Seguridad cibernética

Una propuesta de sistematización de las infraestructuras críticas nacionales

Brigadier de Reserva Pedro Arthur Linhares Lima, PhD,
Fuerza Aérea Brasileña

Introducción

Con el advenimiento de la Era de la Informática, también conocida como Era Digital, y su sucedánea, la Era del Conocimiento, la información fue elevada a la categoría de activa estratégica para organizaciones y Estados-Naciones. Esto ha conferido a aquellos que la sostienen y de ella se utilizan efectiva y oportunamente, una incuestionable ventaja en el ambiente competitivo y en los contenciosos ámbitos internacionales.

La *Internet*, proporcionando conectividad en tiempo real y alcance mundial, ha traído consigo un crecimiento sin precedentes en el volumen de información disponible a los modernos responsables. Sin embargo, su gran vulnerabilidad, junto a la existencia de nuevos actores de funestas intenciones en el escenario internacio-

nal, hace crecer la preocupación por la protección de la información que por ella se trafica.

Según Raphael Mandarino,[1] las infraestructuras críticas (IC) son "las instalaciones, servicios, bienes y sistemas que, si se interrumpen o destruyen, provocarían un serio impacto social, económico, político, internacional o la seguridad del Estado y de la sociedad".

La definición más usual de IC es aquella que, una vez perjudicada por fenómenos de causas naturales, como terremotos o inundaciones o por acciones intencionales de sabotaje o terrorismo, trae grandes impactos negativos para toda una nación y su sociedad. Entre los ejemplos clásicos de IC se encuentran: las redes telefónicas; los sistemas de captación y distribución de agua; y las fuentes generadoras y las redes de distribución de energía.[2]

Con un mundo hiperconectado, la vulnerabilidad de las IC se ha convertido en uno de los mayores desafíos de la actualidad, confirmado en el análisis presentado por el *Boston Consulting Group*.[3]

De este modo, las evidencias de riesgos tecnológicos tratados en el ambiente cibernético y dirigidas a las IC que se utilizan de sistemas de control industrial en la monitorización de sus procesos, se resaltan en la medida en que tales sistemas vienen sufriendo una significativa transformación, pasando de sistemas de tecnologías propietarias y aisladas para el empleo de arquitecturas abiertas, a estar interconectadas, sobre todo, con sistemas corporativos y con la red mundial de computadoras.[4]

Siguiendo esta línea de raciocinio, cualquier impacto, ya sea positivo o negativo, en las Infraestructuras Críticas Nacionales (ICN) afectará al poder nacional. Esto se traduce en la capacidad que tiene el conjunto de personas y de los medios que constituyen la Nación, actuando en conformidad con la voluntad nacional, para alcanzar y mantener los objetivos nacionales, manifestado en cinco expresiones: la política, económica, psicosocial, militar y científica-tecnológica.

De esta forma, es imperativo que el Estado se organice para hacer frente a cualquier acción, ya sea natural o intencional, que venga a poner en riesgo una IC. Por eso, este artículo propone ciertas alternativas estratégicas, para contribuir a mejorar la estructuración, la sistematización y la integración de las ICN con los órganos estratégicos del gobierno y las Fuerzas Armadas.

El ambiente cibernético y las amenazas a las infraestructuras críticas

La evolución tecnológica aceleró vertiginosamente la capacidad de procesamiento automatizado de datos y el intercambio de informacion entre personas e

instituciones, aportando grandes beneficios a la humanidad. Por otro lado, posibilitó la aparición de herramientas de intrusión en esos sistemas informatizados utilizados por personas en el desarrollo de sus actividades particulares y profesionales.

En los más diversos niveles de la gestión pública o de la gestión de negocios privados de interés público, estos recursos informatizados se utilizan en actividades diversas, incluso en los sistemas de control de sectores estratégicos de una nación, como son las ICN de energía, telecomunicaciones, transporte, abastecimiento de agua, finanzas y defensa, entre otras. Al analizar los ataques virtuales que tuvieron como objetivo las IC de algunos países, ocurridos en la actualidad, se verifica que la complejidad y la planificación de esos ataques tuvieron como origen la voluntad de ejercer sus intereses de algunos Estados sobre otros.

En este contexto, diversas acciones de ataques cibernéticos contra redes de computadoras y de comunicaciones utilizadas en sistemas estratégicos pueden impactar hasta la seguridad nacional, en la medida en que pueden interrumpir o degenerar el funcionamiento de las estructuras esenciales a la sociedad y al estado brasileño, como es el caso de las ICN.

Acciones implementadas en Brasil relacionadas con el sector cibernético

La Estrategia Nacional de Defensa y las acciones de Seguridad y Defensa Cibernética

La Estrategia Nacional de Defensa (END)[5] estableció, en sus directrices, el fortalecimiento de tres sectores de importancia estratégica y esenciales para la defensa nacional: el espacial, el nuclear y el cibernético.

En el mencionado decreto también se establece que las capacidades cibernéticas incluirán, como parte prioritaria, las tecnologías de comunicaciones entre todos los contingentes de las Fuerzas Armadas, para asegurar su capacidad de actuar en red. En la END se enfatiza que los sectores espacial y cibernético deben permitir que las Fuerzas Armadas, en conjunto, puedan actuar en red. Destaca también que todos los órganos del Estado deberán contribuir al incremento del nivel de seguridad nacional, con particular énfasis en los siguientes aspectos del sector cibernético: las medidas para la seguridad de las áreas de infraestructuras críticas; y el perfeccionamiento de los dispositivos y procedimientos de seguridad que reduzcan la vulnerabilidad de los sistemas relacionados con la defensa nacional contra ataques cibernéticos y, si fuere el caso, que permitan su pronto restablecimiento.

En el contexto de la END, el sector cibernético no se restringe a las actividades relacionadas con la Seguridad y Defensa Cibernética, sino que abarca también la Tecnología de la Informática y las Comunicaciones (TIC), herramienta básica para la implementación de redes de ordenadores.

