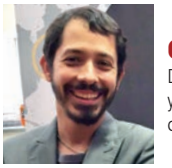

César Moliné Rodríguez
Director de Ciberseguridad, Comercio Electrónico
y Firma Digital del Indotel.
cmoline@indotel.gob.do

Hacia una Ley de Ciberseguridad para la República Dominicana[1]

RESUMEN:
La adopción de la Estrategia de Ciberseguridad de la República Dominicana 2018-2021 ha marcado un hito para el desarrollo del ciberespacio dominicano. Los retos asociados a la ciberseguridad son de naturaleza variada y compleja, siendo uno de los principales la definición del marco legal aplicable. En este artículo se describe, a grandes rasgos, los aspectos mínimos y esenciales que han de incluirse en una ley de ciberseguridad para la República Dominicana.

PALABRAS CLAVES:
Ciberseguridad, infraestructuras críticas, telecomunicaciones, República Dominicana.

En los últimos treinta años, las tecnologías de la información y las comunicaciones (TIC) han estado en constante evolución y han revolucionado desde la forma en que trabajamos hasta la forma como nos relacionamos. De la misma manera en que el uso de las TIC se amplía cotidianamente de manera significativa, así también se multiplican los riesgos y peligros asociados a su uso, a medida que aparecen nuevos servicios basados en las TIC.

Los esfuerzos por crear un ciberespacio nacional seguro pueden rastrearse a actividades que se han venido realizando por más de quince años, desde la redacción y aprobación de legislación contra el delito cibernético, hasta la ratificación de importantes tratados internacionales, como el Convenio sobre Ciberdelincuencia del Consejo de Europa, y la creación de organismos especializados para la persecución y enjuiciamiento de estos delitos, como es la Dirección de Investigación de Crímenes y Delitos de Alta Tecnología de la Policía Nacional (DICAT) y la Procuraduría Especializada en Delitos de Alta Tecnología (PEDATEC).

No obstante estas acciones, la capacidad nacional de respuesta del país para hacer frente a las amenazas e incidentes cibernéticos presenta grandes retos y oportunidades de mejora a través de la implementación de instrumentos legislativos y políticas públicas orientadas a la coordinación interinstitucional, intersectorial y fortalecimiento de la capacidad de respuesta eficaz.

Lo anterior cobra vital relevancia ante el hecho de que en el año 2016 fue aprobado por el Gobierno dominicano el programa República Digital, concebido como un conjunto de políticas y acciones que promueven la inclusión de las TIC en los procesos productivos, educativos, gubernamentales y de servicios a los ciudadanos. República Digital establece la ciberseguridad como transversal a sus cuatro ejes estratégicos.

La adopción de la Estrategia Nacional de Ciberseguridad de la República Dominicana 2018-2021 (ENCS), mediante el decreto 230-18, ha sido un momento decisivo para fortalecer el papel del país en la configuración de nuestras políticas de ciberseguridad, tanto a nivel nacional como a nivel mundial. En términos

1 Este documento ha sido preparado por César Moliné Rodríguez. Los puntos de vistas aquí expresados son aquellos del autor y no necesariamente reflejan las opiniones del Indotel y su personal o funcionarios.

generales, la visión a la que aspiramos en el país, según la ENCS, es contar con un ciberespacio más seguro, en el que estén implementadas las medidas necesarias para el desarrollo confiable de las actividades productivas y lúdicas de toda la población, dentro del marco del respeto a los derechos humanos.

Esto se propone lograrlo a través de sus cuatro pilares: i) marco legal y fortalecimiento institucional, ii) protección de infraestructuras críticas e infraestructuras TI del Estado, iii) educación y cultura de ciberseguridad y iv) alianzas nacionales e internacionales.

La ciberseguridad tiene un campo de aplicación que abarca todas las industrias, todos los sectores, tanto vertical como horizontalmente. Uno de los mayores retos que presenta la ciberseguridad es la adecuación de su marco legal.

Las medidas de carácter legal (incluidas la legislación y la regulación) autorizan a un Estado a establecer mecanismos de respuesta básicos para la investigación y el enjuiciamiento de delitos y la imposición de sanciones por el incumplimiento de la ley. Además, el marco legal establece la base mínima de comportamiento sobre la cual se soportan los demás pilares de la ENCS.

