciativas del OIEA sobre la mejora de la igualdad de género, como el Programa de Becas del OIEA Marie Skłodowska-Curie y el Programa Lise Meitner, encaminadas a incorporar más mujeres al ámbito nuclear.

Christer Viktorsson, Director General de la FANR, expuso su punto de vista sobre este asunto: "La FANR cuenta con actividades específicas para promover la igualdad de género. El compromiso con el liderazgo y su apoyo son cuestiones vitales; por ejemplo, llevar a cabo estudios para averiguar cómo podemos mejorar la inclusión de todo el personal y ofrecerle un trato justo. Es igualmente importante contar con un marco adecuado y una aplicación eficaz que sean inclusivos."

— Artem Vlasov

Los países de habla árabe conversan sobre planes de seguridad física nuclear

Los participantes de una reunión regional celebrada recientemente en Túnez compartieron sus experiencias en materia de desarrollo y ejecución de un INSSP. (Fotografía: Z. Hassan/OIEA y AAEA)

Los países miembros de la Red Árabe de Reguladores Nucleares (ANNuR) se reunieron recientemente en Túnez con el fin de intercambiar prácticas óptimas, desafíos y oportunidades relativos a la ejecución de actividades sobre seguridad física nuclear, en el marco de sus respectivos planes integrados de apoyo a la seguridad nuclear (INSSP). La reunión puso de relieve la importancia de contar con enfoques regionales para mejorar la capacidad reguladora y operativa, que son inherentes al programa de seguridad física nuclear del OIEA.

"Abordar la seguridad física nuclear desde una perspectiva regional permite mejorar la cooperación internacional y facilita la ejecución del programa de seguridad física nuclear del OIEA —indica Elena Buglova, Directora de la División de Seguridad Física Nuclear del OIEA—. La cooperación con redes regionales como ANNuR afianza aún más la eficacia del mecanismo de apoyo del INSSP, a través de la creación de oportunidades para determinar y examinar las necesidades y los desafíos comunes que enfrentan los países con proximidad geográfica o que hablan el mismo idioma".

En la reunión, 28 participantes de 14 países brindaron información acerca de la ejecución de sus INSSP nacionales. Entre las principales esferas abordadas se encontraban actividades relacionadas con los marcos legislativos y reguladores para la seguridad física nuclear; la evaluación de amenazas y riesgos a nivel nacional; los regímenes de protección física; la detección de actos delictivos y no autorizados que guarden relación con materiales nucleares y otros materiales radiactivos no sometidos a control reglamentario; la respuesta a sucesos de seguridad física nuclear que guarden relación con otros materiales radiactivos no sometidos a control reglamentario, y el mantenimiento de los regímenes nacionales de seguridad física nuclear.

El Líbano es actualmente uno de los países que utilizan el INSSP como mecanismo para fortalecer su infraestructura nacional de seguridad física nuclear. "El taller nos permitió compartir nuestra experiencia en el plano nacional con la ejecución del INSSP, así como examinar los desafíos que enfrentan nuestros países en relación con la seguridad física nuclear y las posibles maneras de abordarlos —dice Hassan Basat, Jefe de Sección responsable de la autorización, la inspección y los reglamentos de la Comisión Libanesa de Energía Atómica—. El resultado práctico más importante fue la identificación de esferas prioritarias comunes del INSSP que deben seguir mejorándose entre todos los miembros de ANNuR".

En la actualidad 19 de los 22 miembros de ANNuR cuentan con un INSSP

aprobado y en todo el mundo, son 92 los países que tienen INSSP aprobados.

"A nivel regional compartimos fronteras y desafíos específicos —dice Shaima Khalid AlJanahi, Jefa de la Unidad de Análisis Físico, Dirección de Protección Radiológica, Consejo Supremo para el Medio Ambiente de Bahrein—. El taller ha permitido compartir experiencias y conocimientos que esperamos que den lugar a medidas concretas para mejorar y fortalecer la seguridad física nuclear en la región".

El Organismo Árabe de Energía Atómica (AAEA) fue el anfitrión de la reunión, que contó con el apoyo financiero de la Unión Europea.

El mecanismo de apoyo del INSSP

El OIEA ayuda a aquellos países que así lo soliciten a desarrollar un INSSP, que proporciona el marco para un enfoque sistemático e integral para determinar y priorizar las necesidades del país relativas a la seguridad física nuclear, y establecer un plan para la implementación de mejoras a la seguridad física nuclear a nivel nacional. El proceso del INSSP se complementa con una herramienta de autoevaluación voluntaria que se encuentra a disposición de los países interesados a través del Portal de Información sobre Seguridad Física Nuclear (NUSEC).

El INSSP y su plan de aplicación conexo permite a los países satisfacer sus necesidades más apremiantes y determinar esferas que pueden abordarse a nivel nacional y otras en las que se necesita solicitar la asistencia de la comunidad internacional.

Una vez determinadas las necesidades de cada país, el OIEA puede comenzar a cimentar la asistencia específica, como la que ofrecen las misiones de su Servicio Internacional de Asesoramiento sobre Protección Física (IPPAS) y del Servicio Internacional de Asesoramiento sobre Seguridad Física Nuclear (INSServ).

Cooperación OIEA-ANNuR

La ANNuR es una red regional creada en 2010 bajo la égida de la Red Mundial de Seguridad Nuclear Tecnológica y Física (GNSSN) del OIEA. Se encarga de promover, mejorar, fortalecer y armonizar la protección radiológica y los marcos de reglamentación para la seguridad nuclear tecnológica y física en los países participantes, y sirve de foro para compartir e intercambiar experiencias y prácticas relacionadas con la reglamentación.

— Vasiliki Tafili

Publicaciones del OIEA

Consulta gratuita en línea

Descargar aquí

www.iaea.org/es/publicaciones

Si desea encargar una publicación, escriba a:
sales.publications@iaea.org

DESCARGAR

Seguridad física de la información nuclear
y otras publicaciones del OIEA sobre
La seguridad informática en el mundo nuclear

www.iaea.org/es/bulletin/64-2

Lea este y otros números del *Boletín del OIEA* en línea en
www.iaea.org/es/bulletin

Para obtener más información sobre el OIEA y su labor, visite
www.iaea.org

o síganos en

ISSN 0534-7297 23-01076S