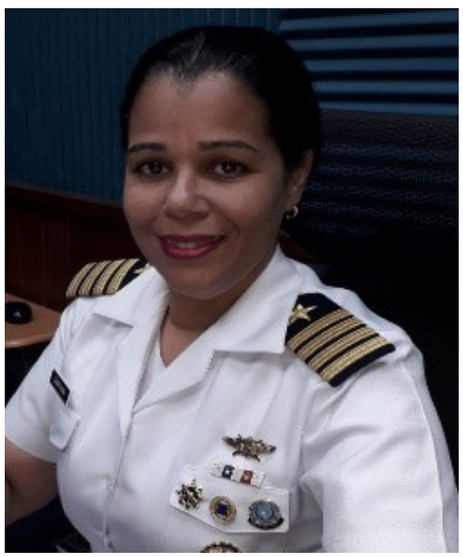
"COSTO ECONÓMICO DE LOS CIBERATAQUES NO TIPIFICADOS EN LAS LEYES DOMINICANAS"

Economic Cost of the Cyberattackes not Typed in Dominican Laws

Recibido: 18 / 09 / 2019 Aprobado: 31 / 10 / 2019



Capitán de Navío
Rocío Santana Gozález
Armada de República Dominicana

La autora es Capitán de Navío, Armada de República Dominicana, Ingeniera en Sistemas. Graduada en la Universidad Iberoamericana (UNIBE). Especialista de Estado Mayor Naval de la Escuela de Graduados de Comando y Estado Mayor Naval, con Maestría en Defensa y Seguridad Nacional, Escuela de Graduados de Altos Estudios Estratégicos del Instituto Superior para la Defensa (INSUDE), con doble titulación con la Universidad Antonio de Nebrija, España. Actualmente doctorando en proyectos con la Universidad Internacional Iberoamericana (UNINI, México). omphsantana@gmail.com

RESUMEN

El ciberespacio es declarado ámbito de seguridad en el 2016 por la OTAN y se caracteriza por su intangibilidad, un mundo no físico, flexible, el cual no tiene límites, sin fronteras, donde cualquier persona puede estar interconectada únicamente con una conexión a la red, de tal manera que pueda interactuar con el mundo entero sin barreras, identificándose o en el anonimato. Es en este espacio donde las economías de muchos Estados han percibido crecimientos muy notables debido a las innovaciones en tecnologías de la información, los procesos económicos y la comunicación, pero eso nos ha dejado más vulnerables al uso ilegal de estas mismas ventajas que, por falta de normativas y leyes adecuadas, República Dominicana no es la excepción en este punto, han generado pérdidas cuantiosa y una sensación de desprotección, en vista de las prontas actualizaciones delictivas empleadas en los Ciberataques, superior a los correctivos especificados en las leyes existentes, evidenciando el vacío legal, en vista de la necesidad de regular el uso, el derecho y la protección en el ciberespacio a fin de encontrar el equilibrio entre seguridad y la "libertad" que se percibe en el mismo.

Palabras clave:
Ciberespacio, economía, ciberdelito, ciberataque, leyes.

ABSTRACT

Cyberspace is declared a security field in 2016 by NATO and is characterized by its intangibility, a non-physical, flexible world, which has no limits, without borders, where anyone can be interconnected only with a network connection, in such a way that it can interact with the entire world without barriers, identifying itself or in anonymity. It is in this space where the economies of many States have perceived very notable growth due to innovations in information technologies, economic processes and communication, but that has left us more vulnerable to the illegal use of these same advantages that, due to lack of adequate regulations and laws, the Dominican Republic is no exception at this point, they have generated substantial losses and a sense of lack of protection, in view of the early criminal updates used in the Cyber-attacks, superior to the corrective measures specified in the existing laws, evidencing the legal vacuum, in view of the need to regulate the use, the right and the protection in cyberspace in order to find the balance between security and the "freedom" that is perceived in it.

Keywords:
Cyberspace, economy, cybercrime, cyber attack, laws.

