2018

White paper series
Edición 2

GESTIÓN DEL RIESGO
— CIBERNÉTICO NACIONAL —

OEA | Más derechos para más gente

CRÉDITOS

Luis Almagro

Secretario General de la
Organización de los Estados
Americanos (OEA)

Autor principal

Melissa Hathaway

Equipo técnico de la OEA

Claudia Paz y Paz
Alison August Treppel
Belisario Contreras
Kerry-Ann Barrett
Bárbara Marchiori de Assis
Nathalia Foditsch
Gonzalo Garcia-Belenguer

CONTENIDO

1

INTRODUCCIÓN

En los últimos 30 años, los gobiernos, las empresas y los ciudadanos se han vuelto críticamente dependientes del Internet y de las tecnologías de la información y las comunicaciones (TIC). Tenemos la creencia que siempre funcionarán los servicios esenciales para el ciudadano, como la energía y las telecomunicaciones, y que los bienes, servicios, datos y capital cruzarán fronteras sin inconvenientes. La realidad, sin embargo, es que muchos sistemas e infraestructuras en red son vulnerables y están siendo explotados. Organizaciones de todo tipo están sufriendo mayores violaciones a sus datos, actividad criminal, interrupción del servicio y destrucción de su propiedad. Colectivamente, nuestra inseguridad está creciendo. Más de 100 países y un número cada vez mayor de actores y personas no estatales pueden causar daños a las infraestructuras en red de gobiernos y de la industria. Los objetivos varían según el actor, desde: el activismo político; fraude y delito informático; robo de propiedad intelectual (PI); espionaje; interrupción del servicio; y destrucción de bienes y activos. Los países y las empresas están viviendo en un mundo de inseguridad cibernética: todos los gobiernos, empresas y personas están enfrentando riesgos cibernéticos. Y todos comparten un nivel de responsabilidad en su gestión. Como lo evidencian eventos recientes, los países y las empresas deben primero comprender que en el centro de su estrategia y agenda digital debe estar un enfoque disciplinado de gestión de riesgos. El riesgo de inacción es demasiado grande.

El riesgo se define en términos de tiempo, cuando algo o alguien está expuesto a un peligro, daño o pérdida[1]. La condición de riesgo puede cambiar en función de las acciones realizadas por al menos dos actores: el atacante, que obtiene y utiliza la capacidad de causar daño; y el objetivo pretendido, que puede tomar precauciones para resistir o frustrar el peligro pretendido por el atacante. Todos los días crece nuestra dependencia digital, pero la comprensión de los riesgos asociados con esa dependencia sigue siendo incipiente. Aún así, el riesgo cibernético está aumentando porque no solo está disponible y es asequible, sino que se está utilizando el mercado de software y herramientas maliciosas, servicios ilícitos y datos sensibles (no públicos). Por ejemplo, se puede comprar software malicioso por un dólar y se puede lanzar un ataque distribuido de denegación de servicio, por menos de mil dólares. Ataques sofisticados de ransomware (secuestro de archivos a cambio de un rescate) están disponibles por doscientos dólares y servicios maliciosos de correo electrónico no deseado se consiguen por aproximadamente cuatrocientos dólares[2]. Incluso las armas más sofisticadas de los servicios de inteligencia de los gobiernos están fácilmente disponibles para descarga[3]. Cualquiera que tenga la intención de utilizar y lograr la realización de ataques y causar daños puede acceder a estas capacidades. Como muestran los eventos en 2017, gobiernos, empresas y personas fueron perjudicadas por algunos de los ataques cibernéticos de mayor perfil hasta la fecha.

En mayo de 2017, el secuestro de archivos a cambio de un rescate tuvo como blanco específico las fallas en los sistemas operativos de Microsoft Windows y esto afectó a millones de computadoras en 150 países en todos los sectores comerciales. Este ataque global, un secuestro de archivos muy sencillo llamado WannaCry, detuvo operaciones de fabricación, sistemas de transporte y sistemas de telecomunicaciones. Según la Oficina Nacional de Auditoría en el Reino Unido, WannaCry afectó al menos 81 de las 236 entidades del Servicio Nacional de Salud inglés, volviendo inoperable el equipo médico y afectando de manera importante la salud y la seguridad pública[4].

En junio de 2017, se lanzó NotPetya, otro malware (un software malintencionado) más destructivo. NotPetya se extendió entre las empresas en red del mundo a través de un mecanismo de actualización de software para un programa de contabilidad ampliamente utilizado (doc.me). En cuestión de minutos, el software malintencionado infectó decenas de miles de sistemas conectados a Internet en más de 65 países, incluidos unos que pertenecen a instituciones gubernamentales, bancos, empresas de energía y otras compañías. Por ejemplo, el ataque de NotPetya contra A.P. Moller-Maersk, la compañía naviera más grande del mundo, cifró y eliminó los sistemas de tecnología de la información de la empresa en todo el mundo. Por lo tanto, Maersk tuvo que detener las operaciones en la mayoría de las 76 terminales portuarias de la compañía en todo el mundo,

interrumpiendo el comercio marítimo por semanas. Las pérdidas financieras de Maersk causadas por NotPetya superaron los $300 millones, ya que tuvo que reconstruir toda su infraestructura, incluidos 4.000 nuevos servidores, 45.000 computadoras nuevas y 2.500 aplicaciones nuevas[5]. Se estima que NotPetya ocasionó pérdidas por miles de millones de dólares debido a la interrupción de los negocios y la destrucción de propiedad en todo el mundo[6]. Las pérdidas primarias y secundarias a la economía digital fueron significativas y el daño a los servicios e infraestructuras críticas llevó meses en recuperarse.

Aún más preocupante, en agosto de 2017, una instalación de petróleo y gas de Arabia Saudita se vio repentinamente obligada a cerrar. Fue víctima de Trisis, un virus informático bien diseñado para sabotear los sistemas de control industrial (SCI). Creado para afectar los componentes operacionales de la tecnología de la información en sitios industriales como petróleo y gas y servicios de agua, este software malicioso, o arma, tiene como objetivo específico los mecanismos de seguridad física (sistema de paro por emergencia) de los SCI. Si bien este es solo un ejemplo público del uso exitoso de este software destructivo, Schneider Electric les recomendó a sus clientes de servicios críticos y propietarios de infraestructura que garantizaran que sus sistemas son redundantes en caso de que uno o más sistemas fallen como resultado de una actividad maliciosa futura[7].

Las actividades cibernéticas maliciosas de 2017 muestran un impacto extraordinario en términos de pérdida y daño, pero las herramientas utilizadas para causar daño realmente no eran sofisticadas. El número de ataques dirigidos contra los sistemas de energía, de telecomunicaciones, transporte y financieros casi se ha duplicado en los últimos cinco años, una tendencia que plantea riesgos de seguridad económica y nacional para todos. Por lo tanto, existe una necesidad urgente de que los líderes gubernamentales y corporativos participen en procesos efectivos de gestión de riesgos cibernéticos y aborden los riesgos digitales dentro de sus procesos de planificación estratégica.

