CAPÍTULO IV

ESTADO DEL ARTE DE LA GESTIÓN DE RIESGOS EN SEGURIDAD DIGITAL EN EL SECTOR GOBIERNO EN EUROPA Y AMÉRICA DEL NORTE*

Rafael Vicente Páez Méndez

* Capítulo de libro resultado del proyecto de investigación titulado "Gestión de Riesgos en seguridad Digital" de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra, que a su vez hace parte de la línea de investigación "Seguridad Digital" del grupo de investigación "Masa Crítica", reconocido y categorizado en (B) por Colciencias. Registrado con el código COL0123247, está adscrito a la Escuela Superior de Guerra "General Rafael Reyes Prieto" de la República de Colombia.

Introducción

La Gestión de Riesgos en el entorno digital es un tema de vital importancia para todos los gobiernos del mundo, por tal razón es necesario generar políticas públicas que permitan proteger el entorno cibernético del país utilizando un modelo de gestión del riesgo basado en el contexto, de manera que se pueda identificar el riesgo, valorarlo y minimizarlo hasta niveles aceptables después de aplicar los controles correspondientes.

La Estrategia de Gestión de Riesgos es un proceso dinámico, ya que es necesario adaptarse a los cambios de la sociedad en ámbitos políticos, sociales, económicos, entre otros, por lo tanto, es necesario generar modelos que permitan realizar una gestión precisa y efectiva en el contexto de la realidad de cada país, sin embargo, existen iniciativas que pueden ser adaptadas a diferentes necesidades para generar y adoptar un modelo propio.

Tanto la industria como los gobiernos están permanentemente desarrollando estrategias de gestión de riesgos y alineándose con buenas prácticas y estándares internacionales como ISO/IEC 27001 y 27002. Por otra parte, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) afirma que la gestión de riesgos ayuda a proteger y soportar las actividades sociales y económicas y provee un marco general de 8 principios de alto nivel en gestión de riesgos en seguridad digital con el fin de orientar a las organizaciones tanto públicas como privadas en el desarrollo de un modelo propio de gestión de riesgos (Organisation For Economic Co-Operation And Development, 2015).

1. Situación actual

En Europa, se conformó la Agencia Europea de Seguridad de las Redes y de la Información (*EuropeanUnion Agency for Network and Information Security* – ENISA)[5] en donde se publican diferentes documentos sobre seguridad y particularmente, en materia de Riesgos los clasifica en una escala temporal en *Riesgos actuales*, *Riesgos emergentes* y *Riesgos futuros*; de esta manera, se proveen las herramientas, los métodos y las buenas prácticas, para que entidades tanto gubernamentales como privadas las utilicen como guía con el fin de enfrentar las amenazas.

En **Albania**, las bases de datos del gobierno y el uso público de la información se encuentran en una etapa temprana de desarrollo y aún se considera como una expectativa potencial futura para una mejor gobernanza, se contemplan avances en la implementación del gobierno electrónico en términos de intercambio de información entre servidores públicos, ciudadanos y agentes sociales y económicos. Así mismo, se busca la transparencia en la gobernanza con relación a los ciudadanos y los medios, así como la descentralización y fortalecimiento de la autonomía local. La participación ciudadana aún es un desafío que se pretende encarar. Los programas políticos de los gobiernos aún no han considerado como una prioridad la información de los sistemas de gestión en Albania, especialmente en la administración pública. Por esa razón, los sistemas de información a nivel local no se han integrado y se encuentran en un estado de incompletitud, este es un proceso complejo que atraviesa etapas como la difusión electrónica de información a través de la presencia en la web hasta la transformación total del gobierno por medio del contacto directo con los ciudadanos, que permita ofrecer acceso a trámites de servicios públicos confiables, seguros y de fácil acceso en línea con una participación activa de los ciudadanos particulares y usuarios del sector económico (empresas). La gestión de riesgos en seguridad digital se tiene en cuenta para lo que el gobierno albanés denominó como

5 Consulte https://www.enisa.europa.eu/topics/threat-risk-management/risk-management

la "Iniciativa de desarrollo", anunciada en abril de 2002 en la conferencia internacional "e-Government para el desarrollo" en Palermo (Italia), que promovió la puesta en marcha en la implementación de proyectos de gobierno electrónico en las naciones beneficiarias, incluida Albania. El proyecto se lanzó a principios de 2005 y se centra en la asistencia técnica para establecer un sistema de correo electrónico gubernamental y el despliegue de los sistemas y bases de datos existentes en el gobierno.

En **Alemania**, la Oficina Federal Alemana para la seguridad de la Información es la autoridad nacional de ciberseguridad y es la encargada de determinar la gestión de riesgos en seguridad digital, haciendo control de la seguridad de la información en la digitalización a través de la prevención, detección y reacción para el gobierno, las empresas y la sociedad. Esta entidad se encarga de promover la seguridad de TI en Alemania por medio de tres divisiones: el CERT-Bund (Equipo de Respuestas de Emergencias Computacionales), el IT *Situation Centre* (Monitoreo y alertas tempranas), el IT *Crisis Reaction Centre* (Manejo de Crisis Nacionales) y el *Cyber Response Centre* (Cooperación con otras entidades federales para la seguridad) (Bundesamt für sicherheit in der informationstechnik, 2009). Al evidenciar que en la última década el proceso de digitalización de la información avanza a grandes pasos y de igual forma impulsan la comunicación, comercio y entretenimiento se ha adoptado el término "gobierno electrónico" al comprobar la necesidad de seguridad de TI, ya que las amenazas pueden llegar a pasar desapercibidas a primera vista. La ciberseguridad se está convirtiendo en una de las áreas de más rápido crecimiento en la política mundial. Es imposible para un Estado gestionar el escape de la ola emergente de ciberataques. Los efectos generalizados de las armas cibernéticas han socavado los sistemas existentes de detección e interceptación de los Estados. Las autoridades de Alemania reafirmaron la importancia de la ciberseguridad y su relevancia para el futuro del país. El Ministerio de seguridad Nacional de Alemania cree que las amenazas a la seguridad cibernética prevalecen en este país debido a la digitalización de la sociedad y al desarrollo de infraestructura estatal.

En **Andorra**, se ha estado a la vanguardia de la práctica de seguridad de la información durante muchos años, creando e implementando programas efectivos para gobernar y administrar los riesgos. Han desarrollado y operado Centros de Operaciones de Seguridad, dirigieron prácticas de respuesta a incidentes de seguridad, crearon marcos de políticas y gobernanza, y han implementado y operado equipos de investigación digital. El Gobierno de este país cree firmemente en el posicionamiento de la seguridad de la información como un habilitador de negocios mediante la promoción de un enfoque arquitectónico y basado en el riesgo para el desarrollo y la gestión de programas. Es por esto que creen necesario implementar un control, y eso es para administrar el riesgo, es decir, para comprender completamente el impacto del control; debe poder medir y evaluar el riesgo.

