Sean bienvenidos una vez más a Código Seguro, en el día de hoy, estimados lectores, les hablaré acerca de un tema que introducimos en la sección anterior de la columna. Hoy día, gracias a la diversificación de las Tecnologías de la Información y las Comunicaciones, se han logrado informatizar la mayoría de los procesos que se llevan a cabo en la sociedad. Las sociedades industrializadas dependen del buen funcionamiento de toda una serie de infraestructuras tecnológicas, como la electricidad, las redes viarias y ferroviarias y las telecomunicaciones que, por su importancia, se denominan genéricamente infraestructuras críticas.

Las infraestructuras críticas son, por lo tanto, aquellos recursos materiales, servicios, sistemas de tecnología de la información, redes y activos de infraestructura que, si se dañan o destruyen, causarían graves repercusiones en las funciones cruciales de la sociedad, incluida la cadena de suministro, la salud, la seguridad y el bienestar económico o social de un Estado y la población en general. Los fallos técnicos, las catástrofes naturales y los actos malintencionados, incluso los terroristas, pueden tener efectos devastadores en estas infraestructuras. Estas infraestructuras incluyen sistemas físicos y virtuales que respaldan disimiles sectores como la energía, el transporte, las comunicaciones y la salud.

Los acontecimientos de los últimos años han acelerado los esfuerzos para identificar y designar las IC a escala internacional y han reforzado la preocupación por aumentar su protección en sectores

sensibles para la seguridad de las personas. Ejemplos son muy variados, desde una compañía aérea que pierde el control sobre un vuelo por un mal funcionamiento provocado desde sus sistemas informáticos, ataques cibernéticos dirigidos al sistema electro energético de una región o un país o el robo y divulgación de datos confidenciales sobre la historia clínica electrónica de los pacientes de un determinado hospital dejan de ser solo ficción del arte cinematográfico para convertirse un peligro potencial a resolver en el mundo real. De ahí que las organizaciones gubernamentales desde lo legal deben asegurar y establecer medidas para la protección de dichas infraestructuras. Generalmente, su objetivo es garantizar la funcionalidad, continuidad e integridad de estas infraestructuras y prevenir daños causados por ataques deliberados de personas malintencionadas. La resiliencia es un principio fundamental en la protección de infraestructuras críticas. Implica la capacidad de recuperarse rápidamente de perturbaciones o ataques.

En Cuba, la seguridad de las infraestructuras críticas está regulada por el Decreto No. 360/2019 del Consejo de Ministros. Este decreto establece el marco legal para el empleo seguro de las Tecnologías de la Información y la Comunicación (TIC), así como la defensa del Ciberespacio Nacional. Mediante su artículo 25 se estable que es precisamente el Ministerio de Comunicaciones, en coordinación con los ministerios del Interior y de las Fuerzas Armadas Revolucionarias, quienes ejecutan las certificaciones de la seguridad de dichas infraestructuras, lo cual refleja el máximo compromiso que tiene el estado cubano en este sentido.

Las amenazas en este sector incluyen ataques cibernéticos, terrorismo, desastres naturales y fallos técnicos. En el ámbito de la ciberseguridad enfrentan diversas amenazas, algunas de ellas pudieran ser:

Ransomware: Los ciberdelincuentes toman el control de los datos y exigen un rescate para restaurar el acceso. En el 2023 y en lo que va de año, estos fueron una de las principales ciberamenazas, y su complejidad sigue aumentando.
Programas malignos: El malware incluye virus, gusanos, troyanos y programas espía, como hemos debatido en otras ocasiones. Tras descender durante la pandemia de la COVID, su difusión aumentó a finales de 2021 y actualmente los números son realmente preocupantes.
Ingeniería social: Se produce al aprovechar el error humano para acceder a información o servicios. El phishing (a través del correo electrónico) o el smishing (a través de mensajes de texto) son los ejemplos más comunes de este tipo de ataque En este caso pudieran estar dirigidos a los especialistas que ofrezcan soporte a dichas infraestructuras.

Ataques de denegación de servicio (DDoS): Sobrecargan la infraestructura de red y hacen que un sistema informático no esté disponible.
Errores humanos: Violaciones de las políticas de seguridad de la información por parte de los responsables de seguridad informática y los usuarios de forma general. Uso de contraseñas débiles, visitas a sitios web no seguros y falta de actualización del software del sistema o aplicaciones.

La interdependencia entre diferentes infraestructuras aumenta la vulnerabilidad, debido a que un fallo en una infraestructura puede afectar otras áreas críticas. Por lo tanto, las medidas deben estar en correspondencia con la medición previa que debe hacerse del impacto que tenga la infraestructura, teniendo en cuenta métricas horizontales como pueden ser: número potencial de víctimas, impacto económico, impacto social, impacto político, entre otras.

Según el mencionado decreto, nuestro país cuenta con un Sistema y un Plan Nacional de Protección de las Infraestructuras Críticas de las TIC. El primero está compuesto por el conjunto de medidas, previsiones y acciones que se generan, adoptan y ejecutan de forma integral y permanente, con el objetivo de preparar, organizar, ejercer y dirigir la protección de estas, para lo cual se establecen las políticas, estructuras organizativas, normas y recursos orientados a ese fin, así como se dispone un flujo de información que abarque a todos sus integrantes. El Plan por su parte tiene como objetivo establecer los criterios y las directrices precisas para movilizar las capacidades operativas de los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, en coordinación con los operadores de las infraestructuras críticas y articular las medidas preventivas necesarias para asegurar su protección permanente, actualizada y homogénea.

Algunas de las principales medidas pudieran ser:

La coordinación entre las diferentes entidades públicas es esencial para proteger estas infraestructuras.
Establecer canales seguros para coordinar equipos de respuesta según se necesite en cada momento.
La planificación escalonada implica identificar riesgos y diseñar estrategias de respuesta. Todo esto debe estar recogido en los planes de seguridad informática previamente elaborados.
La seguridad física y la seguridad de las tecnologías de la información son aspectos claves, tanto para prevenir como para la reducción del impacto ante un ataque inminente.
Realizar pruebas de estrés en los sistemas informáticos de sectores

prioritarios ayuda a evaluar la resiliencia de una infraestructura crítica. Estas pruebas se basan en escenarios extremos, pero realistas.

Sin dudas, la seguridad en infraestructuras críticas es un desafío constante que requiere cooperación, planificación y resiliencia para garantizar el bienestar de la sociedad y la economía. Por hoy nos despedimos hasta la próxima semana.

Cubadebate.