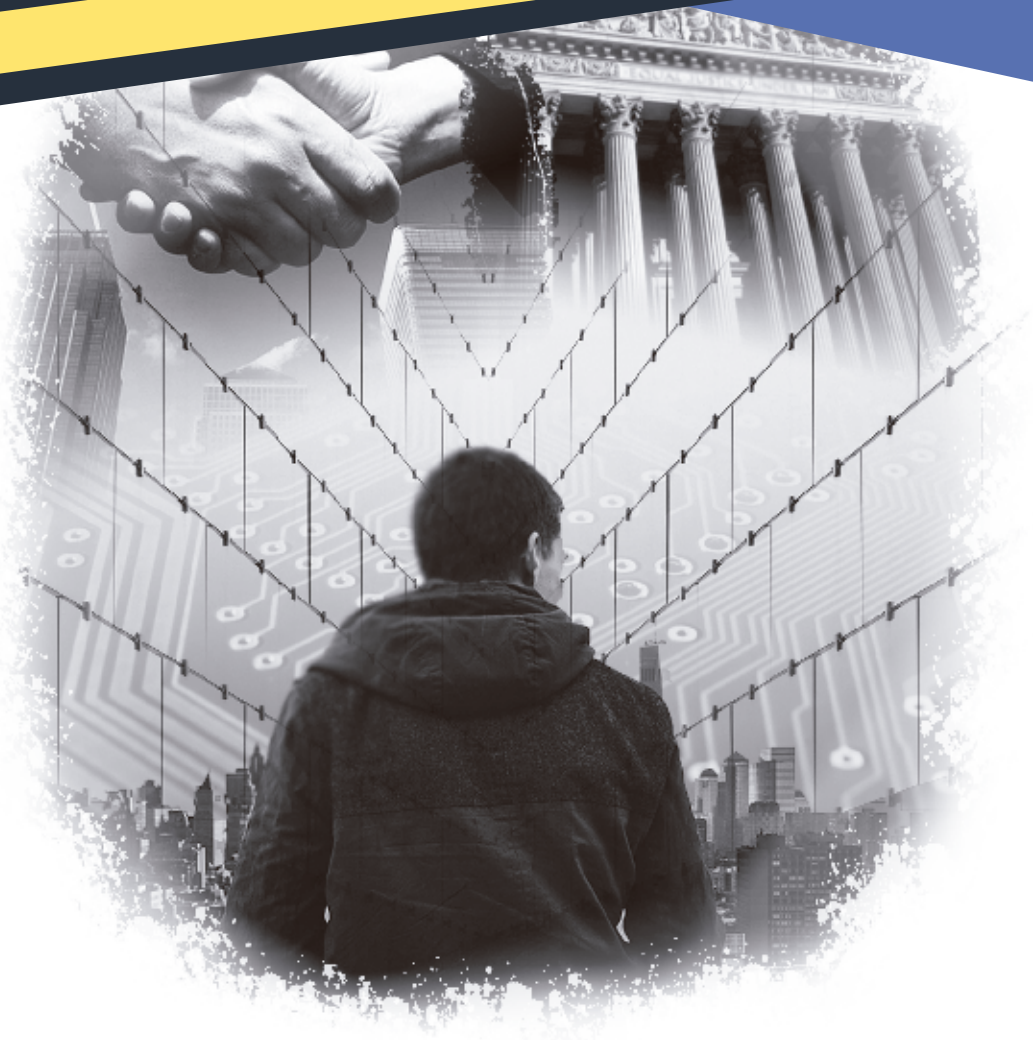
2018

White paper series
Edición 1

UN LLAMADO A LA ACCIÓN

PARA PROTEGER A CIUDADANOS SECTOR PRIVADO Y GOBIERNO



OEA | Más derechos para más gente

aws

CRÉDITOS

Luis Almagro

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

Autor Principal

Miguel Rego

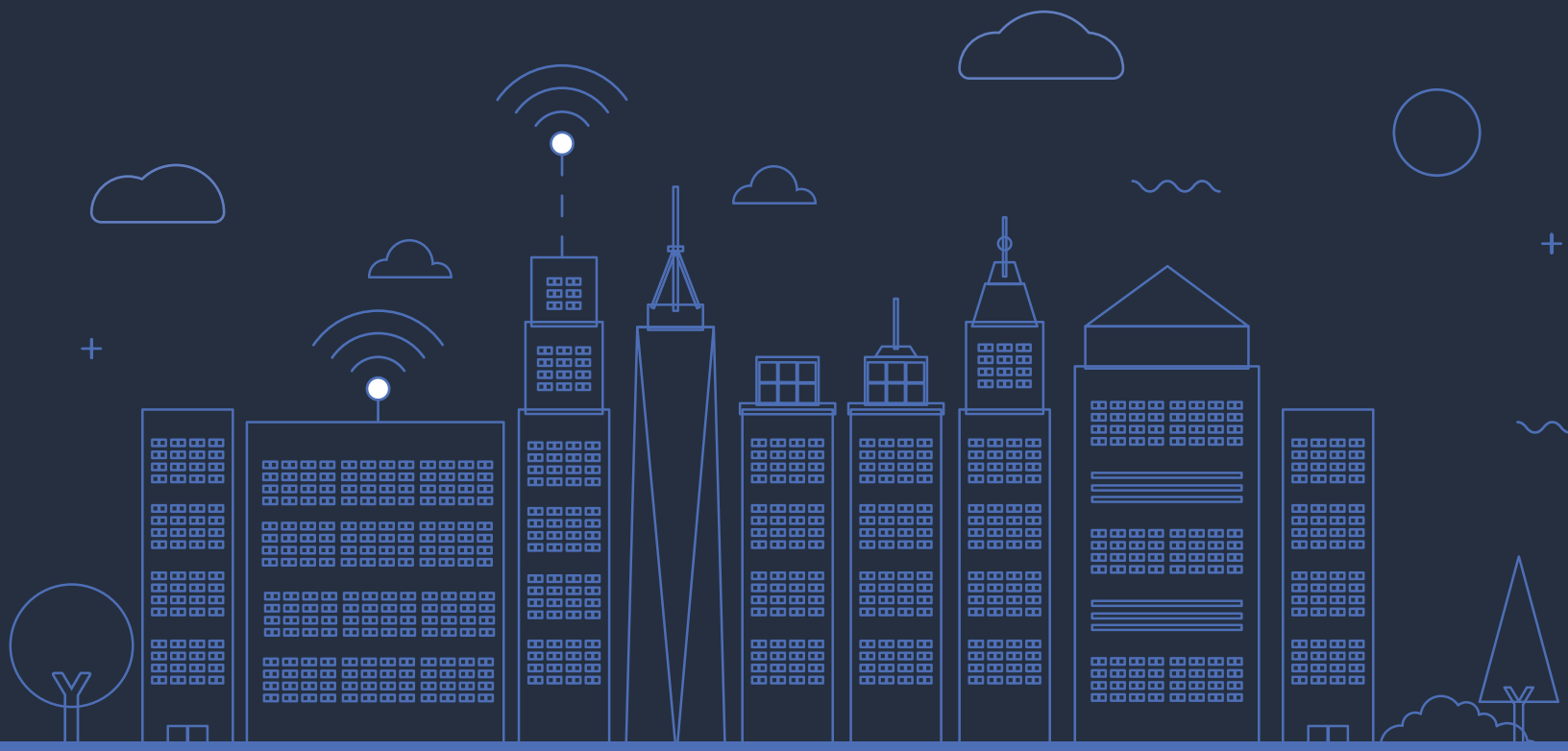
Equipo Técnico OEA

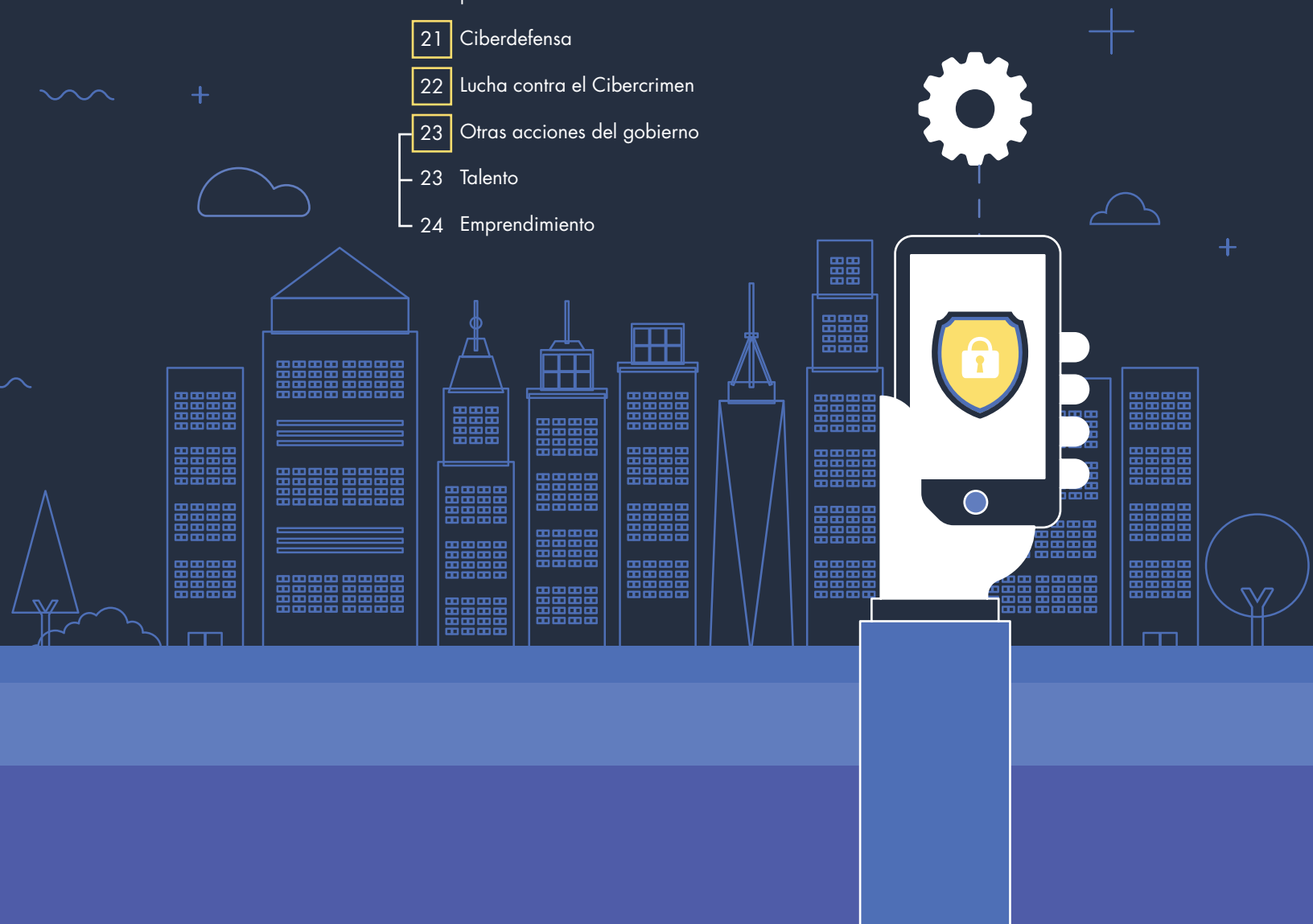
Claudia Paz y Paz
Alison August Treppel
Belisario Contreras
Kerry-Ann Barrett
Bárbara Marchiori de Assis
Nathalia Foditsch
Gonzalo Garcia-Belenguer

Equipo Técnico AWS

Min Hyun
Michael South
Maria Saab

CONTENIDO





1

OBJETIVOS

Las tecnologías de Información y Comunicaciones han revolucionado nuestra forma de vida y han impulsado el desarrollo económico e industrial hasta hacernos altamente dependientes del ciber espacio. Nuestra forma de comunicarnos, de relacionarnos, de estudiar e investigar e incluso de comprar se ha ido transformado con la creciente penetración de la digitalización hasta cambiar nuestros hábitos y comportamientos. Estos procesos de transformación digital han calado también en las empresas y en los organismos públicos, hasta tal punto que cualquier proceso productivo, cualquier servicio público dirigido al ciudadano, no se puede concebir sin un uso intensivo de las tecnologías.

Este escenario de grandes oportunidades para la economía, la industria y la sociedad no está exento de nuevos riesgos y amenazas. El ciberespacio es del mayor interés para delincuentes y terroristas que pueden aprovecharse del anonimato que ofrece internet y de la falta de homogeneidad en las legislaciones nacionales e internacionales, para actuar con impunidad.

Ante este escenario de enormes oportunidades, pero también de riesgos y amenazas, los gobiernos deben actuar estableciendo las condiciones legales, técnicas y organizativas para que sus ciudadanos, sus empresas y sus instituciones públicas puedan aprovechar al máximo las posibilidades de esta realidad digital, con la confianza de estar razonablemente a salvo de sus efectos negativos.

