OEA Más derechos para más gente

MÉXICO
PRESIDENCIA DE LA REPÚBLICA

Documento de trabajo ENCS v.1

Tabla de Contenido

I. Introducción

Estrategia Nacional de Ciberseguridad (ENCS)

Es el plan estratégico impulsado por el Gobierno de la República, que se está elaborado en colaboración de diferentes actores: gobiernos, sector privado, comunidad técnica, sociedad civil y academia, con el que se pretende sumar y unificar esfuerzos para propiciar un entorno seguro, libre, confiable y resiliente ante el uso de las Tecnologías de la Información y Comunicación (TIC) coadyuvando al desarrollo sostenible de México.

Comentarios (Academia): La responsabilidad de los intermediarios no se incluye en este documento. Además, es importante aclarar quien estará liderando la implementación de esta estrategia. Se necesita identificar los responsables por la implementación de la estrategia. Por ejemplo, falta en este documento una entidade coordinadora compuesta por Ministros y Secretarios de Estado para fomentar este documento. Se recomienda aclarar como se dará la implementación de la estrategia, en particular teniendo en cuenta que se llevan 4-5 meses para implementar el presupuesto. Asimismo, es importante aclarar los próximos pasos con respecto al proceso de desarrollo de la estrategia nacional de ciberseguridad.

II. Diseño Colaborativo de la ENCS

1. Contexto de Asistencia Técnica OEA (19-20 abril, Ciudad de México)

El Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (OEA), a través de su Programa de Seguridad Cibernética, convocó una comisión de expertos internacionales para compartir las mejores prácticas con las principales entidades mexicanas para mejorar las capacidades nacionales de seguridad cibernética en el país. Esto se facilitó mediante el uso de un formato de discusión de mesa redonda con la intención de fomentar el diálogo entre el Gobierno, varios interesados nacionales y expertos internacionales para comprender el estado actual de la seguridad cibernética en México y avanzar en la construcción y definición de un **Marco Nacional de Seguridad Cibernética.**

El taller ***"Hacia una Estrategia Nacional de Ciberseguridad"***, encabezado por el Gobierno de la República y con el acompañamiento técnico del Programa de Seguridad Cibernética de la Organización de los Estados Americanos (OEA)[1] con el financiamiento del gobierno de Canadá, 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 intercambiaron entidades mexicanas y actores de la industria, la academia y organizaciones de sociedad civil para mejorar las capacidades nacionales de ciberseguridad del país.

Este primer ejercicio de consulta tuvo como objetivo identificar las inquietudes de los diversos sectores que permitan la definición de la *Estrategia Nacional de Ciberseguridad* de nuestro país, con apego a los más altos estándares internacionales:

- Las discusiones se centraron en el intercambio de experiencias y mejores prácticas.

[1] La Secretaría del CICTE emplea un enfoque integral en la construcción de capacidades de seguridad cibernética entre los Estados Miembros, reconociendo que la responsabilidad nacional y regional para la seguridad cibernética cae sobre una amplia gama de entidades tanto del sector público como el privado, los cuales trabajan en aspectos políticos y técnicos para asegurar el ciberespacio.

- Se identificaron un total de cinco (5) temas, que fueron discutidos en cada mesa redonda en detalle.

- Las discusiones en cada mesa fueron facilitadas por un moderador asignado y un tomador de notas, ambos expertos internacionales. Los siguientes temas fueron identificados para cada mesa redonda (enumerados sin orden de prioridad):

  1) Investigación y Desarrollo; 2) Cultura, Educación y Prevención; 3) Cooperación y Coordinación; 4) Normas, Criterios Técnicos y Regulación; y 5) Marco Legal.

Las conclusiones de las mesas de trabajo se enlistan como:

1. México ya tiene varias políticas y legislación relacionadas con las TIC y la seguridad de la información en funcionamiento. Estos deben ser tomados en cuenta como una buena base para el desarrollo de un marco nacional de seguridad cibernética.

2. El marco nacional de seguridad cibernética y su aplicación deben respetar principios fundamentales como la privacidad, la libertad de expresión, la proporcionalidad, entre otros.

3. El liderazgo fuerte es importante para el desarrollo e implementación exitosa del marco nacional de seguridad cibernética.

4. El proceso de desarrollo e implementación debe adoptar un enfoque de múltiples interesados, basado en la confianza y la transparencia.

5. México debería considerar un organismo nacional dinámico de coordinación de seguridad cibernética/digital que involucre a todos los sectores gubernamentales, con protocolos para involucrar a actores de la industria, la academia y la sociedad civil.

6. La adopción de mejores prácticas internacionales, normas y legislación modelo (como el Convenio de Budapest) puede facilitar mejor la cooperación internacional y la colaboración para la investigación de incidentes y delitos con otros actores regionales e internacionales.

2. Recomendaciones (OEA) para el Desarrollo de la Estrategia Nacional de Ciberseguridad

Entre las recomendaciones generales del documento elaborado por la OEA y de las principales conclusiones y recomendaciones de estas mesas redondas se encuentran las siguientes:[2]

1. **La seguridad cibernética no es un fin en sí misma, sino que sirve a objetivos particulares de alto nivel.** Se trata de un área compleja con diferentes dimensiones complementarias y superpuestas que se derivan de diferentes objetivos y que incluyen a diferentes tipos de interesados con diferentes culturas y modos de operación. Es importante utilizar conceptos fundamentales claros con terminologías específicas para poder distinguir estas dimensiones a lo largo de la estrategia y ser coherentes con ellas a medida que se desarrollan iniciativas más detalladas en varios niveles en el futuro. Estos conceptos fundamentales proporcionarán una base para que cada tipo de actor se centre en su área de prioridad y entienda sus roles y responsabilidades. También ayudarán a organizar la compilación de información recibida de, y transmitir mensajes claros a, varios públicos, durante el desarrollo e implementación de la estrategia.

2. **El marco estratégico debe establecer claramente los objetivos de alto nivel y explicar por qué son esenciales para el país ("visión").** La estrategia debe identificar y priorizar los objetivos a corto, mediano y largo plazo. Aunque constantemente emergen nuevos vectores de amenazas en el entorno digital, es importante que México siga centrado en la estrategia, formando y fortaleciendo sus bloques fundamentales clave y agregando iniciativas de manera incremental, en lugar de multiplicar iniciativas nuevas hacia muchas direcciones.

3. **Amarrar la estrategia** no solo a la política y al derecho nacionales (p. ej., El plan de desarrollo nacional, la política digital nacional, la ley de seguridad nacional) sino también **a los compromisos y obligaciones regionales e internacionales** (p. ej., económicos, comerciales, de derechos humanos, derecho humanitario, fuerzas de la ley, cooperación, seguridad internacional, incluida la prevención de conflictos y la creación de confianza).

4. **Debe ser apoyada por el más alto nivel del gobierno.** Un alto nivel de liderazgo facilitara un enfoque de todo el gobierno y ayudará a lograr el equilibrio adecuado entre partes del gobierno con competencias compartidas. Facilitará una clara asignación de funciones y responsabilidades durante el proceso de desarrollo de la estrategia.

5. La Estrategia debería establecer un **marco institucional claro** que garantice que las **responsabilidades y las modalidades de implementación sean claras** y que las **instituciones tengan la autoridad y los recursos para actuar**. El marco debe incluir un mecanismo fuerte de coordinación para asegurar que se establezca una estrategia coherente y una implementación de políticas a nivel de todo el gobierno. También debe identificar otros actores clave que son vitales para una implementación efectiva.

[2] Ver las Recomendaciones emitidas por los expertos y la comunidad nacional, en el documento que recopilado por expertos a petición de la OEA. Disponible en el siguiente enlace electrónico: http://www.oas.org/documents/spa/press/Recomendaciones-para-el-Desarrollo-de-la-Estrategia-Nacional-de-Ciberseguridad.pdf

6. Algunas áreas, como **la protección de la infraestructura crítica**, incluida la Protección de la Infraestructura Crítica de Información (CIIP), pueden requerir un enfoque de política específico que aborde la intersección entre la seguridad digital y la protección de la infraestructura crítica.

7. La **armonización de las leyes sobre delincuencia cibernética** combinada con iniciativas para facilitar una coordinación más rápida y efectiva entre los organismos encargados de hacer cumplir la ley y el sector privado es esencial. En consonancia con la Constitución de México y sus obligaciones internacionales y regionales, estas gestiones se deben desarrollar en un entorno en el que se respeten plenamente los derechos y libertades fundamentales de los ciudadanos.

8. México debe encontrar el **camino legislativo adecuado** que permita que se genere un entendimiento común de la aplicación de la legislación federal y estatal sobre delincuencia cibernética.

3. Taller con la comunidad nacional (1 y 2 junio)

Como parte de las actividades programadas para la construcción de la Estrategia Nacional de Ciberseguridad, los días 1 y 2 de junio se contó con la participación de distintos actores de la comunidad nacional, quienes compartieron sus ideas, visiones e inquietudes en materia de ciberseguridad.

En total, se efectuaron ocho mesas de trabajo, 4 para cada día del taller. El 1 de junio, la discusión se centró en el sector social, analizando los factores requeridos hacía una cultura de la ciberseguridad; mientras que, el 2 de junio, se centró en el sector económico, dando especial énfasis a la ciberseguridad como impulsor de la economía digital.

En dicho taller se identificaron prioridades que, de acuerdo a la comunidad nacional, deben ser atendidas en la Estrategia Nacional de Ciberseguridad. de las prioridades obtenidas destacan la necesidad de fortalecer la cultura, educación y colaboración entre sectores público y privado para dar atención más oportuna a los incidentes y gradualmente aumentar el grado de madurez en la materia.[3]

A. Prioridades sobre la protección de la población:

Durante el primer día del taller, tres de las cuatro mesas identificaron la educación y concientización de las personas en el entorno digital como un área prioritaria que debe ser atendida en el marco de la Estrategia Nacional de Ciberseguridad. De igual forma, tres de las cuatro mesas coincidieron en la idoneidad de que la Estrategia Nacional de Ciberseguridad considere a la participación multisectorial

[3] Ver el Apéndice con las gráficas de las prioridades obtenidas del taller 1 y 2 junio 2017, el cual se desarrolló de manera colaborativa entre actores de diferentes sectores.

como elemento clave para abordar los problemas relacionados con la ciberseguridad en el país.

Asimismo, la prioridad referente a la adecuación del marco legal que contribuya a la protección de los derechos de las personas en el entorno digital, tuvo lugar en dos de las cuatro mesas. Entre otras prioridades señaladas durante el primer día del taller, se encontraron: protección de infraestructuras críticas, conciencia en el manejo de datos personales, responsabilidad compartida, formación de recursos humanos especializados, coordinación y cooperación multidisciplinaria, sectorial e internacional, etcétera.

B. Prioridades sobre la protección de la economía:

Durante el segundo día del taller, en tres de las cuatro mesas se identificó como una prioridad que debe incluirse en la Estrategia Nacional de Ciberseguridad, la concientización sobre los riesgos a los que se enfrentan los usuarios al realizar actividades comerciales en línea.

