Nuevas exigencias europeas para la Protección de las Infraestructuras Críticas

Un nuevo ataque masivo contra la infraestructura energética de Ucrania, el posible sabotaje a un cable de comunicaciones en el Báltico, las implicaciones potenciales derivadas del resultado de las elecciones en EE.UU., marcarán un nuevo orden, un cambio de paradigma en la seguridad global que hace que sea aún más necesario que nos replanteemos nuestra seguridad colectiva.

En España, según los datos de la Oficina de Coordinación de Ciberseguridad (OCC) del Ministerio del Interior, los ciberataques que comprometen la disponibilidad de los servicios, tipo DDos (denegación de servicio distribuido) o DoS (denegación de servicio) están predominando entre las infraestructuras críticas, alcanzando este año el 55% de todas las tipologías.

Debemos aplicar las nuevas normas impulsadas por la UE que protegerán con mayor eficacia las infraestructuras esenciales de la Unión, introduciendo unas condiciones mínimas para la evaluación del riesgo y unas estrategias nacionales de resiliencia, al tiempo que armonizarán la definición de «infraestructura crítica» en todos los Estados miembros sobre la base de las amenazas complejas e incrementar los recursos de análisis y liberarlos de viejas patologías, así como desarrollar un nuevo esquema de gestión integral del riesgo y las seguridades.

Manuel Sánchez Gómez-Merelo
Consultor Internacional de Seguridad

Estas nuevas normas obligarán a los Estados miembros a contar con estrategias nacionales de ciberseguridad y resiliencia y a que la comunicación transfronteriza se realice a través de unos puntos de contacto únicos que designará cada Estado.

Legislación y normativa europea

En diciembre de 2022, el Consejo adoptó una Recomendación sobre un enfoque de coordinación a escala de la Unión para reforzar la resiliencia de las infraestructuras críticas, en la que se insta a los Estados miembros a acelerar los trabajos preparatorios para la transposición y aplicación de la SRI 2 y de la Directiva sobre la resiliencia de las entidades críticas (CER).

En enero de 2023 entraron en vigor dos directivas clave sobre infraestructuras críticas para reforzar la resiliencia de la UE frente a las amenazas, desde los ciberataques hasta la delincuencia, los riesgos para la salud pública o las catástrofes naturales.

Las dos Directivas que entraron en vigor son:

- Directiva NIS2, sobre medidas destinadas a elevar el nivel común de ciberseguridad en toda la Unión.
- Directiva CER, sobre la resiliencia de las infraestructuras críticas.

La Directiva NIS2 garantizará una Europa más segura y fuerte, al ampliar significativamente los sectores y el tipo de entidades críticas que entran en su ámbito de aplicación y sus responsabilidades.

Además, reforzará los requisitos de gestión de riesgos de ciberseguridad que las empresas están obligadas a cumplir. La Directiva NIS2 sustituye a las normas sobre seguridad de las redes y sistemas de información, la primera legislación a escala de la UE sobre ciberseguridad.

Frente a un panorama de riesgos cada vez más complejo, la nueva Directiva CER sustituye a la Directiva Europea de Infraestructuras Críticas de 2008. Las nuevas reglas fortalecerán la resiliencia de la infraestructura crítica frente a una serie de amenazas, incluidos peligros naturales, ataques terroristas, amenazas internas o sabotaje.

En este sentido, hemos de destacar la obligación de los Operadores Críticos a acreditar tanto el Plan de Seguridad del Operador, como sus Planes de Protección Específicos, así como la implantación de las medidas exigidas por la autoridad competente, a través de la certificación oportuna. Es decir, viene a realzar la importancia de la certificación de las medidas de seguridad implementadas, tanto como la elaboración de los mismos planes con unos mayores niveles de exigencia en los criterios y requisitos de seguridad, más orientados a procesos de certificación, como lo es el caso del ENS.

La NIS-2 no solo exige la implementación de medidas más rigurosas, sino que también reconoce que las empresas deben adoptar un enfoque más proactivo y estructurado frente a las ciberamenazas. La seguridad de la cadena de suministro, por ejemplo, se ha convertido en un tema clave, ya que un ataque a un proveedor externo puede tener un impacto devastador en toda la cadena.

La falta de preparación para enfrentar las amenazas cibernéticas no solo pone en riesgo la reputación y el funcionamiento de las organizaciones, sino que también compromete la seguridad de las infraestructuras críticas en toda la Unión Europea.

Aunque muchas empresas son conscientes de la directiva NIS2 y de lo que supone, el nivel de preparación varía considerablemente.

En conclusión, la Directiva NIS-2 representa un gran avance para garantizar la protección de sectores clave en la UE, pero su éxito depende de la capacidad de las empresas para adaptarse.

Nuevo paradigma de seguridad

La Protección de Infraestructuras Críticas (PIC) requiere de un nuevo marco europeo de cooperación.

La guerra de Ucrania y los conflictos en Oriente Medio, sus actuales amenazas, sabotajes y consecuencias está provocando un nuevo planteamiento de Seguridad Global y de Protección de Infraestructuras Críticas, principalmente en el ámbito de la Unión Europea.

