SITUACIÓN DE LA SEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS

Tania G. Rojo Chávez / *Staff* Seguridad en América

Emprender acciones en la protección de estas instalaciones es imprescindible para el bienestar nacional

Foto: © Achirawich Artapant | Dreamstime

En la actualidad, la seguridad en infraestructuras críticas (IC) se ha visto vulnerada por amenazas derivadas del terrorismo internacional, organizaciones delincuenciales transnacionales y ataques cibernéticos que ponen en riesgo los sectores de actividad que proporcionan servicios de vital importancia para el desarrollo de la vida de los ciudadanos y sus actividades diarias, así como para la continuidad de las funciones del Estado. Lo que ha tenido como resultado que los Gobiernos se interesen en desarrollar estrategias e implementar medidas de protección para garantizar la seguridad de éstas.

Foto: ©Ugly Duckling/Dreamstime

Ataques a infraestructuras críticas

Han sido diversos los atentados en todo el mundo los que han resaltado la importancia de las nuevas amenazas y vulnerabilidades con las que los Gobiernos deben lidiar en la actualidad al planear la seguridad de estas infraestructuras ya que, por ejemplo, el ataque contra las Torres Gemelas dejó pérdidas tanto humanas como económicas.

Otro de los casos más representativos es el de Estonia, uno de los países en que las elecciones parlamentarias se realizan mediante voto electrónico, que en 2007 sufrió un ataque cibernético contra distintas agencias gubernamentales, la policía, y varios medios de comunicación que desembocó en una crisis nacional con graves pérdidas económicas para el país, según informes del Centro de Excelencia de Defensa Cibernética Cooperativa de la Organización del Tratado del Atlántico Norte (OTAN).

De acuerdo con Manuel Sánchez, vicepresidente de la Asociación para la Protección de Infraestructuras Críticas (APIC), aunque hoy en día hay diferencias importantes en las vulnerabilidades, los riesgos y las amenazas que enfrentan los diferentes continentes y países, de manera general, todos están relacionados con el terrorismo internacional, la globalización económica y comercial, y la mayor apertura de fronteras.

David Ramírez, director de Ingeniería en Fortinet, señaló que entre los nuevos riesgos se encuentra que algunas IC, que antes no eran susceptibles a ataques porque no estaban conectadas a Internet, actualmente necesitan no sólo de protección física sino también contra *malwares* por su compatibilidad con IP.

¿Cómo protegerlas?

Para garantizar la seguridad de las IC y protegerlas de los ataques físicos e informáticos a los que están expuestas, los expertos coincidieron en que las soluciones de seguridad como videovigilancia, control de acceso, detectores de incendios, programas *anti-malware*, etcétera; juegan un papel importante en la protección unificada de estas estructuras.

Según Pedro Janices, director de la Oficina Nacional de Tecnologías de la Información (ONTI) de la Jefatura del Gabinete de Ministros de la Nación Argentina, las IC deben resguardarse con una arquitectura de capas que protejan la información de éstas, los recursos humanos que las operan, y la protección física de acceso mediante dispositivos de seguridad electrónica. Por ejemplo, los drones que son utilizados para monitorearlas de forma ágil y programada permitiendo el acceso a la información en tiempo real.

Asimismo, Sánchez indicó que todas las soluciones tienen que estar integradas en el sistema de gestión global de seguridad en donde deben constituirse la seguridad lógica (protección de la información), física (sistemas perimetrales y barreras), servicios de seguridad (vigilantes y logística operativa) y los sistemas de centralización y gestión.

Acciones por emprender

Es importante que los Gobiernos establezcan sistemas para compartir la información sobre los riesgos y amenazas globales que afectan a las IC. Además, Sánchez señaló que deben constituir o potenciar grupos de trabajo multidisciplinarios internacionales para intercambiar experiencias y modelos de éxito; así como planes de formación y capacitación especializada que en esta materia se han ido desarrollando desde hace años, principalmente en Europa, y que se han transmitido en acuerdos con países latinoamericanos.

Por su parte, Oscar Priego Verdugo, *programmer* II en Diseño e Implementación de Servicio Computacional (DISC), destacó la importancia de cuidar y promover la protección de IC, implementar las normativas y estándares en seguridad adecuados como ISO 27001, para el resguardo informático, e ISA 99, para la salvaguarda en la automatización industrial y sistemas de control. Aparte de contar con la previsión de evaluar e incluir medidas con el propósito de evitar posibles percances y contingencias que las afecten, concluyó. ■

Manuel Sánchez,
APIC

Oscar Priego Verdugo,
DISC

David Ramírez,
Fortinet