Este documento tiene como objetivo ayudar a identificar los elementos fundamentales en los que apoyar la construcción de un entorno digital seguro que sirva para el desarrollo social y económico de las naciones.

2 INTRODUCCIÓN

Un mundo más digital e hiperconectado

La transformación digital ha supuesto la integración de la tecnología digital en la sociedad y en todas las áreas de funcionamiento de una organización, lo que ha facilitado cambios en nuestra manera de trabajar y de relacionarnos, ha supuesto una mejora de los procesos productivos industriales y ha impactado muy positivamente en el desarrollo económico. Cada vez somos más digitales y estamos más hiperconectados, haciendo que la presencia de la tecnológica en el ámbito personal y profesional crezca exponencialmente.

Estas circunstancias vienen facilitadas por las siguientes realidades:

La interconexión masiva, en lo que se ha venido a llamar la Internet de las cosas (IoT) que nos hará pasar de 6.500 millones de elementos interconectados por internet a más de 21.000 millones, y que facilitará la monitorización y el control remoto de múltiples dispositivos inteligentes.

Los sistemas ciber físicos que son el resultado de dotar a los componentes/objetos físicos de capacidades de computación y de comunicación para convertirlos en objetos inteligentes que pueden cooperar entre ellos formando ecosistemas distribuidos y autónomos. Esta tendencia, junto con el IoT son la base para el desarrollo de las SmartCities, y en general los "SmartX", es decir, la aplicación de estos conceptos a casi cualquier ámbito, proceso u organización (coches, drones, hogares, hospitales…)

La maximización en el almacenamiento de datos y su análisis y explotación. La cantidad masiva de información que está creando el IoT permite generar predicciones y proyecciones, permitiéndonos trabajar de forma más eficiente y rentable que nunca.

Las criptomonedas y el blockchain, aunque con un valor muy volátil, ya ha revolucionado la forma de realizar los negocios en la Red. Con un grado de implantación creciente, supondrán en 2020 el 25% de todas las operaciones financieras.

