OEA | Más derechos para más gente

MÉXICO
PRESIDENCIA DE LA REPÚBLICA

Hacia una Estrategia Nacional de Ciberseguridad

Consolidación de las Consultas a Actores Nacionales

2 de agosto de 2017

Tabla de Contenido

Resumen ejecutivo

A solicitud del Gobierno de México, la Secretaría del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (OEA), a través de su Programa de Ciberseguridad, convocó una comisión de expertos internacionales para apoyar en la segunda etapa del proceso "Hacia una Estrategia Nacional de Ciberseguridad", que llevó a cabo entre el 12 y 13 de julio de 2017. Los expertos internacionales facilitaron cinco (5) mesas de discusión con los siguientes actores: (i) Industria; (ii) Sector Financiero; (iii) Sociedad Civil, Derechos Humanos (DD.HH.) y Usuario Final; (iv) Academia y Comunidad Técnica; y (v) Gobierno. En este contexto, este documento consolida las discusiones y los comentarios de los actores nacionales y expertos internacionales.

Los comentarios de los distintos actores están divididos en cinco (5) temas principales: (i) cultura, educación y capacitación; (ii) coordinación y colaboración; (iii) investigación y desarrollo; (iv) estándares y criterios técnicos; y (v) marco jurídico. Además, este documento cuenta con la sección "Comentarios Generales" que, a su vez, señala los temas de más destaque en las mesas de discusión, descritos brevemente a continuación:

A. **Alcance de la Estrategia Nacional de Ciberseguridad (ENCS):** sería importante clarificar el alcance de la estrategia nacional de ciberseguridad no sólo en términos de contenido, sino también de actores impactados. Es decir, si es documento será una estrategia para el ciberespacio, ciberseguridad o mismo la seguridad de la información. Además, la estrategia enfoca en el gobierno federal, y poco se discute sobre el rol de los gobiernos locales.

B. **Enfoque Basado en el Riesgo:** se recomienda abordar la ciberseguridad mediante un enfoque basado en el riesgo, en el cual se gestiona el riesgo, lo que significa que se reduce a un nivel aceptable de acuerdo con el contexto y los objetivos establecidos en la estrategia nacional. En este contexto, los participantes destacaron la importancia de definir las infraestructuras críticas del país, a modo de identificar sus vulnerabilidades.

C. **Terminologías:** se recomendó revisar las definiciones presentes en el borrador de la estrategia nacional a modo que estén en consonancia con las definiciones establecidas en la legislación mexicana y con el entendimiento internacional.

D. **Gobernanza:** es fundamental que la estrategia de ciberseguridad tenga un marco de gobernanza claro que defina las funciones y las responsabilidades de los distintos actores. El modelo de gobernanza también debe proporcionar un marco para el diálogo entre los distintos actores y la coordinación de diversas actividades emprendidas en el ciclo de vida de la estrategia.

E. **Implementación ('Plan de Acción'):** se recomendó definir acciones concretas, identificando explícitamente las entidades (o actores) responsables, un presupuesto estimado y el horizonte de tiempo para su ejecución.

Finalmente, el Apéndice de este documento presenta el borrador de la ENCS con comentarios específicos de las distintas mesas de discusión.

1. Contexto

Por solicitud del Gobierno de México, el Programa de Seguridad Cibernética de la Organización de los Estados Americanos (OEA) implementa un acompañamiento de asistencia técnica con el gobierno de México a fin de mejorar las capacidades nacionales de ciberseguridad del país. La primera misión de asistencia técnica "Hacia una Estrategia Nacional de Ciberseguridad" se llevó a cabo los días 19-20 de abril en las instalaciones de la Secretaría de Relaciones Exteriores en la Ciudad de México.

El taller reunió una comisión de expertos internacionales para compartir las mejores prácticas en materia de ciberseguridad, en la que compartieron entidades mexicanas y actores de la industria, la academia y organizaciones de sociedad civil para mejorar las capacidades nacionales de ciberseguridad del país. El taller consistió en diferentes mesas de trabajo, en las que se intercambiaron experiencias, puntos de vista y mejores prácticas sobre temas relacionados con la ciberseguridad en México. Este primer ejercicio de consulta tuvo como objetivo identificar las inquietudes, así como aportes de los diversos sectores que contribuyan a la definición de la Estrategia Nacional de Ciberseguridad del país, con apego a los más altos estándares internacionales. Como resultado de esta misión, se preparó el documento "Recomendaciones para el desarrollo de la Estrategia Nacional de Ciberseguridad – Misión de Acompañamiento Técnico",[1] que fue entregado por la Secretaria General de la OEA al gobierno de México en el marco de la Asamblea General de la OEA en el 20 de junio de 2017.[2]

Durante el 11 y 12 de julio, se realizó la segunda misión de acompañamiento que tuvo como objetivo consolidar las contribuciones generadas en la primera misión y en los talleres de la comunidad nacional con las recomendaciones emitidas por los expertos internacionales resultado del primer taller. En esta misión también se analizó el borrador inicial de la estrategia por medio de mesas de discusión con distintos actores nacionales.

De acuerdo con la estrategia nacional, el objetivo principal es:

> *'Propiciar que individuos, empresas y entes públicos -de los diferentes poderes y órdenes de gobierno, realicen sus actividades con el uso de tecnologías de información y comunicación, incluyendo el ciberespacio; de manera libre, confiable, segura y resiliente, y con ello impulsar el desarrollo económico, social y político de México.'*

En base en el objetivo general, se dividió esta estrategia en 4 Objetivos Estratégicos y 8 Ejes Transversales que los abordan, como destacado en el diagrama a continuación:

[1] "Recomendaciones para el desarrollo de la Estrategia Nacional de Ciberseguridad – Misión de Acompañamiento Técnico". Disponible en: http://www.oas.org/documents/spa/press/Recomendaciones-para-el-Desarrollo-de-la-Estrategia-Nacional-de-Ciberseguridad.pdf. Acceso en el 27 de julio de 2017.
[2] "OEA entregó al gobierno de México recomendaciones para el Desarrollo de la Estrategia Nacional de Ciberseguridad". Disponible en: http://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-049/17. Acceso en el 27 de julio de 2017.