Con base en la END, los siguientes son los componentes de la red cibernetica: estructura de mando, control, comunicaciones, computación e inteligencia (C4I por sus siglas en inglés) para la operación y administración de las Fuerzas Armadas; recursos de TIC; y una arquitectura matricial que facilita la transmisión de informacion para la toma de decisiones en tiempo real.

Seguridad cibernética

En el nivel político, las actividades relacionadas con la Seguridad de la Información y la Seguridad Cibernética son tratadas por los siguientes organismos:

a. Consejo de Defensa Nacional (CDN)[6]: órgano de estado asesor al presidente de la república en asuntos relacionados con la soberanía nacional y la defensa del Estado de derecho democrático. Tiene su Secretaría Ejecutiva ejercida por el ministro jefe del Gabinete de Seguridad Institucional de la Presidencia de la República (GSI-PR). Las competencias del CDN están previstas en el artículo 91 de la Constitución Federal de 1988[7] y la reglamentación de su organización y de su funcionamiento está contenida en la Ley núm. 8.153, del 11 de abril de 1991.[8]

b. Cámara de Relaciones Exteriores y Defensa Nacional (Creden): es un órgano de gobierno para asesoramiento del presidente de la república en los asuntos pertinentes a las relaciones exteriores y a la defensa nacional. Su presidencia corresponde al ministro jefe del GSI-PR y, entre sus atribuciones, se encuentra la seguridad de la información, actividad que se inserta en el ámbito del sector cibernético. Sus competencias, organización y normas de funcionamiento están contenidas en el Decreto Nº 4.801, de 6 de agosto de 2003;[9]

c. Casa Civil de la Presidencia de la República:[10] Entre sus atribuciones vale destacar, por su relación con el sector cibernético, aquella relacionada con la ejecución de las políticas de certificados y normas técnicas y las operaciones aprobadas por el Comité de Infraestructura de Claves Públicas Brasileñas (ICP-Brasil). Esta atribución es competencia del Instituto Nacional de Tecnología de la Información, una autoridad federal vinculada a la Casa Civil de la Presidencia de la República, que tiene el objetivo de mantener la ICP--Brasil, que es la Autoridad Certificadora Raíz en la cadena de certificación.

d. El GSI-PR:[11] Es el órgano de la Presidencia de la República responsable de la coordinación, en el ámbito de la Administración Pública Federal (APF), de asuntos estratégicos que afectan la seguridad de la sociedad y del Estado, tales como: Seguridad de las ICN, Seguridad de la Información y las Comunicaciones (SIC) y Seguridad Cibernética.

Para que pueda cumplir la asignación de coordinar las actividades de Seguridad de la Información, el GSI-PR cuenta, en su estructura organizacional, con tres órganos subordinados, a saber:

a. Departamento de Seguridad de la Información y las Comunicaciones (DSIC): Tiene la atribución de operacionalizar las actividades de SIC en la APF, en los siguientes aspectos: reglamentar la SIC para toda la APF; capacitar a los servidores federales, así como a los terciarios, sobre SIC; realizar acuerdos internacionales de intercambio de información confidencial; representar al país ante la Organización de Estados Americanos para asuntos de terrorismo cibernético; y mantener el Centro de Tratamiento y Respuesta a Incidentes de Redes de la APF (CTIR-GOV).

b. Agencia Brasileña de Inteligencia (ABIN): Es el órgano central del Sistema Brasileño de Inteligencia (SISBIN), que tiene como objetivo estratégico desarrollar actividades de inteligencia dirigidas a la defensa del Estado de derecho democrático, de la sociedad, de la eficacia del poder público y de la soberanía nacional. Entre sus atribuciones, a la que involucra específicamente el sector cibernético, se destaca la de evaluar las amenazas internas y externas al orden constitucional, entre ellas la cibernética.

c. Centro de Investigación y Desarrollo de Seguridad de las Comunicaciones (CEPESC): tiene como atribución buscar promover la investigación científica y tecnológica aplicada a proyectos de seguridad de las comunicaciones.

Otro dispositivo importante que trata del asunto en pauta es el Decreto Núm. 3.505, del 13 de junio de 2000,[12] que aprueba la Política de Seguridad de la Información para su aplicación en los órganos de la APF y confiere a la Secretaría Ejecutiva del CDN, asesorada por el Comité Administrador de Seguridad de la Información, creado por ese mismo Decreto, y apoyado por la ABIN, por intermedio de su Centro de Investigación y Desarrollo para la Seguridad de las Comunicaciones, diversas atribuciones para la implementación de medidas relativas al tema en cuestión.

En el análisis de estos dispositivos legales y el Decreto Núm. 9.031, del 12 de abril de 2017,[13] que aprueba la estructura regimental del GSI-PR, se verifica que el GSI-PR centraliza la coordinación de la gran mayoría de las medidas relativas

a la Seguridad Cibernética y sus áreas de Seguridad de la Información y de las Comunicaciones y Seguridad de las Infraestructuras Críticas.

Además del ya citado Comité de Seguridad de la Información, el GSI-PR coordina otros organismos importantes, como grupos de trabajo y grupos técnicos relacionados con la seguridad de las infraestructuras críticas, seguridad de las infraestructuras críticas de la información, seguridad cibernética y criptografía.

En cuanto a las ICN, la END selecciona seis áreas prioritarias, a saber: energía, telecomunicaciones, transporte, agua, finanzas e información, siendo que esta última, penetra todas las anteriores, pues las IC dependen cada vez más de redes de informática para a su gerencia y control.

Defensa Cibernética

El Ministerio de Defensa (MD) y las Fuerzas Armadas, como miembros de la APF, ya participan activamente en el esfuerzo nacional en las áreas de Seguridad de la Información y Comunicaciones, Seguridad Cibernética y Seguridad de las Infraestructuras Críticas.