En el mismo tenor, tres de las cuatro mesas hicieron referencia a la coordinación de acciones y la colaboración entre los distintos actores para hacer cara, en el marco de la economía digital, a los retos en materia de ciberseguridad. Asimismo, en dos de las mesas se hizo mención de la importancia que trae consigo la confianza proporcionada a los usuarios de Internet.

Otras prioridades fueron señaladas, tales como: creación de una política que delimite actores y responsabilidades, responsabilidades de los proveedores de servicios en línea, la armonización legislativa, incluyendo la adopción del Convenio de Budapest, el mejoramiento de modelos de respuesta a los ataques cibernéticos, la implementación de protocolos preventivos en el sector empresarial, etcétera.

4. Foro en el Senado, 11 julio 2017.

Con la presencia de diferentes actores; sociedad civil, academia, industria y gobierno, en el marco del proceso "Hacia una Estrategia Nacional de Ciberseguridad" se llevó a cabo un Foro en el Senado de la República, en el que se abordaron las siguientes mesas: Construyendo la política nacional de ciberseguridad; Mejores prácticas para la protección del ciberespacio; Cultura de ciberseguridad; y Propuestas y acciones a tomar: hacia un México ciberseguro.

Durante el Foro se expresaron temas por demás interesantes, destacando los siguientes:

- Los diferentes actores expresaron su convicción de que es necesaria y conveniente contar con una Estrategia Nacional de Ciberseguridad, que se construya con evidencia, de maneta colaborativa y continúe en revisión periódica bajo el modelo de múltiples partes interesadas.

- La política pública en la materia debe atender a la necesidad propia de México y los esfuerzos de entes públicos, privados y sociedad civil deben estar articulados de forma que la ENCS esté centrada en las personas, no en la tecnología, con lo cual se resaltó como una de las prioridades la construcción y consolidación de la Cultura de Ciberseguridad, misma que tendrá impacto en el ámbito de la seguridad nacional, de la economía, del gobierno y favorecerá al bienestar social y económico de México. como se dará la implementación Las diversas participaciones coincidieron en que es necesario contemplar recursos financieros, y sobretodo un constante esquema de colaboración y cooperación entre las diferentes instancias públicas, para establecer un canal de comunicación basado en la confianza entre sector privado, sociedad y sector público.

- Se precisó que es necesario llevar a cabo un esfuerzo de armonización legislativa que considere la perspectiva de Derechos Humanos como eje de la política y las posibles iniciativas, con la finalidad de fortalecer el actuar de las autoridades y aprovechar al máximo las capacidades con las que hoy día cuenta el país, coincidiendo en que cualquier proceso de modificación a los ordenamientos debe ser de manera colaborativa buscando un mejor escenario jurídico para el desarrollo digital, la innovación, competitividad y economía en general. Varias voces señalaron la importancia de que México se adhiera al Convenio 108 del Consejo de Europa, en materia de cibercrimen.

Comentarios (Industria): El Convenio 108 es de protección de datos personales, se sugiere corregir.

- Finalmente, diversos actores expresaron la importancia de poner especial atención en las medidas de concientización y educación para la población, especialmente para niñas, niños y adolescentes.

III. Visión y Objetivos

Comentarios (Academia): Se necesita trabajar en una cultura de prevención. Se recomienda aclarar cual sería el rol de la academia y lo que la academia necesita para hacer su trabajo para establecer una visión para la sociedad. Se mencionó el caso de Israel, dónde la Universidad de Tel Aviv tiene un papel en la creación de conocimiento y conciencia cultura en ciberseguridad para la nación.

Visión

México será, para el año 2030, un país mejor preparado y resiliente ante ciberataques, y un actor relevante en el escenario internacional en mejores prácticas en la cultura de ciberseguridad.

Comentarios (Industria): Se sugiere incluir la aproximación desde el riesgo en todo el documento. Revisar el documento desde la perspectiva de los ejes transversales. Y revisar redacción general porque hay errores. Falta sentido estratégico en el documento, mayor claridad y mejor redacción. Incluir ruta de implementación.

Comentarios (Sector Financiero): 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 el cibercrimen. 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.

Objetivo General

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.

Comentarios (Gobierno): Propuesta de cambio en el texto

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

Comentarios (Sector Financiero): Se recomienda revisar si el verbo "Propiciar" indica de la mejor manera la acción general (que se identifique con el plan de acción de la estrategia) que resolverá la problemática agregada en el país en torno a la ciberseguridad. Se recomienda revisar la conveniencia de definir el concepto de "Múltiples Partes Interesadas", con el fin de involucrar en el mismo concepto tanto a la población objetivo de la estrategia como a todos los actores encargados de adelantar las acciones establecidas de la estrategia. Por ejemplo, "Propiciar que las múltiples partes interesadas realicen sus actividades (...)". Se recomienda incorporar como múltiple parte interesada tanto a las Sociedades como a las Asociaciones. Se aprecia que en términos generales la estrategia nacional no incorpora de manera explícita y activa a la Sociedad Civil ni al Sector Privado, y por lo tanto no se aprecian en la estrategia obligaciones ni responsabilidades específicas para dichos actores. Se recomienda aclarar el significado de la expresión "de manera libre", ya que el grupo de trabajo no llegó a un consenso en su entendimiento. Se recomienda revisar la conveniencia de usar la frase "realicen sus actividades con el uso de las TIC, incluyendo el ciberespacio (...)", ya que se entendería que el ciberespacio es una TIC. Es decir, aclarar si se debe hacer mención específica a las actividades que se desarrollen en el ciberespacio, mediante el uso de las TIC. Se recomienda revisar la conveniencia de incluir que se realicen las actividades de manera "responsable", en adición a las demás formas de realizarlas.

Objetivos Secundarios:

A. Proteger a la población. Consolidar un entorno digital propicio para que las personas realicen sus actividades habituales y futuras, de manera segura, libre y confiable; y se beneficien del desarrollo digital para mejorar su calidad de vida, en un marco de respeto a sus derechos; favoreciendo la libertad de expresión, fomentando el respeto y responsabilidad del uso de las tecnologías, así como la privacidad y protección de datos personales, y proveyendo de medidas de protección y autoprotección para prevenir riesgos y amenazas y aminorar los efectos contra afectaciones a su persona, patrimonio o dignidad.

Comentarios (Sector Financiero): Se recomienda definir el objetivo como un planeamiento propositivo que plantee soluciones concretas, alcanzables y medibles respecto a la problemática particular identificada. Se recomienda definir de quien o de que se debe proteger la población. Se recomienda especificar quien debería "Consolidar un entorno digital propicio". Se recomienda hacer énfasis en el tema de generar confianza para el desarrollo de las actividades socioeconómicas en el entorno digital. Se recomienda revisar si el objetivo solamente está enfocado a las personas, dejando de lado a otras múltiples partes interesadas, como las organizaciones públicas y privadas, dado que en los otros tres (3) objetivos no se hace mención respecto a la protección de estos otros actores. Se recomienda aclarar que se entiende con "desarrollo digital". Se recomienda revisar el texto "favoreciendo la libertad de expresión" ya que se entendería que dicho derecho prevalecería entonces sobre el resto de derechos de los ciudadanos de México. Se sugiere "asegurando" o "protegiendo" la libertad de expresión. Se recomienda revisar si se están combinando varios aspectos en el objetivo con el fin de reestructurarlo, por ejemplo se mencionan los siguientes aspectos: i) la salvaguarda de derechos como la libertad de expresión, la privacidad y la protección de datos personales, ii) los deberes de las personas al adelantar actividades mediante el uso de las TIC, por ejemplo el respeto y la responsabilidad, iii) las herramientas que alguien debería proveer para adelantar dichas actividades, por ejemplo medidas de protección y autoprotección.

B. Impulsar la innovación y estimular la economía del país. Robustecer los esquemas de protección de la información y las infraestructuras del sector público y privado, contemplando la ciberseguridad como una palanca para la innovación y el crecimiento económico, desde un enfoque preventivo, de atención y seguimiento de incidentes de manera coordinada entre el sector privado y gobierno para fortalecer la información, infraestructura y patrimonio de individuos, empresas y finanzas públicas.

Comentarios (Sector Financiero): Se recomienda definir el objetivo como un planeamiento propositivo que plantee soluciones concretas, alcanzables y medibles respecto a la problemática particular identificada. Se recomienda especificar quien debería robustecer los esquemas de protección. Se recomienda especificar si este objetivo está dirigido a un grupo de múltiples partes interesadas o al total de las mismas. Se recomienda revisar si lo que se quiere transmitir es que la innovación en asuntos de ciberseguridad podría consolidarse como palanca para el crecimiento económico del país. Se recomienda revisar la expresión "fortalecer la información, infraestructura y patrimonio", dado que dicho verbo no parece ser usado adecuadamente en la frase. Se recomienda revisar el texto en su integridad ya que al parecer es redundante en su finalidad: robustecer esquemas de protección de información e infraestructura para fortalecer la información y la infraestructura.

Comentarios (Gobierno): Propuesta de cambio en el texto

*"**Impulsar la innovación y estimular la economía del país.** Robustecer los esquemas de protección de la información y las infraestructuras del sector público y privado, contemplando la ciberseguridad como una palanca para la innovación y el crecimiento económico, desde un enfoque preventivo, de atención y seguimiento de incidentes de manera coordinada entre el sector privado, la academia y gobierno para fortalecer la información, infraestructura y patrimonio de individuos, empresas y finanzas públicas."*

C. Garantizar la continuidad y seguridad de las Infraestructuras Críticas del Estado Mexicano. Identificar riesgos y amenazas a las infraestructuras críticas y sistemas de información de los diferentes entes públicos y aquellas relacionados con actividades de sectores estratégicos; mediante políticas, acciones, normas y protocolos claros para la administración de riesgos y el establecimiento de protocolos y esquemas de resiliencia adecuado para garantizar la continuidad de la operación de dichas infraestructuras y sistemas, tanto para aquellas del sector privado como las del sector público, considerando acciones específicas y especiales para aquellas Infraestructuras Críticas de Información que son vitales para mantener la seguridad nacional.

Comentarios (Sector Financiero): Se recomienda definir el objetivo como un planeamiento propositivo que plantee soluciones concretas, alcanzables y medibles respecto a la problemática particular identificada. Se recomienda aclarar que cuando se menciona que se busca "Garantizar la continuidad (...)" se refiere a la continuidad de la prestación de servicios mediante las mencionadas infraestructuras críticas. Se recomienda usar solamente el término infraestructura crítica ya que se mencionan también otros sistemas de información. Se recomienda homogeneizar la propiedad de las infraestructuras dado que al inicio del objetivo se mencionas las infraestructuras "de los diferentes entes públicos (...) y aquellas de sectores estratégicos" y al final se mencionan las infraestructuras "del sector privado como las del sector público". Se sugiere referirse solamente las infraestructuras críticas del Estado Mexicano, ya que en el momento de adelantar su identificación y catálogo se determinará la naturaleza de su propiedad. Se recomienda revisar la redacción del objetivo ya que plantearía una solución un poco confusa: "Identificar riesgos y amenazas a las infraestructuras (...), mediante políticas, acciones, normas y protocolos (...), considerando acciones específicas y especiales (...)". Se recomienda revisar la conveniencia de reestructurar el objetivo buscando más bien que el Gobierno nacional deberá adecuar las políticas, las acciones, las normas y los protocolos con el fin de que los propietarios de infraestructuras críticas identifiquen y gestionen los riesgos y las amenazas cibernéticas para mantener la seguridad nacional.