Gráfico 1 - Estructura de las ENCS

Las mesas de discusión con los distintos actores nacionales contemplaron estos objetivos estratégicos y ejes transversales en sus contribuciones. Se conformaron cinco (5) mesas de discusión encabezadas por un moderador designado y un relator, ambos expertos internacionales. Se dividieron los actores nacionales por los siguientes sectores: (i) Industria; (ii) Sector Financiero; (iii) Sociedad Civil, Derechos Humanos (DD.HH.) y Usuario Final; (iv) Academia y Comunidad Técnica; y (v) Gobierno. En este contexto, este documento consolida las discusiones y los comentarios de los actores nacionales y expertos internacionales.

2. Contribuciones de las Mesas de Discusión

2.1. Cultura, Educación y Capacitación

La Academia destacó la necesidad estratégica de formar profesionales de ciencias, tecnologías, ingeniaría, matemáticas y otros técnicos altamente especializados, así como de desarrollar especialistas desde el nivel de la escuela primaria y pasando por el nivel universitario. Dado que la formación de personal es un esfuerzo de largo plazo, los esquemas de certificación y los modelos alternativos de formación creativa deben fortalecerse para llenar la brecha de mano de obra (en los niveles federal, estatal y municipal) mientras tanto especialistas en tecnologías y ciberseguridad están siendo educados a través del sistema educativo tradicional. Estos modos alternativos de educación deben ser sensibles a las necesidades de los profesionales que trabajan y también a las necesidades de los ciudadanos económicamente desfavorecidos.

En la creación de programas de desarrollo profesional en ciberseguridad, la mesa de discusión de Gobierno destacó que sería importante tener en cuenta las necesidades específicas del trabajo en ciberseguridad para que los profesionales sean entrenados y tengan una formación mínima adecuada para su función y organización. No es lo mismo fortalecer las capacidades a la sociedad civil, a las organizaciones públicas o privadas, o a los funcionarios especializados que trabajen en asuntos relacionados con la ciberseguridad. La mesa de discusión del sector financiero también recomendó que se haga énfasis sobre el tipo de capacidades se deben fortalecer por tipo de actor ya que existen capacidades operativas, administrativas, humanas, científicas, de infraestructura física y tecnológica.

Además, la Academia recomienda que la contribución a la estrategia se amplíe a un enfoque de toda la sociedad y no se limite a un pequeño grupo. También se recomendó crear un ambiente donde todos sean un defensor de la red, basado en sus roles apropiados. No sólo eso, sino que hay una necesidad de reconocer la importancia de otras disciplinas en la ciberseguridad, tales como las humanidades y la ingeniería tradicional o el personal de la fuerza de trabajo actual que puede tener aptitud técnica que puede contribuir al desarrollo de iniciativas cibernéticas.

Con respecto a la sección de la sociedad de la ENCS, se destacó la necesidad de establecer una responsabilidad compartida entre el gobierno y los usuarios de la población general acerca del uso del Internet. Las campañas de sensibilización deben adaptarse a públicos específicos y deben incluir mensajes a todos los ciudadanos, incluidos los ciudadanos marginados. En general, los ciudadanos deben tener una buena comprensión de las amenazas, pero también de las oportunidades del Internet. La mesa de discusión del sector financiero recomendó que los programas y campañas de concientización inculquen la cultura de prevención de ataques cibernéticos entre el público usuario de servicios financieros en el país.

En este contexto, una amplia comunicación debe llevarse a cabo para apoyar el fomento de la confianza. Específicamente, dentro del sector educativo, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y la Secretaría de Educación podrían colaborar en el desarrollo de campañas dirigidas a grupos específicos, tal como los niños y las niñas. Estas campañas deben traducirse a varios idiomas, incluyendo las lenguas indígenas.

En relación con lo anterior, la mesa de discusión de Gobierno mencionó la idea de unificar el mensaje de concientización en ciberseguridad para que sirva de "marca" para la estrategia de divulgación. Junto con ese mensaje, se podría desarrollar un repositorio de alta visibilidad de contenidos de ciberseguridad útiles para la población.

No obstante un mensaje general de ciberseguridad que sirva para la población es importante, también se podría focalizar acciones y campañas en comunidades específicas. Por ejemplo, no existe un programa diseñado específicamente para enseñar a los menores sobre la protección de su información. A veces los niños muy pequeños saben más sobre el uso de nuevas tecnologías, aparatos que se pueden utilizar para navegar, generar y almacenar información cibernética o redes sociales que sus maestros y padres. Por esta razón, los padres y los maestros deben ser educados, y la sociedad civil puede participar en el proceso para desarrollar y entregar estas campañas.

La privacidad y la protección de datos deben formar parte del currículo nacional básico. La reforma educativa ofrece una buena oportunidad para que este cambio tenga lugar, ya que esto ayudaría a promover una cultura de ciberseguridad. El gobierno podría desempeñar un papel más activo al tomar la iniciativa en la implementación de estas campañas y demostrar tanto los beneficios como los riesgos asociados para los educadores y los padres.