2

MARCOS PARA COMPRENDER EL RIESGO CIBERNÉTICO

Los países, organizaciones internacionales e instituciones académicas están desarrollando marcos para ayudar a los líderes gubernamentales y corporativos a diagnosticar y reducir el riesgo cibernético. Estos marcos son inmensamente necesarios porque en las últimas tres décadas, estos mismos líderes han estado convencidos de los supuestos beneficios -dadas sus características- de las tecnologías de información comercial, que significan mayor productividad, mayor eficiencia, menores costos de equipo de capital, almacenamiento y procesamiento de datos, y crecimiento de los resultados. Por lo tanto, los dirigentes han postergado la inversión en seguridad y resiliencia de sus infraestructuras de red y negocios digitales. Las actividades cibernéticas destructivas y disruptivas de hoy en día requieren que estos líderes enfrenten el hecho de que, inadvertidamente, han entretejido la inseguridad en el núcleo mismo de la sociedad. Las pérdidas se están acumulando, el daño está creciendo, y el peligro es inminente.

Marcos gubernamentales

Los gobiernos han comenzado a desarrollar marcos, puntos de referencia y estrategias nacionales más amplias para comprender mejor sus dependencias y vulnerabilidades de infraestructura de Internet, y para asegurar las redes nacionales, las infraestructuras y los servicios de los que dependen su futuro digital y su bienestar económico. Sin embargo, cuando se trata de mapear y alertar sobre el riesgo cibernético de un país, la pregunta que queda en el aire es: ¿cómo se diagnostica y se reduce un riesgo que se ha acumulado durante 30 años?[8] Es importante comenzar por comprender qué es el plan estratégico de 3-5 años de un país y determinar qué se puede hacer para alcanzar ese objetivo a largo plazo. Por ejemplo, los holandeses han estimado que para 2020, al menos el 25 por ciento de su producto interno bruto (PIB) estará compuesto por la economía digital (es decir, bienes digitales y servicios electrónicos). Los Países Bajos han afirmado que su futuro depende de la capacidad de asegurar su economía digital, y están realizando algunas de las inversiones necesarias y reformas estructurales para lograr ese objetivo. Otros países, como Estados Unidos y Alemania, están identificando las principales compañías que representan más del 2 por ciento del PIB del país y están trabajando con ellas para garantizar que la gestión del riesgo y la resiliencia sean parte de sus procesos generales de planificación comercial. La mayoría de los otros países, sin embargo, han adoptado un enfoque más amplio exigiendo la protección de las "infraestructuras críticas", es decir, los activos, sistemas y redes esenciales que se considera que se están volviendo vulnerables a través de una mayor interconexión y confianza en Internet, y como tal, quedan susceptibles a fallas en los equipos, errores humanos, clima y otras interrupciones causadas naturalmente, y ataques físicos y cibernéticos[9]. El desafío con este enfoque es que no existe una delimitación clara entre la responsabilidad del gobierno y de la industria. Esto hace que sea difícil responsabilizar a alguien en particular por la inacción. Mientras tanto, la inseguridad de la sociedad crece a medida que existe la falta de compromiso para reducir el riesgo y aumentar la resiliencia.

Algunos gobiernos han determinado que es hora de intervenir en el mercado y están utilizando regulaciones o leyes para exigir que ciertos sectores identifiquen, evalúen y corrijan las deficiencias en su postura de seguridad. Los sectores regulados incluyen: servicios eléctricos, servicios financieros, atención en salud, transporte y telecomunicaciones. Otras medidas regulatorias que están siendo adoptadas por los países implican la obligación de notificación detallada y envío de informes a la autoridad local y/o nacional con respecto a: una violación que haya ocurrido y el tipo de datos que se hayan expuesto o perdido; la técnica o método utilizado en una violación; y cortes o interrupciones en el negocio (telecomunicaciones) que puedan haber ocurrido.

La Unión Europea (UE) está imponiendo este tipo de enfoques preceptivos sobre sus infraestructuras críticas y operadores de servicios esenciales. En agosto de 2016, la UE adoptó un reglamento titulado la Directiva de Seguridad de las Redes y Sistemas de Información (NIS, por sus siglas en inglés) de la UE. La regulación estableció reglas de seguridad cibernética (o conjuntos de controles de seguridad) para las empresas que suministran servicios a la sociedad que se han categorizado como esenciales. Los servicios cubiertos por la regulación incluyen energía, transporte, banca, finanzas, agua y salud, así como servicios digitales, como los mercados en línea (p. ej., eBay, Amazon), motores de búsqueda (p. ej., Google) y proveedores de servicios en la nube. Los Estados miembros de la UE tienen hasta mayo de 2018 para incorporar el reglamento a sus leyes nacionales. La Directiva NIS requiere que los operadores de servicios esenciales en esos países tomen las medidas de seguridad apropiadas y notifiquen a su autoridad nacional pertinente (p. ej., la autoridad competente o el equipo de respuesta a incidentes de seguridad informática, CSIRT) sobre cualquier incidente cibernético grave. Este enfoque obliga a la rendición de cuentas y puede reducir el riesgo cibernético porque está "obligando" a la industria a tomar medidas para reducir las vulnerabilidades y aumentar la resiliencia.

China adoptó un enfoque similar al de Europa e incluso incorporó elementos de la Directiva NIS en su nueva ley nacional de seguridad cibernética adoptada por el parlamento chino en noviembre de 2016, que entró plenamente en vigencia el 31 de diciembre de 2017. La ley tiene siete capítulos y 79 artículos, y es "integral y abarcador" en el sentido que especifica las responsabilidades de las agencias gubernamentales relevantes, los proveedores de servicios de Internet y los usuarios de Internet. La ley establece que, en términos generales, las compañías deberán tomar medidas técnicas y otras medidas necesarias para garantizar que el Internet funcione de manera segura y estable, atender los incidentes de seguridad cibernética de manera efectiva, evitar las actividades delictivas cibernéticas y mantener la integridad, el secreto y la facilidad de uso de los datos de Internet[10]. Esta regulación obliga a las empresas a invertir en nuevas salvaguardas e instalar una serie de controles para garantizar estas directrices. También cuenta con un régimen de inspección y auditoría para garantizar que las empresas adelanten las actividades adecuadas de reducción de riesgos y rindan cuentas si se comprueba que no cuentan con procesos suficientes operando.

Estados Unidos se ha abstenido de adoptar un enfoque regulatorio en esta materia, y más bien ha hecho un llamamiento a la industria para que invierta voluntariamente en reducir el riesgo cibernético a las infraestructuras y servicios críticos del país. En febrero de 2013, el presidente le solicitó al Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) que desarrollara un conjunto de estándares, metodologías, procedimientos y procesos que alineen los enfoques de políticas, negocios y tecnología para abordar los riesgos cibernéticos. El Marco para mejorar la seguridad cibernética de infraestructura crítica se publicó un año después, en febrero de 2014, y contiene un conjunto de estándares voluntarios que ayudan a las organizaciones a evaluar, administrar y responder al riesgo de seguridad cibernética. El marco les indica a las organizaciones la evaluación del riesgo bajo cinco encabezados: identificar, proteger, detectar, responder y recuperar. Según algunas estimaciones de la industria, cerca del 30 por ciento de las organizaciones estadounidenses (incluido el gobierno) está utilizando el marco como ayuda en la evaluación de su postura de riesgo y para asumir una mayor responsabilidad en la protección de sus redes y datos confidenciales contra intrusos, daños o destrucción[11]. El apéndice de este documento presenta varios estándares acordados internacionalmente para las categorías de reducción de riesgos del Marco de seguridad cibernética del NIST. Sin embargo, las lecciones aprendidas de violaciones recientes sugieren que las organizaciones que usan el Marco de seguridad cibernética del NIST están aplicando las categorías con miras más bien hacia el cumplimiento, en lugar de hacia la evaluación del riesgo de forma continua. Por ejemplo, unas organizaciones que evaluaron su postura de seguridad y preparación utilizando el Marco de seguridad cibernética del NIST creyeron que habían alcanzado un nivel maduro de seguridad cibernética, pero resultaron perjudicados significativamente por WannaCry y NotPetya[12].