Ante las constantes nuevas exigencias y retos, las organizaciones públicas y privadas han de asumir la irreversible situación de que las infraestructuras críticas deben alinear e integrar los sistemas y planes de seguridad física y lógica o ciberseguridad necesarios para proteger sus actividades frente a los riesgos y las amenazas en evolución permanente, así como cumplir con las nuevas regulaciones que las distintas instituciones, nacionales e internacionales, están implementando para proteger la seguridad global de tan esenciales sistemas estructurales.

Por esta razón, la UE y sus Comisiones se han dedicado durante mucho tiempo a fomentar la resiliencia de las infraestructuras críticas frente a todo tipo de riesgos naturales o provocados por el hombre.

Para mantener nuestro compromiso de servicio a la comunidad, hemos de realizar un seguimiento permanente de las actualizaciones legales y reglamentarias, con el objetivo de mantener informadas a las organizaciones y a los usuarios en general, sobre los cambios que puedan afectar al funcionamiento y gestión de sus instalaciones.

Así, se determinaron los Sectores Estratégicos y Críticos como las infraestructuras relacionadas con Servicios Esenciales.

El grueso del Sistema PIC en España tiene más de 3.500 infraestructuras estratégicas (entre ellas varios cientos de infraestructuras críticas) identificadas e incluidas en el Catálogo Nacional.

Los nuevos retos y exigencias para la Protección de las Infraestructuras Críticas requieren de un mayor y mejor Control de la Seguridad, con evidentes e importantes vulnerabilidades, frente a un entorno de riesgos y amenazas en permanente cambio.

Seguridad y Gestión del Riesgo

Vivimos un panorama globalizado de nuevas amenazas, mayores riesgos en las actividades sociales, industriales y comerciales que ratifican nuevas demandas y exigencias de la sociedad para la protección de sus actividades con plenas garantías para su seguridad.

Para ello, debemos invertir en Gestionar el Riesgo, para analizarlo y prevenirlo, tratando de garantizar en todo lo posible el minimizarlo, a fin de poder superar las incidencias y conseguir el suficiente grado de resiliencia.

Hemos de plantear soluciones holísticas para la Gestión del Riesgo de las Infraestructuras Estratégicas y Críticas que, sin duda, requieren productos y servicios de seguridad adecuados a sus específicos riesgos, amenazas y vulnerabilidades.

El proyecto de desarrollo y despliegue de un modelo para la Gestión Integral del Riesgo y las Seguridades (prevención + protección) debe estar basado en una metodología de planificación, desarrollo y gestión de aplicación específica.

Un modelo Integrado de seguridad, que contemple el catálogo de riesgos más amplio y transversal, con flujos de información interdepartamentales y sostenible, con el objetivo de proporcionar una serie de herramientas y soluciones en sus diferentes posibilidades, en forma de aplicaciones tanto documentales como procedimentales.

Al tiempo que un modelo de recursos integrales e integrados, con el objetivo de que los Departamentos de Seguridad enfoquen de manera más panorámica la gestión global y la resiliencia, de cara a una mayor eficacia, sostenibilidad y viabilidad económica.

Implementar y adoptar una gestión integral del riesgo con estrategias robustas de reducción de las amenazas y aumento de la resiliencia es una inversión proactiva que ofrece una serie de ventajas para las organizaciones como son: la reducción de las interrupciones, la mejora en la toma de decisiones, el ahorro de costes, la mejora de la eficacia y la mejora de la garantía reputacional y la continuidad del funcionamiento.

Seguridad Global. Integral e Integrada

La Seguridad Nacional y las Infraestructuras Críticas pueden considerarse un problema global que se ha de abordar a nivel institucional, siguiendo políticas nacionales y un enfoque internacional.

Hemos de redefinir la Seguridad pues los desafíos que sugiere el nuevo contexto global de riesgos y amenazas requieren soluciones de seguridad innovadoras, que incorporen a la inteligencia y la tecnología como bases de una estrategia de seguridad necesaria para operar en las organizaciones y la sociedad en su conjunto.

En especial, hemos de analizar el posible impacto en lo que se refiere a los riesgos y amenazas en las infraestructuras críticas y reestudiar las complejidades de la toma de decisiones y liderazgo de la seguridad global como tarea imprescindible para un futuro esperable de la prevención y la protección.

Definitivamente, hemos de integrar protección física y cibernética de las infraestructuras frente a cualquier tipo de amenaza.

Reflexiones y recomendaciones

Sin duda hoy hay que dar una respuesta con una Seguridad Única con mayúscula, integral e integrada, pública y privada.

Solo una seguridad global, integral e integrada, puede garantizar una protección eficiente frente a amenazas globales y supone una aplicación de la seguridad, en la que se han de tener en cuenta los aspectos geoestratégicos, humanos, legales, sociales, económicos y técnicos de todos los riesgos y amenazas que pueden afectar a las personas y bienes integrantes en la actividad de unos países aliados por el bien común y la seguridad conjunta.

Con todo ello, y como recomendaciones finales, debemos potenciar una nueva cultura de seguridad con visión holística sobre la base de las amenazas complejas, incrementar los recursos de análisis y liberarlos de viejas patologías y rigideces, así como desarrollar el esquema de gestión integral del riesgo y las seguridades, partiendo de esquemas básicos o decálogos para el desarrollo que incluyan el pensamiento global y la actuación local.

La Seguridad Nacional y las Infraestructuras Críticas pueden considerarse un problema global que se ha de abordar a nivel institucional, siguiendo políticas nacionales con un enfoque internacional.