Un rol más activo del gobierno sería particularmente importante en situaciones más sensibles, como la violencia de género en línea y la pornografía infantil, donde la tasa de denuncia suele ser baja y las ocurrencias son fácilmente encubiertas. Informar a los niños y otros grupos vulnerables de sus derechos humanos es fundamental para que puedan comprender como hacerlos valer y cómo pueden protegerse.

Otra recomendación interesante de la mesa de discusión de la sociedad civil fue que el Gobierno considerara aumentar la concienciación del usuario final sobre el valor de sus datos y el impacto del robo o divulgación indebida de sus datos personales. Este enfoque fomentaría la confianza en el uso de la plataforma digital, incluyendo los servicios electrónicos gubernamentales, ya que los usuarios finales sentirán un sentido de propiedad y empoderamiento.

2.2. Coordinación y colaboración

La Academia expresó su deseo de comprender mejor cómo el documento de la Estrategia Nacional se alinea con los mandatos existentes y otras estrategias como el manual MAGTICSI y la Estrategia Digital, incluyendo cómo se asignarán los recursos para nuevas iniciativas estratégicas y si las asignaciones actuales se verán afectadas. Adicionalmente, se indicó que era necesario aclarar qué órgano o mecanismo de coordinación gubernamental sería responsable de asegurar que esta estrategia esté bien coordinada con la comunidad académica y técnica, y que también tenga un modelo de múltiples partes interesadas más allá de esa comunidad. Además, sería importante identificar quiénes serían los puntos de contacto dentro de la comunidad académica y técnica para la coordinación.

La mesa de discusión de la sociedad civil, de los derechos humanos y del usuario final indicó que es necesario establecer una clara demarcación de funciones, responsabilidades y rendición de cuentas, ya que hay muchos esfuerzos a nivel nacional en materia de seguridad cibernética y digital, y deben coordinarse. Por ejemplo, una idea sería el establecimiento de un órgano centralizado para coordinar cuestiones nacionales de ciberseguridad, como un centro dedicado. La mesa de discusión del sector privado igualmente recomendó la creación de una entidad coordinadora nacional encargada de dirigir la implementación de la estrategia nacional y hacer seguimiento continuo de la misma, así como de llevar a cabo la coordinación interinstitucional e intersectorial en temas de ciberseguridad.

En este contexto, los comentarios de la mesa de discusión del sector financiero son relevantes, ya que la mesa también destacó que en el país falta información oportuna sobre modos de

operación que se detecten y sean compartidos en forma segura, confidencial y eficiente a la comunidad de manera que se pueda prevenir la materialización de incidentes en otras instancias o entidades expuestas al mismo riesgo o con la misma vulnerabilidad. Actualmente, no existe un marco para esto, pero esto debe ser explorado por el documento de la ENCS para la continuidad y mejor implementación de la estrategia.

Debido a un cambio frecuente en los funcionarios públicos, hay una pérdida de conocimiento institucional, que debe ser gestionada para proporcionar continuidad de las políticas.

La mesa de discusión de Gobierno destacó que sería interesante establecer mecanismos de colaboración y gestión de conocimiento. Del mismo modo, la mesa de discusión del sector financiero recomendó el diseño de mecanismos de participación activa y permanente de las múltiples partes interesadas y de un mecanismo dinámico de coordinación que defina los roles, las responsabilidades y las funciones de las múltiples partes interesadas. Por ejemplo, se podrían crear grupos especializados en ciberseguridad para trabajar en temas específicos. Sería importante también verificar los mecanismos existentes de cooperación y ampliarlos. Se podría replicar un modelo similar al de ventanilla digital, que permita contar con enlaces y facilitar la coordinación y colaboración en materia de ciberseguridad.

También sería importante tener en cuenta un modelo para la cooperación entre los distintos actores internacionales (ej. Estados, organismos internacionales, sector privado, etc.). El sector financiero destacó la necesidad de mecanismos de cooperación internacional respecto de las consideraciones derivadas de la jurisdicción en que se realizan los delitos cibernéticos.

2.3. Investigación y Desarrollo

La mesa de discusión de la sociedad civil subrayó la importancia de la participación de la academia en la sección económica de la ENCS, dado que la academia tiene un papel importante en impulsar la innovación. De hecho, la mesa de discusión de Gobierno propuso que el eje transversal también incluya la palabra innovación y cambie para "investigación, desarrollo e innovación (I+D+i)".

Con esto en mente, es necesario un presupuesto recurrente (multianual) para la investigación en seguridad cibernética. Los fondos federales de investigación, incluidos los provenientes de la Secretaría de Educación y el CONACYT por ejemplo, (i) necesitan proporcionar fondos sostenibles en el largo plazo destinados a la educación y seguridad cibernética, (ii) deben ser conscientes de la importancia de la ciberseguridad, y (iii) deben asignar fondos para proyectos multidisciplinarios. Esto debe cubrir los programas técnicos, pero también educativos. En razón de los fondos limitados para investigación, muchas personas necesitan trabajar y estudiar al mismo tiempo. La mesa de discusión del Gobierno señaló la importancia de una articulación entre academia, sector privado y los entes públicos para el financiamiento de proyectos de I+D+i. En este contexto, sería importante tener una mejor comprensión de la actual situación de la oferta en el país de I+D+i. La mesa de discusión del sector financiero sugirió revisar la conveniencia de crear un Foro de discusión y análisis con las múltiples partes interesadas para abordar los asuntos de ciberseguridad mediante la investigación, el desarrollo y la innovación.

