

..

El papel de los CERTs en la Estrategia Nacional de Ciberdefensa



DERECHOS DE USO

La presente documentación es propiedad de la Superintendencia de Servicios de Certificación Electrónica SUSCERTE, tiene carácter privado y confidencial y esta dirigido exclusivamente a su(s) destinatario(s), no podrá ser objeto de reproducción total o parcial, ni transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, digital, registro o cualquier otro, no podrá ser distribuido sin el permiso previo y escrito de SUSCERTE, bajo ningún concepto. Si usted ha recibido este mensaje por error, debe evitar realizar cualquier acción descrita anteriormente, asimismo le agradecemos comunicarlo al remitente y borrar el mensaje y cualquier documento adjunto. El incumplimiento de las limitaciones señaladas por cualquier persona que tenga acceso a la documentación será sancionada conforme a la ley.



El papel de los CERTs en la Estrategia Nacional de Ciberdefensa

Son múltiples los ejemplos que atestiguan la amenaza real que representan los ataques telemáticos para la Seguridad Nacional de un país y de los servicios básicos ofrecidos a sus ciudadanos. El ciberespacio ha pasado a ser otro frente a defender por los Estados, en el que se libran todo tipo de batallas y en el que los atacantes son múltiples, sofisticados y, en numerosos casos, anónimos. El consenso internacional sitúa a los Equipos de Respuesta a Incidentes Telemáticos (CERTs) como una de las principales herramientas para hacer frente a este tipo de ataques. Sus servicios, tal y como los que viene desarrollando el VenCERT desde su creación en el año 2009, contribuyen sin lugar a dudas a proteger el funcionamiento normal de un país, la información almacenada en todos sus sistemas y la defensa y seguridad nacional.

En los últimos meses asistimos a la proliferación en todo el mundo del desarrollo, más o menos profuso, de diferentes estrategias nacionales de defensa. Analizar los intereses de una Nación, sus riesgos y amenazas, así como su capacidad de respuesta y las principales herramientas para garantizar la seguridad del país suele ser el principal objetivo de este tipo de proyectos.

Esta proliferación no es casual. Hoy en día, la mayor parte de los países han decidido adecuar su “Seguridad nacional” a los nuevos tiempos, actualizando la dimensión de la misma e incluyendo un nuevo espacio a defender, con unas fronteras poco tangibles, y con un enemigo en constante evolución y perfeccionamiento: el ciberespacio.

Así pues, la defensa de la Nación¹, que tradicionalmente ha estado soportada por el Ejército, la Armada y Aviación (además de la Guardia Nacional en el caso venezolano) está siendo “repensada” ante este nuevo escenario en el que, la información se ha convertido en un arma estratégica de primer orden, cuyo manejo puede poner en cuestión la gobernabilidad de un país. Por ello, la ciberdefensa es un factor clave dentro de cualquier Estrategia Nacional de Defensa que se precie.

Así lo han entendido buena parte de los gobiernos y así lo recomiendan organizaciones internacionales expertas en la materia, como la Unión Internacional de Telecomunicaciones (UIT), la Agencia Europea de Seguridad de las Redes y la Información (ENISA) o la Organización de Estados Americanos (OEA). La UIT², por ejemplo, señala que *“un buen programa de ciberseguridad nacional contribuirá a proteger el funcionamiento normal de la economía de un país, a promover la continuidad de la planificación en todos los sectores, proteger la información almacenada en los sistemas de información, preservar la confianza*

¹ Recogida en el caso de la República Bolivariana de Venezuela en el artículo 9 de la Ley Orgánica de la Fuerza Armada Nacional, que entró en vigencia el 26 de septiembre de 2005

² <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf>

pública, mantener la seguridad nacional y garantizar la salud y la seguridad públicas”.

Gran Bretaña³, Estados Unidos⁴, Nueva Zelanda⁵, España⁶, Argentina⁷ o Colombia⁸ son algunos de los países que han hecho pública una Estrategia o Programa Nacional de Ciberdefensa en los últimos meses.

En el caso de la República Bolivariana de Venezuela, ya en el año 2001, se creó la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE)⁹, integrado a la estructura orgánica del Ministerio del Poder Popular para la Ciencia, Tecnología e Industrias Intermedias desde 2009, y cuya misión es “*desarrollar y promover los Sistemas Nacionales de Seguridad de Información, Certificación Electrónica y Gestión de Incidentes Telemáticos, como herramientas habilitadoras del desarrollo tecnológico nacional, favoreciendo la inclusión del soberano en los servicios de gobierno electrónico y fortaleciendo los Sistemas de Información de los Órganos y Entes del Poder Público Nacional*”. Uno de sus objetivos estratégicos es, además, “*contribuir al desarrollo de la soberanía nacional en materia de seguridad de la información*”.