Se pretende también que el uso efectivo de la gestión de riesgos en la seguridad de la información tenga dos grandes beneficios. En primer lugar, permitir a los diferentes actores gubernamentales poder tomar decisiones razonables sobre las inversiones en seguridad de TI e impulsar la aceptación de nuevos controles, de manera que se pueda clasificar como tratamientos de gestión de riesgos. Esto con el fin de ayudar a posicionar la seguridad de la información como un habilitador de negocios, y no solo como un centro de costos. En segundo lugar, se espera garantizar que las decisiones fundamentales de gestión de riesgos no sean retenidas por los líderes empresariales y ponga la responsabilidad del riesgo en el lugar al que pertenece como lo es directamente los ministerios de Defensa, del Interior y de Tecnología de la Información. Lo anterior con el fin de medir el costo, que puede ser financiero, reputacional o reglamentario, a lo largo del tiempo y su impacto en la eficiencia del negocio también puede ser extremadamente desafiante.

En **Austria,** la política de ciberseguridad de vanguardia es una cuestión transversal que se tiene en cuenta en muchas esferas de la vida y las políticas de esta nación. Se considera que debe modelarse sobre la base de un enfoque integral e integrado, de modo que se pueda permitir la participación activa y se logre implementar con un espíritu de solidari-

dad, es por esto que el canciller Sebastian Kurtz actualmente pretende implementar: una Política Integral de Ciberseguridad, es decir, que la seguridad externa e interna, así como los aspectos de seguridad civil y militar están estrechamente relacionados.

Cabe indicar, que la ciberseguridad va más allá del alcance de las autoridades de seguridad tradicionales y comprende instrumentos de muchas otras áreas de políticas. Esta nación considera que una Política Integrada de Seguridad Cibernética debe hacer hincapié en la distribución de tareas entre el Estado, la economía, el mundo académico y la sociedad civil. Así, incluyendo medidas en las siguientes áreas: gestión estratégica, educación y capacitación, evaluación de riesgos, prevención y preparación, reconocimiento y respuesta, limitación de efectos y restauración, así como desarrollo de capacidades y capacidades gubernamentales y no gubernamentales. Una Política Integrada de Seguridad Cibernética debe basarse en un enfoque cooperativo tanto a nivel nacional como internacional, además debe ser proactiva de modo que se pueda trabajar para prevenir las amenazas al ciberespacio y las personas en el ciberespacio o para mitigar su impacto.

Además, se quiere basar la gestión de riesgos en seguridad digital en la solidaridad teniendo en cuenta el hecho de que, debido a la naturaleza global del espacio cibernético, la seguridad cibernética de Austria, la UE y toda la comunidad de naciones está muy interconectada. Por lo tanto, se requiere una cooperación intensiva basada en la solidaridad a nivel europeo e internacional para garantizar la ciberseguridad. Los principios universales de seguridad de las TIC para una **Austria digital** son plenamente aplicables a la ciberseguridad: confidencialidad, integridad, aplicación obligatoria, autenticidad, disponibilidad, así como privacidad y protección de datos.

En **Australia**, el Gobierno cuenta con un marco de referencia denominado PSPF (Protective Security PolicyMarco de referencia)[6] e incluye la gestión de riesgos que está alineada con el estándar ISO

6 Consulte https://www.protectivesecurity.gov.au/resources/Documents/Protective-security-Policy-Framework-Map.pdf

31000:2009 (Australian/Standards, 2009) y HB 167:2006 *Security Risk Management* y con las políticas de gestión de riesgos de la Mancomunidad de Naciones, de modo que se pueda tener un sector público más productivo, innovador y eficiente, dando así un enfoque a la gestión del riesgo para alcanzar los objetivos estratégicos de la Mancomunidad y limitar la burocracia innecesaria. La gestión efectiva de riesgos, basada en el buen juicio y la mejor información disponible, mejora la capacidad de la Commonwealth para identificar, administrar y obtener los máximos beneficios de los nuevos desafíos y oportunidades. (Commonwealth of Australia, 2014). La Oficina de Gestión de Inversiones Digitales se ha establecido dentro de la Agencia de Transformación Digital (ATD) del Gobierno australiano para supervisar todos los proyectos importantes de TIC e inversión digital en todo el Gobierno. Cada año, el Gobierno gasta alrededor de $ 6.2 mil millones en inversiones en TIC. Al desarrollar enfoques nuevos y más estratégicos para el análisis de inversiones, la gobernanza, la gestión de riesgos y la gestión de programas y beneficios, podremos proporcionar una mayor transparencia y optimización de la cartera de inversiones del Gobierno. Una prioridad inicial para la oficina será llevar a cabo una revisión de la inversión anual en TIC del Gobierno y proporcionar una imagen completa de los costos, beneficios, riesgos y el estado de todos los proyectos y programas por valor de más de $ 10 millones de dólares. La oficina también se enfoca en establecer alianzas estratégicas continuas en todo el Gobierno para proporcionar garantías independientes y una mejor prestación de beneficios tanto para las agencias como para las personas que utilizan los servicios del gobierno en línea.

Azerbaiyán evidencia cómo los efectos generalizados de la tecnología de la información desarrollaron el sistema internacional como un área fértil para la guerra cibernética. El ciberespacio internacional carece por completo del órgano rector central o de cualquier sistema internacional principal de administración. Sin duda, los Estados están formulando sus alianzas para luchar activamente en el ciberespacio. Pero hasta ahora es difícil separar a los amigos de los enemigos, por-

que las relaciones de déficit de confianza entre las naciones crearon un sistema ciberespacial anárquico internacional, que en última instancia ha hecho que cada Estado sea vulnerable ante las Fuerzas rivales. Este Estado que se encuentra en la encrucijada de Eurasia, está rodeado por el mar Caspio y la cordillera del Cáucaso, debido a la ocupación armenia de Nagorno-Karabaj y al conflicto armado internacional vino consigo inseguridad cibernética al mar Caspio y los Estados vecinos antagónicos del Irán clerical y la Rusia nuclear.