Comentarios (Gobierno): Se debe dar una discusión sobre alcance del concepto de infraestructura crítica y otras infraestructuras que hoy no están clasificada como IC (Ej. Infraestructra de las elecciones, que sería crítica en periodo electoral).

D. Fortalecer la colaboración y cooperación internacional. Consolidar los esquemas de diálogo, concertación y cooperación internacional, en una fórmula de acciones de diplomacia digital con el enfoque transversal de ciberseguridad; que fomente el intercambio de información, y de buenas prácticas, la cooperación técnica, el fortalecimiento mutuo de capacidades, la generación de medidas para la confianza, la transparencia y la estabilidad, el establecimiento de redes de contacto y la conjunción de campañas de prevención y formulación de alertas conjuntas.

Comentarios (Sector Financiero): Se recomienda aclarar si el responsable de consolidar dichos esquemas de diálogo, concertación y cooperación internacional es el Gobierno nacional. Se recomienda revisar si el objetivo solamente está enfocado al Gobierno nacional, dejando de lado a otras múltiples partes interesadas, como las organizaciones privadas como el sector financiero, la academia o la sociedad civil. Se recomienda también la consolidación de esquemas de "colaboración". Se sugiere incluir el término "diplomacia digital" en el Glosario.

Principios

Comentarios (Gobierno): No obstante se realizarán unos comentarios específicos a la propuesta de algunos de los principios, se requiere fortalecer la descripción de cada uno de ellos de forma tal que resulten muy claros en cuanto a su alcance. También se requiere revisar si el uso de estándares abiertos, que se discutió en la mesa, debería incluirse dentro del alcance del F o es uno nuevo.

La Estrategia contempla como principios rectores lo siguientes:

A. **Perspectiva de derechos humanos** en ciberseguridad y equidad de género para fortalecer en un marco de pleno respeto a los derechos de las personas.

B. Con enfoque de **Gestión de riesgos**.

C. **Centrada en las personas**, especialmente de niñas, niños y adolescentes;

D. **Participación abierta, multidisciplinaria y colaborativa** de los diferentes actores y sectores, con un enfoque transversal.

E. **Colaboración y cooperación** nacional e internacional (diplomacia digital).

F. **Potenciador de la innovación** y el desarrollo sostenible.

Comentarios (Gobierno): Se sugiere de incluir características como estándares abiertos, neutralidad en la red, etc.

Comentarios (Sector Financiero): Se recomienda identificar aquellos principios generales de la estrategia, como la garantía de respeto y protección de los derechos humanos al desarrollar cualquier acción de la estrategia, de aquellos principios operativos, como la gestión de riesgo en el desarrollo de las acciones, ya que unos son de una naturaleza y otros principios son de distinta naturaleza. Se recomienda complementar los textos tanto para identificar el principio como para describirlo, por ejemplo, el GTSF propone lo siguiente frente al primer principio listado: "A. Proteger los derechos humanos de los ciudadanos de México al realizar actividades socioeconómicas en el entorno digital." Se recomienda revisar la redacción de los textos ya que el grupo de trabajo tuvo inconvenientes en identificar a quienes iban dirigidos, por ejemplo al analizar la frase "Potenciador de la innovación (...)", se puede pensar en que la estrategia debería ser la potenciadora de la innovación o si debería ser la ciberseguridad. Se recomienda revisar si dichos principios se consideran realmente como principios rectores o si son más bien consecuencia de la implementación adecuada de la estrategia, en específico aquel llamado "Potenciador de la innovación y el desarrollo sostenible".

Etapas

Corto Plazo: El resto del 2017, lo cual implica la construcción de la ENCS en el resto del semestre.

Mediano Plazo: El resto de la Administración 2013-2018. La cual pretende dejar las bases para la implementación de la ENCS, con el fortalecimiento institucional y jurídico para fortalecer la coordinación al interior de la APF, y fortalecer la colaboración del Ejecutivo con los otros entes públicos, y con sectores privado, academia y social.

Largo Plazo: El seguimiento y actualización periódica de la ENCS para apuntalar los esfuerzos de México en materia de la Agenda 2030 para el Desarrollo Sostenible.

Comentarios (Sector Financiero): Se recomienda que en el corto plazo se identifiquen algunos pasos mínimos en el proceso de elaboración de la estrategia, como lo son: i) la evaluación y aprobación de la viabilidad de la elaboración de la estrategia, ii) la elaboración de un documento borrador que contenga una revisión general de consistencia jurídica y financiera, iii) la publicación y socialización de un documento para discusión con las múltiples partes interesadas, y iv) la aprobación de la estrategia bajo el trámite administrativo correspondiente. Se recomienda que en el mediano plazo se revise el texto "fortalecimiento institucional y jurídico para fortalecer la coordinación (...) y fortalecer la colaboración (...)" ya que se usa fortalecer tres veces. Se recomienda que en el largo plazo hacer mención a la efectiva implementación de todas las acciones que solucionen las problemáticas identificadas y que permitan alcanzar tanto los objetivos secundarios como el objetivo general de la estrategia alcanzado la visión propuesta para el año 2030.

IV. Naturaleza y Alcance

La ENCS es un documento de presencia y actualización constante, dada la evolución vertiginosa de las TIC y las cambiantes amenazas y riesgos, por lo que habrá de actualizarse con el apoyo de los diferentes actores involucrados de manera periódica, procurando siempre el apego a los principios de esta ENCS.

Comentarios (Gobierno): Se requiere introducción en cada capítulo como objetivo de protección. Segundo párrafo tiene sesgo de la seguridad de la información. Tener cuidado con el lenguaje o enfoque en el delicuente. Hay otros factores. Prescindir del segundo párrafo.

Comentarios (Sector Financiero): El grupo de trabajo considera que se debe comunicar de manera trasparente el nivel relacionado con el efecto vinculante que la estrategia tenga con las múltiples partes interesadas, en particular para las organizaciones públicas que tendrán alguna responsabilidad para la ejecución de alguna acción específica, ya que dichas entidades son las que tienen capacidad jurídica para ejecutar las funciones que le son propias de acuerdo con sus competencias y de acuerdo con el presupuesto que destinen para la ejecución de dichas acciones. El grupo de trabajo recomienda que la estrategia defina claramente los responsables directos e indirectos para realizar acciones en el marco de la implementación con el fin de hacer el debido seguimiento. De esta manera se logrará identificar a los actores específicos sobre los cuales recae la obligatoriedad en la ejecución de dichas acciones. Finalmente, se recomienda que la estrategia crea agentes, mecanismos y herramientas mediante las cuales se impulse la adopción de la estrategia nacional en los actores sobre los cuales la misma es voluntaria y cooperativa.

Obligatoria:

Será **obligatoria para el ejecutivo federal** dado que se busca emitir en el ámbito de atribución de la Administración Pública Federal (APF), considerando en todo momento el estricto apego a Derecho; respetando las atribuciones y considerando la capacidad presupuestaria del año en curso, buscando año con año fortalecer las acciones en la materia.

Comentarios (Gobierno): Describir un antecedente que indiqué porque la distinción de obligatoriedad y que sin menoscabo de esto, se desarrollará normatividad y regulación que genere obligatoriedad para actores que actualmente no resultan obligados por ser esta una estrategia y no otro instrumento que por su naturaleza tenga la capacidad de generar estas obligaciones.

Comentarios (Industria): Se sugiere señalar que esta estrategia debe incluirse en los programas presupuestales como acción de prioridad nacional (Plan Nacional de Desarrollo), y asegurar que se cuente con los recursos presupuestales para su implementación.

Además, la política nacional debe estar alineada con la experiencia internacional, utilizar estándares internacionales. Y también intragubernamental, interinstitucional con otros actores (multistakeholder). Preocupa cómo comprometer a las entidades federativas.

Se comentó la problemática de la comunicación intragubernamental (CERTs nacionales y locales). Se propone fortalecer los CERTs, con desarrollo de capacidades. Incluir acciones concretas de coordinación y comunicación, y maneras de involucrar a los estados. En esto se sugiere la participación del sector privado y participación legislativa para asignación de presupuesto.

Establecer acciones concretas para asignar recursos, presupuesto y responsabilidades, y establecer los mecanismos para ello. Y plantear cómo se establecerá el marco legal para asegurar esto, dentro de lo que sea factible y los tiempos. También se puede trabajar con lo que existe (por ejemplo, reconocer los ciberataques como tema de seguridad nacional e insertarlo en la política en esa materia). También se mencionó que podría emitirse una NOM en la que se establezcan las normas de la estrategia. Para esto sirve la ruta de implementación, con priorización de las acciones más importantes para la asignación de presupuesto. Todo esto podría incluirse en el eje transversal de coordinación.

De adopción voluntaria y cooperativa:

Para los **entes públicos**: En el ámbito de sus atribuciones y esfera de competencia o actuación se invita a los demás entes públicos, de los diferentes poderes y órdenes de gobierno, a que adopten la ENCS como marco de referencia y construyan una estrategia interna que tome en consideración los principios de la ENCS, las necesidades de la población nacional y contexto internacional, para que todo el sector público se comprometa con la seguridad y confianza de la población nacional ante el uso de las TIC.

Comentarios (Industria): Se sugiere que se incluya un compromiso de los gobiernos locales para la coordinación e implementación.

No será obligatoria para el **sector privado y sociedad** en general. Será de adopción solidaria y bajo esquemas de colaboración, en el entendido del compromiso social con el desarrollo digital seguro, libre y confiable para México

V. Estructura

La ENCS se ha venido construyendo con la participación de diversos puntos de vista de diferentes sectores y especialistas, de dicho proceso colaborativo se obtiene la siguiente estructura; misma que está conformada por 4 Objetivos Estratégicos y 8 Ejes Transversales que los abordan.