A pesar de la participación activa en las áreas citadas, el MD lidera la ampliación de esas actividades y de los marcos para atender al amplio espectro de las operaciones características de la Defensa Cibernética, abarcando:

a. En el nivel estratégico: las acciones cibernéticas necesarias para la actuación de las Fuerzas Armadas en situaciones de crisis o conflicto armado e incluso, en carácter episódico, en situación de paz o normalidad institucional, al recibir mandato para ello, como sucedió, por ejemplo, en la Copa del Mundo de 2014 y en los Juegos Olímpicos de 2016.

b. En el nivel operativo: las acciones cibernéticas, defensivas y ofensivas, relativas a la preparación (capacitación, adiestramiento o entrenamiento) y al empleo en operaciones militares, de cualquier naturaleza e intensidad, que caracterizan el ambiente de la Guerra Cibernética.

La END formula directrices para la preparación y el empleo de las Fuerzas Armadas en atención a sus hipótesis de empleo, definiendo acciones que deben ser observadas desde el tiempo de paz, especialmente las relacionadas con los tres sectores estratégicos establecidos - el espacial, el cibernético y el nuclear.

Con el fin de dar provisión a lo establecido en la END para esos sectores estratégicos, el MD emitió, el 9 de noviembre de 2009, la Directriz Ministerial Núm. 14,[14] definiendo responsabilidades sobre la coordinación y el liderazgo en la conducción de las acciones referentes a los sectores nuclear, cibernético y espacial, respectivamente, a la Marina, al Ejército ya la Aeronáutica.

En la referida directriz se estableció que los trabajos fueran desarrollados en dos fases: en la primera, se definiríam los objetivos de cada sector y el alcance del tema; y en la segunda, se definirían las acciones estratégicas y se elaborarían las propuestas de estructuras, con el máximo aprovechamiento y adecuación de las ya existentes.

En lo que se refiere al sector cibernético, el Ejército concluyó la primera fase en diciembre de 2009, con base en los estudios y propuestas de un Grupo de Trabajo (GT) . Los trabajos de ese grupo prosiguieron y el Ejército concluyó la segunda fase en marzo de 2010.

El MD aprobó las propuestas del Ejército, las cuales establecieron los objetivos estratégicos a ser alcanzados para el sector cibernético, junto con las acciones estratégicas previstas para cada uno de ellos.[15]

Los objetivos estratégicos aprobados incluyen acciones dirigidas especialmente para las actividades de Seguridad de la Información y Comunicaciones, Seguridad Cibernética y Seguridad de las Infraestructuras Críticas, tanto en el ámbito del MD como en la participación colaborativa, a nivel nacional, con las demás instituciones involucradas, en interacción con estas, principalmente con el GSI-PR.

Esta participación colaborativa entre el MD y las instituciones involucradas a nivel nacional, pudo ser puesta en práctica en los dos últimos grandes eventos internacionales ocurridos en Brasil, que fueron la Copa del Mundo de 2014 y los Juegos Olímpicos de 2016, conforme al modelo presentado en la Figura 1, donde, a pesar de la diversidad de organizaciones involucradas, los trabajos ocurrieron con fluidez, colaborando para el éxito de esos eventos.

Figura 1 - Modelo de participación colaborativa empleado en los dos últimos grandes eventos ocurridos en Brasil (Fuente: disponible por el ComDCiber, el 18 de agosto de 2018)

En el área de Defensa Cibernética, cabe destacar dos acciones estratégicas, ya consolidadas, referentes al objetivo estratégico número uno, que establece la creación de una estructura de Defensa Cibernética subordinada al Estado Mayor Conjunto de las Fuerzas Armadas para insertar el tema en los planteamientos militares conjuntos y la creación del Comando de Defensa Cibernética de las Fuerzas Armadas (ComDCiber) para dar cumplimiento a los objetivos estratégicos establecidos para el sector y sus acciones estratégicas correspondientes.

Bajo la coordinación del Núcleo del ComDCiber, a partir de 2015 y después de su vigencia en 2016, varias Acciones Sectoriales de Defensa fueron consolidadas, como la implantación del Sistema Militar de Defensa Cibernética y varias otras fueron iniciadas, como la promoción de la interoperabilidad del sector cibernético en la Defensa Nacional, la creación e implementación de la Escuela Nacional de Defensa Cibernética, la creación e implementación del Sistema de Homologación y Certificación de Productos de Defensa Cibernética, la capacitación y generación de recursos humanos necesarios para la conducción de las actividades del sector cibernético en el ámbito de la defensa nacional, la implementación del Sistema de Informaciones Seguras, con enfoque en el área de SIC, la contribución al fomento de la investigación y del desarrollo de productos de defensa y la contribución a la producción del conocimiento de inteligencia oriundo de la fuente cibernética.

Como podemos percibir, en el área de Defensa Cibernética, ya están establecidos los parámetros básicos para la expansión, el perfeccionamiento y la consolidación del sector, en atención a lo establecido en la END y a las demandas para alcanzar una estructura sistémica eficaz, a nivel nacional.

Acciones propuestas

Al analizar la situación actual de la Seguridad y Defensa Cibernética en Brasil, constatamos que hay varias normas que estructuran y orientan el sector y, aun así, no tenemos los órganos que componen las ICN, los órganos estratégicos del Gobierno y el Ministerio de Defensa integrados e interactuando de forma sistémica. Preguntamos: ¿Por qué aún no ha sido posible esta integración más estrecha de todos los entes implicados en este proceso? ¿Qué falta? Para intentar responder a estas preguntas, a continuación, proponemos ciertas sugerencias de acciones.

Con respecto a la Seguridad Cibernética, como se ha mostrado, varias acciones ya se han tomado para proteger y garantizar la utilización de activos de información estratégicos, principalmente los relacionados con las infraestructuras críticas de la información que controlan las ICN. Sin embargo, aún no se consigue una interacción efectiva que proporcione la tan anhelada integración de todos los órganos públicos y privados involucrados en el funcionamiento de las ICN, especialmente los órganos de la APF.