El propósito de este artículo es sentar las bases sobre puntos esenciales que debería contener una ley de ciberseguridad para la República Dominicana, especialmente en lo que se refiere a aspectos básicos del derecho administrativo, como sus organismos encargados y sus respectivas facultades legales, así como aspectos intrínsecos a la ciberseguridad, como son los requisitos y medidas para fortalecerla y las obligaciones de los operadores de infraestructuras críticas.

Por las razones expuestas, los aspectos que entendemos imprescindible cubrir en una legislación de esta naturaleza son los siguientes:

1. SOBRE EL ORGANISMO COMPETENTE Y SUS FACULTADES

El decreto 230-18 en su artículo 10 crea el Centro Nacional de Ciberseguridad (CNCS) como dependencia del Ministerio de la Presidencia de la República Dominicana. El objeto del centro es "la elaboración, desarrollo, actualización y evaluación de la Estrategia Nacional de Ciberseguridad, la formulación de políticas derivadas de dicha estrategia y la definición de las iniciativas, pro-

gramas y proyectos que lleven a la realización exitosa de esta, así como la prevención, detección y gestión de incidentes generados en los sistemas de información relevantes del Estado e infraestructuras críticas nacionales".

Ahora bien, para fortalecer su rol y facultades es necesario que dicho centro cuente con autonomía, de tal manera que el legislador le otorgue la calidad de ente de derecho público con personalidad jurídica propia, autonomía funcional, presupuestaria, administrativa, técnica y patrimonio propio, para que este pueda regular su estructura y funcionamiento. Sin embargo, debe hacerse el señalamiento de que el centro debería seguir estando sujeto a la tutela o adscripción del Ministerio de la Presidencia, de forma que pueda constatarse que su funcionamiento se ajusta a las disposiciones legales aplicables y bajo los principios que deben orientar el quehacer de su función administrativa.

2. SOBRE LA DESIGNACIÓN DE UNA INFRAESTRUCTURA COMO "INFRAESTRUCTURA CRÍTICA"

El funcionamiento de las sociedades modernas se basa en gran medida en el funcionamiento de infraestructuras críticas, como la electricidad, el gas, los puertos y aeropuertos, la gestión del agua y las tecnologías de la información y las comunicaciones. La interrupción de estas infraestructuras puede tener graves consecuencias para la economía y el bienestar de los ciudadanos.

En términos generales, las infraestructuras críticas son aquellas cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las administraciones públicas[2]. Es por esta razón que la protección de las infraestructuras críticas va más allá de la responsabilidad de las empresas, los sectores y, a veces, incluso más allá de los Estados.

En la República Dominicana, si bien es cierto que la ENCS ordena realizar un inventario de las infraestructuras críticas[3], no podemos desconocer que con anterioridad a dicho mandato ya existían disposiciones legales que hacen una mención de varios tipos de infraestructuras que podrían considerarse como críticas y de las implicaciones que tendría el ataque o amenaza a ellas[4].

En esa tesitura, la citada Ley No. 267-08, sobre Terrorismo, en su artículo 8 determina una lista de infraestructuras estratégicas, enumerando las siguientes:

a) las terminales y depósitos de combustible, propiedad del Estado o de empresas privadas;
b) los puertos de cabotaje o internacionales, los aeropuertos internos e internacionales, civiles o militares;
c) las presas, embalses, lagos, canales principales de riego, acueductos o plantas de tratamiento de agua;
d) las industrias o establecimientos públicos o propiedad de particulares que tengan especial significación en la economía del país;
e) las plataformas marítimas construidas dentro de áreas marítimas de jurisdicción nacional, incluida la zona económica exclusiva;
f) las redes de transmisión eléctrica, telefónicas, de transporte de pasajeros y de cargas, así como los sistemas de áreas protegidas conforme a la Ley General de Medio Ambiente y Recursos Naturales;
g) los sistemas de correo o envío de correspondencia, públicos y privados;
h) los monumentos nacionales de importancia histórica o cultural;
i) sistemas de generación de energía eléctrica y plataforma tecnológica.

Es cierto que la clasificación aquí realizada solo se enfoca en infraestructuras que pueden afectarse por actos de terrorismo, pero también hay que tener en cuenta que una amenaza o un ataque cibernético no necesariamente puede ser tipificado como un acto de terrorismo[5].

Es por esto que nuestra propuesta es la creación de un mecanismo por medio del cual el CNCS pueda designar un sistema de información6 como una infraestructura crítica, siempre que dicho sistema sea necesario para la prestación continua de un servicio que se haya identificado como crítico, y que la pérdida o la vulnerabilidad del sistema de información tenga un efecto debilitante en la disponibilidad de dicho servicio.