Comentarios (Sector Financiero): Se aprecia que los "objetivos estratégicos" propuestos tratan sobre cuatro (4) sujetos distintos no homogéneos, i) por una parte se menciona a la "economía" como un objetivo estratégico que puede considerar como un sistema en donde los actores interactúan con el fin de maximizar su beneficio, ii) por otra parte se mencionan a dos actores que pueden considerarse como partes interesadas de la estrategia nacional como objetivos estratégicos, siendo estos la "Sociedad" y el "Gobierno", y iii) finalmente se menciona a la "Seguridad Nacional" que al parecer se puede considerar en el país como un concepto que enmarca institucionalidad, actores, situaciones de normalidad, entre otras. Se aprecia que dichos "objetivos estratégicos", más bien dan el enfoque bajo el cual se deberían adelantar las acciones para cada eje transversal de la estrategia. Dado que la estrategia ya considera un objetivo general y unos objetivos secundarios, el GTSF recomienda revisar la conveniencia de usar el concepto de "dimensiones estratégicas" o "pilares estratégicos" en lugar de llamarlos "objetivos estratégicos", ya que los textos presentados para describirlos no reúnen las condiciones propias para llamarlos objetivos. Se asume que dichos "objetivos estratégicos" se refieren más bien a tipos de población que pertenecen a un grupo de partes interesadas, por ejemplo , se percibe que al hablar de "Economía" se hace relación a las acciones que se deben adelantar por parte de las organizaciones públicas y privadas de los sectores económicos de México; "Sociedad" hace relación con la población mexicana en general, haciendo énfasis en sociedad civil; "Gobierno" hace relación con la totalidad de los organismos estatales que ejercen el poder ejecutivo en México; y "Seguridad Nacional" hace relación con todas las instancias de seguridad nacional del país (que en algunos casos también pertenecen a la Administración Pública Federal -APF- de México). Se recomienda identificar más claramente las dimensiones estratégicas, que permitan articular el plan de acción propuesto con el objetivo general y los objetivos secundarios de la estrategia.

Objetivos Estratégicos

1. ECONOMÍA

Comentarios (Academia): No obstante los puntos de esta sección están buenos, se necesitará trabajar sustancialmente en la definición de los detalles. Importante considerar que el liderazgo en el sector privado es completamente distinto del liderazgo en el gobierno. Además, hay que se considerar que, si se imponen regulaciones gubernamentales de estándares de seguridad para la industria, estes estandáres pueden ser menos fuertes que los estándares ya implementados por muchas industrias. Es esencial considerar los aspectos económicos del Internet, tal como su uso para el comercio electrónico. Considerar la ciberseguridad en términos de riesgo y de su costo.

A medida que aumenta el uso de las TIC en las diferentes actividades de la sociedad, mientras se incrementan las operaciones en línea y se depende cada vez más de información digital, de las TIC o de estar conectado a Internet; aunado a la continua evolución, crecimiento y sofisticación de los incidentes informáticos y amenazas cibernéticas, al igual que la convergencia tecnológica, ponen de manifiesto la necesidad de adoptar las medidas y controles que permitan proteger al Estado Mexicano ante estas nuevas amenazas.

El papel que juegan las TIC -principalmente Internet- en la economía moderna es trascendental, y por ello es necesario implementar proyectos relacionados con el desarrollo y la innovación tecnológica, así como, políticas y estrategias para mantenerlo seguro para la población.

Se requiere promover acciones de innovación tecnológica, marco jurídico, cooperación internacional y desarrollo industrial; así como colaborar en acciones de formación de recursos humanos de alto nivel en la materia, a fin de crear una cultura de prevención e impulsar al país como una de las economías emergentes más proliferas.

OE	Eje Transversal	Acción general
ECONOMÍA	**1.1** Concientización Cultura y Prevención	Elaborar una estrategia de comunicación para generar confianza en la población usando los distintos servicios de comercio electrónico seguros, así como concientizar a los actores de los riesgos asociados con el ciberespacio. Crear conciencia sobre las responsabilidades que tiene cada actor en el uso de las TIC, basadas en estrategias de concientización, labores formativas y de sensibilización para guiarse en apego al buen uso de las mismas. **Comentarios (Academia):** Esto se ha centrado tradicionalmente en sólo traer dispositivos a los niños. Esto debería cambiar para centrarse en la educación técnica desde el principio, y esta educación técnica debe incluir también las preocupaciones de inclusión y representación de género. **Comentarios (Industria): Propuesta de cambio en el texto** *"Elaborar una estrategia de comunicación* ***clara y sencilla*** *para generar confianza* ***en los usuarios que les permita identificar el nivel de seguridad y*** ~~*la población usando*~~ *los distintos servicios del* ***ecosistema*** ~~*comercio electrónico*~~ ***digital*** ~~*seguros*~~*, así como concientizar a los actores de los riesgos asociados con el ciberespacio.* ***La estrategia de comunicación tendrá las siguientes características:*** ***Brindar recomendaciones para que el usuario tome acciones orientadas a evitar transacciones inseguras*** • ***La estrategia debiera orientarse a audiencias/grupos de población específicos específicas utilizando los lenguajes ad-hoc*** • ***Homologar conceptos para aportar claridad de conformidad con el glosario de términos que se adjunta al documento;*** • ***Generar conciencia en la población sobre los riesgos en el entorno digital para reforzar la confianza en la economía digital y no desincentivar sus actividades.*** ***Cada dependencia gubernamental aportará las recomendaciones conducentes de conformidad con sus atribuciones legales.*** *Crear conciencia sobre las responsabilidades que tiene cada actor en el uso de las TIC, basadas en estrategias de concientización, labores formativas y de sensibilización para guiarse en apego al buen uso de las mismas."*

ECONOMÍA	**1.1** Concientización Cultura y Prevención	**Comentarios (Industria):** Se sugiere estructurar la política desde la perspectiva de riesgos en ciberseguridad. Generar una estrategia de publicidad clara y sencilla y concientización estratificada que se enfoque a cada tipo de audiencia (usuarios, industria, gobierno, etc). El gobierno mencionó que es importante no generar pánico con la estrategia, sino incentivar el uso de las tecnologías generando confianza. Como comentario general, se sugiere que en todo el documento se modifique el término comercio electrónico por economía digital o ecosistema digital.
	1.2 Desarrollo de capacidades	Promover el desarrollo de proyectos de investigación e innovación en ciberseguridad para propiciar el crecimiento de la economía a través del fomento de capital humano especializado en materia de ciberseguridad. **Comentarios (Industria):** Añadir el ámbito internacional. Se enfoca sólo en capital humanos, pero valdría la pena extenderlo a desarrollo tecnológico. Asimismo, se sugiere insertar que la industria puede aportar en el tema. **Comentarios (Academia):** La Academia debe estar muy involucrada en la sección 1.2. Es importante definir cual entidad estará liderando la sección 1.2. El desarrollo de capacidad es también una cuestión económica - formación y educación, comenzando con la educación básica. La educación debe ser fortalecida en matemáticas. Se necesitan ingenieros que puedan desarrollar criptografía y matemáticas superiores para una ingeniería segura. Se necesita fortalecer el pensamiento crítico matemático.
	1.3 Coordinación y colaboración	Fomentar la coordinación nacional sobre ciberseguridad para la mitigación de riesgos y amenazas que puedan afectar la economía, y, por ende, la estabilidad del Estado Mexicano. Disponer de foros de comunicación que faciliten el intercambio de buenas prácticas sobre innovación tecnológica.

ECONOMÍA

1.3
Coordinación y colaboración

Comentarios (Industria): Propuesta de cambio en el texto
"Fomentar la coordinación nacional ***e internacional*** *sobre ciberseguridad para la mitigación de riesgos y amenazas que puedan afectar la economía, y, por ende, la estabilidad del Estado Mexicano. Disponer de foros de comunicación que faciliten el intercambio de buenas prácticas sobre innovación tecnológica."*

Comentarios (Industria): Se sugiere agregar elementos tales como la contención, identificación, reacción y recuperación. Asimismo, referenciar a buenas prácticas y marcos internacionales (presentes y futuros).

Comentarios (Academia): Se trata de contar con expertos altamente calificados en ciberseguridad, en investigación, etc., e incluir a profesionales con otras áreas del conocimiento. Todo el mundo forma parte del sistema económico cibernético, no sólo de las personas de TI. Todas las profesiones deben entender lo que realmente está sucediendo en el ciber entorno, según sea apropiado para su trabajo. Por ejemplo, profesionales del área de salud necesitan tener en cuenta que manejan datos sensibles de los pacientes y que deben implementar medidas de seguridad para la protección de datos. Las escuelas de medicinas deben preparar los profesionales para esta realidad. Cabe señalar que es muy difícil hacer un cambio en el currículo académico en este grado, y es un proceso muy largo. En este contexto, se necesita buscar esquemas creativos para que se pueda enseñar esto a los jóvenes profesionales. Otro desafío es garantizar que los profesores estén preparados para capacitar a los estudiantes. Asimismo, en la mayoría de las universidades falta personal.

1.4
Investigación y desarrollo

Desarrollar un programa nacional que promueva la investigación y desarrollo en ciberseguridad para la generación de tecnología propia, reduciendo la dependencia de otros Estados, articulando los esfuerzos de la investigación científica en la academia con la práctica industrial y comercial a través de esquemas de incentivos.

ECONOMÍA

1.4
Investigación y desarrollo

Comentarios (Industria): Estos recursos sirven también para la generación de riqueza, también son oportunidad. México como parte de un mercado importante en materia de tecnología. Aprovechar las oportunidades que da la tecnología. La industria puede sumar esfuerzos a través de desarrollos tecnológicos para la ciberseguridad y el desarrollo de la economía.Modificar la parte de "dependencia de otros Estados". Los productos no se desarrollan por una sola empresa ni en un solo país. Se sugiere eliminar esa expresión. Más bien hacer énfasis en el tema de la investigación, desarrollo e innovación en seguridad de los productos, con independencia de dónde provengan.
La ciberseguridad debe verse como una oportunidad en lugar de un problema, que suma y crea bienestar económico.

1.5
Estándares y criterios técnicos

Fomentar la creación de grupos de especialistas en materia de ciberseguridad en los distintos sectores de la sociedad para desarrollo de buenas prácticas, normas y estándares conforme a las necesidades del país.

Los actores involucrados deben evaluar y emitir recomendaciones respecto a la aplicabilidad y vigencia de los estándares y criterios, normas y demás metodología conforme a la tendencia tecnológicas y las nuevas amenazas para que sean tomados en cuenta en las innovaciones y la política pública.

Comentarios (Industria): Revisar el término de nuevas amenazas, tal vez usar términos como retos o desafíos. Se sugiere hablar de desarrollo pero también de adopción de lo que ya está funcionando.

Comentarios (Industria): Propuesta de cambio en el texto
*"Fomentar la creación de grupos de especialistas en materia de ciberseguridad en los distintos sectores de**l gobierno,** ~~la~~ sociedad **y demás actores para la adopción y/o** ~~el~~ desarrollo de buenas prácticas, normas y estándares conforme a las necesidades del país.*
Los actores involucrados deben evaluar y emitir recomendaciones respecto a la aplicabilidad y vigencia de los estándares y criterios, normas y demás metodología conforme a la tendencia tecnológicas y las nuevas amenazas para que sean tomados en cuenta en las innovaciones y la política pública."