El comercio electrónico continuará aumentando sus cuotas en prácticamente todos los mercados por la comodidad para los clientes y la rapidez y fiabilidad en las entregas.

Existen otras tendencias que contribuirán a este crecimiento imparable "de lo digital", como la inteligencia artificial y el "learning machine" y la realidad aumentada (AR) y virtualizada, entre otras.

Las amenazas son más complejas y cambiantes

Los criminales consiguen desarrollar ataques cada vez más sofisticados y esta situación se agrava por el aumento de la superficie de ataque disponible, en la medida que más procesos se tornan digitales. Los sistemas de control industrial (ICS) que permiten el funcionamiento de servicios esenciales como la energía, el agua o el transporte, o que dan soporte a proceso industriales de fabricación, empiezan a ser el objetivo de atacantes que, motivados por creencias políticas, patrióticas o ideológicas, buscan la disrupción y sabotaje de estos servicios.

Las amenazas evolucionan y se vuelven cada vez más complejas. Las arquitecturas de ciberseguridad de hace diez años cumplieron su función cuando las amenazas y los ataques eran menos frecuentes, pero ahora esos sistemas se están quedando obsoletos y necesitan adaptarse a los nuevos entornos de amenazas. La ciberseguridad requiere innovación e inversión constante en firewalls, proxies, WAFs y otras tecnologías bien sea en infraestructura en el sitio o la nube, además de entrenamiento a los usuarios y procesos de seguridad. La adopción de computación en la nube genera alternativas adicionales de defensa en la medida que permite mayor granularidad en cada capa de la infraestructura, reduciendo la superficie de ataque disponible.

Los tres pilares de seguridad

Es importante, especialmente para los gobiernos, entender que la ciberseguridad no es un desafío que solo la tecnología puede resolver. Una estrategia completa de ciberseguridad debe cubrir los tres pilares de ciberseguridad- personas, procesos y tecnología - en políticas, programas, fondos e implementación.

Los atacantes son numerosos y muy heterogéneos

Cada día se producen más de 230.000 muestras diferentes de malware y la tendencia es que este número vaya creciendo. También a diario se denuncian más de 4.000 ataques de ransomware. Este crecimiento continuo en las cifras de ataques está motivado por el beneficio económico potencial que el ciber criminal espera obtener, habiendo estimaciones que apuntan a que las perdidas asociadas con los delitos informáticos alcance la cifra de 2,1 billones de dólares en 2019.

Sin embargo, el enriquecimiento ilícito no es la única motivación. En ocasiones, el objetivo tras un ataque cibernético puede ser el robo de información confidencial de alto valor militar, económico o político. En este caso, los atacantes podrían estar patrocinados por un Estado o incluso por una compañía con intereses contrapuestos con el atacado.

Las redes de los gobiernos y sus vulnerabilidades

Las redes y sistemas de los gobiernos y administraciones públicas son un objetivo natural para los ciber criminales. Los sistemas tienen abundante información de carácter personal, que incluye información financiera y bancaria. Además de estos datos personales, las instituciones públicas manejan y almacenan información confidencial sobre aspectos del máximo interés: información relativa a terceros países, de interés estratégico, etc.

Adicionalmente, estos entornos tecnológicos podrían ser objeto de ataques ciber terroristas para bloquear el funcionamiento de los servicios críticos proporcionados por el gobierno o la administración, o ser objeto de ataques propagandísticos o motivados por malestar social.

Esta capacidad de atracción de ciberataques se agrava porque, en ocasiones, el parque tecnológico instalado es variado y heterogéneo, conviviendo sistemas "legacy", con soporte discontinuado o muy limitado, ¡unto con tecnologías modernas y avanzadas. Esta situación se puede convertir de alto riesgo cuando los usuarios están poco formados y concienciados en materia de ciberseguridad y el personal técnico de operación y mantenimiento de sistemas sea escaso.

Es esencial que las organizaciones de los sectores público y privado implementen soluciones de TI que puedan responder de manera preventiva y proactiva a las amenazas cibernéticas reales y percibidas. Estas organizaciones pueden aprovechar las soluciones disponibles de ciberseguridad que pueden identificar amenazas, notificar a los proveedores de servicios e implementar mitigaciones en tiempo real.

Los planes de modernización tecnológicos del estado deben ser, también, una oportunidad para que los gobiernos mejoren el nivel de protección de la infraestructura de TI. A medida que la infraestructura instalada se acerque a su obsolescencia, los gobiernos pueden aprovechar las capacidades avanzadas de seguridad de las nuevas tecnologías (como la nube) para buscar modelos más eficaces.

Por último, generalmente, el presupuesto dedicado en el sector público a las tecnologías y servicios de ciberseguridad para la protección de estos entornos suele ser notablemente inferior al de otros sectores.

3

EL PAPEL DE LOS GOBIERNOS EN LA PROTECCIÓN DEL CIBERESPACIO

La alta dependencia en el ciberespacio, y el crecimiento y la complejidad de las amenazas, hace que la ciberseguridad sea un elemento fundamental para la estabilidad social y económica de cualquier nación, llegando a convertirse en una cuestión de prioridad nacional. En este contexto, los gobiernos deben asumir un papel de liderazgo en el impulso de un ciberespacio seguro que genere confianza en ciudadanos y empresas, y facilite el crecimiento social, económico e industrial de la nación.

Este papel protagonista de los estados se traduce en las siguientes líneas de actuación:

Formulación y aplicación de políticas públicas

Los gobiernos deben participar activamente en foros y organizaciones internacionales y en estructuras supranacionales con el objetivo de armonizar y coordinar una posición común para la defensa del ciberespacio. Este esfuerzo se debe materializar en la suscripción de los acuerdos internacionales y en la revisión y adaptación de la legislación nacional. En este sentido, y como primer paso, la acción del gobierno debe concretarse en una estrategia nacional de ciberseguridad que establezca los principios, objetivos y líneas de acción a partir de los cuales se puede desarrollar un modelo de ciberseguridad para el país.

Desarrollo de una respuesta colaborativa

La protección y respuesta ante las amenazas cibernéticas involucra a toda la sociedad y no sólo al gobierno, a la administración y a las instituciones públicas. Las infraestructuras críticas, de las que dependen los servicios esenciales, se gestionan en gran medida por compañías privadas que juegan un papel esencial en la ciberseguridad nacional. Las empresas proveedoras de productos y servicios de ciberseguridad son también importantes ya que tienen como clientes a organizaciones públicas y privadas que utilizan sus soluciones para proteger procesos e información clave.

Al entender que la implementación y el uso de tecnologías en el sector público, por ejemplo, puede ser lento, los gobiernos deben continuar evaluando el pulso de la innovación y la tecnología relacionadas con los medios más sofisticados para mejorar la ciberseguridad. A medida que las amenazas se vuelven más complejas y los actores malintencionados se vuelven más numerosos, la tecnología se debe adaptar para responder eficazmente. El mercado de productos y soluciones de ciberseguridad también evoluciona para ofrecer las soluciones necesarias para abordar la necesidad y la demanda.

Las personas, en la doble faceta de usuarios de los servicios de la sociedad de la información y de empleados al servicio de la administración o del sector privado, son también esenciales, ya que su forma de actuar ante las tecnologías puede facilitar o impedir el éxito de un incidente cibernético. Finalmente, las universidades y los centros de investigación educan a los futuros profesionales y definen modelos o soluciones a problemas de ciberseguridad actuales o futuros.