2 Al respecto ver el Marco para la mejora de la seguridad cibernética en infraestructuras críticas de los Estados Unidos (NIST Cybersecurity Framework) en el que se señala que según la Ley Patriótica de los EE. UU. de 2001 las infraestructuras críticas se consideran aquellos "sistemas y activos, ya sean físicos o virtuales, tan vitales para los Estados Unidos que la incapacidad o destrucción de dichos sistemas y activos tendría un impacto debilitador en la seguridad de la nación, la seguridad económica nacional, la salud y seguridad pública, o cualquier combinación de estos mismos", disponible en https://www.nist.gov/sites/default/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf. Visto por última vez el 24 de abril de 2019 a las 1:18 PM (UTC-4).

3 Ver el artículo 6 del Decreto 230-18 que donde se establece el objetivo específico 1 del Pilar de Protección de Infraestructuras Críticas Nacionales e Infraestructuras TI del Estado, en el cual se dispone su identificación y la determinación de su grado de criticidad.

4 En ese sentido, ver el artículo 1 de la Ley No. 267-08 sobre Terrorismo, y crea el Comité Nacional Antiterrorista y la Dirección Nacional Antiterrorista que define el término "infraestructuras estratégicas" como "toda instalación de propiedad pública o privada que se utilice para prestar o distribuir servicios al público, como los abastecimientos de agua, alcantarillado, energía, combustible o comunicaciones". Así como el artículo 5 que establece cuáles son considerados como actos de terrorismo.

5 Ver el Artículo 5 de la Ley 267-08 cuando se hace referencia a que "constituyen actos de terrorismo todos aquellos que se ejecuten empleando medios susceptibles de provocar en forma indiscriminada o atroz, muertes, heridas, lesiones físicas o psicológicas, de un número indeterminado de personas, o graves estragos materiales a infraestructuras estratégicas de la nación o propiedad de particulares, con la finalidad de:
a) Atemorizar a la población en general o determinados sectores de ésta obligando al gobierno nacional, a otro gobierno o a una organización internacional a realizar un acto o a abstenerse de hacerlo;
b) Ejercer retaliaciones fundadas por motivos políticos, étnicos, religiosos, o de cualquier otra índole; y
c) Afectar las relaciones del Estado dominicano con otros estados o su imagen exterior".

6 De acuerdo al artículo 4 de la Ley 53-07, un sistema de información es aquel dispositivo o conjunto de dispositivos que utilizan las tecnologías de información y comunicación, así como cualquier sistema de alta tecnología, incluyendo, pero no limitado a los sistemas electrónicos, informáticos, de telecomunicaciones y telemáticos, que separada o conjuntamente sirvan para generar, enviar, recibir, archivar o procesar información, documentos digitales, mensajes de datos, entre otros.

A fin de que esto pueda implementarse, dicho mecanismo debería funcionar a través de una simple notificación en la cual se especifique al menos lo siguiente:

a) identificar el sistema de información que se está designando como una infraestructura crítica;

b) informar al propietario del sistema de información sobre los deberes y responsabilidades que surjan de la designación de operador de una infraestructura crítica;

c) proporcionar el nombre y los datos de contacto del funcionario asignado por el CNCS para supervisar la infraestructura crítica.

También se hace necesario que en dicha pieza legislativa se contemple la creación de mecanismos mediante los cuales cuando una persona reciba una notificación de que ha sido designada como operador de infraestructura crítica y entienda que esta no le es aplicable deberá demostrar al CNCS que no puede cumplir con el requerimiento establecido en la notificación debido a que no tiene control efectivo sobre las operaciones del sistema de información ni la capacidad o el derecho de realizar cambios en el sistema de información. En tal caso deberá indicar quién es la persona responsable del sistema de información que tiene control, capacidad y derecho sobre dicho sistema.

En cuanto a la duración de la designación como infraestructura crítica, proponemos que se establezca un plazo de al menos cinco años durante el cual dicha designación tenga efecto, la cual podrá ser retirada por el CNCS antes de la expiración de ese período si este organismo determina que el sistema de información ya no cumple con los criterios para ser considerado como una infraestructura crítica.

3. SOBRE LAS OBLIGACIONES DE LOS OPERADORES DE INFRAESTRUCTURA CRÍTICA

Como ya indiqué, debido a la importancia de una infraestructura crítica, la operación que sea designada como tal debe comprender el cumplimiento de una serie de obligaciones en pos de salvaguardar la ciberseguridad y de aumentar la ciberresiliencia.