ECONOMÍA

1.6
Protección a infra-estructuras críticas

Fortalecer el desarrollo nacional a través de la innovación tecnológica para impulsar la economía del país mediante el impulso de mecanismos, marco jurídico y normas técnicas manteniendo en todo momento la protección de las ICI, coadyuvando a preservar la integridad, estabilidad y permanencia del Estado Mexicano.

Comentarios (Industria): Propuesta de cambio en el texto *"Fortalecer el desarrollo nacional a través de* ***la protección de las ICI y de la promoción de*** *la innovación tecnológica para impulsar la economía del país mediante el impulso de mecanismos, marco jurídico y normas técnicas manteniendo en todo momento la protección de las ICI, coadyuvando a preservar la integridad, estabilidad y permanencia del Estado Mexicano."*

Comentarios (Academia): Es importante definir lo que son las infraestructuras críticas. Se recomendó incluir la industria química entre las infraestrucuras críticas. Se debe pensar en los efectos que podrían ocurrir en el espacio físico. Las empresas que proveen infraestructura crítica tienen que ser estimuladas para ser más seguras y crear modelos más seguros.

Comentarios (Sector Financiero): Se sugiere ampliar el término *"operaciones que se realizan en Internet"* incluyendo en particular las operaciones, servicios y transacciones financieras mediante medios electrónicos.

1.7
Marco jurídico

Armonizar el marco jurídico nacional que regule las operaciones que se realizan a través del Internet y que proporcione a los usuarios seguridad y confianza al realizar transferencia de datos, operaciones de comercio electrónico y cualquier actividad digital. Asimismo, deberá incluir la protección de los derechos fundamentales, actividades económicas, salud y sociales que la ciudadanía del Estado Mexicano efectúe por medio de las TIC.

Comentarios (Academia): En público en general no entiende mucho acerca de la ciberseguridad y sus implicaciones en el comercio electrónico. Sería importante considerar un plan de comunicacones al público para mejor compreender estas definiciones. Se recomienda incluir una definición para comercio eletrónico.

ECONOMÍA

1.7
Marco jurídico

Comentarios (Industria): Se hizo énfasis en que la regulación de las operaciones en internet y "cualquier actividad digital" no es faactible y serían barreras a la economía, a la neutralidad de la red, etc. Teniendo esto en cuenta, se sugiere eliminar esa parte para entrar directamente a "proporcionar a los usuarios..." y modificar el tema de usuarios para referirse a actores en general. Se sugiere incluir que el marco actual en materia de protección de datos permite la innovación en esta materia, por lo que se considera adecuado el marco actual. Tener en cuenta que hay autorregulación y otros mecanismos que no implican necesariamente la emisión o modificación de leyes. Adoptar un enfoque de equilibrio entre la protección al usuario final y el uso y desarrollo de nuevas tecnologías.

Se sugiere retomar en los ejes de marco normativo de todo el documento, lo que se dice al principio: El marco nacional de seguridad cibernética y su aplicación deben respetar principios fundamentales como la privacidad, la libertad de expresión, la proporcionalidad, entre otros.

Tener cuidado de que el término "protección" no se entienda como mecanismo restrictivo en el tema de actividades económicas o innovación.

1.8
Medición y seguimiento

Elaborar y actualizar métricas sobre el uso y confianza de servicios de comercio electrónico por parte de la población, así como impulsar en los diferentes sectores del país la generación de indicadores que reflejen la problemática existente sobre incidentes de ciberseguridad a fin de crear estrategias de innovación tecnológica para la resolución de los mismos, manteniendo la confianza y así incentivar la economía.

Comentarios (Industria): Tener en cuenta los marcos internacionales, por ejemplo el de higiene cibernética. Considerar que los mecanismos de medición deben modernizarse sobre todo en la nueva economía digital.

Comentarios (Academia): Se necesita alinear esta sección económica con la capacidad de educación técnica y de ingenería del país.

2. SOCIEDAD

Comentarios (Academia): La estrategia debe ser considerada bajo una base de gestión de riesgos en todo el documento. Se debe definir el nivel aceptable de riesgo para la sociedad. Ese nivel aceptable de riesgo debe ser determinado por las autoridades, porque establecen las leyes y los objetivos nacionales. Para que se fomente la confianza, es necesario que la sociedad sea informada de como la ciberseguridad la ayudará y explicarla como los delitos cibernéticos serán investigados. La gente debe ser consciente de los riesgos implicados. No se puede estar 100% seguros. El principal problema aquí es entender cuánto riesgo vamos a aceptar y la sociedad debe compreender esta situación. La sociedad también debe ser responsable por su uso del Internet. Estamos fomentando el uso de Internet y la sociedad debe usarlo de manera responsable, pero no lo logramos poniendo miedo, sino ayudando a la sociedad a comprender su responsabilidad. Se necesita incluir el uso inteligente y responsable. Los mensajes a la sociedad deben ser positivos (ej. crear buenas contraseñas). La responsabilidad compartida es primordial.

El aumento de usuarios de Internet ha propiciado que las instituciones públicas incrementen sus servicios en línea que simplifican procesos y tiempo a los ciudadanos; sin embargo, aún no hay confianza plena en realizar trámites gubernamentales debido a que una gran parte de la población desconfía del uso de las TIC.

La protección de la sociedad ante el entorno digital es fundamental para que se desarrolle y por ello las acciones tendientes a protegerla deben enfocarse en incrementar la cultura de ciberseguridad, ya que de lo contrario una sociedad conectada y cada vez más globalizada puede ser potencialmente víctima de la ciberdelincuencia, que afecta la integridad, dignidad y patrimonio de las personas. Adicionalmente, es indispensable fomentar la confianza de las personas para que utilicen los servicios en línea que ofrecen las instituciones públicas y privadas, así mismo concientizar sobre la importancia de adoptar las medidas de ciberseguridad para evitar que sean víctimas de ciberdelitos.

Así, contribuir a través de la ciberseguridad a que las personas logren una mayor calidad de vida, para lo cual se debe proteger su información digital y las TIC como los componentes de un entorno digital seguro y libre, a fin de desarrollarse en todos los aspectos, incluyendo las relaciones personales, laborales, educativas, de trabajo y negocios.

Impulsar mecanismos de cooperación sobre ciberseguridad enfocado a promover el manejo adecuado y seguro de las TIC enriqueciendo la concientización de la sociedad.

OE	Eje Transversal	Acción general
SOCIEDAD	**2.1** Concientización Cultura y Prevención	Fomentar estrategias para el desarrollo de campañas de concientización y prevención en materia de ciberseguridad, que contemplen la autoprotección, esquemas de autorregulación y mejores prácticas. Generar las propuestas en relación al acceso a contenidos digitales, que permitan la protección de adolescentes, niños y niñas a la exposición con depredadores informáticos y riesgos asociado con material nocivo innecesario a través de las redes inalámbricas de las instituciones educativas del país. **Comentarios (Industria):** El enfoque a los niños y adolescentes debe ir enfocado a la autoprotección, autorregulación, empoderamiento, para evitar que se expongan a riesgos. Revisar el término de depredadores informáticos. Incluir poblaciones vulnerables en general, no sólo niños y adolescentes, o incluso referirse a usuarios en general. Incluir una acción más de fondo en el sentido de estructurar la educación básica en materia de ciberseguridad, y reflejarlo en los temas de Sociedad y también en Gobierno.
	2.2 Desarrollo de capacidades	Fomentar la modernización de infraestructura y la digitalización de procesos destinados a proveer servicios a la sociedad, así como estimular la profesionalización de la ciberseguridad en la academia a través del desarrollo de programas de estudio y de certificaciones para formar profesionales con competencias y habilidades en ciberseguridad. **Comentarios (Industria):** Incluir en planes de estudio (lo que se dijo en el punto anterior). Involucrar a jóvenes en la elaboración de los planes. Se propuso crear la figura del Ombudsman Digital –incluirlo en Sociedad y en Gobierno.
	2.3 Coordinación y colaboración	Impulsar mecanismos de coordinación, colaboración y compartición de información interinstitucional para la prevención y combate de incidentes cibernéticos mediante la participación y concientización ciudadana a fin de preservar la estabilidad social.

SOCIEDAD	**2.3** Coordinación y colaboración	**Comentarios (Industria):** No sólo compartir información, sino la contención, identificación, reacción y recuperación. Extender al ámbito internacional. Redactar más ampliamente no sólo referido al combate.
	2.4 Investigación y desarrollo	Consolidar y ampliar la investigación y desarrollo enfocado a construir un ciberespacio seguro y confiable donde la sociedad confíe en interactuar con las TIC para realizar cualquier tipo de operación digital. **Comentarios (Industria):** Incluir el término fomentar, así como innovación y hablar de todos los actores.
	2.5 Estándares y criterios técnicos	Coordinar y capacitar a las instancias de los tres órdenes de gobierno para la orientación de sus políticas, lineamientos y acciones hacia estándares internacionales en materia de ciberseguridad que coadyuven al bienestar de la población. **Comentarios (Industria):** Llevar los estándares a todos los actores.
	2.6 Protección a infra-estructuras críticas	Establecer e implementar procedimientos y mecanismos para la protección de las ICI e IIE que proporcionan servicios y productos relacionados con el bienestar social. **Comentarios (Industria):** Revisar terminología de ICI y IIE porque no está homologado. Siempre usar ambos términos o explicar si hay razón para distinguirlos o usarlos de manera separada. Estandarizar los acrónimos.
	2.7 Marco jurídico	Implementar la armonización del marco jurídico nacional que contemple un enfoque a los derechos humanos, de carácter preventivo, y fomento al ejercicio libre, seguro y confiable de las TIC. Considerando instrumentos internacionales en la materia.

SOCIEDAD

2.7
Marco jurídico

Fortalecer el marco institucional para que la cooperación y coordinación sea más efectiva entre policías y procuradurías, así como colaborar con el poder judicial para la formación y actualización de perfiles que conozcan sobre términos y funcionamiento de las TIC para mejorar la investigación del delito que usa TIC para su comisión y reforzar la metodología para la conservación y análisis de evidencia digital.

Armonización jurídica de nuestro país en materia de conductas delictivas cometidas como fin o medio y que se encuentran sancionadas en los distintos códigos penales (Ciberdelitos), con la finalidad de identificar las áreas de oportunidad de forma puntual en algunos artículos tanto en el Código Penal Federal, como en el Código Nacional de Procedimientos Penales, en la Ley Federal de Telecomunicaciones y Radiodifusión, entre otras, con el objetivo de adecuar sus contenidos a las tendencias delictivas a través del uso de nuevas tecnologías. Lo anterior con la finalidad de evitar duplicar esfuerzos y eficientar recursos y tiempo para tener un marco legal acorde a las necesidades que la sociedad requiere a corto plazo.

Comentarios (Industria): Se sugiere designar un pequeño equipo que trabaje en la reingeneiría de Marco jurídico en todos los temas, ya que hay varios comentarios y elementos que podrían prestarse a confusión. Por ejemplo, competencias de las autoridades, carácter preventivo de la norma, el hecho de que no siempre es necesario a través de una ley, y no criminalizar el medio comisivo sino la conducta. Algunos actores sugieren la creación de tribunales especializados.
Añadir un párrafo que señale que se analizarán puntualmente los instrumentos internacionales para identificar la adecuada protección y los temas que deben retomarse o que ya están regulados mejor en México.