En este contexto, donde hay tantos agentes diferentes que contribuyen de forma relevante a la ciber seguridad nacional, el gobierno tiene que desempeñar un papel de coordinación y armonización de todos estos esfuerzos hacia un objetivo común.

Generación de una cultura de ciberseguridad

Es importante que cale en todos los estamentos de la sociedad la relevancia que ha alcanzado la ciberseguridad y que este conocimiento se traduzca en pautas de comportamiento. La generación de una cultura nacional de ciberseguridad debe ser impulsada desde el gobierno a través de distintos medios y canales, y debe comprender a los ciudadanos, las empresas y las administraciones públicas, y abarcar desde los responsables de la toma de decisiones a los empleados.

Un posible ejemplo aquí es el Mes Nacional de Concientización sobre Ciberseguridad (NCSAM, por sus siglas en ingles) de EE. UU., Declarado por primera vez por el presidente e implementado en la mayoría de los estados.

Fomento de un ecosistema profesional y empresarial

Mejorar y mantener un nivel adecuado de ciberseguridad en las empresas y en las instrucciones públicas requiere de un número importante de profesionales que cuenten con la cualificación adecuada. A su vez, las tecnologías de información necesitan dotarse de soluciones de ciberseguridad que las protejan ante los ciberataques. Ambos aspectos son críticos para poder desarrollar un modelo de ciberseguridad nacional.

Por otro lado, el déficit global de profesionales y el incremento en la demanda de productos y servicios de ciberseguridad puede ser una oportunidad de desarrollo económico y de mejora de la capacidad de influencia internacional para las naciones que sean capaces de exportar talento y tecnologías de ciberseguridad.

Los gobiernos deben jugar un papel esencial en el impulso de un ecosistema de emprendimiento y de generación de talento en ciberseguridad, estimulando el interés en la ciberseguridad desde las primeras etapas educativas, y fomentando y apoyando la generación de ideas y proyectos que pueden derivar en iniciativas emprendedoras.

4

¿POR DÓNDE DEBEN EMPEZAR LOS ESTADOS?

La definición de una estrategia nacional de ciberseguridad debería ser el primer paso para la construcción de un ciberespacio seguro. Esta estrategia debería está definida tras la identificación y valoración de los riesgos cibernéticos que pueden afectar al país, dado que esta aproximación permitirá:

- Proteger los intereses nacionales en el ciber espacio contra las amenazas reales que puedan actuar contra ellas.
- Ser eficiente, lo que supone que las acciones a desarrollar deben ser proporcionadas a la importancia de los bienes y activos a proteger y a su nivel real de exposición.
- Contemplar las medidas de ciberseguridad ya existentes e integrarlas en el nuevo modelo.
- Incluir una priorización de las actuaciones y de las líneas de acción que se hayan definido.
- Evaluar el estado de la tecnología más utilizada por los organismos del sector público y privado, y determinar su nivel de modernización y sensibilidad a las amenazas y riesgos cibernéticos.
- Incluir los tres pilares de ciberseguridad - personas, procesos y tecnología - en políticas, programas, fondos e implementación.

Los pasos a seguir son:

PASOS PARA LA DEFINICIÓN DE LA ESTRATEGIA

1. . . . Definir el alcance y los objetivos

En este primer paso se debe definir el alcance de la estrategia determinando que aspectos quedan recogidos: gobierno, sector privado, infraestructuras críticas, los ciudadanos, el ámbito universitario, etc.

Se deberían describir cuales son los principios rectores por los que se va a regir el modelo. Estos principios se asientan en los valores y aspectos culturales de la sociedad, y están condicionados por los fundamentos en que se asiente los derechos y libertades de este país.

2. . . . Identificar las amenazas

Al desarrollar esta fase los gobiernos deben identificar y clasificar los distintos tipos de potenciales atacantes y su grado de motivación. Para ello habrá que buscar aportes de una variedad de fuentes, incluyendo agencias gubernamentales y policiales, el sector privado y la academia. La priorización de las amenazas difiere según los países, dado que están condicionadas por la situación geopolítica del país, el nivel de desarrollo económico e industrial, y su propia cultura y realidad social.

En términos generales, se pueden clasificar las amenazas en:

- Proteger los intereses nacionales en el ciberespacio contra las amenazas reales que puedan actuar contra ellas.
- Ser eficiente, lo que supone que las acciones a desarrollar deben ser proporcionadas a la importancia de los bienes y activos a proteger y a su nivel real de exposición.
- Contemplar las medidas de ciberseguridad ya existentes e integrarlas en el nuevo modelo.
- Incluir una priorización de las actuaciones y de las líneas de acción que se hayan definido.
- Evaluar el estado de la tecnología más utilizada por los organismos del sector público y privado, y determinar su nivel de modernización y sensibilidad a las amenazas y riesgos cibernéticos.
- Incluir los tres pilares de ciberseguridad- personas, procesos y tecnología - en políticas, programas, fondos e implementación.

3. . . . Definir escenarios de riesgo

Se debe entender el riesgo como una estimación de la probabilidad de que una ciberamenaza, interna o externa al país, pueda actuar contra ciudadanos, empresas e instituciones públicas, afectando a procesos, servicios y tecnologías esenciales. Al analizar el riesgo se debe considerar, por tanto, las amenazas y su capacidad de generar daños (impactos) a los elementos e intereses a proteger (activos), aprovechando ciertas debilidades (vulnerabilidades) en el entorno o en las tecnologías que la soportan, que determina la probabilidad de ocurrencia. En consecuencia, el riesgo queda determinado por ser una función que depende de estas variables, pudiéndose expresar de forma resumida como:

Riesgo: f (Activo, Vulnerabilidad, Impacto)

Los escenarios de riesgo permiten analizar eventos que pueden afectar a la seguridad del ciberespacio y de los intereses nacionales, facilitando un método para su valoración y gestión.

Las naciones necesitan definir un conjunto de escenarios de riesgo, identificando los eventos que pueden impactar en sus intereses, identificando las potenciales amenazas que podría actuar sobre ellos y cuáles serían los factores temporales asociados, como el tiempo necesario para detectarlos o la posible duración. Estos elementos, objetivos, amenazas, tiempo y eventos deben combinarse y analizarse para identificar su realismo y relevancia. El número de escenarios finalmente considerado debería limitarse a un número gestionable, preferentemente entre 10 y 20.

Definir y diseñar escenarios relevantes requiere experiencia, un conocimiento detallado del entorno y de la realidad nacional y, lo que es más importante, involucrar todas las visiones y sensibilidades: sector público, compañías privadas, las universidades y centros de investigación etc.

4. . . . Identificar la probabilidad de ocurrencia (Vulnerabilidad)

El objetivo en esta fase es determinar cuál es la probabilidad de que se pueda materializar cada uno de los escenarios identificados. Hay dos factores que pueden ayudar a estimar la posibilidad de ocurrencia:

- Análisis de las amenazas. La amenaza se puede caracterizar estudiando aspectos como la motivación, la sofisticación de los medios técnicos que tendría que utilizar, el nivel de conocimiento exigido y el número de potenciales atacantes.

- Análisis de la vulnerabilidad. Estudiando si las vías para realizar el ataque son suficientemente conocidas, si son fáciles de detectar y de corregir. En este punto es necesario resaltar como la obsolescencia de los sistemas y tecnologías del país pueden ser un elemento coadyuvante para que las amenazas puedan materializarse con éxito. Es importante, en esta etapa, realizar un análisis que determine el nivel de modernización digital.

Combinado estos dos factores, estudio de la amenazas y estudio de las vulnerabilidades, se podrá extrapolar una valoración de la probabilidad de materialización del escenario que hemos estudiado.

