ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

MÉXICO 2017

CONTENIDO

RESUMEN EJECUTIVO

La Estrategia Nacional de Ciberseguridad es el documento que establece la visión del Estado mexicano en la materia, a partir del reconocimiento de:

A. La importancia de las tecnologías de la información y comunicación (TIC) como un factor de desarrollo político, social y económico de México; en el entendido de que cada vez más individuos están conectados a Internet y que tanto organizaciones privadas como públicas desarrollan sus actividades en el ciberespacio.
B. Los riesgos asociados al uso de las tecnologías y el creciente número de ciberdelitos.
C. Las necesidad de una cultura general de ciberseguridad.

El aumento de riesgos, amenazas y ataques informáticos sofisticados, el surgimiento de nuevas formas y técnicas para aprovechar vulnerabilidades, así como el incremento de conductas delictivas que se cometen a través de las TIC, son circunstancias que hacen de la ciberseguridad un tema complejo. A lo anterior se suma la naturaleza global del ciberespacio y la concurrencia de diferentes soberanías y marcos jurídicos.

En términos económicos, de acuerdo con el reporte *Tendencias de seguridad en América Latina y el Caribe*[1] el cibercrimen le cuesta al país entre 3,000 y 5,000 millones de dólares al año. Además, se advierte que los riesgos y amenazas en el ciberespacio son problemas internacionales que han ganado presencia en diferentes espacios y mecanismos de diálogo y cooperación.

Los riesgos y amenazas en el ciberespacio pueden constituir un posible ataque a la dignidad humana, a la integridad de las personas, a la credibilidad, reputación y patrimonio de las empresas y las instituciones públicas; así como afectaciones a la seguridad pública o incluso la seguridad nacional.

Diversos países han desarrollado estrategias de ciberseguridad con sus propias circunstancias y particularidades, en razón de su capacidad económica, social y política. Algunas de las estrategias ya están en una etapa de madurez y se encuentran en su segunda o tercera versión, con varios años de implementación y experiencia, con instituciones consolidadas y recursos dedicados al tema. Otros países llevan pocos años, o incluso meses, de haber publicado su estrategia de ciberseguridad. Los diferentes grados de avance de los países y sus estrategias de ciberseguridad dejan en claro la necesidad e importancia de impactar positivamente a los individuos, organizaciones privadas, academia e instituciones de gobierno con acciones concretas en ciberseguridad.

[1] Reporte *Tendencias de seguridad en América Latina y el Caribe, OEA, disponible en el sitio de Internet:* https://www.sites.oas.org/cyber/Documents/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf consultado en octubre 2017.

La Estrategia Nacional de Ciberseguridad (ENCS) define objetivos y ejes transversales, plasma los principios rectores, identifica a los diferentes actores involucrados y da claridad sobre la articulación de esfuerzos entre individuos, sociedad civil, organizaciones privadas y públicas en materia de ciberseguridad; además señala el modelo de gobernanza para la implementación, seguimiento y evaluación de la Estrategia.

En México, el Gobierno de la República, en su rol de facilitador, promovió espacios de diálogo, discusión y aprendizaje mediante foros y talleres en un proceso de colaboración denominado "Hacia una Estrategia Nacional de Ciberseguridad" de marzo a octubre de 2017. En estos espacios, los distintos actores de la sociedad compartieron ideas, inquietudes y propuestas en materia de ciberseguridad que arrojaron grandes coincidencias sobre las necesidades que debía atender la Estrategia, tales como:

- Que la ENCS articule el desarrollo de las acciones de ciberseguridad que sirvan a individuos, empresas e instituciones públicas del Estado mexicano.
- Colaboración y cooperación entre los diferentes sectores como pieza clave para el desarrollo, seguimiento y evaluación de la Estrategia.
- Conocer la dimensión de los riesgos y amenazas en el ciberespacio, el estado que guarda la ciberseguridad en el país, la construcción de un diagnóstico nacional, así como obtener evidencia para mejorar la toma de decisiones en materia de ciberseguridad.
- Contemplar el escenario global como parte de la problemática y la diplomacia como vía para entablar diálogos y acuerdos que permitan hacer frente a los riesgos, amenazas y ciberdelitos.
- Desarrollar capital humano especializado en materia de ciberseguridad.
- Promover el uso responsable de las TIC y reforzar una cultura de ciberseguridad que contemple acciones de concientización, educación y formación.

En el caso de México, si bien es cierto que no existía una Estrategia, durante la presente administración se impulsaron acciones por parte del gobierno de la República y existían ejercicios y esfuerzos valiosos en la materia por parte de la sociedad civil, organizaciones privadas, comunidad académica, comunidad técnica e instituciones públicas en los diferentes poderes y órdenes de gobierno.