Con relación a los ciberataques, Azerbaiyán está tomando varias iniciativas para la protección de su infraestructura digital. El ministro de Comunicación e Informática varias veces destacó la visión del Gobierno en una declaración para el fortalecimiento de la seguridad de la información de Azerbaiyán. Además, mencionó la ambición de su país de desarrollar una colaboración internacional contra las amenazas prevalecientes de ciberataques organizados. De esta forma, tres importantes instituciones de Gobierno complementan la Defensa de las fronteras cibernéticas de Azerbaiyán: el Ministerio de Comunicación y Tecnología Informacional (MCIT), el Ministerio de seguridad Nacional (MNS) y la Academia Nacional de Ciencias de Azerbaiyán (ANAS). En resumen, el Gobierno de Azerbaiyán está desarrollando rápidamente su infraestructura de gestión de riesgos en seguridad digital con la ayuda de ANAS y mejorando la infraestructura digital del Estado. Un entorno digital emergente necesita un sistema de red de comunicación infalible. Sin duda, un enfoque de cooperación multilateral podría aumentar las leyes existentes de ciberseguridad, pero los esfuerzos individuales activos de los Estados podrían desempeñar un papel más efectivo. Por lo tanto, la combinación de enfoques unilaterales y multilaterales puede contrarrestar mutuamente las abrumadoras amenazas no militares y transnacionales de ciberataques. La base legal de la ciberseguridad debe fortalecerse en Azerbaiyán porque, las armas cibernéticas en diferentes formas (como el virus *Stuxnet*) ya han intentado destruir la infraestructura cibernética del gobierno (Makili-Aliyev, 2013). Por lo tanto, una red cibernética fuerte y bien asegurada puede prevenir los riesgos de los ciberataques en la infraestructura digital del país. Además, la promoción y avance

de las leyes cibernéticas con el establecimiento de un ciberejército se ha convertido en una demanda vital para Azerbaiyán a fin de fortalecer la ciberseguridad Nacional del Estado. De esta manera, la seguridad del ciberespacio es una cuestión de inmensa importancia para Azerbaiyán, porque la creciente dependencia de la industria, el Gobierno y las instituciones financieras de las redes cibernéticas necesita un sistema de información completamente seguro y confiable, que pueda mantener la disuasión cibernética en el mundo ciberespacio.

Bélgica adoptó su Estrategia Nacional de ciberseguridad en 2013 y en 2014. Estableció el Centro para la Ciberseguridad (CCB) con tres objetivos estratégicos: asegurar un ciberespacio seguro y confiable; proporcionar seguridad y protección óptimas para las infraestructuras críticas y los sistemas de información gubernamentales y promover el desarrollo de capacidades de seguridad cibernética a nivel nacional. Toda una sección está dedicada a la gestión del riesgo cibernético, que abarca amenazas, vulnerabilidades e impacto (Department, 2014). Desde el lanzamiento del CCB se han tomado medidas para proveer a las autoridades públicas y a las empresas con el apoyo y asesoramiento sobre cómo protegerse más eficazmente contra las amenazas cibernéticas. Además, identifica las infraestructuras críticas de Bélgica para garantizar la cooperación entre todos los actores involucrados, es así como en 2017 se lanzó un plan de respuesta de emergencia cibernética, destinado a establecer una forma estructurada para manejar las crisis e incidentes de ciberseguridad que requieren coordinación a nivel nacional. El objetivo es armonizar las acciones que los servicios gubernamentales toman para gestionar incidentes cibernéticos nacionales y garantizar el rápido, intercambio preciso de información entre servicios (Croo, 2017).

En **Bosnia y Herzegovina**, los principios básicos para el desarrollo y la aplicación de la gestión de riesgos en seguridad digital son los siguientes: el principio de voluntad política una lucha activa contra la delincuencia digital como una de las prioridades de las instituciones en

Bosnia y Herzegovina, de la mano de la no discriminación y respeto a las libertades de derechos de los ciudadanos, de modo que las actividades de la estrategia estén guiadas a garantizar el disfrute de todos los derechos y libertades humanas, de conformidad con la Constitución de Bosnia y Herzegovina, las leyes y las normas jurídicas internacionales. Además, se tienen en cuenta el *Principio de legalidad*, es decir el respeto de la Constitución y las leyes nacionales en esta área, así como ciertas disposiciones de los acuerdos internacionales (instrumentos jurídicos internacionales), de los cuales Bosnia y Herzegovina es signatario de modo que se pueda juzgar de modo eficiente a los ciberterroristas (Ministry of Interior of Republika Srpska, 2017).

Es así que el Gobierno pretende tener una visión única y global en la lucha contra los crímenes cibernéticos, basándose en un enfoque único y global del problema para así tener una correcta coordinación y cooperación de las prácticas y procedimientos para combatir la delincuencia digital tomando como pie un concepto único de sector público y privado, organizaciones internacionales en Bosnia y Herzegovina, la sociedad civil y los ciudadanos. Esto es encaminado de modo que se cuente con profesionalismo y coherencia en todas las áreas de acción en contra de los ciberdelitos de modo que se tiene en cuenta que hace falta una formación profesional continua, educación y capacitación de los servidores públicos, así como el intercambio de experiencias de mejores prácticas y eventos contemporáneos y su cumplimiento de medidas preventivas y represivas. Por otra parte, se espera tener una cooperación internacional activa en los preparativos para unirse a la Unión Europea y garantizar el papel activo de Bosnia y Herzegovina a nivel internacional para así poder garantizar el cumplimiento de los compromisos en la implementación de la Estrategia de gestión de riesgos en seguridad digital por medio de la supervisión de su implementación con la identificación de las instituciones responsables de la implementación de la misma con compromisos claramente definidos y plazos planificados para monitorear de forma correcta y en consecuencia, se llevará a cabo la evaluación de las medidas correctivas.

Croacia ha identificado algunas debilidades a nivel general en la parte digital como por ejemplo, la baja aceptación de las responsabilidades de seguridad de los propietarios de datos e infraestructura, una cultura de gestión de riesgos desarrollada de manera inadecuada, incoherencia de regulación frecuente a niveles generales y sectoriales, falta de adecuación de los nuevos conceptos de seguridad, como protección de infraestructura crítica, tradición jerárquica de la administración del gobierno, prácticas de intercambio de información muy limitadas (departamentales y sectoriales), falta de educación que apoye el desarrollo de la sociedad virtual y criterios poco claros para la verificación de programas educativos. A raíz de esto la Agencia de seguridad Nacional croata, desarrolló una serie de recomendaciones e iniciativas enfocadas al sector gubernamental, el programa industrial y la reorganización de iniciativas para compartir información de acuerdo con la Política Nacional de seguridad para generar una nueva gestión de riesgos en seguridad digital que involucrara desde la seguridad física hasta el fortalecimiento de la infraestructura informática por medio del refuerzo de sus agencias gubernamentales en esta área. En este país se ven como oportunidades a fututo por medio de dicha Gestión, el desarrollo social en educación y cultura, desarrollo económico en capacidad ciberespacial de interrelacionar los múltiples sectores de la nación brindando una mejor infraestructura y por ende mejores capacidades y productos potenciales.