2.8
Medición y seguimiento

Habilitar indicadores de medición de efectividad de las campañas de concientización y cambio cultural así como de los incidentes en materia de ciberseguridad registrados por los actores públicos y privados, a fin de generar estadísticas oficiales en la materia que permitan evaluar la situación actual e implementar acciones de mejora para la población.

Comentarios (Industria): Agregar que se actualicen los indicadores ya existentes periódicamente, con parámetros comparables. Revisar el mapa de riesgos nacionales (por ejemplo el mapa de seguridad nacional).

3. GOBIERNO

Fortalecer el conjunto de procesos, sistemas de información y otros recursos de los entes públicos del Estado Mexicano -de los diferentes poderes, tipos de autonomías y de cualquier orden de gobierno- con la finalidad de que estos puedan seguir prestando su servicio a la población; trámites y servicios que contribuyan a mejorar la calidad de vida de las personas y el desarrollo de país.

El creciente uso de las TIC en las distintas funciones y actividades de los entes públicos del Estado Mexicano ha propiciado grandes beneficios en favor de la población y a la propia gestión interna de las instituciones. Lo anterior representa un entorno digital en el que la información que resguardan las instituciones públicas es cada vez más valiosa y por ello es altamente atractiva para los delincuentes. La gestión pública a través de las TIC contiene gran variedad de datos e información sensible, tanto de los entes públicos como de la población, que en caso de sufrir un ataque informático o amenaza a través de alguna tecnología o ser blanco de un delincuente que use las TIC se podrían afectar seriamente los servicios públicos, e incluso la integridad, y patrimonio de la población y del país entero.

Para la protección de la gestión pública, por lo que esto representa hacia la población, se requiere promover acciones estratégicas en materia de ciberseguridad que permita la operación continua y resiliente de las instituciones; se sus sistemas e información vinculada a su operación y a la prestación adecuada de trámites y servicios de manera segura.

OE	Eje Transversal	Acción general
GOBIERNO	**3.1** Concientización Cultura y Prevención	Diseñar e instrumentar estrategias para campañas de concientización y prevención, en las que se definan esquemas de colaboración entre los distintos entes públicos y privados del Estado Mexicano que permitan evaluar la efectividad y eficiencia de las mismas, y con ello mejorar el nivel del servicio público. **Comentarios (Industria):** Incluir en el planteamiento general así como en Gobierno o Seguridad Nacional: reconocer e identificar riesgos para establecer un mapa específico para el tema de ciberseguridad que sirva de guía para la estrategia. Hacer énfasis en que debe incluirse la educación en materia de ciberseguridad en los programas de educación básica. **Comentarios (Gobierno): Propuesta de cambio en el texto** *"Diseñar e instrumentar estrategias para campañas de concientización y prevención, en las que se definan esquemas de colaboración entre los distintos entes públicos y privados del Estado Mexicano ~~que permitan evaluar la efectividad y eficiencia de las mismas, y con ello mejorar el nivel del servicio público."~~* **Comentarios (Gobierno):** Adicionalmente se sugiere definir el alcance y beneficiarios (públicos objetivo) de las campañas.
	3.2 Desarrollo de capacidades	Establecer políticas y programas de actualización tecnológica y de fortalecimiento de habilidades de servidores públicos en materia de ciberseguridad y la prevención de la ciberdelincuencia. **Comentarios (Industria):** Agregar el tema de financiamiento, inversión y recursos. Relación con el tema general de presupuesto en el Congreso, relacionado con lo que se mencionó arriba como comentario general
	3.3 Coordinación y colaboración	Implementar acciones de cooperación entre las distintas instituciones públicas y privadas del estado mexicano que coadyuven a fortalecer la ciberseguridad en la gestión de la información relativa a la prestación de trámites y servicios a la población.

GOBIERNO	**3.3** Coordinación y colaboración	**Comentarios (Industria):** Los trámites y servicios son sólo un elemento. Distinguir primero el desarrollo e investigación, y luego hablar de mejores servicios. Agregar colaboración interinstitucional, nacional e internacional. Se sugiere hacer referencia al diseño institucional vigente en materia de seguridad nacional y seguridad pública. **Comentarios (Gobierno): Propuesta de cambio en el texto** *"Implementar acciones de cooperación entre las distintas instituciones públicas y privadas del estado mexicano,* ***así como con actores internacionales*** *que coadyuven a fortalecer la ciberseguridad ~~en la gestión de la información relativa a la~~* ***en la*** *prestación de trámites y servicios a la población."*
	3.4 Investigación y desarrollo	Establecer acciones, con actores nacionales, para el impulso del desarrollo tecnológico, investigación e intercambio de conocimiento con la finalidad de fortalecer la ciberseguridad al interior de las instituciones públicas del Estado Mexicano y que ello se traduzca en una prestación más eficiente segura y confiable de los trámites y servicios para la población. **Comentarios (Industria):** Agregar el tema de presupuesto. Agregar actores internacionales también, y cooperación de la industria. **Comentarios (Gobierno): Sugerencia de cambio en el texto** *"Establecer acciones, con actores nacionales d****el ámbito académico y científico,*** *para el impulso ~~del desarrollo tecnológico~~ de la investigación,* ***el desarrollo y la innovación (I+D+i), promoviendo la generación*** *e intercambio de conocimiento con la finalidad de fortalecer la ciberseguridad al interior de las instituciones públicas del Estado Mexicano y que ello se traduzca en una prestación más eficiente segura y confiable de los trámites y servicios para la población."*
	3.5 Estándares y criterios técnicos	Estudiar y definir aquellos criterios y controles que permitan estandarizar las distintas etapas del proceso de seguridad de la información y tratamiento de datos dentro de los entes públicos

GOBIERNO

3.5
Estándares y criterios técnicos

del Estado Mexicano, considerando aquellas normas, estándares internacionales y mejores prácticas en materia de ciberseguridad.

Identificar el estado actual de infraestructura y recursos orientados en el tema de ciberseguridad con los que cuenta nuestro país, mediante un modelo de Política rectora de TIC, en el ámbito de las atribuciones de cada ente público, para generar un proceso gradual de consolidación de la base tecnológica y la eficiencia en tecnologías a nivel país.

Comentarios (Industria): Revisar la redacción general y sintetizarla en el sentido de referirse a un marco de referencia (que ya existe) y con una aproximación basada en el manejo del riesgo.

Comentarios (Industria): Propuesta de cambio en el texto
"Estudiar y definir aquellos criterios y controles que permitan el ***adecuado manejo del riesgo (****estandarizar las distintas etapas del proceso de seguridad de la información y tratamiento de datos dentro de los entes públicos del Estado Mexicano, considerando aquellas normas, estándares internacionales y mejores prácticas en materia de ciberseguridad****)."*

Comentarios (Gobierno): Propuesta de cambio en el texto
"Estudiar y definir aquellos criterios y controles que permitan estandarizar las distintas etapas del proceso de seguridad de la información y tratamiento de datos dentro de los entes públicos del Estado Mexicano, considerando aquellas normas, estándares internacionales y mejores prácticas ***que resulten pertinentes*** *en materia de ciberseguridad para el* ***Estado Mexicano.***

~~*Identificar el estado actual de infraestructura y recursos orientados en el tema de ciberseguridad con los que cuenta nuestro país, mediante un modelo de Política rectora de TIC, en el ámbito de las atribuciones de cada ente público, para generar un proceso gradual de consolidación de la base tecnológica y la eficiencia en tecnologías a nivel país."*~~

GOBIERNO

3.6
Protección a infra-estructuras críticas

Fomentar la creación de grupos de especialistas en materia Establecer políticas y medidas de gestión de riesgo y de protección a infraestructuras críticas de los entes públicos del Estado Mexicano que permitan su operación habitual y prestación óptima de trámites y servicios a la población, así como la instauración de canales de comunicación seguros para la coordinación ante posibles ataques y resiliencia.

Comentarios (Industria): Este párrafo ya está reflejado en el punto anterior. Revisar si la precisión de infraestructura crítica tiene algún razonamiento o no debiera hacerse (mismo comentario que arriba).

Comentarios (Gobierno): Cambiar el texto para *"Establecer políticas y medidas* ***para identificar, gestionar y lograr la*** ~~*de gestión de riesgo y de*~~ *protección a infraestructuras críticas de los entes públicos del Estado Mexicano que permitan su operación habitual y prestación óptima de trámites y servicios a la población, así como la instauración de canales de comunicación seguros para la coordinación ante posibles* ***incidentes*** ~~*ataques*~~ *y* ***elevar la*** *resiliencia* ***de las mismas."***

3.7
Marco jurídico

Analizar y armonizar el marco jurídico, instrumentos y esquemas de cooperación internacional aplicable, que define el actuar de los entes públicos y privados del Estado Mexicano para establecer políticas, acciones y procesos que incrementen la ciberseguridad, así como para brindar certeza jurídica en la prestación de trámites y servicios a la población.

Comentarios (Industria): Se retoma el comentario anterior en Marco jurídico. Enfasis en no minar el desarrollo de nuevas tecnologías. No todo debe ser ley, sino hacer referencia al tema preventivo y los diversos mecanismos que pueden utilizarse, distintos de la ley. Un ejercicio de análisis más sistemático de marco legal, de esquemas de autorregulación, de política pública, etc. Tomar este comentario en todos los desarrollos de marco jurídico del documento. No sólo referirse a trámites y servicios.

GOBIERNO

3.7
Marco jurídico

Comentarios (Gobierno): Cambiar el texto para *"Analizar y armonizar el marco jurídico, instrumentos y esquemas de cooperación internacional aplicable, que define el actuar de los entes públicos y privados del Estado Mexicano para establecer políticas, acciones y procesos que incrementen la ciberseguridad."*

3.8
Medición y seguimiento

Construir indicadores y generar una metodología para la medición de las capacidades de prevención y respuesta a los incidentes de ciberseguridad registrados por los entes públicos nacionales y establecer esquemas de cooperación con el sector privado para aproximarnos gradualmente a la dimensión de la problemática considerando reportes e índices internacionales.

Desarrollar un proceso gradual de adopción voluntaria de los procesos referidos en el "Manual de Gestión de Tecnologías de la Información y Seguridad informática (MAGTICSI)" en las Entidades Federativas, con la finalidad de obtener un panorama del estado y necesidades inherentes al tema de ciberseguridad en nuestro país.

Comentarios (Gobierno): Propuesta de cambio en el texto
"Construir indicadores y generar ***indicadores*** ~~*una metodología*~~ *para la medición de las capacidades de prevención y respuesta a los incidentes de ciberseguridad registrados por los entes públicos nacionales y establecer esquemas de cooperación con el sector privado para aproximarnos gradualmente a la dimensión de la problemática considerando reportes e índices internacionales.*

Desarrollar un proceso gradual de adopción voluntaria de los procesos referidos en el "Manual de Gestión de Tecnologías de la Información y Seguridad informática (MAGTICSI)" en las Entidades Federativas, con la finalidad de obtener un panorama del estado y necesidades inherentes al tema de ciberseguridad en nuestro país."