Específicamente, la seguridad cibernética debe agregarse a la lista de prioridades del CONACYT y del sistema nacional de investigadores (SNI) acompañada de recursos suficientes. Se podría desarrollar una investigación sobre los derechos humanos en línea en México. Hay una gran cantidad de información general, por ejemplo, un estudio de la ONU de 2015 titulado "La ciber-violencia contra las mujeres y las niñas", pero este estudio no es enfocado en México, y hay otros grupos más vulnerables a considerar. Los grupos de la sociedad civil deberían disponer de financiación para la investigación de temas, tal como la privacidad de los datos relacionados con la violencia doméstica y la violencia de género. Actualmente sus investigaciones están siendo financiadas por fundaciones estadounidenses

y europeas. Por ejemplo, "porno venganza" es un problema, pero no está claro dónde la gente puede buscar ayuda (incluyendo a los sitios de medios sociales).

2.4. Estándares y Criterios Técnicos

La mesa de discusión de la sociedad civil, de los derechos humanos y de la mesa de discusión del usuario final cree que el cumplimiento de ISO 27000 casi se ha logrado en México. Sin embargo, los participantes recomendaron que el Gobierno colaborara más con el sector privado, para fomentar una relación de confianza y colaboración en caso de robo de datos.

La mesa de discusión de Gobierno recomendó que se analizara la pertinencia de aplicar los estándares y buenas prácticas internacionales. De ahí la importancia que subrayaron algunos expertos de ampliar el objetivo de política internacional de la estrategia. Por ejemplo, sería importante conducir una revisión de los estándares y criterios técnicos que serían aplicables en cada sector. La mesa de discusión del sector financiero recomendó que una entidad coordinadora nacional se encargue de identificar y compilar los estándares y criterios técnicos que aplican por sector económico, ya que por ejemplo en el sector financiero existen diversos estándares, metodologías y procedimientos relacionados con la gestión de riesgos.

También se recomendó generar estándares diferenciados para las entidades de los niveles federal, estatal y municipal, teniendo en cuenta en nivel de madurez de cada entidad. La mesa de discusión de Gobierno sugirió que se desarrolle el modelo de madurez en ciberseguridad a nivel de la Administración Pública Federal, y que ese modelo sea ampliado y aplicado a los Estados y Municipios.

2.5. Marco Jurídico

La mesa de discusión de la academia indicó la necesidad de entender las ramificaciones legales de lo que la estrategia requiere, incluyendo si la legislación puede ser reformada para estar en línea con la estrategia y cómo sería esta reforma. Un ejemplo que se discutió es la necesidad de responsabilidades legales por la violación de datos.

La mesa de discusión de la sociedad civil, de los derechos humanos y de los usuarios finales recalcó que se debería considerar la posibilidad de ratificar el Convenio de Budapest, dado que el delito cibernético no se limita al nivel nacional, sino es un problema mundial. Para la mesa de discusión de Gobierno, sería importante conducir un análisis y adecuación normativa de la tipificación de los delitos, a modo de garantizar su compatibilidad con la Convención de Budapest. No obstante el documento de la ENCS menciona la importancia del intercambio de información, la mesa de discusión del Gobierno señaló que sería interesante establecer normas para el intercambio de información, así como para el fortalecimiento institucional de las entidades que actúan con la ciberseguridad.

Además de modificar la legislación nacional, es importante garantizar que todos los actores pertinentes del sistema de justicia penal (jueces, magistrados, fuerzas de seguridad, etc.) estén suficientemente capacitados en materia de pruebas digitales y cadena de custodia. Particularmente, es importante entender cómo se presenta la evidencia digital en un caso, ya que en algunos casos este tipo de evidencia ha sido rechazada durante el proceso penal. Esto debería incluir una asignación suficiente de fondos en los presupuestos pertinentes para la capacitación, la aplicación de la ley y la investigación. Otra consideración es desarrollar una carrera clara para la ciberseguridad dentro del sistema de justicia penal.

Se sugiere consultar con el sector financiero asuntos particulares relacionados con los mecanismos de autenticación únicos y su implicación con la ciberseguridad.

La mesa de discusión de la sociedad civil también reconoció que, si bien existe un marco jurídico para la protección de datos, no existen mecanismos suficientes para garantizar el cumplimiento de los

requisitos de presentación de informes cuando existe una violación de datos. También debe hacerse referencia a que México se adhiera a las normas internacionales sobre derechos humanos y protección de datos.

La mesa de discusión de la sociedad civil también destacó los cambios recientes en la legislación de protección de datos del país. De acuerdo con la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados* (Nueva Ley DOF 26-01-2017) el artículo 74 establece:

> *'Artículo 74. Cuando el responsable pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a su juicio y de conformidad con esta Ley impliquen el tratamiento intensivo o relevante de datos personales, deberá realizar una Evaluación de impacto en la protección de datos personales, y presentarla ante el Instituto o los Organismos garantes, según corresponda, los cuales podrán emitir recomendaciones no vinculantes especializadas en la materia de protección de datos personales...'*

Dado que el cumplimiento de las recomendaciones emanadas de estas consultas no es vinculante, se recomendó que se desarrollen mecanismos para asegurar que la implementación de estas recomendaciones cuente con un adecuado monitoreo y seguimiento.

3. Comentarios Generales

3.1. Alcance de la ENCS

Se recomienda aclarar el alcance de la estrategia, en términos de lenguaje. Por ejemplo, si hay una posición política que debe tenerse en cuenta, esto debe ser claramente expresado para que el entienda el alcance y enfoque. La mesa de discusión de la Sociedad Civil reconoció que tener una estructura para la ENCS con objetivos y temas transversales fue un buen enfoque.