En **Dinamarca**, las estrategias digitales del Gobierno conciernen a las autoridades en todos los niveles de este, desde el Estado hasta las regiones y los municipios; es decir, tanto las instituciones administrativas como los ministerios, agencias y las administraciones municipales y regionales, y las instituciones ejecutivas como hospitales, escuelas públicas, universidades, entre otros. La idea de este país es establecer un sector público más simple y cohesionado en el que se logre proporcionar servicios buenos y eficientes a individuos o empresas, sobre la base del conocimiento que ya se tiene. Para que esto se convierta en realidad, las autoridades deben en mayor medida poder intercambiar y acceder a datos relevantes sobre individuos de manera segura; no menos importante

en situaciones en las que muchas autoridades están involucradas. Por lo tanto, los gobiernos locales, regionales y centrales tienen que trabajar para compartir más los datos siempre que sea posible, relevante y seguro (Danish Ministry of Finance, 2016).

Paralelamente, el uso creciente de datos puede ser respaldado por estándares de datos comunes, formatos de datos estandarizados, arquitecturas de TI comunes y una infraestructura de TI robusta. El mayor intercambio de datos permitirá a las nuevas generaciones de soluciones digitales que puedan encontrar automáticamente los datos necesarios. Las personas y las empresas ahorrarán tiempo porque no tienen que reportar datos innecesariamente. Además, los procesos administrativos y el trabajo de casos se facilitarán si se pueden automatizar los flujos de trabajo manuales y, en algunas situaciones, las decisiones. Un intercambio e intercambio de datos más eficiente entre varios sistemas de TI y unidades organizativas proporcionará a las personas y empresas procedimientos de procesamiento de casos más eficientes y más intervenciones adaptadas y coherentes. En el futuro, las personas y las empresas deberían, en la medida de lo posible, solo enviar la información a las autoridades una vez, en lugar de tener que ingresar la misma información en varios lugares en las soluciones digitales públicas. Un mayor uso y reutilización de los datos también mejorará la base de los servicios públicos prestados. Esto también contribuirá a un sector público más moderno y eficiente y, por lo tanto, liberará recursos que se pueden aplicar a otras prioridades políticas. Estos esfuerzos deben continuar, teniendo en cuenta la legislación sobre el procesamiento de datos personales y el derecho individual a la privacidad.

En **Estonia**, la agencia encargada de proteger la sociedad digital es la *Estonian Information System Authority* (RIA) y la Estrategia de ciberseguridad se enfoca en asegurar la provisión de servicios vitales elevando la conciencia del riesgo de seguridad entre el sector público y los proveedores de servicios críticos y la gestión de riegos. Desde el año 2008 se ha venido utilizando un sistema de tres niveles denominado ISKE[7] el

7 Consulte System of security measures for information systems (Government of the Republic regulation no. 252 of 20 December 2007; RT I 2007, 71, 440).

cual asegura un nivel mínimo de seguridad en el procesamiento de datos en bases de datos estatales y gubernamentales (Vaks, 2017). En el Ministerio de asuntos nacionales y comunicación crearon un sistema llamado "My number" el cual consiste en un número individual de 12 dígitos que le corresponde a cada ciudadano con el fin de facilitar el pago de impuestos, seguros y procedimientos administrativos. El Gobierno estonio se caracteriza por tener unas políticas en la cual le da prioridad a la TIC, lo que hace que dicho actor sea avanzado digitalmente. Así mismo, la difusión del uso de equipos electrónicos en las instituciones educativas y en las instituciones gubernamentales es del 100 %, el uso de la banca virtual para realizar pagos es del 99.8 % siendo este un porcentaje alto. Aparte de realizar transacciones básicas y necesarias para el ciudadano, también ofrecen servicio administrativo en línea de declaración de impuestos, registro de entidades privadas.

La firma Cybernetica inicialmente fue una entidad privada que se consolidó en el año 1997, sin embargo, hoy en día la entidad es conocida como un actor fundamental para proyectos gubernamentales a nivel internacional. La anterior se destaca en el desarrollo de *software* de votos electrónicos, la construcción de un sistema de seguridad en bases de datos gubernamentales por medio del sistema *X-Road*, siendo este sistema una base fundamental para las políticas dirigidas al desarrollo digital. El sistema *X-Road* consiste en una plataforma en la cual protege el intercambio de información entre las entidades participantes. Por otra parte, el Gobierno de la mano de la firma Eltes establece como riesgo digital aquellos que se producen debido al desarrollo tecnológico, proveyendo soluciones gracias a la tecnología única y alianzas entre corporaciones y diferentes entidades públicas. Estonia además iniciará una cooperación con Japón con la cual usan la herramienta *VizKey* con el fin de realizar investigaciones delictivas a causa de las transferencias de moneda ilegal y uso de información privilegiada.

Finlandia, propone una gestión de riesgos en seguridad digital proyectada para 2020 y promueve en los ciudadanos, las autoridades y las empresas las mejores y más efectivas formas de uso cibernético seguro y

el uso de las mejores herramientas en cuestiones de seguridad cibernética tanto a nivel nacional como internacional buscando ser un precursor mundial en la preparación para la amenaza cibernética y en la gestión de las perturbaciones causadas por estas amenazas. Lo anterior requiere un desarrollo de capacidades en términos de acción y recursos de diferentes entidades de gobierno, las administraciones regionales y locales, así como la comunidad empresarial y las organizaciones, por lo que se estableció un Comité de seguridad para desempeñar un papel activo en el campo de la seguridad integral y que actúe como un organismo de cooperación permanente para la planificación de contingencia (Ministry of Transport and Communications, 2016).

Francia plantea una Estrategia en Seguridad Digital con cinco objetivos de seguridad: *Sistemas de información e Infraestructuras críticas; Datos personales* (Privacidad, confianza digital, etc.), *conciencia* (formación y educación continua); *entorno de las empresas de tecnología digital* (Políticas industriales, exportación e internacionalización) y *el contexto europeo* (Autonomía estratégica digital, estabilidad cibernética). Francia es el objetivo de ataques cibernéticos que dañan sus intereses fundamentales. Hoy, cuando un atacante apunta al Estado, operadores de vital importancia o negocios estratégicos, el objetivo es la instalación a largo plazo en el sistema de información para robar datos confidenciales (políticos, diplomáticos, militares, tecnológicos, económicos, financieros o comerciales). Razón por la cual desde 2011, las administraciones competentes y los proveedores de servicios han abordado alrededor de un centenar de ataques cibernéticos principales, en la mayoría de los casos con total confidencialidad.