En este sentido, en el año 2009, se constituyó, en el seno de SUSCERTE, el VenCERT: el Sistema Nacional de Gestión de Incidentes Telemáticos cuyo principal objetivo, como CERT gubernamental (más adelante se abordará este aspecto) es la prevención, detección y gestión de los incidentes generados en los sistemas de información de la Administración Pública Nacional y los Entes Públicos a cargo de la gestión de Infraestructuras Críticas de la Nación. Según la propia visión del VenCERT, sus servicios *permitirán proteger y garantizar la defensa y seguridad de la Nación, así como la suprema vigilancia de los intereses generales de la República, la conservación de la paz pública y la recta aplicación de la ley en todo el territorio nacional*.

Amenazas reales contra objetivos concretos

Todas las iniciativas o programas en materia de ciberseguridad anteriormente citadas son la respuesta de los distintos gobiernos al continuo incremento de las amenazas y ataques a través de Internet (en el ciberespacio), provenientes de muy diversos frentes: servicios de inteligencia extranjeros, propaganda subversiva, terrorismo, crimen organizado, espionaje industrial... Ataques que pueden llegar a interrumpir e incluso inutilizar los servicios esenciales de un país (aquellos ofrecidos por las denominadas infraestructuras críticas, como energía, transporte, comercio, sistema financiero, etc..) provocando un impacto considerable

³Cyber Security Strategy of the United Kingdom. Safety, security and resilience in cyber space. June 2009. Cabinet Office. www.cabinetoffice.gov.uk

⁴The Comprehensive National Cybersecurity Initiative. Año 2010.
<http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative>

⁵<http://www.med.govt.nz/upload/New%20Zealands%20Cyber%20Security%20Strategy%20June%202011.pdf>

⁶<http://www.lamoncloa.gob.es/ConsejodeMinistros/Enlaces/24062011Enlace2.htm>

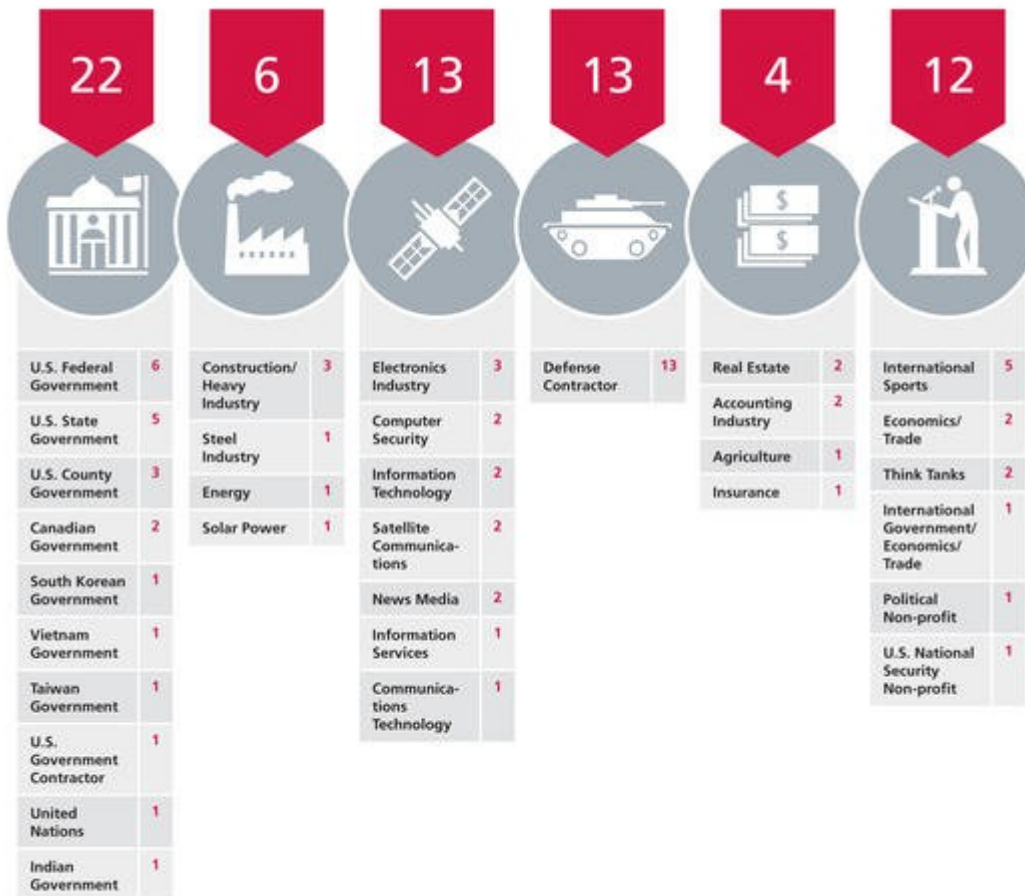
⁷<http://www.infoleg.gov.ar/infolegInternet/anexos/185000-189999/185055/norma.htm>