5. . . Valorar las consecuencias (Impactos)

El objetivo es delimitar las consecuencias de que el escenario de riesgo llegará a materializarse. Esta valoración se puede apoyar en dos factores:

- Técnicos. Consiste en valorar las consecuencias desde una perspectiva estricta de seguridad, atendiendo a la importancia de los servicios afectados en relación con su confidencialidad, su integridad o su disponibilidad.
- No técnicos. Se tendrán en cuenta que consecuencias tendría la materialización de la amenaza para el país en términos tales como la afectación a los compromisos internacionales o con terceros países, a la credibilidad y la imagen del país, al incumplimiento de obligaciones legales, al aumento de los indicadores que determinan el "riesgo país".

La combinación de los dos factores, técnicos y no técnicos permite extrapolar una valoración de las consecuencias de la materialización del escenario considerado que, teniendo en cuenta el ámbito y el alcance, se puede clasificar en niveles (tiers):

- Tier 1: cuando el impacto puede considerarse de consecuencias "estratégicas", por afectar a nivel nacional u organizativo.
- Tier 2: cuando el impacto es considerado "operacional", ya que afecta objetivos de negocio o líneas de servicio.
- Tier 3: en el caso de que haya afectación sobre activos específicos (personas, instalaciones, tecnologías, etc).

6. . . Valorar las capacidades actuales

Tras identificar y valorar los escenarios, se debería continuar con la identificación y estudio de las capacidades existentes en el país, evaluando su nivel de madurez y determinando cómo pueden actuar en los escenarios de riesgo analizados. Para ello se podrían utilizar, adaptándolos a la realidad nacional, modelos de evaluación de la madurez ya existentes como el "Cyber Security Maturity Model for Nations" desarrollado por el Global Cyber Security Center (GCSC), adscrito a la Universidad de Oxford, y en el que contribuyó la Organización de Estados Americanos (OEA). Este modelo, ya fue utilizado por la OEA para elaborar, con el apoyo del Banco Interamericano de Desarrollo (BID), su estudio "Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?".

El modelo desarrollado por GCSC cubre las siguientes dimensiones:

1. Diseñar una política y estrategia de ciberseguridad;
2. Fomentar una cultura de ciberseguridad responsable dentro de la sociedad;
3. Desarrollar el conocimiento de ciberseguridad;
4. Crear marcos legales y regulatorios efectivos;
5. Controlar los riesgos a través de estándares, organizaciones y tecnologías.

Para determinar la madurez cada de una de estas dimensiones se han definido los siguientes niveles:

- **Puesta en marcha:** en esta etapa o bien no existe madurez de ciberseguridad o es de naturaleza muy embrionaria.
- **Formativo:** algunas características de los aspectos han comenzado a crecer y formularse, pero pueden ser ad-hoc.
- **Establecido:** los elementos del aspecto están en su lugar y funcionan. Sin embargo, no se considera bien la asignación relativa de recursos.
- **Estratégico:** se han tomado decisiones sobre qué partes son importantes y cuáles son menos importantes, condicionadas a las circunstancias particulares de la nación.
- **Dinámico:** existen mecanismos claros para modificar la estrategia en función de las circunstancias prevalecientes.

La revisión de la madurez real de las capacidades nacionales de ciberseguridad permite comprender el nivel real de riesgo de los escenarios identificados y determinar los requisitos que se deben incluir en la estrategia de ciberseguridad nacional y en su desarrollo.

7. . . . Definir la Estrategia Nacional de ciberseguridad y las Líneas de Acción

La estrategia nacional de ciberseguridad es el documento que describe los objetivos que se deben alcanzar para gestionar los riesgos del ciberespacio de una forma integral y desde una visión nacional. Se redacción debe incluir todos los aspectos relevantes en el proceso de identificación y análisis de riesgos, y debe servir como palanca para el impulso necesario a las capacidades nacionales en materia de ciberseguridad y ciberdefensa.

Las estrategias nacionales deben ser documentos "vivos", revisados y actualizados periódicamente y diseñados en asociación con todos las actores públicos y privados que puedan estar interesados. Es esencial que las estrategias reflejen los valores sociales, las tradiciones y los principios legales implantados en el país y que sean capaces de cubrir el doble objetivo de ser la base del modelo de ciberseguridad nacional y, al mismo tiempo, servir como catalizador para facilitar la transformación de la digitalización del país.

Por último, la estrategia debe incluir un conjunto de líneas de actuación que permitirán que el gobierno tome acción sobre las actividades que debe promover o sobre las que tiene la responsabilidad de ejecutar, para alcanzar los objetivos definidos y lograr la gestión de los escenarios de riesgo identificados.

5

¿CÓMO CONTINUAR? DE LA ESTRATEGIA A LA ACCIÓN

Tras la definición de los objetivos estratégicos incluidos en la estrategia nacional de ciberseguridad, y la definición de las líneas de actuación, los gobiernos tendrían que pasar a desarrollar los instrumentos legales y regulatorios, a asignar roles y responsabilidades y a construir las capacidades técnicas y organizativas necesarias. Es por tanto el momento de pasar de la estrategia a la acción.

Acciones para el ciudadano y el sector privado

Se debería impulsar las actividades de concienciación para asegurar que los ciudadanos y empresas conocen las vulnerabilidades y posibles ciber amenazas, y saben incorporar en el uso de las tecnologías e internet un patrón adecuado de comportamiento. La "ciber-higiene", es decir, la educación hacia modelos de comportamiento correctos que prevengan los efectos adversos en el uso de las tecnologías podría fomentarse a través de las siguientes acciones:

- Campañas de comunicación en los medios dirigidas a ciudadanos y a la pequeña y mediana empresa (PyME), para fomentar el uso seguro de Internet, promoviendo la adopción de herramientas y difundiendo prácticas "ciber higiénicas".
- Programas de concienciación y de educación en colaboración con agentes del sector público y privado, buscando la coordinación y la racionalización de esfuerzos.
- Desarrollar módulos educativos dirigidos a todos los niveles de la enseñanza.
- Generando o fomentando el desarrollo de eventos a nivel nacional, regional o municipal, donde que incluyan talleres para fomentar las buenas prácticas en todos los usuarios y en colectivos específicos como el de padres, educadores y menores.
- Desarrollando y compartiendo contenidos multimedia atractivos y herramientas educativas basadas en "gamificación".

Una atención especial se debería dirigir a la prevención de los riesgos del ciberespacio en la que los menores son las víctimas. Los gobiernos deberían diseñar un programa educativo y de contenidos específicamente dirigido a prevenir y detectar casos de "cyber bulling", "sexting" y "grooming", estableciendo de forma complementaria un centro específico de denuncia, control y seguimiento de estos casos.

Respecto al sector privado, el gobierno podría realizar las siguientes acciones específicas:

- Facilitar la utilización de soluciones para el intercambio de información sobre amenazas, vulnerabilidades e incidentes entre compañías del mismo o destino sector, de forma que se cree una "inteligencia colectiva" que permita actuar de forma preventiva y agilice la respuesta.
- Desarrollar códigos de buenas prácticas y apoyar el desarrollo de estándares de certificación.
- Promover ciberejercicios para probar los mecanismos de coordinación entre las distintas compañías y con los organismos públicos y mejorar la eficacia en la respuesta ante los incidentes.
- Desarrollar estudios comparativos entre entidades del mismo sector y de distritos sectores, con el objetivo de definir líneas base y de "benchmarking".