En este sentido, es imperativo que todos los entes involucrados con la Seguridad Cibernética de las ICN implementen también acciones que garanticen, primeramente, que sus activos críticos de información estén mínimamente protegidos contra las amenazas internas y externas. Para ello, deben promover acciones internas, es decir, dentro de sus propias organizaciones, para disminuir las fragilidades de sus activos de información contra ataques malintencionados y aumentar su resiliencia.

Procedimientos para la evaluación de riesgos y la gestión y continuidad de negocio

Como primer paso para disminuir las fragilidades de sus activos informacionales, es necesario realizar una evaluación de riesgos. Sólo después de esa evaluación, se tendrá una noción de las acciones que se deben tomar para que se puedan minimizar los riesgos encontrados.

Yendo al encuentro de ese objetivo, y buscando orientar a todos los órganos de la APF, el GSI-PR publicó en 2010 la "Guía de Referencia para la Seguridad de las Infraestructuras Críticas de la Información - Versión 01",[16] con el objetivo de orientar a todos los órganos de la APF. Esta guía, además de la caracterización y contextualización del tema de seguridad de las infraestructuras críticas de la información, presenta una sistemática para evaluación de riesgos con una propuesta más detallada de gestión de riesgos y continuidad de negocios.

Las acciones propuestas en esta guía deben ser ejecutadas por todos los órganos involucrados en el proceso de protección de las ICN, pues son fundamentales para la realización del próximo paso, que abarca la implantación de centros y equipos de monitoreo de amenazas, que permitirán la interacción y el cambio de información con los órganos de seguimiento y control.

Creación de Centros y Equipos de Tratamiento de Incidentes de Redes

Con el fin primordial de atender a los incidentes en redes de ordenadores pertenecientes a la APF, el DSIC, instituyó el Centro de Tratamiento de Incidentes de Seguridad de Redes de Computadoras de Administración Pública, CTIR-Gov, que es el Centro de Manejo de Incidentes de Seguridad de la Red de Computadoras para la administración pública federal.

En el marco de la Coordinación General de Tratamiento de Incidentes de Redes (CGTIC),[17] corresponde al CTIR-Gov, operar y mantener el Centro de Tratamiento de Incidentes de Seguridad en las Redes de Computadoras de la APF-CTIR-Gov; promover el intercambio científico-tecnológico relacionado con los incidentes de seguridad de en las redes de computadoras junto a otros centros;

apoyar órganos y entidades de la APF en las actividades de tratamiento de incidentes de seguridad de en las redes de computadoras; supervisar y analizar técnicamente los incidentes de seguridad en las redes de computadoras de la APF; implementar mecanismos que permitan la evaluación de los daños ocasionados por incidentes de seguridad en las redes de computadoras de la APF; y apoyar, fomentar y contribuir en el ámbito de la APF para la capacitación en el tratamiento de incidentes de seguridad en las redes de computadoras.

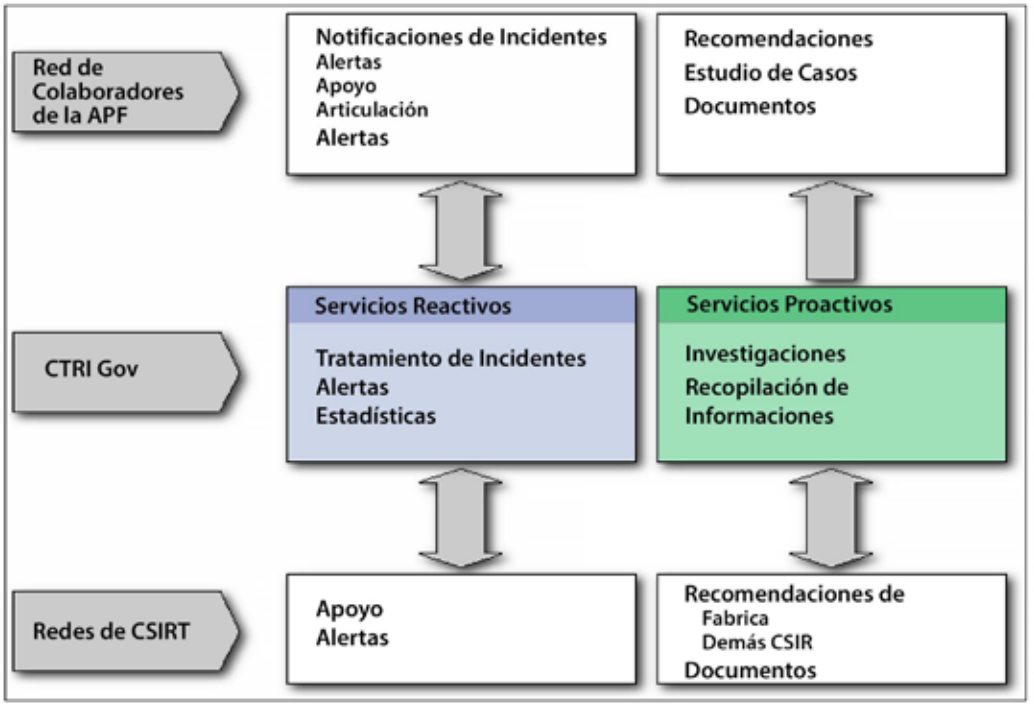

Figura 2 - Interacciones del CTIR Gov

Un incidente de seguridad es cualquier evento adverso, confirmado o bajo sospecha, relacionado con la seguridad de los sistemas informáticos o de las redes de computadoras. El proceso de tratamiento de incidentes, como se muestra en la Figura 2, es básicamente dividido en:

a. Notificación del incidente: La recepción de notificaciones de incidentes le permite al CTIR-Gov actuar como punto central para coordinar soluciones de los problemas resultantes, a través de la recopilación de actividades e incidentes reportados, análisis de las informaciones y correlación de éstas en el ámbito de la organización informante o de la comunidad de la APF. La información puede ser utilizada también para determinar tendencias y patrones

de actividades de ataques y para recomendar estrategias de prevención adecuadas para toda la APF.

