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.*