Hay una preocupación por parte de los participantes de que los conceptos de seguridad de la información y ciberseguridad están siendo confundidos. Igualmente se destacó que la ENCS debería enfocarse en la prevención en lugar de la protección. Además, la mesa de discusión de la sociedad civil destacó la necesidad de incluir los derechos humanos en la visión de la estrategia. En este contexto, la mesa de discusión destacó que se debería incluir no sólo los derechos a la libertad de expresión o privacidad, sino también el derecho a la salud y acceso a la educación y cultura, así como a la infraestructura cibernética. También se destacó que el Gobierno debe establecer políticas que permitan el auto-empoderamiento del usuario.

Se recomendó aclarar qué significa ser un "actor relevante".

Con respecto a la visión de la estrategia, la mesa de discusión del sector financiero considera que la misma debe reflejar realmente lo que el Gobierno de México pretende alcanzar con la ejecución de todas las acciones en conjunto al final de periodo de tiempo definido. Se recomienda revisar las definiciones de *"ciberataque"* y *"ciberseguridad"* para México con el fin de corroborar si están acorde con el alcance de la estrategia y si incluyen todos los ámbitos que debe abarcar la misma; por ejemplo, revisar si el país sólo debería estar preparado ante ciberataques o también ante ciberamenazas o ante incidentes cibernéticos o ante las múltiples y diferentes manifestaciones del ciberdelito. Se recomienda revisar si el país solamente será relevante en *"mejores prácticas en la cultura"* o si debería también ser actor relevante en otras áreas en el marco de la ciberseguridad. Al parecer se refiere exclusivamente a asuntos relacionados con la cultura. Se recomienda revisar si para el Gobierno de México la condición de *"un país mejor preparado"* es suficiente o si la misma debería ser más ambiciosa en el periodo de tiempo establecido.

3.2. Enfoque Basado en el Riesgo

La mesa de discusión de la academia consideró que los riesgos debían considerarse no sólo desde la tecnología, sino también desde los procedimientos y las personas. El tema de la gestión de riesgos se destacó particularmente en la sección de Seguridad Nacional. El grupo discutió el hecho de que la información sobre seguridad nacional exige un nivel de protección particularmente alto, ya que ofrece mayor riesgo si se compromete. El grupo de trabajo también expresó su preocupación por las prácticas de adquisición y los vendedores de terceros, particularmente en lo que respecta a la información de Seguridad Nacional, y la necesidad de asegurar que cualquier persona que trabaje con el gobierno mantenga altos estándares de seguridad cibernética.

La mesa de discusión de Gobierno sugirió la elaboración de un catálogo de infraestructuras críticas de la información. Se recomendó

homologar una metodología para análisis de riesgo e instrumentos de retroalimentación dentro del marco del Manual Administrativo de Aplicación General en las materias de tecnologías de la información y comunicaciones (MAAGTICSI).

La mesa de discusión del sector financiero recomendó la generación de una estrategia integral de protección y defensa de la infraestructura crítica en el país, que adelante las siguientes acciones específicas con el fin de implementarla: la creación de una guía para identificar la IC en cada sector, la posterior identificación de la IC, la creación de un catálogo de IC nacional, la actualización periódica de dicho catálogo y la definición del grado de criticidad de las IC definidas en el catálogo.

3.3. Terminologías

Las terminologías deben ser estandarizadas en toda la legislación / documentación mexicana. Especialmente para que en el futuro las nuevas leyes no reemplacen o cambien la comprensión del texto que se acuerda. Se recomienda buscar definiciones, estándares y documentos internacionales. La Academia quisiera ser incluida en el desarrollo del glosario. Hay una preocupación de que las definiciones a veces conducen a interpretaciones más subjetivas.

Es importante incluir la definición de "seguridad nacional" para proteger los derechos humanos y evitar que la seguridad nacional se use como justificación para acciones de vigilancia. Existe la preocupación de que la seguridad nacional se haya utilizado como justificación de muchos actos que atentan contra los derechos humanos. La definición de seguridad nacional podría tomarse de la Ley de Seguridad Nacional. Los participantes destacaron la importancia de definir claramente las siguientes palabras: acoso cibernético; ciberterrorismo; infraestructuras críticas; diferencia entre seguridad de la información y ciberseguridad (por ejemplo, infracciones de datos personales, infracciones de seguridad que afectan a la propiedad intelectual o secretos comerciales). Además, se recomendó ampliar la definición de datos personales para incluir cómo se define a una persona, así como incluir definiciones sobre seguridad de la información económica y financiera.

Según la mesa de discusión de Gobierno, es necesario debatir y asegurar que el glosario contiene las definiciones que realmente serán aceptadas por todas las partes interesadas en la estrategia. Las mismas deben ser "neutrales" en cuanto a actores se refiere y deben poderse definir de forma tal que no permitan diferentes interpretaciones en función del actor que la observe.

Respecto al Glosario, la mesa de discusión del sector financiero concluyó que se debe revisar en detalle el listado de términos empleados a lo largo de la estrategia con el fin de que ayuden a dar un mayor contexto o detalle sobre la misma. Se recomienda que las definiciones sean concisas y claras, que sean aceptadas por todas las múltiples partes interesadas en México, que no se excedan de un párrafo y que se presenten en orden alfabético. Finalmente, se recomendó incluir enlaces al glosario para proporcionar más información.

3.4. Gobernanza

Es fundamental que la estrategia de ciberseguridad tenga un marco de gobernanza claro que defina las funciones y las responsabilidades de los distintos actores, y que establezca como se dará la rendición de cuentas. El modelo de gobernanza también debe proporcionar un marco para el diálogo entre los distintos actores y la coordinación de diversas actividades emprendidas en el ciclo de vida de la estrategia. La coordinación para la implementación de la estrategia puede darse a través de una agencia pública asignada/creada específicamente para liderar la ciberseguridad en el país, y/o de distintas entidades públicas en que cada una tiene un papel definido. Por ejemplo, mientras una entidad sería encargada de desarrollar políticas de concientización y capacitación en ciberseguridad, otra sería responsable por la protección de infraestructuras críticas.