b. Análisis de incidentes: Esta actividad consiste en examinar toda la información disponible sobre el incidente, incluyendo artefactos y otras evidencias relacionadas con el evento. El propósito del análisis es identificar el alcance del incidente, su extensión, su naturaleza y los daños causados. También forma parte del análisis del incidente proponer estrategias de contención y recuperación.

c. Apoyo a la respuesta de incidentes: En este caso, el CTIR-Gov auxilia en el proceso de recuperación. Esta ayuda se presta por correo electrónico o por la indicación de documentos que puedan ayudar en el proceso de recuperación. Esta actividad puede implicar la ayuda en la interpretación de los datos recopilados y en la recomendación de estrategias de contención y recuperación.

d. Coordinación en la respuesta de incidentes: En esta actividad, el CTIR-Gov coordina las acciones entre los involucrados en un incidente, lo que puede incluir redes y otros centros de tratamiento (CSIRT) externos a su ámbito de actuación. El proceso de coordinación implica la recopilación de información de contactos, la notificación de los responsables de las redes, computadoras o sistemas que puedan estar involucrados o comprometidos y la generación de indicadores y estadísticas relativos a los incidentes. El CTIR-Gov actúa como un facilitador en el proceso de recuperación de los incidentes y en el intercambio de información entre las partes implicadas.

e. Distribución de alertas, recomendaciones y estadísticas: Esta actividad consiste en diseminar información relativa a nuevos ataques o tendencias de ataques observados por el CTIR-Gov, por otros centros de tratamiento o por empresas especializadas. Estas alertas, en general, son producidas por el propio CTIR-Gov, basadas en las notificaciones recibidas o en incidentes tratados, o son redistribuciones de alertas emitidas por otros centros con responsabilidad nacional. El CTIR-Gov, al redistribuir alertas, puede añadir recomendaciones específicas para su audiencia y asignar diferentes grados de severidad.

f. Cooperación con otros equipos: El CTIR-Gov, a través de la coordinación general, actúa en la implementación de acuerdos de cooperación con otros Equipos de Tratamiento de Incidentes de la APF, así como con otros CSIRT, públicos y privados, nacionales e internacionales, con miras a la cooperación técnica y la ayuda mutua en el tratamiento de incidentes de seguridad.

Por medio de la Instrucción Normativa Nº 1,[18] el GSI-PR orienta a los órganos y entidades de la APF, directa e indirectamente, discriminando todas las acciones necesarias para implementar la Gestión de Seguridad de la Información y Comunicaciones. Entre estas orientaciones, se puede destacar: nombrar al gestor del SIC; instituir e implementar Equipo de Tratamiento y Respuesta a Incidentes en Redes Computacionales (ETIR); y aprobar la política del SIC y demás normas de seguridad de la información y comunicaciones.

Con respecto a la creación de las ETIR en los órganos y entidades de la APF, directa e indirectamente, el GSI-PR editó la Norma Complementaria Nº 5,[19] la cual disciplina la creación de esos equipos.

En esta Norma Complementaria, además de ofrecer varios modelos de implementación de las ETIR, se presentan muchas maneras diferentes de que estos equipos sean estructurados, dependiendo del modelo de implementación a ser adoptado, del tamaño de la organización, del número de ubicaciones geográficas distribuidas y en dónde las funciones están localizadas, del número de sistemas y plataformas apoyados, del número de servicios a ofrecerse y del conocimiento técnico del personal existente.

Al igual que las normas citadas arriba, el GSI-PR editó otras normas complementarias que vienen auxiliando a todos los órganos de la APF a estructurar y operacionalizar la protección de sus redes computacionales.

Aprovechando toda esa experiencia exitosa de la APF, se propone que todas las entidades que componen las ICN adopten esta misma estructura para el tratamiento de los incidentes de red computacional, es decir: implementación de CTIR y ETIR en todos los actores que se ocupan de la seguridad de las personas y las infraestructuras críticas del país.

Una forma de implementar esta estructura sería:

a. La creación de un CTIR en cada agencia reguladora de las áreas prioritarias, como por ejemplo: Comunicaciones (ANATEL), Energía (ANEEL), Agua (ANA), Transportes (ANTT).

b. La creación de las ETIR en los diversos órganos que componen las ICN, por ejemplo, energía eléctrica: una ETIR en cada una de las Operadoras, Distribuidoras, Transmisoras y Generadoras de energía eléctrica, conectadas al CTIR de la ANEEL.

c. La conexión de todos los CTIR, incluyendo el Comando de Defensa Cibernética (ComDCiber), que actuaría como un CTIR del Ministerio de Defensa, al CTIR-Gov u otro órgano que pueda ser creado para ese fin. En ese caso, el CTIR-Gov también estaría vinculado a ese órgano.

Con la creación de esos CTIR y ETIR, estarían abiertas las puertas para una mayor interacción entre todas las entidades vinculadas a la Seguridad y Defensa Cibernética de las ICN. Además, se lanzaría la base para la creación y efectividad de un Sistema de Seguridad y Defensa Cibernética Brasileña.

Creación del Sistema de Seguridad y Defensa Cibernética Brasileña

Como se puede observar de lo que fue hasta aquí presentado, Brasil ya posee una estructura básica significativa en las áreas de Seguridad Cibernética (aquí incluida la Seguridad de la Información y de las Comunicaciones y Seguridad de las Infraestructuras Críticas) y Defensa Cibernética.

En el área de Seguridad Cibernética, la estructura actual confiere ventaja fundamental al concentrar la coordinación de las acciones principales en un órgano de la estructura de la presidencia de la república, en el caso del GSI-PR.

El trabajo del GSI-PR en ese sector es facilitado por su estructura organizacional que permite congregar esfuerzos de las principales áreas de interés, reuniendo los campos técnicos de la actividad a la inteligencia, a la prevención y gestión de crisis y al campo militar.