INTRODUCCIÓN

¿Sabes cuánto dinero pierde el sector público y privado de un Estado en promedio por ataques cibernéticos? ¿Qué le ha costado a República Dominicana? ¿La ausencia de fronteras físicas y la dificultad de encontrar a los responsables en el ciberespacio tienen algo que ver con estas pérdidas económicas? ¿Están las regulaciones cónsonas con la novedad del fenómeno y los avances tan rápidos que se producen en el ciberespacio?

Después de la aceleración de la década de los noventas y en términos de seguridad, los ajustes realizados después del 11 de septiembre del 2001, el 2017 fue un año donde los ataques cibernéticos tuvieron papeles protagónicos, mostrando ciertas ventajas frente a las autoridades y dejando una gran tarea de revisión de las leyes que protegen a los ciudadanos víctimas en el ciberespacio.

El aumento del acceso al internet y el riesgo de abuso en torno a su apertura se han convertido en uno de los temas más apremiantes de nuestro tiempo. No hay duda de que esta híper-conectividad es una poderosa herramienta de desarrollo que debe permanecer abierta y accesible. Funciona como motor de crecimiento y una oportunidad para gobiernos, empresas y personas por igual. Sin embargo, esta apertura y accesibilidad vienen con riesgos.

COSTO OPERACIONAL DE LA CIBERSEGURIDAD

La compañía analista Gartner[1] pronosticó que para el año 2020 habrá 20.400 millones de dispositivos conectados. La atención a este dato debe estar en si cada una de esas conexiones conllevan a la concientización del usuario final acerca de la comprensión de las políticas de privacidad y de los derechos que lo amparan antes de aceptar. Es necesaria la concientización de la población de que la seguridad es asunto de todos, que a todos nos compete, y que un ciberespacio más confiable redunda en su beneficio.

Las amenazas, riesgos y vulnerabilidades van en aumento exponencial y no es paranoia, un ciber-delito podría originarse desde cualquier lugar y pasar por una serie de computadoras comprometidas por piratas informáticos de todo el mundo antes de alcanzar su objetivo previsto. Este es solo un ejemplo de cómo el ciberespacio complica el concepto de tiempo, distancia y jurisdicción.

Como sabemos, el desarrollo tecnológico ha transformado las operaciones de las empresas e instituciones y la forma en cómo interactúan las personas, pero a la vez han traído riesgos y dificultades en cuanto a la seguridad de la información. En un mundo híper conectado y con todo lo positivo de estos avances e innovaciones tecnológicas, las comunicaciones también han permitido y fortalecido las redes del crimen…quienes están protegidos de un ciberataque, la respuesta es una: nadie.

Según el Informe sobre Riesgos Globales para 2016 del Foro Económico Mundial[2], los ataques cibernéticos se han considerado como uno de los principales riesgos globales entre los más probables de ocurrir y con mayores consecuencias. En los últimos años han aumentado rápidamente, atacando a los negocios en todo tipo de sectores empresariales, y con ellos al ciudadano. Por lo tanto, se necesitará implementar nuevas directivas que garanticen la seguridad, minimizando los riesgos de ataques cibernéticos.

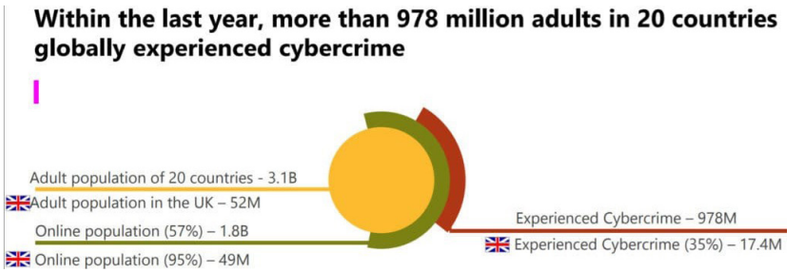
Si bien es cierto que es a partir de la década de los 90, que estos conceptos de seguridad aplicados a la ciberseguridad, comienzan a tener protagonismo y a incrementar su uso y su importancia, como consecuencia de la aceleración mundial que ha generado la tecnología en todos los ámbitos de poder, también es cierto que la delincuencia da la apariencia que lleva unos pasos más adelante que la comprensión y ajustes en torno a los nuevos conceptos y las normativas que los ampara.