Con respecto a este último modelo caracterizado por una descentralización, algunos países optaron por la creación de una comisión interinstitucional

o interministerial que reúna las distintas entidades públicas de manera a garantizar una mejor coordinación de esfuerzos. Además de una comisión, algunos países también establecieron la figura de un Coordinador Nacional, como es el caso de Australia, Colombia y los Estados Unidos, a fin de mejor centralizar el liderazgo en la implementación de la estrategia y coordinar con los actores nacionales pertinentes. Esta autoridad central de ciberseguridad es generalmente tiene amplias responsabilidades y competencias en todos los sectores.

COORDINADOR NACIONAL

Se recomienda que el Coordinador Nacional de Ciberseguridad sea nombrado por el Presidente de la República y que tenga experiencia en la ejecución de programas de gran complejidad a nivel nacional. También se recomienda que el Coordinador tenga una visión general de la ciberseguridad o conocimiento acerca de las tecnologías de información y comunicación. En general, para garantizar la eficacia de esta función, el Coordinador Nacional de Ciberseguridad debe, entre otras cosas:

- Tener la autoridad conferida por el Presidente para asegurar que la ciberseguridad en México es operacionalmente efectiva y que se desarrolle según se requiere, en el marco de los objetivos establecidos en la ENCS;
- Tener la autoridad para asegurar que los diversos departamentos gubernamentales implementan sus objetivos y son responsables de su desempeño ante el Coordinador. Tenga en cuenta que la función del coordinador no es operativa, pero tiene la responsabilidad de verificar los objetivos operativos y coordinación de actividades por todas los actores relevantes;
- Asegurar la distribución de nuevo presupuesto, de acuerdo con los planes del programa;
- Fomentar la cooperación entre el sector público, el sector privado, academia y sociedad civil para la formulación e implementación de políticas de seguridad cibernética;
- Coordinar la preparación de reportes periódicos sobre el avance en la implementación de la ENCS.

ROLES Y RESPONSABILIDADES

Es importante determinar un modelo de gobernanza para asegurar que la ENCS se implemente de manera efectiva que y todos los actores nacionales relevantes entiendan sus roles y responsabilidades. En este contexto, es importante comprender un ejercicio de mapeo de los interesados y alinear la implementación de los objetivos de estratégicos con los actores nacionales más relevantes.

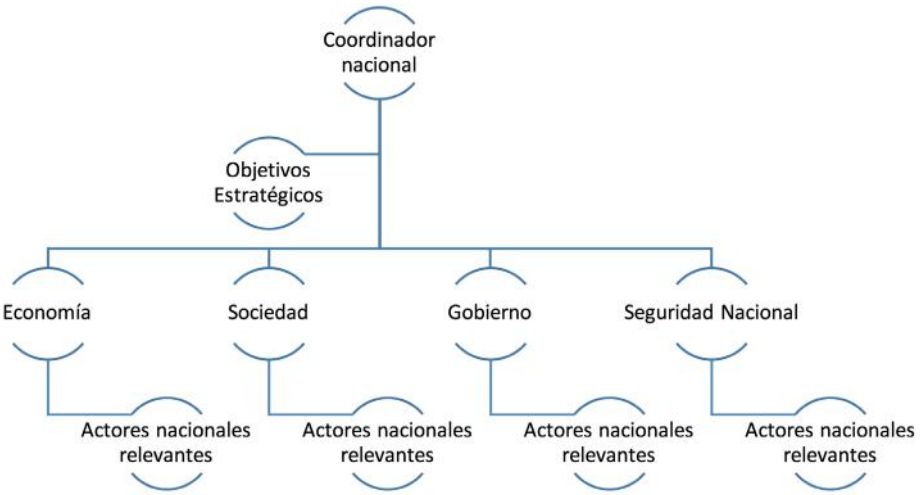

Gráfico 2 - El ejercicio de mapeo de las partes interesadas

Con el objetivo de fomentar una mejor colaboración entre los demás actores nacionales, algunos países establecen en sus estrategias nacionales la conformación de comités técnicos o grupos de trabajo con entidades invitadas para tratar de asuntos específicos. A título de ilustración, en España actores relevantes del sector privado y especialistas, cuya contribución se considere necesaria, pueden participar del Comité Especializado de Ciberseguridad.[3] En los Países Bajos, por ejemplo, se implementó un modelo de participación multisectorial a través de la creación de un Consejo de Ciberseguridad compuesto por representantes del gobierno, sector privado y de la comunidad científica. Este consejo proporciona recomendaciones, no vinculantes, en temas de ciberseguridad al gobierno.[4]

MODELOS EN OTROS PAÍSES

Diferentes estructuras pueden ser adoptadas como las que se enumeran a continuación:

Australia	Estrategia de Ciberseguridad de Australia (2016)	Coordinación de Políticas: Asesor Especial del Primer Ministro en Ciberseguridad: lidera la aplicación de la Estrategia de Ciberseguridad y fomenta la creación y el fortalecimiento de asociaciones entre el gobierno australiano, el sector privado, las organizaciones no gubernamentales y el mundo académico para proporcionar capacidad nacionales en ciberseguridad. Órganos Operacionales (ej.): CERT Australia: principal punto de contacto para las cuestiones de ciberseguridad que afectan a las principales empresas australianas, incluidos los propietarios y operadores de la infraestructura crítica de Australia y otros sistemas de interés nacional. Centro de Crimen de Alta Tecnología de Australia: responsable de investigar crímenes de tecnología.