Otro factor relevante es la responsabilidad atribuida al GSI-PR de ejecutar las actividades necesarias para el ejercicio de las competencias del CDN y de Creden, organismos que poseen prerrogativas esenciales dirigidas al sector cibernético en los campos de las decisiones estratégicas, en el caso del CDN y de la formulación de las normas políticas públicas y directrices, así como de la articulación de acciones que involucren más de un ministerio, en el caso del Creden.

Por lo tanto, es deseable que se mantengan todas esas atribuciones vinculadas a un órgano de la estructura de la Presidencia de la República, en el caso actual el GSI-PR, que actuaría como Órgano Central de ese Sistema.

Esto se aplica también a las actividades de Defensa Cibernética, que, aunque están más directamente ligadas al Ministerio de Defensa y a las Fuerzas Armadas, necesitan la vinculación al CDN, a las decisiones estratégicas y a la Creden, principalmente para la articulación de acciones con otros organismos públicos y privados de interés.

Tomando como punto de partida las propuestas presentadas por OLIVEIRA,[20] se propone el fortalecimiento de las estructuras ya existentes y la adopción de mecanismos que proporcionen su actuación sistémica, como la formulación de las políticas y directrices públicas correspondientes y de la emisión de dispositivos legales que amparen y regulen la actuación articulada de los órganos participantes del sistema.

De una forma simplificada, la Figura 3 presenta una visión general del Modelo Institucional del Sistema de Seguridad y Defensa Cibernética Brasileño, adaptado de BARROS.

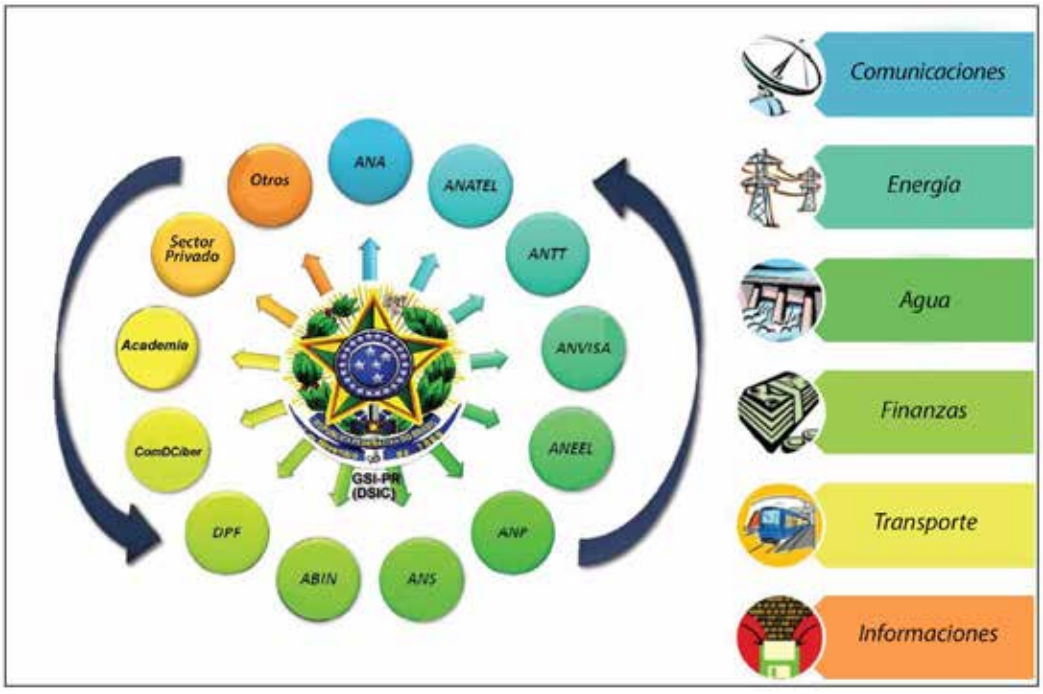

Figura 3 - Modelo Institucional del Sistema de Seguridad y Defensa Cibernética Brasileño (adaptado BARROS)

En cuanto a la Defensa Cibernética, los objetivos estratégicos y las acciones estratégicas correspondientes ya están establecidas, como se ha explicado anteriormente, se trata ahora de buscar implementarlos.

Para hacer viable la creación de este sistema y facilitar los entendimientos para su aplicación, es necesario el establecimiento de un GT Interministerial de alto nivel, en el marco de la Creden, a fin de estudiar y proponer la organización de este nuevo sistema en la expansión, adecuación y perfeccionamiento de las estructuras existentes.

Otro punto importante a destacar es la imperiosa necesidad del sistema de contemplar la participación y la interacción permanent con la actividad de inteligencia.

Integración de las actividades de Inteligencia a la Seguridad y Defensa Cibernética

La actividad de inteligencia desempeña un papel fundamental en los ambientes de Seguridad y Defensa Cibernética. Es esencial en la búsqueda de información, emple-

ando todas las fuentes disponibles, para identificar y prevenir amenazas cibernéticas y proporcionar respuestas adecuadas, con oportunidad. Además, los profesionales que actúan en el sector cibernético deben desarrollar una actitud intrínseca de contrainteligencia, a fin de proteger el conocimiento y la información inherentes a sus actividades.

En este particular, es importante la expansión de las actividades de Inteligencia de Señales para abarcar, también, las necesidades cibernéticas, como está ocurriendo en otros países. Se podría aprovechar la experiencia de actuación en ese ambiente de las Fuerzas Armadas y del SISBIN. Por lo tanto, los órganos de inteligencia del SISBIN deben cumplir actividades importantes, dentro del Sistema de Seguridad y Defensa Cibernética Brasileño.