⁸<http://www.mindefensa.gov.co/irj/go/km/docs/documents/News/NoticiaGrandeMDN/60a20bd2-8890-2e10-7dab-8a117a5461d8.xml>

⁹Decreto- Ley N° 1.204 de fecha 10 de febrero de 2001, sobre Mensajes de Datos y Firmas Electrónicas, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 37.148 del 28 de febrero de 2001,

en su economía o, incluso, en su seguridad nacional.

Son numerosos los ejemplos que existen, el último dado a conocer por la firma McAfee¹⁰ que ha revelado que en los últimos cinco años se ha producido un ataque masivo a 72 organizaciones, gobiernos y empresas en todo el mundo. Entre los atacados figuran los gobiernos de Estados Unidos, Taiwan, India, Corea del Sur, Vietnam y Canadá; además de la ONU, la Asociación de Naciones del Sudeste de Asia (ASEAN, por su sigla en inglés); el Comité Olímpico Internacional (COI); la Agencia Mundial Antidopaje, y una serie de firmas, desde contratistas de defensa a empresas de alta tecnología.



Source: McAfee

Fig. 1 Compañías identificadas por McAfee dentro de la operación Shady RAT

Anteriormente, son conocidas las agresiones contra la OTAN, INTERPOL, el Departamento de Defensa Norteamericano, el Fondo Monetario Internacional, inclusive contra países como Letonia, Nueva Zelanda o Australia, lo que demuestra que los ciberdelincuentes están decididos a realizar ataques altamente coordinados y sofisticados, que tienen como finalidad obtener información estratégica o, como ya ha sucedido en algunos casos, sabotear las instalaciones de infraestructuras críticas, tal y como ocurrió con el ataque a los sistemas de control de supervisión y adquisición de datos SCADA en una central nuclear de Irán.

¹⁰ McAfee ha denominado a los ataques "Operación Shady RAT" en donde se utiliza un software de control remoto <http://blogs.mcafee.com/mcafee-labs/revealed-operation-shady-rat>



De hecho, la Oficina Europea de Policía, Europol, en mayo de este año publicó su informe anual sobre amenazas criminales en Europa y allí destacaba el incremento constante de las actividades delictivas a través de Internet ¹¹ (tráfico de personas, fraudes en tarjetas de pago, distribución de drogas, inmigración ilegal, comercialización de seres humanos, etc.) y, lo que es más preocupante, por medio de bandas criminales organizadas que se ponen en contacto entre ellas para ampliar su capacidad de operación y la dificultad de sus ataques.

Recomendaciones estratégicas

Ante este panorama, son muchos los estudios realizados por los distintos organismos internacionales. Entre ellos, una de las organizaciones con más prestigio internacional, la ITU ¹², considera que la problemática de la seguridad telemática requiere un esfuerzo colectivo y coordinado entre los diferentes países, y establece cinco elementos fundamentales para desarrollar una estrategia de ciberseguridad, acorde con la realidad de cada una de las naciones:

1. Desarrollo de un marco legal, incorporando en las políticas nacionales la cuestión de la ciberseguridad, persuadiendo a los actores claves del país sobre la necesidad de adoptar medidas globales para hacer frente a los ciberataques.
2. Desarrollo y aplicación de medidas técnicas y procedimentales
3. Diseño y aplicación de estructuras organizadas, encabezadas por una institución que sea la encargada de dirigir los equipos de respuesta ante estos ataques.
4. Formación y desarrollo de equipos y una cultura de ciberseguridad
5. Cooperación internacional para abordar con eficacia los ataques, dado el necesario intercambio de información y la ausencia de fronteras en este ciberespacio.

CERT/CIRT/CSIRT, entidades claves en la ciberdefensa

Un denominador común de todas las estrategias o programas nacionales de seguridad publicados hasta la fecha es la necesidad de contar con un Equipo de Intervención en caso de Incidentes de Seguridad Telemáticos. Es decir, un *CERT/CIRT/CSIRT*¹³ que actúe como punto de contacto principal del Gobierno, en especial en caso de incidentes de envergadura nacional, y que coordine la defensa frente a incidentes e intervenga si ocurren.