[3] Gobierno de España. Presidencia del Gobierno. Estrategia de Ciberseguridad Nacional 2013. "El Comité Especializado de Ciberseguridad dará apoyo al Consejo de Seguridad Nacional para el cumplimiento de sus funciones y, en particular, en la asistencia al Presidente del Gobierno en la dirección y coordinación de la Política de Seguridad Nacional en el ámbito de la ciberseguridad. (...) La composición del Comité Especializado de Ciberseguridad reflejará el espectro de los ámbitos de los departamentos, organismos y agencias de las Administraciones Públicas con competencias en materia de ciberseguridad, para coordinar aquellas actuaciones que se deban abordar de forma conjunta (...) En el Comité podrán participar otros actores relevantes del sector privado y especialistas cuya contribución se considere necesaria", p.44

[4] Información disponible en: https://www.cybersecurityraad.nl/index-english.aspx Acceso en 2 de agosto de 2017.

Canadá	Estrategia de Ciberseguridad de Canadá (2010)	Coordinación de Políticas: Seguridad Pública Canadá: coordina la implementación de la Estrategia Órganos Operacionales (ej.): Centro de Respuesta a Incidentes Cibernéticos (Seguridad Pública): punto focal para monitorear y brindar asesoramiento para mitigar las amenazas cibernéticas y dirigir la respuesta nacional. Servicio Canadiense de Inteligencia de Seguridad: investiga las amenazas nacionales e internacionales. Policía Montada Real de Canadá: investiga los actos delictivos contra redes canadienses e infraestructuras críticas. Secretaría del Consejo del Tesoro: fortalecer las capacidades de gestión de incidentes cibernéticos mediante el desarrollo de políticas, normas y herramientas de evaluación; Responsable del Gobierno de Canadá IT.
Colombia	Política Nacional de Seguridad Digital (2016) CONPES 3854	Coordinación de Políticas: Coordinador nacional de seguridad digital: El coordinador nacional de seguridad digital tendrá a su cargo un equipo de apoyo operativo intersectorial, el cual estará conformado por representantes de, al menos, las siguientes entidades: Ministerio de Tecnologías de la Información y las Comunicaciones, Ministerio de Defensa Nacional y la Dirección Nacional de Inteligencia. Órganos Operacionales (ej.): Centro Cibernético Policial (CCP): responsable de garantizar la integridad de las redes policiales y de la sociedad civil. Comando Conjunto Cibernético (CCOC) o el Comando Cibernético Conjunto: responde a ataques contra los activos militares de la nación. ColCERT: Entidad de coordinación a nivel nacional que afronta todos los aspectos de la ciberseguridad y la ciberdefensa.

Estonia	Estrategia de Ciberseguridad (2014–2017)	Coordinación de Políticas: Consejo de Seguridad Cibernética del Comité de Seguridad del Gobierno de la República: apoyar la cooperación interinstitucional de nivel estratégico y supervisar la aplicación de los objetivos de la Estrategia de Seguridad Cibernética mediante el seguimiento del progreso de la implementación de los objetivos establecidos en el Plan de Implementación. Órganos Operacionales (ej.): Autoridad del Sistema de Información de Estonia (RIA): desarrollar estándares para la implementación de la seguridad de la información y supervisar su implementación, enfocándose principalmente en asegurar la ciberseguridad de los proveedores de servicios vitales. Ministerio del Interior y el Ministerio de Asuntos Económicos y Comunicaciones: cooperar con otros ministerios responsables de los diferentes sectores de infraestructuras críticas para implementar medidas de seguridad. CERT-EE: responsable de la gestión de incidentes de seguridad en redes informáticas .ee.
Los Países Bajos	Estrategia Nacional de Ciberseguridad (NCSS)2 (2013)	Coordinación de Políticas: El Consejo de Seguridad Cibernética: proporciona asesoramiento solicitado y no solicitado al gobierno, y también tiene como tarea garantizar el cumplimiento de la Estrategia Nacional de Ciberseguridad. Enviado Especial para la Ciberpolicia Internacional: con especial énfasis en un Internet libre, abierto y seguro, así como un ciberespacio seguro y estable. Órganos Operacionales (ej.): Centro Nacional de Seguridad Cibernética (CCSN): asesora a las partes privadas y públicas, tanto cuando se les solicita como por iniciativa propia, cuando se detectan vulnerabilidades importantes o en caso de situaciones de crisis (inminentes).

Estados Unidos	Estrategia de Ciberseguridad y Plan de Implementación 2015	Coordinación de Políticas: Coordinador de Seguridad Cibernética de la Casa Blanca: responsable de coordinar todas las actividades de seguridad cibernética en todo el gobierno.[5] Órganos Operacionales (ej.): Equipo Federal de Operaciones de Seguridad Cibernética de los Estados Unidos: Departamento de Justicia (DOJ) - Líder en investigación y aplicación de la ley. Departamento de Estado (Departamento de Estado) - Oficina del Coordinador de Asuntos Cibernéticos encargada de coordinar todo el espectro de cuestiones relacionadas con el ciberespacio, incluyendo la seguridad, las cuestiones económicas, la libertad de expresión y el libre flujo de información en Internet. Departamento de Seguridad Nacional (DHS, por sus siglas en inglés): responsable por actividades centradas en cuestiones nacionales de ciberseguridad e interactuar con operadores privados de infraestructuras críticas y recursos claves del país. El DHS es la agencia federal responsable por coordinar los esfuerzos de infraestructura crítica. Departamento de Defensa (DoD) – reponsable por defender las redes, sistemas e información del Departamento de Defensa, defender el país contra ataques cibernéticos de impacto significativo, y por proporcionar apoyo cibernético a los places operacionales militares.