En tal virtud, propongo que en una futura ley de ciberseguridad se incluyan al menos las siguientes obligaciones:

Obligación de entregar información: Esta obligación comprende la entrega de información relevante relacionada con el sistema de información dentro de un período razonable, según lo requiera el CNCS, con el fin de determinar si el sistema de información cumple con los criterios de una infraestructura crítica.

La obligación aquí descrita comprende la siguiente información:

a) la función que el sistema de información cumple;

b) las personas u otros sistemas de información que son atendidos por dicho sistema;

c) información relacionada con el diseño del sistema de información;

d) información sobre el diseño, configuración y seguridad de la infraestructura crítica;

e) información sobre el diseño, la configuración y la seguridad de cualquier otro sistema de información bajo el control del propietario que esté interconectado o que se comunique con la infraestructura crítica;
f) información relacionada con la operación de la infraestructura crítica y de cualquier otro sistema de información bajo el control del propietario que esté interconectado o que se comunique con la infraestructura crítica;
g) cualquier otra información que el CNCS pueda requerir para determinar si el sistema de información cumple con los criterios de una infraestructura crítica o el nivel de ciberseguridad de la infraestructura crítica.

Debido a la naturaleza de la información aquí solicitada, es necesario contemplar excepciones o dispensas a la entrega de información que pudiese ser considerada como confidencial. En ese sentido, nuestra propuesta es que en esta pieza legislativa se contemple una disposición donde se especifique claramente que la entrega de esta información al CNCS no será considerada como una vulneración de la confidencialidad previamente establecida por leyes, reglamentos, contratos o códigos de conducta profesionales.

Con respecto a los cambios sustanciales en el diseño, la configuración, la seguridad o el funcionamiento de la infraestructura crítica, es necesario adicionalmente prever que estos sean notificados al CNCS una vez realizados. Ahora bien, para determinar si un cambio realizado se trata de un cambio sustancial en los términos aquí descritos, propongo que solo se notifiquen aquellos cambios que afecten o puedan afectar la ciberseguridad de la infraestructura crítica o la capacidad del propietario de la infraestructura crítica para responder a una amenaza o incidente de ciberseguridad que la afecte.

Obligación de notificar incidentes de ciberseguridad: Esta obligación pretende que el propietario de una infraestructura crítica deba notificar al CNCS la ocurrencia de:

a) un incidente de ciberseguridad que haya afectado a la infraestructura crítica;
b) un incidente de ciberseguridad que haya afectado a cualquier sistema de información bajo su control que esté interconectado o que se comunique con la infraestructura crítica;
c) cualquier otro tipo de incidente de ciberseguridad que el CNCS haya especificado al propietario de la infraestructura crítica.

Basado en la obligación general previamente descrita, se desprende una obligación subsidiaria que es aquella mediante la cual los propietarios de las infraestructuras críticas deberán establecer mecanismos técnicos y procedimentales con el fin de detectar amenazas e incidentes de ciberseguridad. Estos mecanismos incluyen el uso de equipos de respuesta a incidentes, la implementación de estándares de ciberseguridad, entre otros.

Obligación de realizar auditorías de ciberseguridad y evaluaciones de riesgo: En este caso lo que se propone es la creación de los medios que permitan evaluar la idoneidad del cumplimiento de medidas técnicas, estándares de desempeño y otros elementos que deben aplicar los propietarios de las infraestructuras críticas.

Para esta obligación recomiendo que se disponga la realización de auditorías de ciberseguridad y evaluaciones de riesgos al menos una vez cada dos años. Estas auditorías deberán ser comunicadas al CNCS proporcionándole una copia del informe de su resultado.

El CNCS deberá retener la facultad de que cuando constate que el informe de una auditoría realizada no se llevó a cabo de manera satisfactoria pueda ordenar al propietario de la infraestructura crítica que haga que el auditor lleve a cabo ese aspecto de la auditoría de nuevo o, en caso de que se encuentren no conformidades con el resultado de la auditoría de los sistemas, podrá ordenarle al propietario de la infraestructura crítica que lleve a cabo pasos adicionales para asegurar el nivel de ciberseguridad de dicha infraestructura crítica.