En septiembre de 2017, el NIST publicó ajustes a otra de sus publicaciones sobre el Marco de gestión de riesgos para sistemas de información y organizaciones: un enfoque del ciclo de vida del sistema para la seguridad y la privacidad[13]. Este marco recomienda un proceso para que las organizaciones identifiquen activos de alto valor y sistemas de alto impacto para que puedan evaluar mejor el riesgo operacional. También proporciona una estructura para determinar y seleccionar controles de seguridad y privacidad e implementar y evaluar la efectividad del control. El marco destaca la importancia del monitoreo continuo del riesgo en tiempo real y el cumplimiento de un cierto momento dado. También reconoce que las decisiones de gestión de riesgos son esenciales para las funciones comerciales y el logro de la misión. Este marco complementa el Marco para mejorar la seguridad cibernética de infraestructura crítica y, cuando se toman en conjunto, pueden ofrecerles a las organizaciones un enfoque más estratégico para la gestión de riesgos.

Marcos internacionales

Las organizaciones internacionales también están opinando en el debate sobre la gestión del riesgo cibernético y están trabajando para acelerar la adopción de medidas efectivas de seguridad cibernética utilizando sus propios marcos y recomendaciones. El debate internacional sobre gestión de riesgos surgió después de las dos fases consecutivas (2003 y 2005) de la Cumbre Mundial sobre la Sociedad de la Información (CMSI), una reunión mundial de la comunidad de 'TIC para el desarrollo'. En ese momento, al menos 170 países resolvieron garantizar que todos pudieran beneficiarse de las oportunidades que las TIC pueden ofrecer: mejorar el acceso a la infraestructura y tecnologías de información y comunicación, así como a la información y el conocimiento; aumentar la confianza y la seguridad en el uso de las TIC; desarrollo y ampliación de aplicaciones TIC; y alentar la cooperación internacional y regional[14]. Desde ese momento, las instituciones internacionales se embarcaron en un esfuerzo para desarrollar y propagar marcos para gestionar el riesgo de las vulnerabilidades de las TIC y aumentar la confianza y la participación en la economía digital mundial.

Una de las primeras organizaciones internacionales en asumir el reto fue la Organización de Estados Americanos (OEA). En 2004, la OEA, a través del Comité Interamericano contra el Terrorismo (CICTE), y su Programa de Seguridad Cibernética, comenzó a fomentar el desarrollo de la agenda de seguridad cibernética en las Américas. La OEA coopera con una amplia gama de entidades nacionales y regionales de los sectores público y privado en cuestiones políticas y técnicas, y busca construir y fortalecer la capacidad de seguridad cibernética al interior de sus Estados Miembros mediante asistencia técnica y capacitación, mesas redondas de políticas, ejercicios de gestión de crisis y el intercambio de mejores prácticas relacionadas con las TIC. La OEA utiliza marcos gubernamentales y académicos para ayudar a promover la creación de capacidad de seguridad cibernética y está ayudando a cambiar la conversación nacional en sus Estados Miembros para reconocer que deben ser seguras tanto la conexión a Internet como la infraestructura de TIC que la sustenta. Si los países no invierten por igual en la seguridad de su infraestructura clave y en la resiliencia de sus sistemas, los costos derivados de actividades cibernéticas nefastas afectarán su crecimiento económico.

En 2007, la Unión Internacional de Telecomunicaciones (UIT), una agencia especializada de las Naciones Unidas (ONU) responsable de las cuestiones TIC, anunció su Agenda sobre Ciberseguridad Global (GCA, por sus siglas en inglés) y publicó un marco que fomenta la cooperación y la colaboración con y entre las partes. La GCA contiene cinco pilares estratégicos para guiar a los países en el desarrollo de capacidades a fin de abordar la seguridad cibernética de manera responsable. Estos incluyen: (1) Medidas legales; (2) Medidas técnicas y procedimentales; (3) Estructuras organizacionales; (4) Desarrollo de capacidades; y (5) Cooperación internacional. A este marco lo siguió el desarrollo de la Guía de Ciberseguridad Nacional de la UIT en 2011, que hace hincapié en los valores, la cultura y los intereses nacionales como la base de cualquier desarrollo efectivo de la estrategia nacional. También analiza cuestiones importantes que todo gobierno debe abordar cuando se trabaja para transformar el tema de la seguridad cibernética de un simple debate/problema técnico a un área de política nacional estratégica. Sobre la base de estos esfuerzos iniciales, en 2014, la UIT lanzó un Índice de Ciberseguridad Global (GCI, por sus siglas en inglés) para ayudar a los países a establecer la línea de base y medir sus programas de seguridad cibernética frente a las inversiones y programas de otros países. Este índice está destinado a medir el desarrollo o "bienestar" de un país en las cinco categorías de la Agenda sobre Ciberseguridad Global: medidas legales, medidas técnicas, medidas organizacionales, desarrollo de capacidades y cooperación[15]. Esta metodología e índice fue uno de los primeros marcos internacionales disponibles para los líderes nacionales, que les sirviera para informar el desarrollo de su estrategia nacional y proporcionar un enfoque para medir el riesgo cibernético en términos no técnicos.

En 2015, el Consejo de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) adoptó y publicó la Recomendación sobre gestión del riesgo de seguridad digital para la prosperidad económica y social de la OCDE[16] para informar el desarrollo de estrategias nacionales destinadas a la gestión de la seguridad digital y la optimización de los beneficios del desarrollo económico y social esperados por la apertura digital. El marco alienta a los países a adoptar un enfoque basado en la gestión de riesgos y en un marco de ocho Principios de alto nivel interrelacionados, interdependientes y complementarios, que incluyen (1) sensibilización, adquisición de habilidades y empoderamiento; (2) responsabilidad de los interesados; (3) derechos humanos y valores fundamentales; (4) cooperación; (5) evaluación del riesgo y ciclo de tratamiento; (6) medidas de seguridad apropiadas y acordes con el riesgo y la actividad económica y social en juego; (7) innovación; y (8) planificación de la preparación y continuidad. La OCDE defiende el concepto de si los líderes implementan estos ocho principios junto con otros marcos internacionales, los países estarían posicionados para desarrollar mejores políticas (y estrategias) basadas en la gestión digital del riesgo de seguridad. Los ocho principios no son un marco per se, sino que son componentes clave donde se pueden establecer o mejorar los mecanismos de coordinación al interior del gobierno y con las partes interesadas no gubernamentales. La OCDE reconoce que la cooperación público-privada es esencial para la reducción del riesgo cibernético.