Paralelamente, las posiciones adoptadas por Francia en la escena internacional, sus operaciones militares y ciertos debates públicos son seguidas de ataques cibernéticos destinados a marcar la opinión pública. Por ejemplo, la desfiguración de muchos sitios *web* después de los ataques terroristas contra Francia en el comienzo de 2015 tuvo un impacto técnicamente bajo, pero simbólicamente alto, deseado por los atacantes. Desde hace varios años, muchos Estados han implementado su voluntad

política y medios humanos, técnicos y financieros considerables para llevar a cabo operaciones ciberespaciales en gran escala contra Francia. El Ministerio de Defensa realiza la doble función de garantizar la protección de las redes que sustentan su acción y de colocar la lucha digital en el centro de las operaciones militares. Para consolidar la acción del Ministerio en este campo, se estableció una Unidad de Comando de Ciberdefensa (COMCYBER) que informa al jefe del Estado Mayor de Defensa a principios de 2017. El Ministerio del Interior tiene la tarea de abordar todas las formas de delito cibernético que afectan a las instituciones y los intereses nacionales, los agentes económicos, las autoridades públicas y las personas. Para ello, moviliza las redes centrales especializadas y las redes regionales de los Directores Generales de la Policía Nacional, la Gendarmería Nacional y la seguridad Interna. Son responsables de realizar investigaciones para identificar a los perpetradores de ciberataques y llevarlos ante la justicia. Estos servicios contribuyen, entre otras cosas, a los esfuerzos de prevención y a la sensibilización de las personas interesadas (Valls, 2015).

Desde 2010, se han tomado varias medidas para elevar el nivel de seguridad de los sistemas de información del Estado. Se desarrolló una Política de seguridad de los Sistemas Estatales de Información (PSSIE), una red de comunicaciones electrónicas interministeriales está en rápido crecimiento y se ha iniciado el despliegue de terminales móviles seguros. Estas medidas, como las destinadas a producir el equipo de seguridad para proteger la información soberana, movilizan recursos humanos y presupuestarios. Se perseguirán para proporcionar al Gobierno y a sus capacidades militares el nivel de seguridad adecuado para la preservación a largo plazo de la autonomía de Francia en la toma de decisiones y la adopción de medidas. La aplicación de la Política de seguridad de los sistemas estatales de información y la eficacia de las medidas adoptadas se evaluarán anualmente. Se transmitirá un informe confidencial anual al Primer Ministro y se informará al Parlamento por medio de indicadores. Con el mismo objetivo de informar al Parlamento, a partir de 2016, los proyectos de ley tendrán una sección en su evaluación de impacto dedicada a la tecnología digital que también incluirá seguridad cibernética,

establecida bajo los auspicios de los funcionarios superiores a cargo de la calidad de la regulación. En términos más generales, los funcionarios superiores a cargo de la calidad de la regulación se asegurarán de que las cuestiones relacionadas con el refuerzo de la seguridad de los sistemas de información se tienen en cuenta en la dirección del proceso normativo.

La prioridad para las autoridades de seguridad de los sistemas de información competentes debe ser la anticipación y la prevención. Esto implicará garantizar que los productos y servicios digitales o aquellos que involucran tecnología digital, diseñados, desarrollados y producidos en Francia, se encuentren entre los más seguros del mundo. Para lograr este objetivo, las autoridades competentes deberían dirigir sus esfuerzos de comunicación hacia la comunidad científica pública y privada, y los centros de innovación. Cuando los productos y servicios digitales almacenan datos personales o están destinados a los sectores comerciales de vital importancia, los servicios estatales proporcionarán los elementos que son útiles para el análisis de riesgos o las recomendaciones requeridas para obtener el nivel de seguridad que corresponde al uso del producto o el servicio que se diseña o desarrolla. Para los usos que lo justifiquen, también contribuirán a establecer sistemas para evaluar independientemente el nivel de seguridad y confiabilidad de estos productos y servicios, y para proporcionar a sus usuarios potenciales garantías adaptadas a través del etiquetado. Paralelamente, se debe anticipar el entorno legal para acomodar nuevos productos y servicios. Por ejemplo, la llegada inminente de automóviles autónomos debería incitar al regulador a preparar las condiciones para garantizar la seguridad de su circulación. La ciberseguridad debe tenerse en cuenta en los grupos de trabajo internacionales que definen el marco y controlan los procedimientos técnicos. Para otros tipos de productos o servicios, un sistema de identificación adaptado debe informar al consumidor de sus características digitales esenciales y, en particular, del procesamiento de los datos que se recopilan. Para ciertos sectores, como el sector de la salud, se considerará el etiquetado sistemático de productos y servicios digitales.

En **Grecia** la ciberseguridad, es decir, la protección de redes, sistemas informáticos y datos del delito cibernético se ha convertido en una prioridad de Política Nacional como en muchos países que se dan cuenta de su importancia; se están desarrollando nuevas estrategias de seguridad cibernética para proporcionar protección contra amenazas cibernéticas y salvaguardar la prosperidad económica y social. El objetivo de tales estrategias es mejorar la coordinación gubernamental y definir roles y responsabilidades respecto a la lucha contra la ciberdelincuencia, pero también apoyar la cooperación entre el público y entidades privadas, particularmente proveedores de servicios de Internet, y cooperación internacional. Al igual que en otros países europeos, Grecia necesita fortalecer su marco para una protección adecuada. No solo es necesario actualizar el marco legal, sino que también se deben tomar nuevas iniciativas en el área de la ciencia y la educación con el apoyo gubernamental. Las normas y reglamentaciones suficientes, por un lado, y los organismos gubernamentales específicos para abordar los casos de delitos cibernéticos, por otro lado, indiscutiblemente beneficiarían a la seguridad de la información en Grecia.

Holanda cuenta con una Estrategia de ciberseguridad (NCSS2) que va por la segunda versión y en la que se incluye la correlación con los derechos humanos, la libertad de Internet, la privacidad, la innovación y los beneficios económicos y sociales. Para lograr los objetivos cuenta con un modelo de 7 capas y en una de ellas está el enfoque basado en riesgos (Centrum, 2013). La principal amenaza para los holandeses está dirigida a las violaciones de la confidencialidad de la información y la no continuidad de los servicios en línea. Para la comunidad empresarial, la interrupción de los servicios en línea se ha incrementado y a gran escala de la infraestructura digital en los sectores vitales pueden conducir a la interrupción del servicio y, por lo tanto, a efectos sociales indeseables. También existe el riesgo de robo de información competitiva sensible y abuso de datos financieros para fraude. Es por esto que las partes públicas y privadas están iniciando iniciativas, tanto por separado como juntas, para aumentar la resilien-

cia digital anticipándose a la dependencia cada vez mayor de TI y las amenazas cambiantes. Hasta el momento, muchas organizaciones no tienen medidas básicas en orden, como la administración de parches y actualizaciones o una política de contraseñas. Esta es la razón por la cual las viejas vulnerabilidades y los métodos de ataque aún son efectivos. El usuario final está cargado con una gran responsabilidad de seguridad, pero la mayoría de las veces tiene poca influencia o incluso conocimiento de las vulnerabilidades que enfrenta en dispositivos y servicios. Por este motivo, el foco sigue siendo aumentar la conciencia de ciberseguridad de los usuarios.