4. SEGURIDAD NACIONAL

La creciente dependencia de las TIC en todos los ámbitos ha propiciado el incremento de las amenazas cibernéticas globales y los delitos que se generan van más allá de obtener un beneficio económico; a nivel mundial, existen grupos delictivos, subversivos y terroristas que pretenden desestabilizar gobiernos atacando sus ICI. La vulneración de las ICI, que suministran energía, transporte, salud, agua, entre otras, podría ocasionar riesgos a la estabilidad social, económica y política del Estado Mexicano.

Proteger la Seguridad Nacional es de vital importancia para que la población pueda desarrollarse con normalidad, en un entorno de paz y armonía que permita el desarrollo de las actividades de la sociedad, de la industria, del gobierno.

El fortalecimiento de la Seguridad Nacional en el entorno del ciberespacio permitirá preservar la integridad, estabilidad y permanencia del Estado Mexicano.

Para lo anterior, se requiere desarrollar, implementar y mantener políticas, procedimientos, marco jurídico y normas técnicas que coadyuven a la protección de la información digital crítica e infraestructuras críticas relacionadas con la Seguridad Nacional. Así como realizar acciones en materia de ciberdefensa, por parte de fuerzas armadas, para protección contra ataques cibernéticos nacionales e internacionales.

Comentarios (Industria): Aclarar cuándo se habla sólo de infraestructura crítica, y qué entra en seguridad interior y qué en seguridad nacional. También ver si se inserta el tema de seguridad pública en el tema de Gobierno. Decir que en materia de delitos locales debe haber cooperación entre autoridades locales y federales. Tal vez también distinguir entre ciberdelincuencia y ciberdefensa.

Todo esto se refiere a la precisión conceptual. Mencionaron que en el MATIGSI ya se tiene esta distinción de lo que es seguridad nacional y lo que no. El tema de transparencia es importante para determinar la publicidad o clasificación de documentos de seguridad nacional.

OE	Eje Transversal	Acción general
SEGURIDAD NACIONAL	**4.1** Concientización Cultura y Prevención	Desarrollar e implementar estrategias para campañas de concientización, cultura y prevención dedicadas a las Instancias de Seguridad Nacional considerando los aspectos sobre ciberseguridad, comunicaciones, manejo de información general, personal y laboral.
	4.2 Desarrollo de capacidades	Establecer políticas y programas de actualización tecnológica y de fortalecimiento de habilidades para formar funcionarios expertos en materia de ciberseguridad, así como contar con una base de conocimientos centralizada. **Comentarios (Industria):** También incluir crear capacidades en desarrollo de infraestructura y el diseño de arquitecturas seguras. En el tema de soberanía de datos, se precisó que lo importante es garantizar la seguridad de la información. **Comentarios (Gobierno): Sugerencia de cambio en el texto** *"Establecer políticas y programas de* ***adecuación*** *~~actualización~~ tecnológica y de fortalecimiento de habilidades de servidores públicos en materia de ciberseguridad ~~y la prevención de la ciberdelincuencia~~."*
	4.3 Coordinación y colaboración	Establecer mecanismos de colaboración y cooperación entre las dependencias vinculadas con actividades de Seguridad Nacional con la finalidad de intercambiar información e inteligencia relacionada a procedimientos, buenas prácticas, atención de incidentes y experiencias para la prevención, atención y recuperación ante incidentes cibernéticos. **Comentarios (Industria):** Insertar cooperación internacional. Canales de contacto e intercambio de información internacional. Eventualmente consultar el desarrollo de la discusión en materia del Digital Geneva Convention.

SEGURIDAD NACIONAL	**4.4** Investigación y desarrollo	Definir acciones y procedimientos desde las Instancias de Seguridad Nacional para el impulso del desarrollo tecnológico, investigación e intercambio de conocimiento a fin de fortalecer la ciberseguridad en las dependencias que cuenten con ICI del Estado Mexicano para preservar la integridad, estabilidad y permanencia del Estado Mexicano. **Comentarios (Industria):** Insertar el tema de intercambio de conocimientos entre los demás actores. Considerar si no sería mejor incluirlo mejor en la sección "Sociedad".
	4.5 Estándares y criterios técnicos	Analizar y adoptar marcos normativos que faciliten la estandarización de las distintas etapas del proceso de seguridad de la información y el tratamiento de activos de información en las Instancias de Seguridad Nacional considerando aquellas normas, estándares internacionales y mejores prácticas en materia de ciberseguridad. **Comentarios (Industria):** Complementar con demás conceptos como infraestructura y seguridad de redes.
	4.6 Protección a infra-estructuras críticas	Desarrollar un esquema que permita conocer aquellas ICI y definir políticas basada en la gestión de riesgos y contener esquemas de cooperación nacional e internacional con actores públicos y privados para el intercambio de información, mejores prácticas, acciones de prevención, atención y resiliencia. Para ello se deben identificar las ICI con base en mejores prácticas y estándares internacionales para integrar y mantener actualizado un Catálogo Nacional de Infraestructuras Críticas de Información (CNICI). Además, fortalecer el marco institucional en materia de ICI y establecer los protocolos de comunicación y cooperación entre los distintos sectores involucrados para la ciberdefensa en situaciones en que se presente un ciberataque que afecte las ICI o IIE y se considere una posible afectación al orden y paz social. **Comentarios (Industria):** Habría que aclarar por qué se quiere hacer la distinción de ICI e IIE, y homologar acrónimos.

SEGURIDAD NACIONAL

4.6
Protección a infra-estructuras críticas

Comentarios (Industria): Propuesta de cambio en el texto
"Desarrollar un esquema que permita conocer aquellas ICI y definir políticas basada en la gestión de riesgos y contener esquemas de cooperación nacional e internacional con actores públicos y privados para el intercambio de información, mejores prácticas, acciones de prevención, atención y resiliencia. Para ello se deben identificar las ICI con base en mejores prácticas y estándares internacionales para integrar y mantener actualizado un Catálogo Nacional de Infraestructuras Críticas de Información (CNICI).

Además, fortalecer el marco institucional en materia de ICI y establecer los protocolos de comunicación y cooperación entre los distintos sectores involucrados para la ciberdefensa en situaciones en que se presente un ciberataque que afecte las ICI o IIE y se considere una posible afectación ~~al orden y paz social~~ ***la estabilidad del Estado Mexicano.****"*

4.7
Marco jurídico

Armonizar el marco jurídico en materia de Seguridad Nacional y su relación con la ciberseguridad, para establecer mecanismos de adopción de mejores prácticas y armonizar la legislación en relación a delitos como ciberterrorismo, delitos que usan TIC para su comisión (ciberdelitos), ciberataques y ciberamenazas, estableciendo las directrices generales para el uso seguro del mismo, el cual debe contemplar la investigación, y sanción correspondiente.

Comentarios (Industria): Sería importante afinar y precisar el lenguaje. Nuevamente no criminalizar el medio comisivo, sino la conducta. Incluir la adapatabilidad del marco jurídico basado en principios, que permita la adaptación de la norma a la tecnología. Retomar comentarios anteriores de Marco jurídico.

SEGURIDAD NACIONAL

4.8
Medición y seguimiento

Realizar metodología y ejecutar análisis y mantener prácticas de gestión de riesgos y vulnerabilidades, implementación de planes de continuidad y recuperación ante desastres, así como evaluaciones de impacto. Adicionalmente, se debe generar estadísticas globales para conocer las tendencias de los incidentes cibernéticos a fin de evaluar la situación actual e implementar acciones de mejora.

Comentarios (Industria): Redactar de manera más general que permita la flexibilidad en el tema de medición, que refleje la madurez del Estado Mexicano en ciberseguridad en seguridad nacional.

VI. Marco Institucional

Dada la complejidad del tema de Ciberseguridad y en el entendido de que la implementación de la ENCS requiere un esfuerzo coordinado y cooperativo, los actores de la comunidad nacional coinciden en la necesidad de reforzar el marco institucional y jurídico para la adecuada coordinación, desarrollo y seguimiento de las acciones derivadas de la ENCS al interior de la Administración Pública Federal, y además pueda establecer alianzas y formalizar esquemas de colaboración con actores de industria, academia, otros entes públicos y sociedad en general, ya sean nacionales e internacionales.

Es importante formalizar los esquemas de colaboración necesarios y suficientes para poder abordar el tema de ciber amenazas e incidentes informáticos, así como la prevención, investigación y sanción de los delitos.

Las instituciones de la APF buscarán mantener y promover el diálogo, la cooperación entre los diferentes actores de la comunidad nacional e internacional en materia de Ciberseguridad y combate a la delincuencia. Y en tanto no se cree un ente responsable del tema, las diferentes dependencias y entidades asumirán un rol activo en el ámbito de sus respectivas atribuciones.

En tanto, es recomendable que se generen los canales de comunicación convenientes para mantener el intercambio de información y mejores prácticas para que el sector privado, sociedad y academia puedan contribuir en la consolidación de la Cultura de Ciberseguridad y co-crear junto con todos los actores las condiciones propicias para que México se siga desarrollando en el ámbito económico, político y social.

Comentarios (Industria): Este apartado no es claro en cuanto a lo que se recomienda: si se quiere o no crear un ente responsable, en cuyo caso tendría que incluirse un apartado que lo desarrolle (naturaleza jurídica, atribuciones, etc.)

Comentarios (Sector Financiero): Se recomienda incluir otros capítulos adicionales a la estrategia nacional: Diagnóstico, Seguimiento y Financiamiento.

En el capítulo de Diagnóstico se debería describir de forma clara el problema a resolver por medio de la estrategia nacional, manifestando su magnitud, estableciendo sus causas, factores de riesgo y consecuencias. Este capítulo debería considerarse como la herramienta que dará sustento a las alternativas de solución y a las acciones concretas que se deben incorporar en el plan de acción. Aquí se debería identificar el (los) problema (s) que se busca resolver y para esto se debería realizar una adecuada y completa revisión de la situación actual en el país, haciendo levantamiento de la información necesaria junto con el listado de actores relevantes que actualmente adelantan actividades relacionadas con la ciberseguridad en el país. Los problemas deberían sustentarse y argumentarse con base en información estadística o cualitativa, asegurando que las afirmaciones tengan sustento. También se podrían jerarquizar o priorizar los problemas identificados con el fin de lograr establecer claramente el objetivo general y los objetivos secundarios de la estrategia.

En el capítulo de Seguimiento se deberían describir las herramientas utilizadas para hacer seguimiento a la ejecución física y presupuestal de las acciones propuestas para el cumplimiento de los objetivos de la estrategia nacional. Adicionalmente se debería establecer de forma clara un resumen esquematizado del plan de acción, identificando los responsables del desarrollo de cada acción, las fechas de corte de los informes de seguimiento y la fecha de cierre de la estrategia.