Consideraciones finales

Si, por una parte, los avances obtenidos en el área de Tecnología de la Información y de las Comunicaciones facilitan nuestras vidas y traen beneficios importantes para la humanidad en su conjunto, por otro lado, traen también efectos colaterales nocivos con los que tenemos que aprender a tratar. Así como el espacio cibernético evoluciona, es de esperar que las amenazas y los desafíos que emanan de él también evolucionen.

La amenaza cibernética es patente y real. Se revela en la rutina de las personas e instituciones, tanto en los ambientes individuales, colectivos o profesionales y se estampa en el noticiero de los medios de comunicación prácticamente todos los días.

En el ambiente estratégico del Estado, el combate a esta amenaza debe formar parte de sus prioridades, a fin de prevenir daños a la sociedad y al propio Estado, que pueden asumir proporciones considerables. En Brasil, a pesar de ser relativamente reciente la preocupación con el tema, las acciones se han intensificado en los últimos años.

En el campo de la Seguridad Cibernética, las acciones ganaron mayor impulso a partir de la creación del DSIC en el GSI-PR, en 2006, y en el campo de la Defensa Cibernética, énfasis mayor pasó a ser observado a partir de la edición de la END, en 2008.

De cualquier modo, el momento actual es propicio para acelerar medidas, a fin de mejorar la interacción e integración de todos los actores que lidian con la seguridad de las infraestructuras críticas nacionales y que compondrían el Sistema de Seguridad y Defensa Cibernética Brasileño. En ese sentido, se propusieron ciertas acciones para contribuir con el logro de estos objetivos:

a. Sistemática para la Evaluación y Gestión de Riesgos y Continuidad de Negocios, como el primer paso para la protección de los activos críticos de la información.
b. Creación de Centros y Equipos de Tratamiento de Incidentes de Redes (CTIR y ETIR), como una forma de facilitar la interacción y el intercambio

de informaciones entre todos las entidades involucradas en la protección de las ICN.

c. Creación del Sistema de Seguridad y Defensa Cibernética Brasileña, para sistematizar, integrar y permitir que las informaciones fluyan con rapidez, para que los actores responsables puedan tomar oportunamente las decisiones acertadas y establecer un ambiente colaborativo permanente.

d. Integración de las actividades de Inteligencia a la Seguridad y Defensa Cibernética, como una forma de predecir, prever y hasta impedir que los intentos de ataques ocurran.

En general, este trabajo buscó enfocarse en la mejora de las interacciones e integración de los órganos que componen la ICN, con relación a la Seguridad y Defensa Cibernética. Asimismo, para la estructuración y fortalecimiento de la protección cibernética de las ICN, varios otros factores, además de las propuestas aquí presentadas, deben ser considerados y analizados por el GT Interministerial, propuesto arriba, una vez que escapen el alcance de este trabajo. ❑

Notas

1. MANDARINO J.R., Raphael. Segurança e Defesa do Espaço Cibernético Brasileiro (Seguridad y defensa del espacio cibernético). Brasília. 2010. p. 38.

2. International Critical Information Infrastructures Protection Handbook 2008/2009. Center for Security Studies, ETH Zurich, p. 36-37. Apud CANONGIA, Claudia, marzo de 2009.

3. Boston Consulting Group, World Economic Forum in "Our critical infraestructure is more vulnerable than ever" (Foro Económico Mundial en "Nuestra infraestructura crítica es más vulnerable que nunca"). Disponible en: <https://www.weforum.org/agenda/2017/02/our-critical-infrastructure-is-more-vulnerable-than-ever-it-doesn-t-have-to-be-that-way/>, Consultado el 12 de agosto de 2018.

4. ENISA, Protecting Industrial Control Systems. Recommendations for Europe and Member States. (Protegiendo los sistemas de control industrial. Recomendaciones para Europa y los estados miembros), 2011. Disponible en: < https://www.enisa.europa.eu/publications/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states>. Consultado el 12 de agosto de 2018.

5. BRASIL. Presidência da República. Decreto nº 6.703. Aprova a Estratégia Nacional de Defesa, e dá outras providências. (Presidencia de la República. Decreto Núm. 6.703. Aprueba la Estrategia Nacional de Defensa y otras medidas). Brasília. Diário Oficial da União, Poder Executivo. Brasília. 19 de diciembre de 2008. Disponible en: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Decreto/D6703.htm>. Consultado el 12 de agosto de 2018.

6. BRASIL. Presidência da República. Lei nº 8.153. Dispõe sobre a organização e o funcionamento do Conselho de Defesa Nacional e dá outras providências (Ley Núm. 8.153, Dispone sobre la organización y el funcionamiento del Consejo de Defensa Nacional y otras medidas). Brasília. 11 de abril de 1991. Disponible en: <http://www.planalto.gov.br/ccivil_03/LEIS/L8183.htm>. Consultado el 12 de agosto de 2018.

7. BRASIL. Constituição da República Federativa do Brasil (Constitución de la República Federativa del Brasil). Brasília. 1988. Disponible en: < http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Consultado el 12 de agosto de 2018.

8. BRASIL. Presidência da República. Lei nº 8.183. Organização e funcionamento do Conselho de Defesa Nacional - CDN. (Presidencia de la República. Ley Núm. 8.183. Organización y funcionamiento del Consejo de Defensa Nacional – CDN). Brasília. 11 de abril de 1991. Disponible en: <http://www.planalto.gov.br/ccivil_03/LEIS/L8183.htm>. Consultado el 12 de agosto de 2018.

9. BRASIL. Presidência da República. Decreto nº 4.801. Cria a Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo Presidencia de la República. Decreto Núm. 4.801 Crea la Cámara de Relaciones Exteriores y Defensa Nacional del Consejo de Gobierno). Brasília. 6 ago. 2003. Disponible en: <http://www.planalto.gov.br/ccivil_03/Decreto/2003/D4801.htm>. Consultado el 12 de agosto de 2018.

10. BRASIL. Lei nº 13.502, de 1º de novembro de 2017. Estabelece a organização básica dos órgãos da Presidência da República e dos Ministérios (Ley Núm. 13.502 del 1º de noviembre de 2017. Establece la organización básica de los órganos de la Presidencia de la República y de los Ministerios). Disponible en: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/Lei/L13502.htm>. Consultado el 12 de agosto de 2018.