En 2018, el Foro Económico Mundial (FEM) publicó el Cuaderno de resiliencia cibernética para la colaboración público-privada[17], una herramienta destinada a guiar la colaboración público-privada dentro del estado en el desarrollo de políticas de seguridad cibernética. La Sección 4.7 del Cuaderno, en particular, aborda la necesidad de establecer un marco nacional claro de gobernanza cibernética, que

incluya roles, responsabilidades y capacidades que deben esperarse de los sectores público y privado. El marco de tres niveles propuesto por el FEM tiene como objetivo ayudar a los gobiernos nacionales a asignar responsabilidades y alinear mejor las funciones y responsabilidades específicas con tres capacidades de seguridad claras: solidez, resiliencia y defensa, cada una fortaleciendo a las otras. La solidez se define como "la capacidad de prevenir, repeler y contener amenazas". La resiliencia se define como "la capacidad de gestionar y solucionar violaciones exitosas". Y la defensa se define como "la capacidad de adelantarse a, interrumpir y responder a ataques"[18]. Este marco se basa en las iniciativas que datan del Consejo de la Agenda Global FEM 2014 sobre Riesgo y Resiliencia y el Libro blanco de 2016 Comprender el Riesgo Cibernético Sistémico. El FEM ha avanzado a la conversación sobre el riesgo cibernético y ha hecho conexiones directas a impactos económicos y consecuencias comerciales de la inseguridad cibernética.

3

MARCOS DE COMUNIDAD TÉCNICA Y LA ACADEMIA

Las instituciones académicas, los grupos de expertos y la comunidad técnica también han comenzado a involucrarse y han propuesto diversas metodologías para acelerar la preparación cibernética y los niveles de madurez de los países y las organizaciones.

El Índice de preparación cibernética 2.0 (CRI 2.0, por sus siglas en inglés)[19], publicado por un equipo de expertos en el Instituto Potomac para Estudios de Políticas en 2015, se basa en el Índice de Preparación Cibernética 1.0 de 2013, que aportó un marco metodológico para evaluar la preparación cibernética. El CRI 2.0 ofrece una metodología integral, comparativa y basada en la experiencia para evaluar el compromiso y la madurez de los países para cerrar la brecha entre su postura de seguridad cibernética actual y las capacidades cibernéticas nacionales necesarias para respaldar su futuro digital. El CRI 2.0 usa más de setenta indicadores únicos a través de siete elementos esenciales para discernir actividades operacionalmente preparadas e identificar áreas de mejora en las siguientes categorías: (1) estrategia nacional; (2) respuesta a incidentes; (3) delito informático y aplicación de la ley; (4) intercambio de información; (5) inversión en I+D; (6) diplomacia y comercio; y (7) defensa y respuesta a crisis. El plan accionable resultante entrega una hoja de ruta de reducción de riesgos como guía para los países. Pero lo más importante es que el CRI 2.0 vincula el crecimiento económico y el desarrollo con las políticas de seguridad nacional. También reconoce que para aprovechar todo el potencial de la economía de Internet, en términos de crecimiento del PIB, mayor productividad y eficiencia, mayor capacidad de trabajo y un mejor acceso a los negocios y la información, es necesario alinear las estrategias de desarrollo económico con las prioridades de seguridad nacional. En otras palabras, las TIC solo pueden generar crecimiento económico si se implementan políticas, procesos y tecnologías para proteger y asegurar la infraestructura y servicios cibernéticos de los que depende el futuro digital y el crecimiento de un país. El CRI 2.0 se centra en las herramientas que los líderes globales pueden aprovechar, incluyendo políticas, legislación, regulaciones, estándares, incentivos de mercado y otras iniciativas, para proteger el valor de sus inversiones digitales y abordar la erosión económica en curso, producto de la inseguridad cibernética.

El Modelo de Madurez de Capacidad de Seguridad Cibernética de Oxford (CMM, por sus siglas en inglés), publicado en 2016 por el Centro Global de Capacitación de Seguridad Cibernética (GCSCC, por sus siglas en inglés) en la Universidad de Oxford, muestra distintos niveles de madurez de seguridad cibernética de los países, en cinco dimensiones de capacidad: (1) política y estrategia de seguridad cibernética ; (2) cultura cibernética y sociedad; (3) seguridad cibernética, educación, capacitación y habilidades; (4) marcos legales y regulatorios; y (5) estándares, organizaciones y tecnologías. Cada una de estas dimensiones se divide en factores e indicadores más específicos, que en conjunto son emblemáticos de un estado más maduro de capacidad de seguridad cibernética. El CMM emplea dos métodos para ayudar a diagnosticar la preparación cibernética. El primer método usa una herramienta de encuesta (similar a la de la UIT) donde un estado puede autodiagnosticar su estado de preparación. Luego se revisan las respuestas de la encuesta y un equipo participa en un taller de intercambio técnico con partes interesadas clave del gobierno, la academia, los sectores público y privado para evaluar mejor la capacidad cibernética a nivel estatal en cinco niveles de madurez cibernética (es decir, nivel de inicio, de conformación, establecido, estratégico y dinámico). El CMM de Oxford es una herramienta excelente para medir la comprensión de las partes interesadas clave sobre el estado actual de la capacidad cibernética y la madurez del país, presentando así la base para tanto los objetivos de políticas futuros como los resultados en reducción de riesgos.

Por último, la Academia de Gobierno Electrónico en Estonia lanzó un Índice Nacional de Seguridad Cibernética (NCSI, por sus siglas en inglés) durante la Conferencia de Gobierno Electrónico de Tallin en mayo de 2016 y actualizó/modificó la metodología para un nuevo lanzamiento en enero de 2018[20]. La metodología incorpora las lecciones aprendidas por

Estonia ya que fue uno de los primeros en adoptar la gobernanza electrónica para la sociedad en general. La versión 2.0 del NCSI incluye doce áreas de capacidad y 46 indicadores para ayudar a evaluar la capacidad de un país, a nivel nacional, para construir un estado electrónico "seguro" que proteja los datos y las transacciones mientras limita el riesgo y la exposición digital de un país. Estas doce áreas de evaluación de capacidades son: (1) Capacidad para desarrollar políticas nacionales de seguridad cibernética; (2) Capacidad para analizar las ciberamenazas a nivel nacional; (3) Capacidad para proporcionar educación sobre seguridad cibernética; (4) Capacidad para garantizar seguridad cibernética de base; (5) Capacidad para proporcionar un entorno seguro para servicios electrónicos; (6) Capacidad para entregar identificación y firma electrónicas; (7) Capacidad para proteger la infraestructuras críticas de la información; (8) Capacidad para detectar y responder incidentes cibernéticos 24/7; (9) Capacidad para gestionar una crisis cibernética a gran escala; (10) Capacidad para luchar contra los delitos cibernéticos; (11) Capacidad para llevar a cabo operaciones militares de defensa cibernética; y (12) Capacidad para proporcionar seguridad cibernética internacional. El NCSI tiene muchos componentes similares a los otros marcos, pero tiene secciones diferentes que son exclusivas de la experiencia de Estonia en materia de gobernanza electrónica, que incluyen cómo crear un entorno seguro para servicios electrónicos y cómo proporcionar identificación electrónica y firmas electrónicas.