Para Holanda, es importante mantenerse al día con los rápidos desarrollos y responder a los riesgos que implican. Precisamente por esta razón, pronto se completará una encuesta legal, que apunta a fortalecer la posición del Centro Nacional Holandés de Seguridad Cibernética. Además, el Consejo de Ministros presentará una Estrategia Nacional de Seguridad Cibernética actualizada después del verano que aborda los rápidos desarrollos en el dominio digital. Esta estrategia 2.0 fortalecerá aún más el amplio enfoque de ciberseguridad con partes públicas y privadas. La Evaluación de seguridad cibernética de los Países Bajos está preparada por el Centro Nacional de ciberseguridad bajo la responsabilidad del Coordinador Nacional de Contraterrorismo y seguridad. Este documento representa las contribuciones de una amplia gama de actores en la comunidad de las TIC, incluidos los partidos de los sectores público y privado, académicos y ONG.

Hungría se basa en los principios de la Ley Fundamental y en la revisión de los valores e intereses relevantes y en el análisis del entorno de seguridad del ciberespacio, para definir el objetivo de la gestión de riesgos en seguridad digital como la determinación de los objetivos nacionales y las direcciones estratégicas, las tareas y el gobierno general. La gestión de riesgos en seguridad digital apunta a desarrollar un ciberespacio libre y seguro y proteger la soberanía nacional en el contexto nacional e internacional, que ha experimentado un cambio significativo debido al surgimiento del ciberespacio, un nuevo medio que se ha convertido en

un factor clave en el siglo XXI. Además, tiene como objetivo proteger las actividades y garantizar la seguridad de la economía y la sociedad nacionales, adaptar de manera segura las innovaciones tecnológicas para facilitar el crecimiento económico y establecer una cooperación internacional en este sentido en consonancia con los intereses nacionales de Hungría. Esta estrategia indica que Hungría está preparada para asumir responsabilidades en tareas de protección del ciberespacio y tiene la intención de desarrollar el ciberespacio húngaro como un elemento clave de la vida económica y social húngara en un entorno libre, seguro e innovador. A través de medidas de protección eficientes basadas en la prevención, el objetivo principal es gestionar las amenazas y los riesgos que surgen y provienen del ciberespacio, así como reforzar la coordinación y las medidas gubernamentales.

En **Italia** se propone un marco de referencia para Gestión de Riesgos basado en el emitido por NIST que consiste en una matriz en la que se evidencian las funciones *Identificar, Proteger, Detectar, Responder, Recuperar* los riesgos, para cada una de ellas se determinan las categorías, subcategorías y las referencias informativas. Este marco de referencia se complementa con unos niveles de madurez y niveles de prioridad (Roberto & Montanari, 2015). El Gobierno italiano aprobó el nuevo Plan Nacional de Ciberprotección y seguridad Digital que define nuevas directrices y objetivos operacionales para la implementación del Marco Estratégico Nacional para la seguridad Cibernética (NSF). El nuevo plan se ha desarrollado de acuerdo con las directrices para la ciberprotección y la seguridad Digital recomendadas por el Primer Ministro como responsable de la Ciber Arquitectura Nacional. El plan de acción se basa en medidas sustanciales que fortalecen la ciberarquitectura nacional, teniendo en cuenta que los datos confidenciales para fines de seguridad Nacional no son exclusivamente administrados por el sector público, sino que están integrados con datos confidenciales de empresas privadas en sectores estratégicos. Por lo tanto, el nuevo plan de acción y gestión de crisis amplía el perímetro de las empresas que operan en áreas identificadas como críticas para la seguridad nacional (proveedores de servicios públicos y provee-

dores de servicios digitales), que estarán sujetas a nuevas obligaciones de notificación ante la ocurrencia de incidentes de seguridad identificados como amenazas a la seguridad nacional basadas en ciertos parámetros y umbrales. Las sanciones en caso de falla son bastante sustanciales. Las prioridades de la intervención de arquitectura nacional se describen como la identificación y actualización de medidas mínimas de seguridad para ser implementadas en la administración pública y redes y sistemas de infraestructura crítica, la adopción de estándares de referencia, mejores prácticas y requisitos mínimos para la seguridad de redes y sistemas, la construcción de un sistema de auditoría de validación y para los organismos responsables de la emisión de certificados digitales, para autenticación y otros certificados digitales de valores.[8]

En **Polonia**, se considera vital establecer un sistema de financiación de las tareas relacionadas con la protección del ciberespacio y se argumenta que la protección efectiva del espacio cibernético debe incluir la adopción de un marco legal para un Sistema Nacional de Protección del Espacio Cibernético, que se establezca una institución estatal que coordinará las actividades de otras entidades. Por otra parte, se pretende destinar recursos para hacer frente a las alertas y desarrollar un modelo de análisis y Gestión de Riesgos nacional (Streżyńska, 2016).

En el **Reino Unido**, el Gobierno cuenta con un marco de referencia gubernamental en Gestión de Riesgos (Service, 2017) en el que se tipifi-

8 A este respecto, se transcribe del original en inglés de The National Cyber Security Strategy, published in 2015. "Is a high level policy statement from Government. It acknowledges the challenges with facilitating and enabling the digital economy and society. The strategy is based on key principles such as the rule of law, subsidiarity, noting that we are ultimately responsible for our own security, and proportionality in response to key risks and threats facing us. Key measures include:
Formally establishing the National Cyber Security Centre, encompassing the national/governmental Computer Security Incident Response Team (CSIRT-IE) Its focus on the protection of critical national information infrastructure in key sectors such as energy and telecommunications.
Delivering improved security arrangements, in partnership with Government Departments and Key Agencies involving situational awareness and incident management.
Introducing primary legislation to formalise arrangements in law and to comply with EU requirements on capabilities, co-operation and reporting.
Co-operating with key State Agencies, industry partners and international peers in the interests of protecting critical infrastructure, improving situational awareness and incident management along with facilitating education, training and public awareness initiatives".

can y gestionan los riesgos asignando responsabilidades de acuerdo con el rol que cumplen dentro de la administración. El marco de referencia establece cuatro diferentes tipos de riesgo: *Internos, Externos, Proyectos principales, Estrategia*; tres elementos de Gestión de Riesgos: Construcción de bloques, actividades periódicas y procesos de rutina; finamente están los roles/responsabilidades garantizando que hay claridad en quien hace que dentro del contexto.