Volviendo a la UIT, en uno de sus últimos trabajos¹⁴ sobre las mejores prácticas para desarrollar una cultura de ciberseguridad, la organización internacional recomienda que *“el Estado cree o identifique una entidad nacional que sirva de piedra angular para la seguridad del ciberespacio y la protección de las infraestructuras de la información esencial, y cuya misión principal abarque esfuerzos de prevención, advertencia, respuesta y recuperación (reduciendo el riesgo y minimizando el impacto) y facilite la colaboración entre las entidades gubernamentales a nacional y local, así como con el sector privado, el sector académico y la*

¹¹https://www.europol.europa.eu/publications/European_Organised_Crime_Threat_Assessment_%28OCTA_%29/OCTA_2011.pdf

¹²<http://www.itu.int/osg/csd/cybersecurity/gca/new-gca-brochure.pdf>

¹³ CERT, acrónimo de *Computer Emergency Response Team* –marca registrada por el CERT-CC- sinónimo de CIRT o CSIRT.

¹⁴ ITU Study Group Q.22/1 Report on Best Practices for a National Approach to Cybersecurity: a Management Framework for Organizing National Cybersecurity Efforts. Chapter 4 <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf>



comunidad internacional”.

Esta entidad nacional (CERT nacional o gubernamental), además de las tareas propias de un CERT (véase Fig. 2), con las que cuenta, por ejemplo el VenCERT, deberá según la UIT, cumplir con los siguientes objetivos:

1. Establecer un mecanismo o procedimiento para la coordinación entre las agencias gubernamentales y las civiles (un CSIRT nacional debe saber difundir la información con la que cuenta, incluidas las amenazas y vulnerabilidades, a toda la comunidad interesada). Para ello deberá coordinarse de forma eficaz con todas ellas, por ejemplo con el mantenimiento de un sitio Web, proporcionando información vía listas de direcciones, boletines de noticias, tendencias e informes de análisis, etc.
2. Establecer relaciones de colaboración y confianza con la industria para prepararse, detectar, responder y mitigar, o llegado el caso, recuperar los sistemas dañados nacionales (particularmente aquellos que soportan infraestructuras críticas de un país).
3. Fijar un punto de contacto fijo con las agencias o departamentos estatales, industria y grupos internacionales que faciliten la cooperación e intercambio de información. Este punto de contacto dentro del CERT Nacional es fundamental si se desea contar con una respuesta coordinada y eficaz, en donde el tiempo de respuesta es clave a la hora de mitigar un ataque y minimizar su repercusión. En este sentido es preferible, en la medida de lo posible, establecer contactos basados en funciones departamentales, más que con individuos, para asegurar que los canales de comunicación permanecen abiertos, aún cuando los individuos abandonan la organización o su puesto de trabajo.
4. Participación en actividades de cooperación y colaboración internacional, sobre todo teniendo en cuenta que un ciberataque no suele circunscribirse a las fronteras nacionales y, llegado el caso, el compartir la información cuando sucede un incidente es básico para una mejor respuesta.
5. Desarrollo de herramientas y procedimientos para la protección de los recursos telemáticos de las distintas entidades gubernamentales.
6. Implantación, en el seno del CSIRT nacional de una capacidad concreta para la coordinación gubernamental en el caso de ataques a gran escala. Si se produce un incidente de especial importancia para la seguridad del país, es necesaria la existencia de un punto central de contacto que se coordine con otras entidades.
7. Promover prácticas de revelación responsables para proteger operaciones y la integridad de la infraestructura ciber

Servicios Reactivos	Servicios Proactivos	Servicios de Gestión
---------------------	----------------------	----------------------

<ul style="list-style-type: none">• Alertas y advertencias• Tratamiento de incidentes• Análisis de incidentes• Respuesta a incidentes <i>in situ</i>• Apoyo a la respuesta a incidentes• Coordinación de la respuesta a incidentes• Tratamiento de vulnerabilidades• Análisis de vulnerabilidades• Respuesta a vulnerabilidades• Coordinación de la respuesta a la vulnerabilidad• Asistencia remota a vulnerabilidades e incidentes	<ul style="list-style-type: none">• Comunicados y anuncios• Observatorio de tecnología• Evaluaciones o auditorías de la seguridad• Configuración y mantenimiento de la seguridad• Desarrollo de herramientas de seguridad• Servicios de detección de intrusos• Difusión de información relacionada con la seguridad• Programas de gestión de listas de configuración segura de sistemas TIC• Monitorización de redes	<ul style="list-style-type: none">• Análisis de riesgos• Continuidad del negocio y recuperación ante desastres• Consultoría de seguridad• Sensibilización• Educación / Formación• Evaluación o Certificación de productos
--	--	--

Fig. 2.: Lista de servicios tradicional de un CERT¹⁵

¹⁵ Handbook for Computer Security Incident Teams, del CERT/CC