Resumen de los marcos

Cada marco tiene un enfoque ligeramente diferente, establecido para ayudar a fortalecer la postura general de seguridad cibernética de un país y gestionar el riesgo cibernético a nivel nacional. Sin embargo, estos marcos existentes tienen muchas características comunes, entre ellas: un amplio reconocimiento de que, en la era moderna, la seguridad nacional y el bienestar económico de los países dependen en gran medida de la capacidad de asegurar su infraestructura cibernética nacional y sus economías digitales; la necesidad de promover la seguridad cibernética en los niveles más altos del gobierno y del liderazgo corporativo; el requerimiento de comenzar previamente por proteger las infraestructuras más críticas y los servicios esenciales; el requerimiento de desarrollar marcos legales y regulatorios apropiados para proteger a la sociedad contra el delito cibernético, la interrupción del servicio y la destrucción de propiedad; la necesidad de que los sectores público y privado, así como las comunidades internacionales y regionales, colaboren para garantizar la adopción de estrategias efectivas de gestión del riesgo cibernético y resiliencia; y la obligación de desarrollar las capacidades nacionales necesarias para aumentar la confianza y la seguridad en el uso de las TIC, corregir las deficiencias y responder a riesgos significativos de seguridad cibernética.

4

LA PREPARACIÓN CIBERNÉTICA
ADMINISTRACIÓN DEL RIESGO

A pesar de los diversos modelos y marcos ahora disponibles para líderes nacionales para poder diagnosticar, evaluar y reducir el riesgo cibernético de sus países, y los numerosos llamados a la acción por parte de profesionales de la industria y expertos en seguridad cibernética, el mejorar la seguridad cibernética a nivel nacional sigue siendo un desafío. Por ejemplo, los Países Bajos, que han reconocido que su salud económica futura se basa en una economía digital confiable y que funcione bien, decidieron dedicar fondos suficientes y establecieron un centro para garantizar que el país pueda lograr sus objetivos de manera segura. En julio de 2015, el Coordinador Nacional de Seguridad y Contraterrorismo llevó a cabo una Revisión de la Política de Infraestructura Crítica. En esa revisión, el gobierno definió la infraestructura crítica "como un conjunto de productos, servicios y procesos subyacentes necesarios para el funcionamiento del país [y que] deben estar seguros y aptos para resistir y recuperarse rápidamente de todos los riesgos"[21]. Sin embargo, cuando el puerto de Rotterdam -el puerto más grande de Europa- se vio significativamente afectado y sus servicios degradados por NotPetya en 2017, las autoridades comenzaron a examinar el estado de las dependencias de Internet del puerto y descubrieron que la infraestructura del puerto en realidad no se había considerado crítica ni en su estrategia nacional de seguridad cibernética ni en las políticas de protección de la infraestructura.

Incluso países como el Reino Unido, que identificaron sectores críticos específicos -como la atención a la salud- que deben cumplir con un estándar de atención, no vaticinaron que sus proveedores de servicios de salud no estaban dispuestos a invertir recursos para mantener actualizado su software y así proteger los servicios críticos de los pacientes del riesgo cibernético. Por lo tanto, cuando 81 de las 236 entidades del Servicio Nacional de Salud fueron víctimas de WannaCry -un sencillo secuestro de archivos a cambio de un rescate-, un incidente que podría haberse evitado fácilmente terminó poniendo en riesgo a muchas vidas. Como resultado, el Reino Unido se vio obligado a examinar si su programa cibernético era suficiente y determinar si era necesaria una mayor intervención y atención del gobierno para gestionar el riesgo para la nación y sus ciudadanos.

Como se indicó anteriormente, Alemania y Estados Unidos identificaron al puñado de empresas que contribuyen al menos el 2% del PIB del país y por lo tanto merecen mayor protección y mayor intercambio de información/cooperación con el gobierno. No obstante, el intercambio de información entre el gobierno y la industria no protegió a las empresas de caer presas de la naturaleza destructiva de NotPetya. Si bien ambos países tienen procesos para compartir información sobre amenazas y inteligencia, y "advertir" a la industria de que pueden ser vulnerables a los ataques, en este caso, no se transmitió ninguna advertencia inminente. Como tal, las empresas con sede en ambos países se vieron profundamente afectadas y el comercio electrónico global enfrentó retrasos de semanas y meses debido a la falta de preparación de estas compañías y del apoyo adecuado de sus gobiernos. Por último, las principales compañías energéticas de Arabia Saudita, que suministran casi el 25 por ciento del gas natural líquido del mundo y alimentan los sistemas de transporte del mundo, quedaron fuera de línea debido a otras actividades cibernéticas maliciosas que afectaron tanto los sistemas de transporte como la economía mundial.

Como ejemplifican estos casos, ningún país está preparado cibernéticamente y la preparación debe comenzar con un enfoque de gestión de riesgos disciplinado. La gestión eficaz del riesgo requiere que los líderes de un país comprendan ante todo lo que más valoran, describan qué es lo más importante que deben proteger y demuestren que están dispuestos a invertir el capital político, el tiempo de los ejecutivos, el dinero y los recursos necesarios para protegerlo.

Por ejemplo, Colombia inició un enfoque de gestión de riesgos para evaluar su preparación cibernética y promover la confianza de la sociedad en el uso del entorno digital. Las gestiones fueron la respuesta a la tarea impuesta por la Política Nacional de Seguridad

Digital (estrategia nacional de seguridad digital), que fue aprobada en abril de 2016 por el Consejo Nacional de Política Económica y Social (CONPES), mediante la emisión del Documento CONPES 3854 de 2016. Colombia adoptó la guía de gestión de riesgos de la OCDE y utilizó ese marco junto con las recomendaciones de la OEA, la UIT y la Organización del Tratado del Atlántico Norte (OTAN) para evaluar las amenazas digitales al país y comprender qué activos críticos estaban en riesgo[22]. El estudio llevó a que el país evaluara los riesgos cibernéticos más apremiantes, identificara cómo afectan los incidentes cibernéticos a las organizaciones colombianas tanto en el sector privado como en el público y convirtiera la seguridad cibernética en una prioridad y un componente importante de su desarrollo socioeconómico. También ayudó a crear conciencia entre los diferentes interesados en el país sobre los tipos comunes y singulares de incidentes, amenazas y ataques cibernéticos que afectan las entidades y empresas del sector público y se comenzaron a cuantificar los costos para la economía del país. Colombia reconoció que la gestión de los riesgos cibernéticos a nivel nacional es un requisito previo fundamental para la digitalización del sector y la transformación digital del país.

La experiencia de Colombia evidencia que la gestión del riesgo comienza con el liderazgo y la gobernanza. Como enfatizan la mayoría de los marcos, índices y guías publicados por varias organizaciones intergubernamentales, académicas y comunidades técnicas en los últimos años, es fundamental la evaluación de lo que realmente está en riesgo y la elevación de la seguridad cibernética a la cima de la estrategia de seguridad nacional de un país. Sin embargo, no es suficiente hacer de la seguridad cibernética una prioridad en una categoría independiente y tratarla como un problema predominantemente de seguridad nacional. De hecho, el garantizar la seguridad cibernética también está estrechamente relacionado con la conectividad a Internet y la rápida adopción de las TIC, que, cuando son seguras y resistentes, pueden llevar al crecimiento económico y prosperidad. Por lo tanto, alinear las iniciativas económicas con la seguridad, el desarrollo y la resiliencia (la evaluación del valor en riesgo y el establecimiento de una estrategia nacional que maneje las actividades de reducción de riesgos) es igualmente importante.