En el año 2017, quedó de manifiesto la evolución de los cibercriminales y sus nuevas formas de delinquir de manera creativa con los robos millonarios de criptomonedas y ataques como los ocasionados por Wannacry y Petya que dejan gran preocupación en las autoridades referente al tema de la seguridad en línea.

[1]Gartner, Inc. es una empresa consultora y de investigación de las tecnologías de la información con sede en Stamford, Connecticut, Estados Unidos.

[2]La versión número 46 de la Asamblea Anual del Foro Económico Mundial en Davos, Suiza, tuvo como tema principal "los desafíos de la cuarta revolución industrial". Más de 2,500 participantes, entre jefes de estado, empresarios, líderes de organizaciones mundiales y regionales y sociedad civil conversaron sobre la situación económica internacional caracterizada por el aumento de los intercambios y sobre las soluciones a los retos que imponen las nuevas tecnologías y modelos empresariales.

Según el informe de Norton Cyber Security Insights en el año 2017, el robo en línea ascendió a unos 172,000 millones de dólares estadounidenses, que afectaron a 978 millones de consumidores en 20 países.



En los primeros siete meses de 2017 se totalizaron 677 millones de ciberataques. Colombia y México son de las naciones de habla hispana que más ciberataques recibe. En relación con el anterior año 2016, este problema experimentó un incremento de 59%.

Dentro de los países que conforman América Latina se han estimado pérdidas por noventa mil millones de dólares estadounidenses, según un estudio realizado por Net Scout Arbor, "Tendencias en Ciberseguridad en Latinoamérica". Un caso muy notorio fue el que experimentó Venezuela en agosto de 2017 y que dejó sin telefonía celular a siete millones de usuarios.

En República Dominicana, desde enero a julio de 2017 se produjeron 24 millones de ciberataques , siendo los servicios financieros, los récords médicos del sector salud, el sector educativo y las universidades los más afectados. Además de secuestrar información de empresas a través de virus como Wannacry, muchos de los ciberataques[3] en República Dominicana tienen por objeto, obtener información confidencial de algún cliente y amenazar con publicarla, comprometiendo así a la empresa que debe resguardar esa información, por lo que se ve en la obligación de pagar a los ciberdelincuentes que se dedican a eso. Se puede observar gráficamente este proceso.

Fuente:TendMicro /Carbon Black

De acuerdo con el reporte anual de ciberseguridad de Cisco 2018 "La sofisticación de los programas maliciosos está creciendo a medida que los ciberpiratas comienzan a incorporar los servicios en la nube y aluden la detección a través de cifrados, utilizándolos como herramienta para ocultar la actividad de comando y control".

Los Estados son los responsables de la Seguridad Nacional y disponen de medios e instituciones para alcanzarla y mantenerla, solo que en este nuevo ámbito se da la sensación de limitación. Las amenazas procedentes del ciberespacio se presentan, como se ha visto en los ejemplos anteriores, como un conjunto variado y continuamente cambiante de elementos, cuyo objeto es atentar a la seguridad de las personas y de las infraestructuras, tomando en cuenta que la información tiene un valor por sí misma. Por lo tanto, es una gran responsabilidad y reto para los Estados diseñar estrategias que garanticen la eficientización de los recursos disponibles, ya que, en cuanto al poder político, económico, social y militar, mientras mayor sea la eficacia con que sean manejados, mayores serán los beneficios.

La Seguridad Nacional debe garantizarse en todos, y desde todos los diversos ámbitos o espacios estratégicos, establecerse su defensa y conseguir y mantener sus objetivos; se debe estar preparado para las confrontaciones, conflictos o incidentes con otros adver-

[3]https://www.eldiaº.com.do/el-60-operaciones-bancarias-en-el-pais-se-hace-via-electronica/

sarios, cuyos objetivos sean incompatibles con los propios, y también, por otro lado, se pueden mantener acuerdos de cooperación con otros países.