[5] El primer ciber czar del gobierno de Estados Unidos fue nombrado en 2001 (Asesor Especial del Presidente en Cberseguridad, Oficina de Gestión y Presupuesto). En 2008, su título cambio para Director Nacional de Seguridad Cibernética, y en seguida para Director de la Oficina de Ciberseguridad de la Casa Blanca, Coordinador de Ciberseguridad en 2009.

España	Estrategia de Ciberseguridad Nacional (2013)	Coordinación de Políticas: Consejo Nacional de Ciberseguridad: Es un órgano colegiado de apoyo al Consejo de Seguridad Nacional en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional, en el marco de la Ley 50/1997, de 27 de noviembre, del Gobierno. El Consejo Nacional de Ciberseguridad se crea por Acuerdo del Consejo de Seguridad Nacional del 5 de diciembre de 2013. Órganos Operacionales (ej.): INCIBE: El Instituto Nacional de Ciberseguridad de España (INCIBE), para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos. Respuesta nacional a incidentes proporcionada por CNN-CERT and CERTsi (entre otros).

3.5. Implementación ('Plan de Acción')

Según los participantes de la academia, hay una falta de datos fiables sobre el acceso a Internet. Es importante establecer métricas para poder evaluar los diferentes parámetros de uso de las tecnologías, así como para conducir la gestión de riesgo, como recomendado por la Organización para la Cooperación y el Desarrollo Económico (OCDE). El Instituto Nacional de Estadística y Geografía (INEGI) estaría mejor preparado para hacer las mediciones. En la mesa de discusión se destacó los aspectos positivos del trabajo conjunto del INEGI y del Instituto Nacional de Desarrollo en el proyecto de datos abiertos.

También se mencionó la importancia de definir metas a corto, mediano y a largo plazo para cada una de las esferas del marco estratégico. En este contexto, sería importante aclarar lo que se entiende por corto plazo, ya que se interpreta como algo inmediato. Asimismo, hay que identificar e implementar mecanismos de reporte de información y retroalimentación sobre el avance en los indicadores que se establezcan para la estrategia. Se recomendó fortalecer la Función Pública para mejorarlos mecanismos de auditoría y acompañamiento.

Igualmente hay una preocupación por el futuro de la ENCS cuando haya cambio del gobierno. Es importante que el Gobierno dé continuidad a la estrategia de seguridad cibernética, de lo contrario se trataría de una pérdida de recursos.

La mesa de discusión del sector financiero recomendó revisar la redacción de las acciones de este eje con el fin de que las mismas describan acciones concretas, identificando explícitamente las entidades (o actores) responsables, un presupuesto estimado y el horizonte de tiempo para su ejecución. Se aprecia que la mayoría de acciones no son concretas en la generación de un producto final que sea medible al realizar el seguimiento a la implementación de la estrategia. Se usan verbos muy generales como estimular, promover o establecer.

Apéndice - Comentarios a la ENCS
(Documento adjunto)

Secretario General
Luis Almagro Lemes

Secretario General Adjunto
Nestor Méndez

Secretaria de Seguridad Multidimensional
Claudia Paz y Paz

Secretaria Ejecutiva Comité Interamericano contra el Terrorismo
Alison August Treppel

Equipo Técnico

Programa Ciberseguridad de la OEA
Belisario Contreras, Gerente de Programa
Kerry-Ann Barrett, Especialista
Barbara Marchiori de Assis, Especialista

Expertos Invitados por la SG/OEA
Alessandro Gemmiti, Gerente de Proyectos, Institución Asuntos Globales, Canadá.
Andres Rengifo, Unidad de Crimen Digital y Propiedad Intelectual, Microsoft.
Camino Kavanagh, Consultor Experto, España.
Carlos Alvarez, Snr Manager, Compromiso de Seguridad, Cooperación de Internet para la Asignación de Nombres y Números (ICANN).
Cynthia Wright, Ingeniero Principal de Seguridad Cibernética, La Corporación MITRE.
Daniel Alvarez, Asesor de Ciberseguridad en la Subsecretaría, Ministerio de Defensa, Chile.
Elizabeth Vish, Consejero político, Departamento de Estado de los Estados Unidos (S / CCI).
Félix Barrio, Jefe de Investigación y Desarrollo, Instituto Nacional de Ciberseguridad de España (INCIBE).
Francisco Vera, Consultor Experto, Global Partners Digital.
Johanna Vazzana, Líder en Cibernética Internacional, La Corporación MITRE.
Jorge Bejarano Lobo, Consultor Experto, Colombia.
Juan Martinez, Asesor de Políticas, Oficina del Coordinador de Asuntos Cibernéticos Departamento de Estado de los Estados Unidos.
Laurent Bernat, Analista de políticas, Organización para la Cooperación y el Desarrollo Económicos (OCDE).
Lina Ornelas, Directora de Políticas Públicas y Relaciones Gubernamentales, Google México.
Orlando Garces, Representante, Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MINTIC)
Victoria Grove, Representante, Ciberseguridad Internacional, Dirección de Seguridad Nacional UKFCO

Esta iniciativa cuenta con el apoyo financiero del Gobierno de Canadá

OEA

Más derechos para más gente

PROGRAMA DE CIBERSEGURIDAD

Comité Interamericano contra el Terrorismo

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS

1889 F Street N.W.
Washington, D.C. 20006
P. 202 370 4674
F. 202 458 3857
cybersecurity@oas.org
@OEA_cyber