Evaluación del riesgo

Los líderes nacionales deben expresar claramente su intención de aprovechar el entorno digital abierto para la prosperidad económica y social mediante la reducción del nivel general de riesgo de seguridad digital dentro y fuera de las fronteras. Deben ser conscientes de que el riesgo cambia con el tiempo en función de las acciones realizadas por al menos dos actores: el atacante que obtiene y utiliza la capacidad de causar daño; y el objetivo pretendido, que puede tomar precauciones para resistir o frustrar el peligro pretendido por el atacante. Los líderes nacionales deben demostrar su compromiso de reducir los riesgos y aumentar la resiliencia realizando evaluaciones continuas de riesgos tanto a nivel nacional como sectorial y adoptando medidas, políticas y procesos apropiados para gestionar los riesgos identificados.

Para alcanzar estos objetivos generales, los líderes nacionales, los responsables de la formulación de políticas y otras partes interesadas relevantes en cada país deben trabajar juntos para evaluar el riesgo. La planificación estratégica y la reflexión pueden ayudar a determinar el estado de preparación:

- ¿Cuál es la estrategia a corto y largo plazo para el país, incluidas las políticas industriales, los objetivos económicos y las prioridades de seguridad nacional?

- ¿Qué podría poner en riesgo estos objetivos? En otras palabras, ¿qué debilidades podrían explotarse (es decir, activos de alto valor no contabilizados) que podrían interrumpir la ejecución de estos objetivos?

- ¿Existen líneas claras de responsabilidad y rendición de cuentas para garantizar la implementación de los objetivos del país y la implementación de medidas de reducción de riesgos?

- ¿Han sido las consideraciones de seguridad cibernética y resiliencia una parte central del proceso de planificación?

Esta evaluación exhaustiva y abarcadora destacará las dependencias digitales más críticas de un país (p. ej., empresas, servicios, infraestructuras y activos) que, en caso de daño, tendrían graves consecuencias económicas y de seguridad nacionales. Solo después de identificar adecuadamente qué es vulnerable, qué podría poner en peligro las "joyas de la corona" de un país y la probabilidad de que estas estén expuestas a peligros, daños o pérdidas, los tomadores de decisiones podrán tomar medidas correctivas para frustrar o reducir esos riesgos.

5 REDUCCIÓN DEL RIESGO A TRAVÉS DE UNA PLANIFICACIÓN CUIDADOSA

Una vez que haya realizado una evaluación de riesgos, un país puede diseñar un plan de reducción de riesgos para cerrar la brecha entre su postura de seguridad cibernética actual y las capacidades cibernéticas nacionales necesarias para corregir las deficiencias y apoyar las futuras prioridades económicas y de seguridad del país. Los esfuerzos de reducción de riesgos deben ser dirigidos por una autoridad nacional de seguridad cibernética competente y dedicada: un líder (tanto una persona como una entidad) que haya sido elevado y que esté fuertemente anclado al más alto nivel del gobierno para dirigir, coordinar acciones y monitorear la implementación del plan, y ser responsable de las deficiencias y los resultados logrados. Dado que la seguridad cibernética es transversal a muchas áreas de problemáticas diferentes (p. ej., derechos humanos, desarrollo económico, comercio, control de armas y tecnologías de doble uso, seguridad, estabilidad y paz y resolución de conflictos), es importante garantizar que la autoridad nacional competente tenga la autoridad posicional, la responsabilidad y el empoderamiento para involucrar y dirigir a tantas partes interesadas como sea necesario.

Si bien son abundantes los lineamientos sobre actividades de reducción de riesgos, como lo demuestran los diversos marcos descritos en secciones anteriores, los líderes nacionales deberían hacer un mayor esfuerzo para comprender el panorama del riesgo cibernético y las amenazas específicas a sus infraestructuras en red, que deberían estar claramente delineadas en sus estrategias de seguridad cibernética nacional y en la (s) evaluación (es) nacional (es) de riesgos cibernéticos. Y luego deberían trabajar con todas las partes interesadas para planificar mejor sus defensas y asignar mejor los recursos humanos y financieros para minimizar esos riesgos. Estrategias comunes para mitigar eficazmente el riesgo cibernético incluyen:

- Comunicar lo que está en juego y mejorar la concientización general sobre los riesgos en todos los niveles, desde los líderes gubernamentales hasta los ciudadanos comunes. Las personas no pueden valorar la seguridad sin antes comprender qué parte de sus actividades diarias está en riesgo, no solo información personal. Por lo tanto, el gobierno debería iniciar una campaña nacional de concientización pública, promover la educación, la capacitación y el desarrollo de habilidades, y empoderar a sus ciudadanos para que formen parte de la solución en la construcción de una sólida cultura de seguridad cibernética.

- Identificar, priorizar y enfocar los recursos necesarios en activos de alto valor y sistemas de alto impacto que requieren mayores niveles de protección: las dependencias digitales más críticas del país (p. ej., empresas, infraestructuras, servicios y activos); comprender las vulnerabilidades de los mismos y priorizar medidas de seguridad apropiadas y acordes con el riesgo económico y social.

- Desarrollar marcos legales y regulatorios apropiados para proteger a la sociedad contra el delito cibernético, la interrupción del servicio y la destrucción de la propiedad.

- Usar una amplia gama de herramientas que incluyen políticas, legislación, normas, estándares, incentivos de mercado, esquemas voluntarios de cumplimiento y otras iniciativas para aumentar la confianza y la seguridad en el uso de las TIC, así como corregir las deficiencias en los procesos y productos (p. ej., Directiva NIS, Ley de Seguridad Cibernética de China, Marco NIST).

• Mejorar el conocimiento de la situación, los indicadores de amenaza y las advertencias mediante el monitoreo continuo de las amenazas a la sociedad interconectada y el uso de las últimas tecnologías para detectar, repeler y contener dichas amenazas.

• Desarrollar las capacidades nacionales necesarias para aumentar la preparación, realizar la planificación de continuidad, y responder y recuperarse de los riesgos significativos de seguridad cibernética cuando surjan (p. ej., una crisis cibernética a gran escala).

• Involucrar a la comunidad internacional para mejorar la seguridad general, la confiabilidad y la resiliencia de las redes interoperables (p. ej., financieras, telecomunicaciones, energía, etc.) a través del desarrollo de estándares de seguridad global y la promoción de acuerdos multilaterales.

• Anticipar los avances tecnológicos futuros y evaluar cómo pueden introducir nuevas vulnerabilidades en el país o, por otro lado, cómo podrían convertirse en oportunidades para crear seguridad, fiabilidad y resiliencia adicionales en las infraestructuras y activos de la próxima generación.

La implementación efectiva de estas tareas y otras actividades requerirá definir y clarificar claramente las funciones, responsabilidades, procesos, derechos de decisión y mecanismos de rendición de cuentas. Los resultados exitosos se beneficiarán al establecer metas de desempeño para varios departamentos ministeriales o gubernamentales, instituciones o personas responsables de tareas específicas en el plan de acción.