El gobierno debería impulsar la creación de una capacidad nacional de respuesta ante incidentes cibernéticos (CERT) que preste servicios específicos para ciudadanos y el sector privado. Dicha capacidad debería ser complementaria y nunca competitiva con los servicios proporcionados por los proveedores de servicio a través de CERTs privados o de Centros de Operaciones de Seguridad (SOC, en sus siglas en inglés). El objetivo de este CERT público es desarrollar servicios de valor para la gestión y conducción de situaciones de crisis nacional o para servicios que respondan a las siguientes características:

- De extrema importancia para la seguridad y la defensa nacional.
- Servicios de valor para la ciberseguridad nacional, que no estén siendo cubiertos por el sector privado al ser de baja demanda o por no ser rentables.

Para ello es imprescindible que el gobierno cuente con una visión detallada de los distintos actores del mercado y de los servicios que están prestando, con el objetivo de buscar sinergias y evitar solapamientos.

Acciones para los operadores de infraestructura crítica

La protección de las infraestructuras críticas debe ser una parte fundamental de la estrategia de ciberseguridad nacional ya que tiene como objetivo optimizar la resiliencia de las infraestructuras de las que dependen servicios esenciales para la nación. La ciberseguridad de las organizaciones públicas o privadas que operan esos sectores estratégicos es de particular importancia dado que un ciberataque exitoso sobre ellas puede suponer un impacto muy grave para la seguridad y para el funcionamiento del país. Este impacto podría incidir en la vida de los ciudadanos, la estabilidad, fortaleza y credibilidad de la economía o la reputación internacional

Las acciones que los gobiernos podrían impulsar para la protección de este tipo de organizaciones son:

- Definir e identificar sectores críticos. El gobierno debería determinar los sectores críticos de los que depende su funcionamiento como nación y cuya no disponibilidad podría generar graves consecuencias. Los países han desarrollado distintas aproximaciones en función de sus condicionantes geopolíticos, económicos e industriales, pero existen determinados sectores que aparecen en todos los modelos nacionales: Administraciones Públicas, Energía (Electricidad, Gas, Petróleo, Energía Nuclear), Transporte (Ferrocarril, Carreteras, Aéreo y Marítimo), Finanzas (Banca y Medios de Pago), Agua, Redes de Telecomunicaciones y, Salud.

- Desarrollar un método para identificar y valorar las infraestructuras críticas, de forma que estos criterios sean uniformes y repetibles en el tiempo.

- Para cada uno de los sectores estratégicos, el gobierno podría definir: el catálogo de amenazas, los criterios específicos para considerar que los servicios que presta una determinada organización deber ser considerados críticos y el catálogo de los operadores y de las infraestructuras críticas.

- Los requisitos mínimos de seguridad que los operadores críticos deben implantar, el modelo de evaluación de riesgos y de gobierno y gestión de la ciberseguridad.

- Facilitar mecanismos para el intercambio de información sobre incidentes y amenazas entre los operadores.

- Definir, para el CERT o CERTs nacionales, un catálogo de servicios específico para los operadores críticos. Este catálogo debería responder a las singularidades de cada sector estratégico considerado: amenazas, servicios y tecnologías de los que dependen, consecuencias e impactos del no funcionamiento.

- Promover ciber ejercicios sectoriales para mejorar el grado de preparación de los operadores ante ciberataques sistémicos. Estos ejercicios, de carácter singular y especializados, se deben complementar con otros intersectoriales, focalizados en la preparación ante situaciones de crisis a nivel nacional.

- Impulsar eventos y otros foros que faciliten el conocimiento e intercambio de experiencias entre los responsables de ciberseguridad. Asimismo, debe fomentar la creación de grupos de trabajo sectoriales para impulsar y desarrollar los modelos de seguridad específicos de cada sector.

- Conocer las necesidades específicas de productos y servicios que tengan los operadores de sectores estratégicos es de gran utilidad para determinar si la oferta actual que ofrece el mercado es adecuada. Este conocimiento puede servir para que el gobierno oriente la investigación académica y para que sirva de estímulo al desarrollo de iniciativas de emprendimiento.

Acciones para el gobierno e instituciones públicas

El gobierno y las administraciones públicas deben contar con un nivel alto de protección ante las ciberamenazas. Las razones para ello se basan en las siguientes consideraciones:

- La búsqueda de una mayor eficacia en el funcionamiento de los servicios públicos y de una mayor cercanía a los ciudadanos ha impulsado a muchos gobiernos a adoptar procesos de transformación digital en las administraciones públicas, en la que se ha venido llamando la eAdministración. El éxito de estas iniciativas depende de que los ciudadanos cambien progresivamente su forma de relacionarse con la administración y se vayan adaptando a esa nueva realidad digital. Para ello, uno de los elementos más importantes es el de la "confianza digital", entendido como el atributo por el que los ciudadanos tienen el convencimiento que sus datos son privados, están seguros y son gestionados de forma transparente. Sin confianza digital la eAdministracion no es viable.

- Las instituciones públicas procesan y almacenan datos de carácter personal de los ciudadanos y para ello, necesitan almacenar esta información en grandes bases de datos que van a ser objeto de interés para los cibercriminales.

- Además de información de carácter personal, el gobierno maneja información clasificada de alto valor estratégico para los intereses nacionales que requiere de medidas de protección adicionales.

Protección de las tecnologías públicas

Las acciones que los gobiernos podrían impulsar son:

- Establecer un marco nacional de ciberseguridad para las administraciones públicas que sirva de referencia para todas ellas y que permita unificar criterios entre el gobierno de la nación, los gobiernos regionales o estatales y los ayuntamientos y administraciones locales. El marco nacional, que debería comprender políticas, procedimientos y normas técnicas, líneas base, metodologías y herramientas, debe permitir mejorar la protección de los servicios públicos, la información y los sistemas de información y comunicaciones en que soporta. Cada país debería adoptar un marco de la industria como su base (ISO, NIST, etc.), y luego proporcionar orientación sobre cómo se aplicará ese marco en su país. Sería muy difícil para las empresas y los proveedores de servicios alinearse a un marco y estándares únicos de cada país, lo que limitará a quienes pueden utilizar estos países. Los marcos comunes de ciberseguridad, la gestión de riesgos, los controles de seguridad, etc. beneficiarán al sector comercial y al gobierno.

- Desarrollar acuerdos multinacionales o acuerdos comerciales que faciliten el intercambio y la coordinación / cooperación de los países que luchan contra las amenazas cibernéticas.

- Desarrollar planes de formación y concienciación dirigidos a los funcionarios públicos con el objetivo de mostrarles cuales son las amenazas específicas que pueden afectar a la ciberseguridad de los servicios públicos, e inculcarles patrones de comportamiento "ciber-higiénicos".

- Desarrollar e implantar capacidades horizontales de ciberseguridad que unifiquen al máximo la prevención, detección y la respuesta ante los ciber incidentes en el ámbito de las administraciones centrales, regionales y locales. Estas capacidades horizontales tienen la ventaja de unificar y estandarizar el servicio de ciberseguridad en todas las instituciones públicas, aporta eficiencia al basarse en economías de escala y, permite una visión holística que aporta inteligencia e información de valor.

- Desarrollar un esquema de ciberseguridad que facilite la evaluación formal y la certificación para los productos y sistemas que vayan a formar parte de las infraestructuras tecnológicas que se soportan los servicios esenciales de la administración. Aprovechar los estándares internacionales y de la industria existentes como SOC, ISO, PCI, NIST, etc. en lugar de crear propios estándares únicos que pueden resultar muy difíciles o imposibles de implementar.