En el capítulo de Financiamiento se deberían mencionar tanto los recursos financieros necesarios como los asignados para la ejecución de las acciones propuestas, considerando el horizonte de tiempo definido por la estrategia. Dado que es crucial verificar que todas las acciones o intervenciones propuestas sean viables jurídica, técnica y presupuestalmente, no se deben incluir en la estrategia acciones que no estén debidamente presupuestadas y concertadas. Para esto, es necesario identificar las vigencias fiscales para las cuales se van a comprometer los recursos, sus respectivas fuentes de financiación y el uso que se les dará. Se aconseja incluir una tabla que detalle los recursos financieros por entidad del sector ejecutivo para cada una de las vigencias fiscales (años) y en el plan de acción detallado se debería consignar la información relacionada con los recursos programados para la ejecución de cada una de las acciones establecidas en la estrategia.

VII. Glosario

Comentarios (Industria): Contrastar este glosario con el CyberCodex del Wilson Center y otros instrumentos (y señalarlos como fuente), así como señalar cuál es la fuente de este glosario actual.

Activo (s) de información: toda aquella información y medio que la contiene, que por su importancia y el valor que representa para cualquier dependencia o entidad de la APF, los Poderes Legislativo y Judicial, los órganos constitucionales autónomos, las empresas productivas del Estado, los Gobiernos Estatales, Municipales y Delegacionales, así como los particulares, debe ser protegido para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue.

Activos de TIC: los programas de cómputo, bienes informáticos, soluciones tecnológicas, sistemas o aplicativos, sus componentes, las bases de datos o archivos electrónicos y la información contenida en éstos.

Amenaza (s): cualquier posible acto que pueda causar algún tipo de daño a los activos de información de las dependencias o entidades de la APF, los Poderes Legislativo y Judicial, los órganos constitucionales autónomos, las empresas productivas del Estado, los Gobiernos Estatales, Municipales y Delegacionales, así como los particulares.

Catálogo Nacional de Infraestructuras Críticas de Información: relación de las Infraestructuras Críticas de Información de los diferentes sectores del país.

Ciberamenaza: causa potencial en el ciberespacio con capacidad de provocar un efecto adverso.

Ciberataque: acción en el ciberespacio con la intención de causar un efecto adverso.

Ciberdefensa: Conjunto de acciones, recursos y mecanismos del estado en materia de Seguridad Nacional para prevenir, identificar y neutralizar toda ciberamenaza o ciberataque que afecte a la infraestructura critica nacional, instrumentado por las fuerzas armadas.

Ciberdelincuencia: conjunto de actividades delictivas realizadas con ayuda de redes de comunicaciones y sistemas de información electrónicos o contra tales redes y sistemas.

Ciberespacio: ámbito intangible, de naturaleza global, soportado por las TIC, que es utilizado para la interacción entre individuos y entidades públicas y privadas.

Ciberseguridad: Conjunto de políticas, controles, procedimientos y normas del Estado para proteger y asegurar sus activos en el uso del ciberespacio que coadyuven a proteger a la sociedad, gobierno, economía y seguridad nacional en un el marco del desarrollo sostenible.

Datos personales: cualquier información concerniente a una persona física identificada o identificable.

Delitos cibernéticos: cualquier delito cometido por medio de las TIC como medio o cuando el fin de la conducta sea dañar o afectar las TIC.

ERISC: Equipo de Respuesta a Incidentes de Ciberseguridad con el fin de proteger las infraestructuras de información esenciales, en base al segmento de servicio al que esté destinado así deberá de ser su alcance para cubrir requerimientos de protección sobre los servicios que brinda.

Información: conjunto de datos organizados y procesados incluidos en documentos y en activos de TIC.

Infraestructura(s) Crítica(s) de Información (ICI): Las infraestructuras de información esenciales consideradas estratégicas por estar relacionadas con la provisión de bienes y de prestación de servicios públicos esenciales y cuya afectación pudiera comprometer la Seguridad Nacional en términos de la ley de la materia.

Infraestructura(s) de Información Esencial(es) (IIE): Las redes, servicios, equipos e instalaciones asociados o vinculados con Activos de Información Tecnologías de Información y Comunicaciones (TIC) y Tecnologías de Operaciones (TO), cuya afectación, interrupción o destrucción tendría un impacto mayor en la operación de las instituciones.

Riesgo: la posibilidad de que una amenaza aproveche una vulnerabilidad y cause una pérdida o daño sobre los activos de TIC, las infraestructuras críticas o los activos de información.

Seguridad de la información: capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como su autenticidad, auditabilidad, protección a la duplicación, no repudio y legalidad.

TIC: Tecnologías de Información y Comunicaciones que comprende los quipos de cómputo, software y dispositivos de impresión que sean utilizados para almacenar,

procesar, con convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video, de conformidad con lo dispuesto en el artículo 2 del acuerdo con el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional en materia de Tecnologías de la Información y comunicaciones y en la de Seguridad de la Información, así como el Manual Administrativo de Aplicación General en dichas materias.

TO (Tecnologías de Operación): Hardware o software que detecta o genera un cambio a través del control y/o monitoreo de dispositivos físicos, procesos y eventos en las instituciones.

Vulnerabilidades: las debilidades identificadas en la ciberseguridad dentro de las dependencias o entidades de la APF, los Poderes Legislativo y Judicial, los órganos constitucionales autónomos, las empresas productivas del Estado, los Gobiernos Estatales, Municipales y Delegacionales, así como los particulares que potencialmente permiten que una amenaza afecte los activos de TIC, a la Infraestructura Información Esencial, así como a los Activos de Información.

Apéndice Único

Taller 1 y 2 junio 2017 en el marco del proceso "Hacia una Estrategia Nacional de Ciberseguridad").

Cuadro 1 - Prioridades identificadas por la comunidad en la Mesa: Concientización y sensibilización sobre los riesgos del ciberespacio.

Cuadro 2 - Prioridades identificadas por la comunidad en la Mesa: Formación y profesionalización.

Cuadro 3 - Prioridades identificadas por la comunidad en la Mesa: Libertades fundamentales y privacidad.

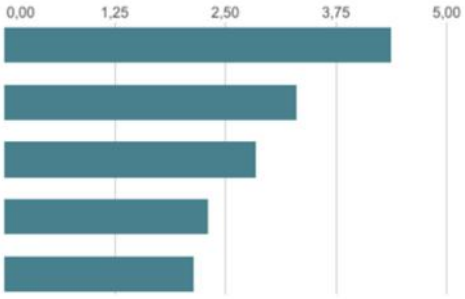
Cuadro 4 - Prioridades identificadas por la comunidad en la Mesa: Medidas de protección a grupos vulnerables.

Cuadro 5 - Prioridades identificadas por la comunidad en la Mesa: Concientización y sensibilización sobre los riesgos de la economía en el ciberespacio.

Sector económico: Ciberseguridad como impulsor de la economía digital

Mesa 1: Concientización y sensibilización sobre los riesgos de la economía en el ciberespacio

	Temas	Promedio ponderado
1	Cultura y concientización para informar correctamente sobre los riesgos de uso	4,38
2	Creación de una política accesible, delimitando actores y responsabilidades / marco jurídico	3,31
3	Generación de confianza / protección / respaldo al usuario	2,85
4	Responsabilidades de proveedores de servicios / estándares mínimos / sello de seguridad	2,31
5	Acciones sectoriales, articuladas y de colaboración permanente	2,15

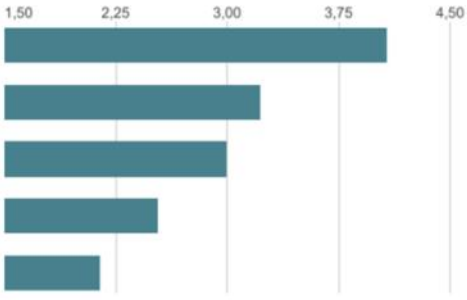


Cuadro 6 - Prioridades identificadas por la comunidad en la Mesa: Armonización del marco regulatorio de la industria y normas internacionales.

Sector económico: Ciberseguridad como impulsor de la economía digital

Mesa 2: Armonización del marco regulatorio de la industria y normas internacionales

	Temas	Promedio ponderado
1	Armonización legislativa conceptual, mejores prácticas y esquemas de autorregulación	4,08
2	Campañas de concientización y posibles consecuencias del uso de la tecnología	3,23
3	Vinculación de infraestructura pública y privada, incorporación de distintos niveles de gobierno	3,00
4	Creación de comités sectoriales alineados a la Estrategia Nacional de Ciberseguridad	2,54
5	Ratificación del Convenio de Budapest y diferentes instrumentos internacionales	2,15

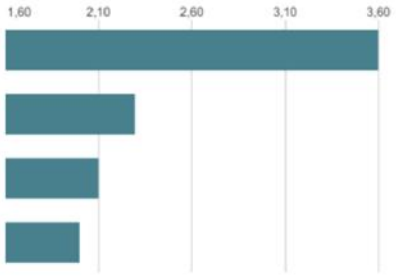


Cuadro 7 - Prioridades identificadas por la comunidad en la Mesa: Confianza en el uso de servicios digitales.

Sector económico: Ciberseguridad como impulsor de la economía digital

Mesa 3: Confianza en el uso de servicios digitales

	Temas	Promedio ponderado
1	Capacitación, educación y promoción de "civismo digital" a usuarios	3,60
2	Mecanismo colaborativo para generar catálogos de mejores prácticas de adopción voluntaria	2,30
3	Certificación de mercados electrónicos para generar confianza en los usuarios	2,10
4	Promover la confianza a través de la transparencia en factores diversos	2,00

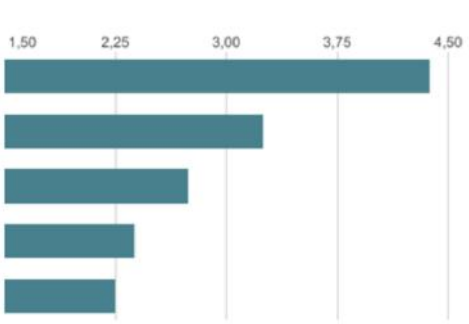


Cuadro 8 - Prioridades identificadas por la comunidad en la Mesa: Prevención, detección y atención de ataques a sistemas económicos.

Sector económico: Ciberseguridad como impulsor de la economía digital

Mesa 4: Prevención, detección y atención de ataques a sistemas económicos

	Temas	Promedio ponderado
1	Coordinación de esfuerzos de prevención ante ataques cibernéticos en sistemas económicos	4,38
2	Mejorar el modelo de respuesta a un ataque cibernético	3,25
3	Corresponsabilidad, comunicación e intercambio de información entre las partes interesadas	2,75
4	Implantar y/o actualizar los planes de continuidad de los negocios y las operaciones	2,38
5	Implementación de protocolos preventivos en el sector empresarial PyMES	2,25



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