República Checa ha tenido un éxito desigual en la implementación de una agenda integral de gobierno electrónico. Si bien la disponibilidad de servicios de gobierno electrónico fue del 56 % para los ciudadanos y del 100 % para las empresas en 2010, el uso real de los servicios de gobierno electrónico solo alcanzó el 29 % para los ciudadanos y el 94 % para las empresas en 2013, lo que indica una gran brecha el uso de servicios de gobierno electrónico por parte de los ciudadanos y las empresas. Esto probablemente se deba al hecho de que a todas las personas jurídicas se les proporcionó un "buzón de datos" gratuito pero obligatorio a partir del 1 de julio de 2009 en adelante. El buzón de datos funciona como una cuenta de correo electrónico normal, pero proporciona la autenticidad y la no negación de los datos almacenados (utilizando el algoritmo de función hash SHA-2), eliminando así la necesidad de un certificado separado para firmas electrónicas. Toda correspondencia oficial entre personas jurídicas y autoridades está restringida al buzón de datos. Como se considera que los mensajes no leídos que se entregan en el buzón de datos han sido leídos por el destinatario 10 días después de la entrega, las empresas no tienen más opción que cumplir con los procedimientos de gobierno electrónico relacionados con el uso del buzón de datos. Por el contrario, las personas físicas no están obligadas a utilizar el buzón de datos y, por consiguiente, menos del 1 % lo tienen. Los certificados para firmas electrónicas no los proporcionan las autoridades públicas y deben comprarse a entidades comerciales, lo que se ha convertido en otro obstáculo para uso generalizado del gobierno electrónico por personas físicas. Por lo tanto, mientras que la República Checa ocupa el octavo lugar dentro de la UE en el uso del gobierno electrónico por

parte de las empresas, ocupa el lugar 23 en la categoría correspondiente para las personas (Minárik, 2016).

La Agencia Nacional de seguridad Checa también tiene un acuerdo sobre el Programa de Seguridad del Gobierno con Microsoft, según el cual, las partes pueden compartir e intercambiar información de seguridad cibernética, lo que significa que la ANS tiene acceso a los códigos fuente y la documentación de los productos de Microsoft. Se ha celebrado un acuerdo de intercambio de información similar entre la ANS y Cisco. Con base en este memorando de entendimiento, estas dos entidades comparten información sobre ciberamenazas e intercambian información sobre las actuales tendencias de seguridad cibernética y las mejores prácticas.

En **Rumania,** el Gobierno propone un plan de gestión de riesgo alineado con las políticas de la Comunidad Europea; en primer lugar, proponen realizar la *Identificación, valoración y mitigación del riesgo;* posteriormente, la información que puede estar expuesta a un riesgo se clasifica en cuatro categorías, *gestión y publicación de información, moderación, recursos y gestión de proyectos*. Se utiliza también una subcategoría de riesgos y finalmente, se plantean los riesgos específicos. De esta manera, se mapean los posibles riesgos y las acciones de mitigación correspondientes (Otniel, 2015).

En **Rusia**, el presidente Vladimir Putin aprobó la Doctrina de seguridad Informática en el año 2016, esta identifica la seguridad cibernética, la privacidad y la seguridad de la información como vitales para los intereses nacionales de Rusia y pretende formar la base de nuevos desarrollos en las políticas públicas y las relaciones públicas, así como mejorar los sistemas para la protección de la seguridad de la información. Entre los pilares de la nueva Estrategia de Gestión de Riesgos en Seguridad Digital se enfatiza en la promoción y protección de la privacidad de la información, el apoyo a las instituciones democráticas, el Estado y los mecanismos de interacción de la sociedad civil. De este modo, se pretende garantizar el funcionamiento sostenible e ininterrumpido de la Infraestructura Nacional de Información Crítica en tiempo de paz y

tiempo de guerra y en respuesta a actos de agresión extranjeros, además de la promoción nacional e internacional de las políticas del Gobierno ruso en materia de ciberseguridad y Defensa (The Ministry of Foreign Affairs of the Russian Federation, 2016).

En **Suiza**, el Consejo Federal encargó al Departamento Federal de Defensa, Protección Civil y Deporte (DDPS) el 10 de diciembre de 2010, elaborar una Estrategia Nacional para la protección de Suiza contra los riesgos cibernéticos. Esta estrategia describe qué aspecto tienen estos riesgos, por ejemplo, qué tan bien Suiza está equipada para contrarrestarlos, dónde se encuentran las deficiencias y cómo pueden eliminarse de manera más efectiva y eficiente. La Estrategia para la Protección de Suiza contra los Riesgos Cibernéticos se dirige principalmente a las agencias federales y se elaboró en colaboración con representantes de todos los departamentos, varios operadores de Infraestructura Crítica, el servicio de proveedores de TIC, proveedores del sistema y el sector privado. La estrategia describe los roles de varios actores y modelos de colaboración requeridos para una mejor protección contra los ciberriesgos (Eidgenössisches Department für Verteidigung, 2012).

En **Estados Unidos**, el presidente Donald Trump firmó la orden ejecutiva de ciberseguridad, la cual hace énfasis en Gestión del Riesgo y resiliencia de Infraestructura Crítica, ciberdisuasión y desarrollo de la fuerza de trabajo cibernética y los procesos se alinean con la planificación estratégica, operativa y presupuestaria. Cada agencia del Gobierno debe adoptar los estándares de la *NationalInstitute of Standards and Technology* (NIST) y enviar los documentos de gestión del riesgo a la Secretaría de seguridad de la Casa Blanca. El último marco de referencia emitido por el NIST es el *Framework for Improving Critical Infrastructure Cybersecurity* y se plantea en términos de identificar, valorar y responder al riesgo, priorizando decisiones respecto a la ciberseguridad (Technology, 2017).

Canadá al igual que Estados Unidos no tiene un marco de referencia pero sí cuenta con unas guías para la gestión del riesgo que sugiere una

división de actividades en dos niveles: El nivel *Departamental*, en donde se establecen las actividades alineadas con el plan de seguridad de la organización y el nivel de *Sistemas de Información*, en el que se encuentran las actividades relacionadas con el ciclo de vida del sistema de información y se implementan los controles de seguridad apropiados con el fin de mantener la continuidad del negocio (Moffa, 2012).

De acuerdo con el estado del arte analizado previamente en diferentes países del mundo de los cinco continentes, es evidente que la Gestión de Riesgos en seguridad Digital es un tema de gran relevancia a nivel de Estado, por tal razón, es necesario involucrar a todas las entidades comprometidas: fuerza pública, academia, y organizaciones públicas y privadas para establecer unos lineamientos generales que permitan identificar las vulnerabilidades, amenazas y riesgos a los que se vería expuesta una nación, para finalmente, consultar a la población en general sobre sus intereses, necesidades y temores a los que se ven expuestos, de esta manera, se podrá establecer un marco general de buenas prácticas que establezca tanto los deberes como las responsabilidades para mantener segura la información sensible que en caso de riesgo inminente, podría afectar la integridad humana o los bienes de los ciudadanos y/o organizaciones.

En ese sentido Colombia debe iniciar un trabajo colaborativo entre las diferentes partes para aprovechar la experiencia de los que ya han venido trabajando en el tema y a su vez adelantar e integrar a los demás actores que se han venido quedando rezagados en cuanto a la Gestión de Riesgos, con el propósito de que se adquiera conciencia de la importancia de proteger los activos de información y de resaltar la responsabilidad que cada uno tiene (organizaciones e individuos) sobre la información que maneja para prevenir, minimizar y evitar los riesgos latentes que se presentan ante un activo digital.