Por supuesto, las actividades de reducción de riesgos también requieren la asignación de recursos dedicados y apropiados para su implementación. Fuentes y mecanismos de financiación ineficientes pueden tanto socavar los resultados pretendidos y reducir la responsabilidad de las entidades encargadas de la seguridad cibernética de la nación, como dejar recursos insuficientes para llevar a cabo sus propias misiones. Los recursos deben definirse en términos de dinero (es decir, presupuesto dedicado), personas, material, así como las relaciones y asociaciones necesarias para una ejecución y resultados exitosos de los planes de mitigación de riesgos. La asignación de recursos para los objetivos y las tareas dentro de una estrategia nacional de seguridad cibernética no debe verse como una iniciativa de una sola vez. El financiamiento suficiente, consistente y continuo proporciona las bases para una postura nacional eficaz de seguridad cibernética. Los recursos se pueden asignar por tarea u objetivo, o por entidad gubernamental. El gobierno también puede considerar el establecimiento de un presupuesto central para seguridad cibernética, administrado por un mecanismo central de gobernanza de seguridad cibernética. Ya sea que reúna diferentes fuentes de financiamiento en un programa coherente e integrado o cree un presupuesto intra gubernamental unificado, el programa general debe ser gestionado y monitoreado por hitos y plazos claramente definidos para garantizar la implementación exitosa de la estrategia.

Evaluación continua del riesgo

Cuando las gestiones de seguridad cibernética se convierten en una evaluación puntual (al seguir un marco de cumplimiento), en lugar de evaluar el riesgo de forma continua, estas fallan. La gestión de riesgos requiere una anticipación proactiva de las amenazas a y una evaluación continua de las vulnerabilidades dentro de las dependencias digitales más críticas del país (p. ej., empresas, infraestructuras, servicios y activos). Como se indicó anteriormente, existe una serie de marcos que destacan la importancia de la evaluación continua del riesgo y la corrección de las fallas de control. Monitorear y medir el desempeño y la ejecución exitosa de las iniciativas de seguridad cibernética (actividades de reducción de riesgos) debe ser parte de los mecanismos de gobernanza que un país establece en su arquitectura nacional de seguridad cibernética. La evaluación continua del plan de implementación (es decir, lo que está funcionando bien y lo que no) ayuda a informar ajustes y una mayor defensa de la estrategia global. Los mecanismos de buena gobernanza delinean la responsabilidad y la rendición de cuentas para garantizar una ejecución exitosa, y se deben usar métricas o indicadores clave de rendimiento (KPI, por sus siglas en inglés) accionables, repetibles, significativos y dependientes del tiempo para reforzar los objetivos y cronogramas realistas. Las métricas o indicadores clave de rendimiento deben cumplir los siguientes criterios

• ***Ser específicos*** – tener como objetivo un área específica de mejora.

• ***Ser medibles*** – cuantificar, o al menos sugerir, un indicador de progreso.

• ***Ser alcanzables*** – establecer qué resultados se pueden alcanzar de manera realista, dados los recursos disponibles.

• ***Ser accionables*** — indicar claramente las acciones que se implementarán.

• ***Tener responsables*** – especificar quién lo hará.

• ***Estar en función del tiempo*** – especificar cuándo se pueden lograr los resultados.

Si bien ningún país está totalmente preparado cibernéticamente

y los riesgos cibernéticos no se pueden eliminar por completo, pueden y deben ser gestionados. La preparación y la capacidad de reacción cibernética comienzan con un enfoque de gestión de riesgos efectivo que incluye una comprensión clara de los activos de alto valor y los sistemas de alto impacto del país que requieren mayores niveles de protección: las dependencias digitales más críticas del país (p. ej., empresas, infraestructuras, servicios, y activos). Una vez que se comprende esto, se pueden definir y priorizar las medidas de seguridad necesarias mediante un análisis de riesgo y una evaluación de vulnerabilidad para corregir las deficiencias que son apropiadas y acordes con el riesgo económico y social.

Solo con un esfuerzo concertado y coordinado entre los interesados nacionales será posible reducir significativamente el riesgo cibernético y avanzar para garantizar la seguridad y la protección futura de una nación.

5 CONCLUSIÓN

Nuestra inseguridad cibernética está creciendo. El volumen, alcance, escala y sofisticación de las amenazas cibernéticas a los servicios e infraestructuras críticas de las naciones están superando las medidas defensivas. Las actividades cibernéticas destructivas y disruptivas de hoy en día requieren que los gobiernos aborden e inviertan urgentemente en hacer que su país pase de un estado de inseguridad cibernética a un estado de preparación cibernética. Las pérdidas se están acumulando; el daño está creciendo; y el peligro es inminente.

Los líderes nacionales deben diseñar estrategias integrales de seguridad cibernética nacional que incluyan una autoridad competente y dedicada, responsable de la postura nacional general de seguridad cibernética del país. Se debe desarrollar una comprensión nacional de los riesgos enfrentados en todos los niveles, desde los líderes gubernamentales hasta los ciudadanos comunes. Todos deben comprender las vulnerabilidades del entorno digital del país y conocer su papel en la mitigación de esos riesgos. Esta hoja de ruta estratégica permite la adopción de medidas, políticas y procesos apropiados para corregir las deficiencias y reducir los riesgos para la sociedad, la economía y la nación. Esto no se puede lograr sin recursos dedicados y apropiados que financien iniciativas para reducir riesgos y aumentar la resiliencia. La adopción de una estrategia nacional de seguridad cibernética es uno de los pasos más importantes para garantizar la infraestructura y los servicios cibernéticos nacionales de los que depende el futuro digital y el bienestar económico de una nación moderna.

6

SOBRE LA AUTORA

Melissa Hathaway es una de las principales expertas en políticas de ciberespacio y seguridad cibernética. Trabajó en dos administraciones presidenciales de EE. UU., dirigiendo la Revisión de políticas del ciberespacio para el presidente Barack Obama y lideró la Iniciativa nacional integral de seguridad cibernética (CNCI, por sus siglas en inglés) para el presidente George W. Bush. Como presidenta de Hathaway Global Strategies LLC, ella asesora a clientes del sector público y privado y ofrece una combinación única de experiencia técnica y de políticas, así como experiencia en juntas directivas para ayudar a otros a comprender mejor la transversalidad de las políticas gubernamentales, el desarrollo de tendencias tecnológicas y de la industria, y los impulsores económicos que impactan la estrategia de adquisición y desarrollo de negocios en este campo. Desarrolló una metodología única para evaluar y medir el nivel de preparación para ciertos riesgos de seguridad cibernética, conocido como el Índice de preparación cibernética (Cyber Readiness Index 2.09 que se puede encontrar en:
www.potomacinstitute.org/academic-centers/cyber-readiness-index.
Ella publica regularmente sobre asuntos de cibernética que impactan compañías y países. La mayoría de sus artículos se pueden encontrar en los siguientes sitios web:
www.belfercenter.ksg.harvard.edu/experts/2132/melissa_hathaway.html y
www.ctm.columbia.edu/people/melissa-hathaway.

5

REFERENCIAS

1. Diccionario Oxford. El NIST SP 800-30 (Rev A) define el riesgo como sigue: Riesgo = Amenaza x Vulnerabilidad. El CRM define las declaraciones de riesgo como: Riesgo = Condición (Probabilidad) + Consecuencia (Impacto).