La obligación de realizar auditorías y evaluaciones de riesgo también deberá proceder cuando el propietario de una infraestructura crítica haya notificado al CNCS que ha realizado un cambio sustancial en el diseño, configuración, seguridad u operación de la infraestructura crítica.

Obligación de efectuar ejercicios de ciberseguridad: La realización de ejercicios de ciberseguridad es importante debido a que ayudan a estar preparados y saber qué hacer durante incidentes reales. Además fortalecen los planes de contingencia, mejorando así la familiaridad con las herramientas y procesos necesarios para abordar y remediar los incidentes de una mejor manera.

La obligación aquí propuesta es que tanto desde el CNCS como dentro de los operadores de infraestructuras críticas se realicen ejercicios de ciberseguridad con el fin de probar el estado de preparación de todos los involucrados en las diferentes infraestructuras críticas para responder a incidentes de ciberseguridad importantes.

4. SOBRE LA DIVULGACIÓN RESPONSABLE DE VULNERABILIDADES

Desafortunadamente, la investigación, la publicación y la divulgación de vulnerabilidades se han visto marcadas por abusos, coacciones e intimidación, desde amenazas y acciones legales presentadas por los propietarios de los sistemas y tecnologías o acciones inapropiadas por parte de las autoridades, hasta ataques públicos al carácter o la motivación de los investigadores[7].

La investigación en materia de ciberseguridad es esencial debido a que muchos de los avances en el área provienen de los grandes esfuerzos de la comunidad de investigación. Esfuerzos que pueden verse menoscabados, y con ello nuestra propia seguri-

7 Sobre este punto, ver Lawsuits threaten infosec research — just when we need it most. Disponible en https://www.zdnet.com/article/chilling-effect-lawsuits-threaten-security-research-need-it-most/. Visto por última vez el 24 de abril de 2019 a las 1:22 PM (UTC-4).

dad, por conductas como las descritas anteriormente o incluso hasta por leyes que pueden resultar vagas o erróneas, y pueden prohibir o criminalizar la investigación o la divulgación de vulnerabilidades.

Motivados por esa razón, esta propuesta va dirigida a crear un marco jurídico que auspicie la investigación, la publicación y la divulgación de vulnerabilidades, siempre que estas se hagan basadas en la buena fe. Es decir, no se consideraría que una persona infringió disposiciones legales sobre la confidencialidad, integridad y disponibilidad de datos y sistemas de información[8] o que incurrió en un incumplimiento de leyes, reglamentos, contratos y códigos de conducta profesionales por el hecho de comunicar, publicar o divulgar vulnerabilidades, siempre que esto se haga basándose en la buena fe y que se tomen en cuenta aspectos como la no solicitud de recompensas bajo coerción o amenaza de publicación de la información, así como el otorgamiento de un tiempo razonable para solucionar la vulnerabilidad antes de publicarla o divulgarla.

En resumen, las propuestas aquí esbozadas son aquellas que se consideran como el mínimo aceptable para incluir en una ley de ciberseguridad para la República Dominicana. En ningún modo consideramos que estas son exhaustivas, ni tampoco que se deben dejar de lado aspectos esenciales que caen en el marco de la ciberdelincuencia, como lo sería una posible actualización de la Ley 53-07 contra Crímenes y Delitos de Alta Tecnología.

Las amenazas a la seguridad cibernética son un problema mundial y necesitan una solución global en la que participen todos los actores involucrados, en la que exista una responsabilidad compartida del Gobierno, el sector privado y la sociedad civil en general. Justo es destacar que desde el Indotel hemos estado apoyando estos esfuerzos y seguiremos trabajando para que cada día la República Dominicana continúe dando los pasos necesarios para lograr un ciberespacio más seguro, lo cual deberá ir de manera mancomunada con el sector privado, que es el verdadero motor detrás del desarrollo de las TIC.

BIBLIOGRAFÍA

ESTADOS UNIDOS. NIST. *Marco para la mejora de la seguridad cibernética en infraestructuras críticas de los Estados Unidos (NIST Cybersecurity Framework)* en línea, disponible en https://www.nist.gov/sites/default/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf, consulta del 24 de abril de 2019.

REPÚBLICA DOMINICANA. Ley 53-07 contra Crímenes y Delitos de Alta Tecnología.

— Ley No. 267-08 sobre Terrorismo, y crea el Comité Nacional Antiterrorista y la Dirección Nacional Antiterrorista.

8 Ver los artículos 5 al 11 de la Ley 53-07 contra Crímenes y Delitos de Alta Tecnología.