2. Perspectivas a futuro

Con base en la hipótesis de que para generar un marco de gestión de riesgos integral se requiere de la participación de todos los actores

principales de la sociedad, se debe involucrar al sector de la academia, sector público, sector privado y Fuerza pública, teniendo en cuenta que estos sectores son claves como motor del desarrollo de cualquier país debido a su impacto e influencia en los diferentes sectores de la sociedad y al que de una u otra manera se encuentran vinculados todos los ciudadanos. De este modo, avanzando en el análisis realizado a nivel de Europa y América en el sector público se pretende dar una mirada holística de lo que se espera que continúe sucediendo en tema de Gestión de Riesgos, si se mantiene una evolución constante en este tema, en todos los países interesados en proveer una infraestructura física, y de servicios en un ambiente digital.

Si bien es cierto que existen coincidencias en el sector público sobre las necesidades y problemáticas que se pretenden abordar, las diferentes entidades del Estado difieren en la priorización que le dan a cada una de ellas. Por tal razón, se han creado políticas internas que den respuesta a esas prioridades identificadas y establecidas por cada organización que le permiten cumplir con su misión y visión, pero también se han generado cooperaciones con otras entidades del mismo sector para reaccionar ante cualquier eventualidad que requiera del concurso de todas las entidades involucradas, igualmente se establecen relaciones de confianza con fines estratégicos que permitan a las partes estar a la vanguardia en términos de tecnología, información y seguridad Digital. Para poder generar dichas sinergias, se debe contar con diferentes perfiles profesionales no solo en materia de tecnología, sino en las diferentes ramas del saber que tengan algún tipo de injerencia en el actuar del medio tecnológico (abogados, ingenieros, economistas, etc.) ya que el entorno virtual ha permitido la apertura de diferentes mercados que requieren de conocimientos multi e interdisciplinares y se debe estar preparado para todo tipo de fenómeno que ocurra en Internet, tal como ocurrió con la aparición de la tecnología *Distributed Ledger Technology* (DLT) y *Blockchain Technology* (Svein Ølnes, 2017) y en particular con las aplicaciones y usos que se le puede dar, como es el caso de las criptomonedas (Antonopoulos, 2015), que han tenido un impacto importante en diferentes economías del mundo, ya que a

partir de ahí se han generado oportunidades de negocio pero también riesgos asociados, no solo para inversores particulares, sino también para empresas y gobiernos.

En Colombia, se están haciendo esfuerzos importantes para avanzar en la disminución de la brecha digital que existe respecto a países desarrollados y se tienen como referencias de facto los estándares internacionales y la normatividad local entre ellas están las emitidas por NIST (Commerce, 2018), ISO (Standardization, 2018) y los documentos nacionales emitidos por el Consejo Nacional de Política Económica y Social (CONPES, Departamento Nacional de Planeación, 2018), así como las normas emitidas por el organismo de estandarización nacional, Instituto Colombiano de Normas Técnicas (Icontec, 2018). De esta manera, se pretende avanzar en la consecución de los objetivos planteados a corto, mediano y largo plazo en temas de gestión de riesgos en seguridad digital. Por esto, siguiendo dicha normativa se han identificado algunos temas prioritarios a investigar entre los cuales se encuentran:

- Diseño de un Modelo Integral de Gestión de Riesgos en Seguridad Digital, para el desarrollo de la economía digital de Colombia y servicios a los ciudadanos
- Marco normativo estableciendo políticas y protocolos en la protección de datos personales e identidad digital
- Definición de capacidades para el desarrollo de la gestión de ciberinteligencia e innovación
- Modelo de intercambio de información (Ley)
- Observatorio de Riesgos de Seguridad Digital basado en *big data* para el análisis descriptivo, cognitivo y predictivo de amenazas vulnerabilidades e incidentes que involucre las partes interesadas (academia, sector público, privado, sociedad) para la efectiva toma de decisiones.

Las temáticas anteriores se pudieron identificar involucrando diferentes entidades del sector público y de acuerdo con la experiencia de sus funcionarios, se realizó la priorizar correspondiente.

Conclusiones

En general, los países en diferentes continentes están efectuando importantes avances en el tema de gestión de riesgos de seguridad digital y Colombia también está haciendo lo propio, con el fin de hacer frente a las posibles amenazas en el ciberespacio y lograr la prosperidad social y económica del país.

Por tal razón, es necesario que los diferentes actores del Gobierno trabajen en conjunto para generar las políticas públicas apropiadas en temas de investigación, definiendo las líneas de interés que más impactan en cuanto al riesgo digital, según la visión particular de cada una de las entidades.

De acuerdo con el análisis realizado en otros continentes y también en el ámbito nacional, fue posible establecer el estado del arte en el que se evidenció el interés por involucrar diferentes sectores para establecer las mejores prácticas en términos de gestión de riesgos en seguridad digital, con el propósito de que las diferentes entidades, organizaciones y personas naturales apropien la tecnología y confíen en un sistema que provea los requisitos de seguridad aceptables, dando así confianza a todos los usuarios para realizar transacciones en el medio digital, entendiendo como transacción cualquier intercambio de información realizado entre un emisor y un receptor.

Otro factor importante que se detectó es que se debe contar con personal experto en diferentes ramas, de manera que se pueda trabar de forma cooperativa y colaborativa entre equipos multi e interdisciplinares, para que la reacción sea mucho más efectiva y se pueda dar una respuesta acorde con las necesidades planteadas por el entorno, que en general, es un entorno hostil al haber intereses de por medio, tanto económicos como reputacionales, sociales, entre otros.

Después de identificar las temáticas prioritarias en el sector público, se debe generar un modelo cíclico, en el que se evidencie que la gestión de riesgos, al igual que la seguridad de la información, es un proceso continuo y no una actividad puntual que tiene un inicio y un final determinado, ya que cualquier cambio en la tecnología, en los usuarios, o en

la misma información hace que cambie tanto el entorno como los riesgos asociados; de manera que se debe realizar una monitorización constante, que permita adelantarse a los eventos que puedan surgir y así prevenir, detectar y remediar la situación en aras de minimizar un impacto negativo sobre los activos de una sociedad, teniendo en cuenta que el análisis se realizó a nivel de gobierno.

En ese sentido, es necesario abordar las temáticas identificadas desde un punto de vista holístico con el fin de tener en cuenta todas las necesidades y establecer un marco de gestión común a todos los actores participantes a nivel Gobierno y continuar con el establecimiento de políticas, procedimientos y buenas prácticas de manera general, para sí, poder adaptar los modelos de gestión internos y cumplir con los objetivos propuestos en cada una de las entidades de acuerdo con su misión y visión, pero también con la capacidad de reaccionar en conjunto y estar alineados hablando el mismo lenguaje en caso de hallarse ante una situación de riesgo.