2. Nicolas Rapp and Robert Hackett, " A Hackers Toolkit." Fortune Magazine 25 October 2017, http://fortune.com/2017/10/25/cybercrime-spyware-marketplace/

3. Eduard Kovaks, "Shadow Brokers Want $20,000 for Weekly Leaks," Security Magazine, 30 May 2017, www.securityweek.com/shadow-brokers-want-20000-monthly-leaks; and
Eduard Kovaks, "Shadow Brokers Promise More Exploits for Monthly Fee," Security Magazine, 16 May 2017, www.securityweek.com/shadow-brokers-promise-more-exploits-monthly-fee; and
Nicole Perloth, "A Cyberattack the 'World Isn't Ready For,'" The New York Times, 22 June 2017, www.nytimes.com/2017/06/22/technology/ransomware-attack-nsa-cyberweapons.html?_r=0

4. National Audit Office, "Investigation: WannaCry cyber attack and the NHS," 27 October 2017, www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/.

5. Richard Chirgwin, "IT 'heroes' saved Maersk from NotPetya with ten-day reinstallation bliz," The Register, 25 January 2018, https://www.theregister.co.uk/2018/01/25/after_notpetya_maersk_replaced_everything/.

6. NotPetya interrumpió negocios y destruyó activos de capital corporativo a nivel mundial. Los informes públicos de A.P. Moller-Maersk, Balersdorf, DHL, DLA Piper, Federal Express, Merck, Mondolez, Nuance, Reckitt Benckiser Group, Rosneft, Saint Gobain, y WPP muestran pérdidas de al menos $2.500 millones. Un informe reciente de Lloyds of London advierte que un ciberataque bien ejecutado podría causar daños en todo el mundo, por valor desde $53.100 millones a $121.400 millones. Véase: Lloyds of London, "Extreme Cyber-Attack Could Cost as Much as Superstorm Sandy," 17 July 2017, www.lloyds.com/news-and-risk-insight/press-releases/2017/07/cyber-attack-report.

7. Kelly Jackson Higgins, "Schneider Electric: TRITON/TRISIS Attack Used 0-Day Flaw in its Safety Controller System, and a RAT," Dark Reading, 18 January 2018, https://www.darkreading.com/vulnerabilities--threats/schneider-electric-triton-trisis-attack-used-0-day-flaw-in-its-safety-controller-system-and-a-rat/d/d-id/1330845.

8. Los dominios de nivel superior (p. ej., .mil, .com, .edu, .gov) se introdujeron en 1985 y permitieron establecer el marco para el comercio electrónico global. La innovación continuó introduciendo nuevas tecnologías como la creación de lenguaje de marcado de hipertexto (HTML) en 1990, que permitió un mayor intercambio de información y de fácil uso en Internet, que finalmente se convirtió en la World Wide Web. Surgieron otros avances tecnológicos como: mensajes SMS (1992), protocolo de voz sobre Internet (1996), WiFi (1997), wikipedia (2001), el buscador de Google (1997), tecnología de redes sociales (2002) y voz y video sobre Protocolo de Internet con Skype (2003). El sector privado está impulsando la innovación y adopción de la tecnología prometiendo reducir costos, aumentar la productividad y la usabilidad del consumidor, sin hablar mucho sobre la seguridad. Véase: Melissa Hathaway, "Falling Prey to Cybercrime: Implications for Business and the Economy," in Securing Cyberspace: A New Domain for National Security, February 2012, Aspen Institute Press.

9. Muchos países tienen diferentes definiciones de las infraestructuras críticas. Para los fines de este documento, se utilizó una definición amplia. Véase: Homeland Security Digital Library, "Presidential Decision Directive 63, PDD/NSC-63," 22 May 1998, https://fas.org/irp/offdocs/pdd/pdd-63.htm.

10. Los funcionarios aún no han definido cuántos sectores se incluirán dentro del alcance de la ley. Sin embargo, muchos expertos creen que esta ley incluye los mismos sectores que la Directiva de Seguridad de las Redes y Sistemas de Información de la UE (p. ej., energía, transporte, banca, infraestructuras del mercado financiero, infraestructuras digitales, salud y agua). Véase: Yanqing Hong, "The Cross-border Data Flows Security Assessment: An Important Part of Protecting China's Basic Strategic Resources," 20 June 2017, Yale Law School, Paul Tsai China Center Working Paper, https://law.yale.edu/system/files/area/center/china/document/dataflowssecurity_final.pdf.

11. NIST, "Cybersecurity 'Rosetta Stone' Celebrates Two Years of Success," 18 February 2016, www.nist.gov/news-events/news/2016/02/cybersecurity-rosetta-stone-celebrates-two-years-success.

12. Hathaway Global Strategies LLC. Insights from engagement with Board of Directors and Management of affected companies.

13. NIST, "NIST Special Publication 800-37 (Rev. 2) DRAFT — Risk Management Framework for Information Systems and Organizations: A System Lifecycle Approach for Security and Privacy (Discussion Draft)," September 2017, www.csrc.nist.gov/CSRC/media/Publications/sp/800-37/rev-2/draft/documents/sp800-37r2-discussion-draft.pdf.

14. WSIS, Geneva 2003 - Tunis 2005, "Tunis Commitment," 18 November 2005, www.itu.int/net/wsis/docs2/tunis/off/7.html.

15. ITU (2014), Global Cybersecurity Index, www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx.

16. OECD (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris, www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf.

17. WEF (2018), Cyber Resilience Playbook for Public-Private Collaboration, pp. 33-36, https://www.weforum.org/reports/cyber-resilience-playbook-for-public-private-collaboration.

18. Ibid.

19. El Cyber Readiness Index 2.0 se basa en el anterior Cyber Readiness Index 1.0, que proporcionó un marco metodológico para evaluar la preparación cibernética en cinco elementos esenciales, a saber: estrategia cibernética nacional, respuesta a incidentes, delito electrónico y capacidad legal, intercambio de información e investigación y desarrollo cibernético. El Cyber Readiness Index 1.0 aplicó esta metodología a un conjunto inicial de treinta y cinco países. Para obtener más información sobre Cyber Readiness Index 1.0, véase: Melissa Hathaway, "Cyber Readiness Index 1.0," Hathaway Global Strategies LLC (2013), http:// belfercenter.ksg.harvard.edu/ les/ cyber-readiness-index-1point0.pdf.

20. NCSI, "NCSI Methodology," http://ncsi.ega.ee/methodology (1.0) and http://ncsi.ega.ee/ncsi-methodology-2-0-launched/ (2.0).

21. National Coordinator for Security and Counterterrorism, "Review of Policy on Critical Infrastructure," July 2015; and Melissa Hathaway and Francesca Spidalieri, "The Netherlands Cyber Readiness at a Glance," May 2017, Potomac Institute for Policy Studies, http://www.potomacinstitute.org/images/CRI/FinalCRI20NetherlandsWeb.pdf.

22. OAS, MINTIC, IDB (2017), Impact of Digital Security incidents in Colombia 2017, https://publications.iadb.org/handle/11319/8552.

OEA
Más derechos
para más gente

GESTIÓN DEL RIESGO
CIBERNÉTICO NACIONAL

White paper series
Edición 2

2018