El Lic. Carlos E. Pimentel Florenzán[4] expresa que la seguridad nacional en el marco institucional de un Estado de Derecho, proporciona las garantías necesarias a la nación para la vigencia de sus intereses y objetivos nacionales frente a cualquier amenaza, que en el caso de República Dominicana son multidimensionales, vinculadas a factores de orden público, entre ellas, la inmigración ilegal, el tráfico ilícito de armas, lavado de activos, trata de personas, corrupción, narcotráfico y la penetración del crimen organizado, entre otras.

También es un hecho reconocido a nivel mundial, que la delincuencia cibernética es una amenaza real y presente para la estabilidad de cualquier sociedad y República Dominicana no es la excepción. La escala y la sofisticación de la delincuencia informática ha hecho que muchos gobiernos replanteen su estrategia para la protección de sus ciudadanos en una economía mundial cada vez más impulsada por, y dependiente de la tecnología.

Garantizar la ciberseguridad es una de las prioridades de la agenda de los países del hemisferio. La Organización de los Estados Americanos (OEA) está trabajando en el desarrollo de una agenda sobre seguridad cibernética en las Américas con el objetivo de que las estrategias presentadas contribuyan notablemente a conseguir un espacio cibernético más seguro para ciudadanos, empresas y administración de pública los diferentes países.

Los delincuentes cibernéticos suelen tener objetivos claros cuando se lanzan a sus actividades ilícitas. Ellos saben cuál es la información que están buscando o los resultados que quieren lograr, y además del camino que deben tomar para alcanzar esos objetivos. Estos criminales le dedicarán un tiempo importante a la investigación de sus objetivos, a menudo a través de la información a disposición del público en las redes sociales, y planean sus acciones cuidadosamente. Asimismo, el interés de muchos de estos ataques maliciosos ha sido exponer y/o explotar información sensible y confidencial, que puede tener efectos perjudiciales para los agentes gubernamentales y la infraestructura crítica.

Existe la idea de que los usuarios de Internet deben asumir que no se puede ni se debe confiar en nada en el mundo cibernético. Sin embargo, las organizaciones de los sectores público y privado, así como las personas, todavía desean tener la seguridad de que se puede confiar en las tecnologías de las que dependen cotidianamente.

En los últimos años, las empresas han ido generando cada vez mayores cantidades de datos personales y sensibles, tales como nombres, direcciones e información de tarjetas de crédito. Además, cada vez más empresas almacenan datos personales y sensibles en plataformas en línea o en otros medios de comunicación electrónicos. A medida que se van volviendo más accesibles grandes cantidades de datos, estos se han convertido en productos básicos de gran valor para los delincuentes cibernéticos, ya que pueden ser vendidos a otros actores maliciosos. En consecuencia, los individuos, empresas y gobiernos por igual, deben tomar las precauciones adecuadas para proteger sus datos.

Las tendencias mundiales en delitos cibernéticos demuestran que el sector financiero es el sector más atacado por los delincuentes cibernéticos. Sus actividades incluyen el phishing, robo de identidad y la creación de aplicaciones bancarias falsas.

Es por todo esto que se debe robustecer el marco normativo, pero, para esto, primero se debe saber con qué se cuenta para poder mejorar y ajustar las leyes, las instituciones y los organismos de respuesta y, en virtud de ello, a continuación se describirán las normas legales vigentes sobre la materia:

- **Constitución de República Dominicana.**

  De acuerdo con el Artículo No. 44 de la Constitución de República Dominicana del 2015, en su numeral 2, que dice "toda persona tiene el derecho a acceder a la información y a los datos que sobre ella o sus bienes reposen en los registros oficiales o privados, así como conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por la ley. El tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando los principios de calidad,

[4]Carlos E. Pimentel Florenzán, abogado, con experiencia profesional en los ámbitos de la transparencia en la administración pública, Miembro Fundador / Oficina de Asesorías, Consultorías e Investigaciones. (OACI).

licitud, lealtad, seguridad y finalidad. Podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos".

Asimismo, en el numeral 3, de dicho artículo hace referencia a que "se reconoce la inviolabilidad de la correspondencia, documentos o mensajes es privados en formato físicos, digitales, electrónicos, o de todo tipo".

• Ley No. 155-17. Ley contra el Lavado de Activos y el Financiamiento del Terrorismo.