- Adicionalmente a estas actividades para defender las redes y sistemas en los que se apoyan los servicios públicos, los gobiernos deberían actuar para desarrollar sus capacidades para la ciberdefensa y para la lucha contra el cibercrimen.

Ciberdefensa

El ciberespacio proporciona un nuevo teatro de las operaciones y esto supone que, en un conflicto armado, las acciones militares puedan llegar a afectar a información, servicios y sistemas críticos. Por ello, es necesario que las fuerzas armadas cuenten con unidades especializadas para la defensa de los intereses nacionales en el ciberespacio.

Las acciones que los gobiernos podrían impulsar para el desarrollo de sus capacidades de ciberdefensa son:

- Desarrollar planes específicos de especialización y entrenamiento en la materia, que permita que los ejércitos cuenten con los efectivos necesarios.
- Definir un modelo de colaboración con empresas especializadas y con expertos en ciberseguridad para reforzar las capacidades de las fuerzas armadas en los casos que se determinen.
- Promover ciberejercicios periódicos que faciliten el entrenamiento continuo sobre escenarios reales.
- Desarrollar conocimiento y experiencia sobre amenazas y vulnerabilidades relacionadas con la ciberdefensa y también métodos de ataque, a través del intercambio de información a nivel nacional e internacional.
- Establecer una cooperación con las principales instituciones académicas y de I + D para el desarrollo de necesidades específicas en el ámbito de la ciberdefensa.

Lucha contra el Cibercrimen

La lucha contra la ciberterrorismo y la ciberdelincuencia debe comprender una doble vertiente, el ciberespacio como herramienta que permite el desarrollo de estas actividades delictivas y el ciberespacio como objetivo final de la acción. Para ello se requiere la colaboración de distintos actores y ser abordada de forma integral, y para ello el gobierno podría actuar en dos frentes:

- Legal, creando leyes específicas y adaptando las existentes para permitir la persecución del cibercrimen.
- Desarrollando capacidades y dotando de recursos especializados a las instituciones encargadas de vigilar el cumplimiento de la ley: jueces, fiscales y unidades de investigación policial.

En este sentido, los gobiernos podrían emprender, entre otras, las siguientes acciones:

- Adaptar el marco legal nacional a los nuevos tipos de delitos y adaptar los tipos ya existentes a la realidad digital.
- Participar internacionalmente en la elaboración de acuerdos y tratados para la persecución del ciberdelito, ratificándolos una vez aprobados.
- Crear unidades especializadas en ciberdelincuencia (policiales y judiciales) y desarrollar planes de formación y capacitación continua.
- Mejorar las capacidades de los organismos competentes y asegurar la coordinación a través del intercambio de información e inteligencia.
- Fortalecer la cooperación policial internacional y la presencia en foros y organizaciones internacionales centrados en la lucha contra el ciber crimen.
- Desarrollar conocimiento y experiencia sobre amenazas y vulnerabilidades relacionadas con la delincuencia cibernética.

- Establecer una cooperación con las principales instituciones académicas y de I + D sobre las nuevas técnicas de investigación policial.
- Establecer la cooperación entre las partes interesadas del sector público y privado para identificar rápidamente y responder a cuestiones relacionadas con el delito cibernético.
- Crear un canal especializado para ciudadanos y para empresas para denunciar los posibles ciberdelitos.
- Desarrollar e implantar acciones específicas de detección y persecución de ciber delitos que afecten a menores.

Otras acciones del gobierno

Talento

La construcción de un modelo nacional de ciberseguridad requiere que el gobierno, las administraciones públicas y el sector privado cuenten con un número adecuado de profesionales con conocimientos y especialización en ciberseguridad. La demanda de profesionales crece progresivamente debido a que los procesos de transformación digital provocan que los departamentos de ciberseguridad aumenten a medida que aumenta la dependencia en las tecnologías de la información y en el ciberespacio. Por otro lado, las universidades y los centros de formación no están siendo capaces de absorber este incremento en la demanda y no generan un número suficiente de profesionales. Además, la alta especialización de los perfiles profesionales demandados no siempre se está cubriendo con los programas de formación existentes.

Algunas de las acciones que el gobierno podría realizar para mejorar esta realidad son:

- Determinar las necesidades de profesionales que tiene el sector privado y el público, y los requisitos de conocimientos y especialización.
- Definir un catálogo general de roles profesionales que incluyan las capacidades y competencias que se adapten a la innovación tecnológica.
- Participar en el diálogo con universidades y otras instituciones educativas para desarrollar nuevos programas o adaptarlos a las necesidades del mercado laboral.
- Promover en colegios y centros de enseñanza talleres y otras actividades que estimulen el interés y la curiosidad por la ciberseguridad.
- Organizar eventos de ciberseguridad que ayuden a identificar expertos nacionales.

Emprendimiento

De forma periódica nos enfrentamos a nuevas formas de ataque que utilizan técnicas y métodos diferentes a los conocidos. Este hecho, junto con la evolución continua de las tecnologías y su aplicación en la industria y la sociedad creando nuevos casos de uso, supone que los gobiernos se enfrenten a un entorno de amenaza de creciente sofisticación y en continuo cambio. Las herramientas y productos de ciberseguridad del presente dejan de ser útiles ante estos nuevos entornos que solo pueden ser gestionados con nuevos y diferentes enfoques. La investigación, el desarrollo y la innovación son necesarios para el desarrollo de soluciones eficaces que den respuesta a los nuevos tipos de ataques.

Para alcanzar este objetivo, los gobiernos deberían ejercer el liderazgo y la coordinación entre todos los agentes interesados:

- La demanda sofisticada, entendida por aquellos sectores (gobierno, banca, energía…) que bien por el grado de penetración digital en sus negocios, bien por la tipología de las amenazas que les afecta, requieren de soluciones novedosas.
- Las universidades y centros de innovación, que son las organizaciones que dedican recursos a la investigación técnico-científica.
- Los emprendedores y "start ups", que cuentan con ideas y proyectos, que pueden contribuir a dar respuesta a estas necesidades.

Las acciones que los gobiernos podrían desarrollar para generar un ecosistema para el emprendimiento es ciberseguridad, son:

- A través de foros y grupos de trabajo, determinar con la demanda sofisticada las necesidades presentes y futuras de productos y servicios de ciberseguridad, trasladando esta necesidad a una agenda nacional de investigación que marque la hoja de ruta de la investigación y el emprendimiento.
- Crear un plan de investigación para evitar solapamientos entre las actividades de investigación emprendidas por diferentes instituciones

- Establecer fondos específicos que soporten los programas de investigación en ciberseguridad.
- Habilitar mecanismos para garantizar la transferencia a la industria.
- Fomentar entre los jóvenes la cultura de emprendimiento mediante un plan de actuación que incluya actividades que faciliten la educación y orientación.
- En línea con la agenda de investigación, crear concursos de ideas donde los jóvenes emprendedores presenten proyectos o prototipos que puedan dar solución a los problemas planteados.
- Crear fondos públicos que ayuden a los emprendedores en las fases tempranas del ciclo de emprendimiento.
- Crear eventos que faciliten el contacto entre los emprendedores y la inversión privada.
- Promover la implantación de programas de incubación y aceleración de startups (empresas emergentes y con potencial de crecimiento).

