Nº 6 mayo 2025

Nuevo paradigma de protección de infraestructuras críticas

Vivimos en una sociedad donde el espacio a cubrir es cada vez más grande y el tiempo exigido para las respuestas resulta cada vez más corto, por lo que, los mejores resultados para ofrecer la mejor protección en nuestra infraestructuras críticas y esenciales, radican en nuestra capacidad de adaptación a la globalización y los cambios ante los nuevos retos y exigencias.

Los avances tecnológicos y su constante evolución nos dan la oportunidad de desarrollar nuevos métodos, herramientas y habilidades para mantenernos seguros y, con ello, se establece un nuevo paradigma de protección de infraestructuras críticas que se caracteriza por un enfoque que va más allá de la seguridad tradicional basada en círculos de protección y se centra en la seguridad de la información, la ciberseguridad, la protección de las comunicaciones y datos, integrando tecnologías como la inteligencia artificial.

Nuevos retos y exigencias de seguridad global

Es necesario recordar que estamos ante nuevos retos y exigencias que han aparecido en el escenario generado por la pandemia, los conflictos armados e invasiones y la guerra de Ucrania que nos sitúan ante un nuevo orden mundial que ha registrado un incremento sin precedentes de la superficie de exposición, principalmente, por nuevos riesgos y amenazas y el incremento de las vulnerabilidades.

Un contexto de inseguridad global, donde conceptos como el ciberterrorismo o cibercrímen se encuentran cada vez más presentes en nuestras actividades, lo que exige nuevos desarrollos de mecanismos de ciberseguridad.

Frente a los nuevos retos y exigencias, en lo referente a los riesgos y amenazas, se debe seguir avanzando en un concepto de seguridad global y conceptual, que, a diferencia de épocas precedentes, se renueva de manera constante, y dentro de un espacio definido por cuatro referentes: circulación, complejidad, contingencia y resiliencia.

Así, la nueva protección de infraestructuras críticas se enfoca en reforzar la resiliencia frente a diversas amenazas, incluyendo ciberataques, delincuencia organizada, riesgos para la salud pública y desastres naturales. Un enfoque basado en una colaboración e integración operativa entre el sector público y privado.

Aspectos clave de la nueva protección

El desarrollo de la nueva protección de infraestructuras críticas, actualmente se basa en los aspectos clave siguientes:

- Legislación: Ley 8/2011 y Reglamento PIC que establecen las obligaciones para los Operadores Críticos en materia de seguridad.
- Directivas Europeas: Reglamentación europea sobre resiliencia de las organizaciones públicas y privadas, como la Directiva 2022/2557, así como la Directiva NIS2 sobre Seguridad de las Redes y los Sistemas de Información, que refuerzan la protección de las infraestructuras en la Unión Europea.

- Nivel de Alerta de Infraestructuras Críticas (NAIC): Normativa que define los niveles de alerta para las infraestructuras críticas, desde el estado normal hasta el estado de emergencia, con medidas específicas para cada nivel.
- Plan Nacional de Protección de Infraestructuras Críticas (PNPIC): Plan, coordinado por el Ministerio del Interior, que define los niveles de alerta y las medidas a tomar en caso de amenaza o emergencia.
- Plan de Protección Específico (PPE): Planificación y organización que los Operadores Críticos deben desarrollar con detalle las medidas de seguridad (prevención y protección) a implementar para proteger sus infraestructuras esenciales.
- Medidas de seguridad física: Establecimiento de mejoras en la seguridad física, como la vigilancia y los sistemas para la protección de personas, infraestructuras y edificios.
- Medios de ciberseguridad: Implementación de soluciones de ciberseguridad para proteger las redes, sistemas y datos de las infraestructuras críticas.
- Resiliencia: Incremento de la capacidad de las infraestructuras para adaptarse a las amenazas, resistir ante incidencias y recuperarse en el menor tiempo.
- Colaboración: Potenciar la cooperación entre el sector público y el privado para la identificación y gestión de riesgos y seguridades e implementación de planes de contingencia y continuidad.

Igualmente, los nuevos paradigmas de seguridad requieren de otros aspectos claves para su implementación como: Fomentar una cultura de seguridad positiva, bajo la idea de que, aunque la seguridad total no existe, es en gran medida un objetivo alcanzable involucrando a las personas en todos los niveles buscando la participación ciudadana, creando un entorno donde toda la información, tanto positiva como negativa, sea valorada y utilizada para mejorar la seguridad global.

La implementación de estos nuevos enfoques requiere un esfuerzo y una adaptación constantes, pero los beneficios en términos de seguridad global y bienestar ciudadano son significativos.

Beneficios de la nueva protección

La nueva protección de infraestructuras críticas se enfoca en fortalecer la respuesta frente a las nuevas amenazas, potenciar la colaboración y coordinación entre el sector público y privado, incrementar e implementar nuevos medios y medidas de seguridad física y cibernética y aumentar la resiliencia, siguiendo siempre las directivas europeas a fin de garantizar la protección de las infraestructuras críticas, la continuidad de los servicios esenciales y la seguridad de los ciudadanos.

El actual ecosistema de Protección de Infraestructuras Críticas (PIC) viene marcado por la trasposición de la Directiva 2022/2557 del Parlamento Europeo y del Congreso relativa a la resiliencia de las entidades críticas. Esta directiva europea marca y coincide, además, con la línea de trabajo por la que se apuesta desde el CNPIC, y describe una serie de acciones y novedades con el fin de adaptarse a un entorno actual cambiante desde distintos puntos de vista: tecnológico, geopolítico, económico, medioambiental o delincuencial.

Novedades del CNPIC

Nuevas amenazas acechan y es de obligación detectarlas, analizarlas y evaluarlas para protegerse, resistir y continuar prestando los servicios esenciales con la menor incidencia posible para la ciudadanía y la estabilidad económica del país.

Para conseguir implantar las medidas relacionadas con la continuidad de funcionamiento, el CNPIC elabora una Evaluación Nacional de Riesgos alineada con la Estrategia Nacional de Seguridad, que contempla todo tipo de amenazas de origen humano, social o de la naturaleza, sin olvidarse de las ciberamenazas y las de carácter híbrido.

Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) Ministerio del Interior

Sobre esta evaluación, los operadores deberán realizar, para cada una de sus infraestructuras catalogadas, una evaluación de riesgos y amenazas, que servirá para elaborar un Plan de Resiliencia de la Entidad Crítica (PREC). Este plan sustituirá o complementará a los llamados: Plan de Seguridad del Operador (PSO) y Plan de Protección Específico (PPE) de las infraestructuras críticas.

En este cambio de paradigma de la protección de infraestructuras críticas también es fundamental, por tanto, un nuevo análisis, revisión y adaptación de todos los planes de seguridad de las entidades y organizaciones implicadas, además de la adecuación de la formación especializada para los profesionales de la seguridad pública y privada involucrados.

Manuel Sánchez Gómez-Merelo

Vocal de la Junta Directiva de AES