Esta Ley sustituye y deroga la Ley No.72-02, sobre el Lavado de Activos Provenientes del Tráfico Ilícito de Drogas, del 26 de abril de 2002.

• Ley No. 310-14. Que Regula el Envío de Correos Electrónicos Comerciales No Solicitados (SPAM).

Tiene por objeto "regular el envío de comunicaciones comerciales, publicitarias o promocionales no solicitadas, realizadas vía correos electrónicos, sin perjuicio de las disposiciones vigentes en materia comercial sobre publicidad y protección al consumidor".

• Ley No. 53-07, sobre Crímenes y Delitos de Alta Tecnología.

Tiene por objeto "la protección integral de los sistemas que utilicen tecnologías de información y comunicación y su contenido, así como la prevención y sanción de los delitos cometidos contra estos o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías en perjuicio de personas física o morales, en los términos previstos en dicha ley."

• Ley No. 126-02, sobre Comercio Electrónico, Documentos y Firmas Digitales.

Tiene por objeto "brindar el soporte normativo sobre todo lo relativo al uso de nuevas tecnologías informáticas, aplicado al comercio electrónico y al uso de nuevas técnicas para la elaboración, transmisión y autenticación de documentos y mensajes por medios digitales e informáticos".

Esta ley es aplicable a todo tipo de información en forma de documento digital o mensaje de datos, salvo en los siguientes casos:

a) En las obligaciones contraídas por el Estado dominicano en virtud de convenios o tratados internacionales.

b) En las advertencias escritas que, por disposiciones legales, deban ir necesariamente impresas en ciertos tipos de productos en razón al riesgo que implica su comercialización, uso o consumo.

• Decreto No.230-18, que Establece y Regula la Estrategia Nacional de Ciberseguridad 2018-2021.

Mediante el Decreto No. 230-18 se aprobó la Estrategia Nacional de Ciberseguridad de República Dominicana 2018-2021. Según el gobierno, este documento ha surgido de la voluntad del Estado dominicano de hacer frente a las amenazas cibernéticas y como mecanismo para crear un ciberespacio más seguro.

Algunas de las instituciones primordiales para el combate de la ciberdelincuencia:

• Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT), que es una dependencia de la Policía Nacional y tiene como misión combatir el crimen de alta tecnología dentro del territorio nacional. Se encarga de realizar las investigaciones de todas las denuncias de crímenes y delitos considerados de alta tecnología. Responder sobre la base de capacidad investigativa a todas las amenazas y ataques a las infraestructuras críticas nacionales. Desarrollar análisis estratégicos de amenazas informáticas y desarrollar inteligencia.

• División de Investigaciones de Delitos Informáticos, es una dependencia de la Dirección Nacional de Investigaciones (DNI). Su principal misión es velar por el fiel cumplimiento de la Ley No. 53-07. Esta división se encarga de investigar los crímenes contra la humanidad; crímenes y delitos contra la Nación, el Estado y la Paz pública; amenazas contra el Estado dominicano, la Seguridad Nacional. Trabaja entrelazada con

el DICAT, el Ministerio de Defensa y la Dirección Nacional de Control de Drogas.

Otras instituciones que trabajan y ayudan a informar acerca de las actividades del cibercrimen, los riesgos que estas implican, así como la implementación de las buenas prácticas, incluyen las siguientes:

- Instituto Dominicano de Telecomunicaciones (INDOTEL), junto con la Procuraduría General de la República, coordinan acciones contra el cibercrimen y promueven las políticas de ciberseguridad en el país.

- Instituto Tecnológico de Santo Domingo (INTEC), universidad con la cual el gobierno realizó un pacto para que sirva de base en las certificaciones del personal de seguridad de la información.

El país mantiene una cooperación bilateral con los gobiernos de España y Colombia y con otros países como Estado Parte del Convenio de Budapest[5] y como miembro de la red 24/7 del G8, de la INTERPOL y la OEA. De igual forma la República Dominicana obtiene información de los proveedores y operadores de servicios de internet desde los Estados Unidos.