6
CONCLUSIONES

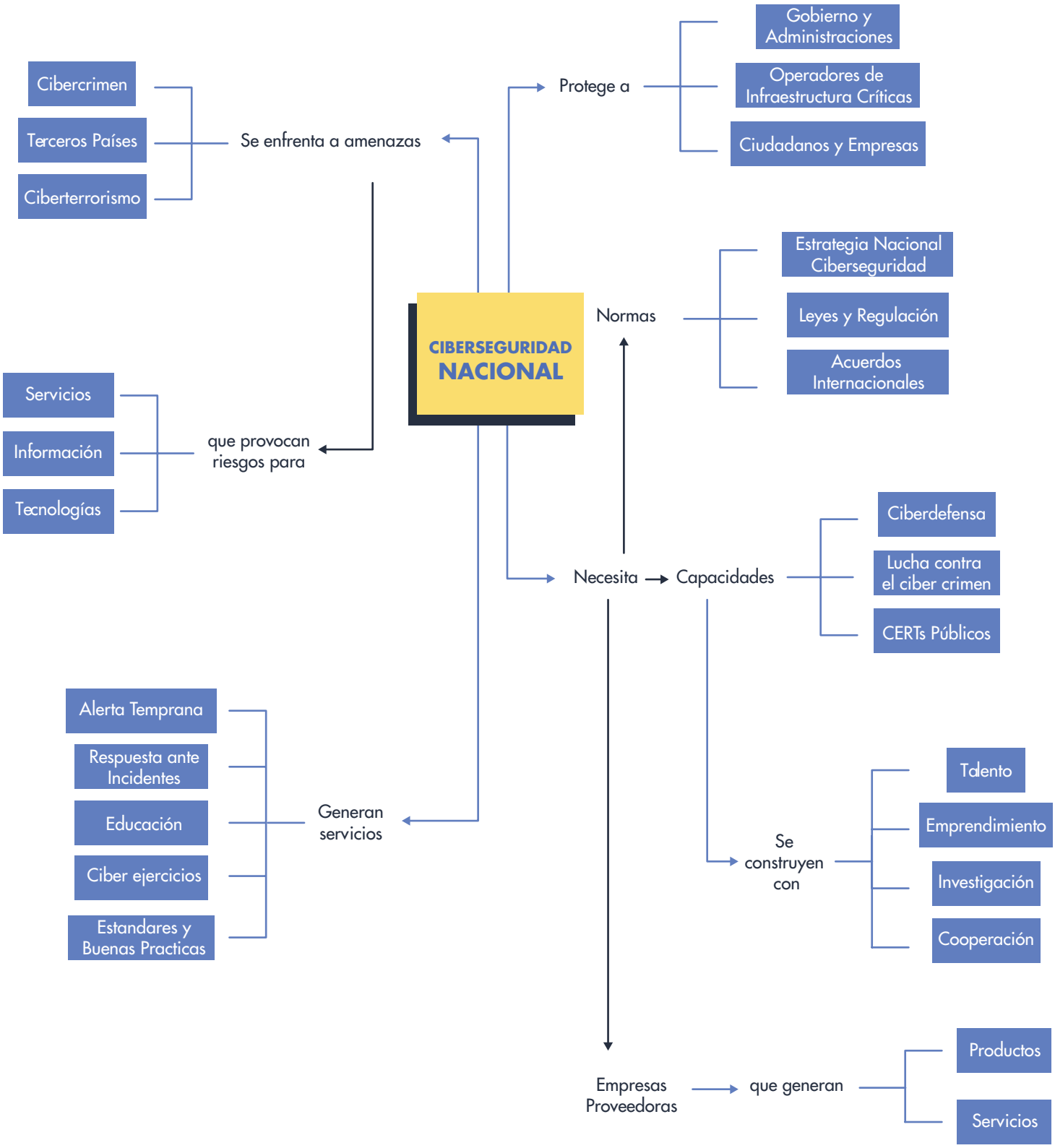
El ciberespacio y las tecnologías son un motor de crecimiento para la economía, un impulsor del desarrollo industrial y han revolucionado nuestra forma de vida. La forma como nos relacionamos con otras personas, como compramos o como hacemos negocios está cambiado con los procesos de transformación digital del presente, y seguirán cambiando con los procesos de transformación que el futuro nos irá trayendo. Este escenario de enormes oportunidades no está exento de riesgos y amenazas, como así ha pasado con los grandes avances que se han producido en la historia de la humanidad. Los gobiernos tienen la responsabilidad de definir las condiciones para que el ciberespacio y las tecnologías se puedan utilizar con unos niveles razonables de seguridad, de la misma manera que han venido actuando para garantizar la seguridad pública y ciudadana ante el crimen tradicional o la seguridad jurídica en las relaciones entre partes.

Este esfuerzo de los gobiernos se debe basar en la colaboración y la cooperación. En el ámbito exterior participando en foros internacionales, adoptando los acuerdos internacionales y estableciendo líneas de colaboración bilaterales con otros países. Dentro de sus fronteras, estableciendo la coordinación efectiva con todos los agentes públicos y privados, con el objetivo de entender y atender los riesgos y amenazas a los que se enfrentan.

El gobierno debe comprender el papel fundamental que juegan los ciudadanos y, en particular los jóvenes, en la seguridad del ciberespacio siendo necesario que se impulse la generación de una cultura global de ciberseguridad que lleve a pautas de conducta "ciberhigiénicas".

Por último, el gobierno tiene que catalizar la creación de talento y de nuevas empresas entendiendo que estas actividades no son sólo un elemento estratégico esencial para la construcción del modelo de ciberseguridad nacional si no, también, una enorme oportunidad de crecimiento y desarrollo.

Para todo ello, el primer paso que un gobierno debería abordar es la definición de una estrategia nacional de ciberseguridad.



MAPA MENTAL CIBERSEGURIDAD NACIONAL

7

REFERENCIAS

Publicaciones

- Amazon Web Services Risk and Compliance 2017
- National Cyber Security Strategy Good Practice Guide-ENISA
- Cybersecurity Capacity Maturity Model for Nations (CMM) Global Cyber Security Capacity Centre. University of Oxford
- Cybersecurity-Are-We-Prepared-in-Latin-America-and-the-Caribbean. -OAS 2016
- Microsoft National Strategies EN 2013
- OCDE cybersecurity policy making
- National Initiative for Education-NIST 800 181
- United States- The National Security Strategy 2017
- Estonian National Cyber Security Strategy 2014 to 2017
- UK National Cyber Security Strategy 2016 to 2021
- Estrategia de Ciberseguridad Nacional de España 2013
- 2017 Global Information Security Workforce Study Benchmarking Workforce Capacity and Response to Cyber Risk. - Center for Cyber Safety and Education (ISC2)
- Cyber Security Trends: Aiming Ahead of the Target to Increase Security in 2017.- Sans Institute
- General Data Protection Regulation (GDPR) (EU) 2016/679 of the European Parliament and of the Council
- Directiva de Seguridad en Redes e Información (UE) 2016/1148 Del Parlamento Europeo y del Consejo
- WEF Global Risks Report 2018

Sitios web

- www.incibe.es/cybercamp
- www.dhs.gov/national-cyber-security-awareness-month
- www.staysafeonline.org/ncsam
- www.cyberspark.org.il
- www.cyberseek.org
- www.europeancybersecuritychallenge.eu
- www.renic.es
- www.stopthinkconnect.org
- www.oxfordmartin.ox.ac.uk/cybersecurity
- www.aws.amazon.com/whitepapers/overview-of-risk-and-compliance
- www.thebestvpn.com/cyber-security-statistics-2018
- www.eugdpr.org/

OEA Más derechos para más gente | aws

UN LLAMADO A LA ACCIÓN

PARA PROTEGER A CIUDADANOS SECTOR PRIVADO Y GOBIERNO

White paper series

Edición 1

2018