11. BRASIL. Decreto nº 9.031, de 12 de abril de 2017. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Gabinete de Segurança Institucional da Presidência da República (Decreto Núm. 9.031 del 12 de abril de 2017. Aprueba la estructura regimental y el cuadro demonstrativo de los cargos en comisión y de las funciones de confianza del Gabinete de Seguridad Institucional de la Presidencia de la República). Disponible en: <http://planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Decreto/D9031.htm>. Consultado el 12 de agosto de 2018.

12. BRASIL. Presidência da República. Decreto nº 3.505. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal (Presidencia de la República. Decreto Núm. 3.505. Instituye la Política de Seguridad de la Información en los órganos y entidades de la Administración Pública Federal). Brasília. 13 de junio de 2000. Disponible en: <http://www2.camara.leg.br/legin/fed/decret/2000/decreto-3505-13-junho-2000-368759-publicacaooriginal-1-pe.html>. Consultado el 12 de agosto de 2018.

13. BRASIL. Presidência da República. Decreto nº 9.031. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Gabinete de Segurança Institucional da Presidência da República. (Presidencia de la República. Decreto Núm. 9.031. Aprueba la Estructura Relaentaria y el Cuadro Demostrativo de los Cargos en Comisión y de las Funcioes de Confianza del Gabinere de Seguridad Institucional de la Presidencia de la República). Brasília. 12 de abril de 2017. Disponible en: <http://planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Decreto/D9031.htm>. Consultado el 12 de agosto de 2018.

14. BRASIL. Ministério da Defesa. Diretriz Ministerial nº 14. Integração e Coordenação dos Setores Estratégicos de Defesa (Ministerio de Defensa. Directriz Ministerial Núm. 14. Integración y Coordinación de los Sectores Estratégicos de Defensa). Brasília. 9 de noviembre de 2009. Disponible en: <https://www.defesa.gov.br/arquivos/File/legislacao/emcfa/portarias/0014_2009.pdf>. Consultado del 18 de agosto de 2018.

15. BRASIL. Ministério da Defesa. Portaria Normativa nº 2.621. Aprova a Estratégia Setorial de Defesa (Ministerio de Defensa. Instrucción Normativa Núm. 2.621. Aprueba la Estrategia Sectorial d Defensa). Brasília. 7 de diciembre de 2015. Disponible en: <http://pesquisa.in.gov.br

/imprensa/jsp/visualiza/index.jsp?data=09/12/2015&jornal=1&pagina=32&totalArquivos=136>. Consultado el 18 de agsto de 2018.

16. BRASIL. Presidência da República. Gabinete de Segurança Institucional da Presidência da República. Guia de Referência para a Segurança das Infraestruturas Críticas da Informação. Versão 1 (Presidencia de la República. Guía de Referencia para la Seguridad de las Infraestructuras Críticas de Información. Versión 1). Brasília. Noviembre de 2010. Disponible en: <http://dsic.planalto.gov.br/legislacao/2_Guia_SICI.pdf>. Consultado el 12 de agosto de 2018.

17. BRASIL. Presidência da República. Gabinete de Segurança Institucional da Presidência da República. Portaria nº 13 (Presidencia de la República. Gabinete de Seguridad Institucional de la Presidencia de la República. Instrucción Núm. 13). Brasília. 4 de agosto de 2006.

18. BRASIL. Presidência da República. Gabinete de Segurança Institucional da Presidência da República. Instrução Normativa Nº 1 (Presidencia de la República. Gabinete de Seguridad Institucional de la Presidencia de la República. Instrucción Normativa Núm. 1). Brasília. 13 de junio de 2008. Disponible en: <https://www.governodigital.gov.br/documentos-e-arquivos/legislacao/14_IN_01_gsidsic.pdf>. Consultado el 19 de agosto de 2018.

19. BRASIL. Presidência da República. Gabinete de Segurança Institucional da Presidência da República. Norma Complementar nº 5 (Presidencia de la República. Gabinete de Seguridad Institucional de la Presidencia de la República. Norma Complementaria Núm. 5). Brasília. 14 de agosto de 2009. Disponible en: <http://dsic.planalto.gov.br/legislacao/nc_05_etir.pdf>. Consultado el 19 de agosto de 2018.

20. OLIVEIRA, J.R. Sistema de Segurança e Defesa Cibernética Nacional: Abordagem Com Foco nas Atividades Relacionadas à Defesa Nacional. In: Desafios Estratégicos Para a Segurança e Defesa Cibernética. 1ª Edição (Sistema de Seguridad y Defensa Cibernética Nacional: Enfoque en las Actividades Relacionadas con la Defensa Nacional. En: Desafíos Estratégicos para la Seguridad y Defensa Cibernética. 1ª Edición). 2011. Brasília. Anais... Brasília: Imprensa Nacional, 2011.

Brigadier de la Reserva Pedro Arthur Linhares Lima, PhD, Fuerza Aérea Brasileña

Egresado de la Academia de la Fuerza Aérea. Extensión en Análisis de Sistemas en la PUC-RJ. Maestría en Ciencias de Computación del Instituto de Tecnología de la Fuerza Aérea de Estados Unidos. Doctor en Ciencias en Ingeniería de Producción de la COPPE/UFRJ. Maestría en Administración de Empresas en Política y Estrategia de la COPPEAD-UFRJ. Fue Jefe del Centro de Computación de Aeronáutica de São José dos Campos; Subdirector de Sistemas e Infraestructura de TI, Subdirector de Proyectos de TI, Asesor-Jefe de Gobierno de TI y Director de Tecnología de la Información de la Aeronáutica. Actualmente es Investigador y Profesor del Programa de Postgrado en Ciencias Aeroespaciales de la Universidad de la Fuerza Aérea - UNIFA.