CONCLUSIÓN

No existen leyes o normas que atiendan la problemática de manera integral. Cabe destacar que la Ley No. 53-07 ha sido un paso de avance respecto al anterior estado de cosas existente en República Dominicana en la materia y también lo ha sido la Estrategia Nacional de Ciberseguridad. Sin embargo, conforme avanza la tecnología, se presentan nuevas maneras de delinquir en el ciberespacio.

El marco legal aplicativo a la ciberseguridad no va al ritmo de las mejoradas formas de los ciberataques, por lo tanto, la práctica es ajustar soluciones con normas preexistentes, como contingencia o respuestas a situaciones que se presentan. Es importante que se creen mecanismos o medidas preventivas, conscientes de que modificar las normas toma un tiempo considerable.

Es a través de la educación y de la buena información que se pueden ir reduciendo los potenciales daños. Es importante la preparación de un personal calificado y experto en estos temas, así como seguir contando con el apoyo del Estado dominicano, que debe colocar a la ciberseguridad como prioridad en la agenda gubernamental, creando las instancias necesarias capaces de emitir y diseñar resoluciones que contribuyan a cubrir las faltas legislativas.

REFERENCIAS

Constitución de la República Dominicana. (2019). *Gaceta Oficial* núm. 10805. 13 julio del 2015. Recuperado de https://poderjudicial.gob.do/documentos/PDF/constitucion/Constitucion.pdf

Decreto No. 230-18. (2018). *Establece y regula la Estrategia Nacional de Ciberseguridad 2018-2021*. Santo Domingo, República Dominicana. Recuperado de https://es.scribd.com/document/382100584/Decreto-230-18

Fallas, S. (2019). *Lo más destacado del reporte de ciberseguridad CISCO* 2018. Recuperado de https://gblogs.cisco.com/la/sg-stfallas-lo-mas-destacado-del-reporte-de-ciberseguridad-cisco-2018/

Gartner (empresa). (2019). *Wikipedia, La Enciclopedia Libre*. Recuperado de https://es.wikipedia.org/wiki/Gartner_(empresa).

Global Partner Programs. (2019). *Trend Micro*. Recuperado de https://www.trendmicro.com/en_us/partners.html

Ley No. 126-02. (2002). *Sobre comercio electrónico, documentos y firma digital.* Santo Domingo, República Dominicana. Recuperado de https://www.indotel.gob.do/media/1060/agenda-regulatoria.pdf

Ley No. 53-07. (2007). *Contra crímenes y delitos de alta tecnología*, de fecha 23 de abril del año 2007. Santo Domingo, República Dominicana.

[5]Hasta ahora el documento que sirve como guía en la materia a nivel internacional es el Convenio de Budapest, celebrado en 2001. Sólo 54 países lo han firmado, ratificándolo 42, y 17 reglamentándolo en su derecho interno. En América Latina y el Caribe sólo Panamá y República Dominicana lo hicieron, aunque hay otros en vías de suscribir, como México, El Salvador, Argentina, Costa Rica, Uruguay y Chile.

Ley No. 310-14. (2014). *Que regula el envío de correos electrónicos comerciales no solicitados (SPAM).* Santo Domingo, República Dominicana. Recuperado de https://indotel.gob.do/media/6187/ley-310-14-2.pdf

Ley No. 155-17. (2017). *Ley contra el lavado de activos y el financiamiento del terrorismo que busca sustituir y derogar la Ley No.72-02, sobre el lavado de activos provenientes del tráfico ilícito de drogas,* del 7 de junio de 2002. Análisis de la Ley 155-17, Contra lavado de activo y el financiamiento del terrorismo | Respuesta Procesal. Recuperado de https://respuestaprocesal.com.do/analisis-de-la-ley-155-17-contra-lavado-de-activo-y-el-financiamiento-del-terrorismo/

Pimentel, C. (2013). *Una iniciativa: gobierno abierto.* Recuperado de https://acento.com.do/author/cpimentel/

Symantec. (2019). *Global Leader In Next-Generation Cyber Security.* Recuperado de https://www.symantec.com/

Vargas, J. (2017). *El 60% operaciones bancarias en el país se hace vía electrónica.* Recuperado de https://www.eldia.com.do/el-60-operaciones-bancarias-en-el-pais-se-hace-via-electronica/