El **objetivo general** de la Estrategia Nacional de Ciberseguridad es identificar y establecer las acciones en materia de ciberseguridad aplicables a los ámbitos social, económico y político que permitan a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las TIC de manera responsable para el desarrollo sostenible del Estado Mexicano.

Para cumplir con el objetivo general, se establecen **5 objetivos estratégicos**:

1. Sociedad y derechos.
2. Economía e innovación.
3. Instituciones públicas.
4. Seguridad pública.
5. Seguridad nacional.

Para el desarrollo de la ENCS se consideran tres **principios rectores**:

A. Perspectiva de derechos humanos.
B. Enfoque basado en gestión de riesgos.
C. Colaboración multidisciplinaria y de múltiples actores.

Para alcanzar los objetivos estratégicos se desarrollarán **8 ejes transversales**:

1. Cultura de ciberseguridad.
2. Desarrollo de capacidades.
3. Coordinación y colaboración.
4. Investigación, desarrollo e innovación TIC.
5. Estándares y criterios técnicos.
6. Infraestructuras críticas.
7. Marco jurídico y autorregulación.
8. Medición y seguimiento.

En una etapa inicial, la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE) a través de la **Subcomisión de Ciberseguridad** será la encargada de coordinar al Gobierno de la República y articular los esfuerzos de los diferentes actores para la implementación y seguimiento de la Estrategia.

El éxito de la ENCS radica en la colaboración de las diferentes partes interesadas y en la corresponsabilidad ante la adopción y uso de las TIC. Este es un documento vivo que pretende actualizarse constantemente conforme la dinámica social lo requiera.

JUSTIFICACIÓN

La Estrategia Nacional de Ciberseguridad se fundamenta en el Plan Nacional de Desarrollo 2013-2018, de igual forma es transversal y contribuye de manera importante al logro de los objetivos del Programa para un Gobierno Cercano y Moderno 2013-2018, al Programa Nacional para la Seguridad Pública 2014-2018 y al Programa para la Seguridad Nacional 2014-2018.

Ante el uso cada vez más generalizado de las TIC en las actividades cotidianas de individuos, organizaciones privadas y públicas, aunado a su importancia como un factor de desarrollo político, social y económico; el valor económico de la información, así como el riesgo inherente del uso de dichas tecnologías, se considera necesario contar con una Estrategia Nacional de Ciberseguridad que articule las acciones dirigidas a individuos, organizaciones privadas e instituciones públicas.

La tendencia de la digitalización conlleva a que más personas usen tecnologías, que más servicios estén conectados a Internet, e incluso que dependan de sistemas de información para su funcionamiento, lo que implica que se incrementen las vulnerabilidades, riesgos y amenazas.

La Unión Internacional de Telecomunicaciones ha señalado en diversos informes que los ciberataques aumentaron un 30 por ciento entre 2011 y 2012, afectando a 550 millones de personas en todo el mundo y ocasionando pérdidas económicas de 110,000 millones de dólares.

El Modelo de Madurez de Capacidad de Seguridad Cibernética desarrollado en el estudio *Informe Ciberseguridad 2016. ¿Estamos preparados en América Latina y el Caribe?*[2] señala que: el cibercrimen le cuesta al mundo hasta US$575,000 millones al año, lo que representa 0.5 por ciento del producto interno bruto global. Eso es casi cuatro veces más que el monto anual de las donaciones para el desarrollo internacional. En América Latina y el Caribe, este tipo de delitos nos cuestan alrededor de US$90,000 millones al año. Con esos recursos podríamos cuadruplicar el número de investigadores científicos en nuestra región.

Con relación al informe de 2014 *Tendencias de Seguridad Cibernética en América Latina y el Caribe*[3] patrocinado por la Organización de Estados Americanos (OEA), se estima que los costos inherentes a la comisión de los delitos informáticos

[2] Banco Iberoamericano de Desarrollo, BID, 2016; Ciberseguridad. ¿Estamos preparados en América Latina y el Caribe?, disponible en: https://digital-iadb.leadpages.co/ciberseguridad-en-la-region/

[3] *Reporte Tendencias de seguridad en América Latina y el Caribe*, OEA, disponible en el sitio de Internet https://www.sites.oas.org/cyber/Documents/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf

alrededor del mundo ascendieron a 113,000 millones de dólares y en México representaron 3,000 millones dólares.

En México, los internautas han pasado de 40 a 65.5 millones en tan solo 4 años (2012 a 2016). De acuerdo al reciente estudio Hábitos de los Internautas en México de la Asociación Mexicana de Internet MX[4], en México se han registrado hasta 70 millones de cibernautas en 2016.

La Policía Federal, a través de la División Científica, impulsó una Estrategia de Ciberseguridad para fortalecer, entre otros, la concientización social sobre el uso responsable de las TIC. Además el número de incidentes cibernéticos identificados, se ha triplicado de 2013 a 2016, pasando de cerca de 20 mil incidentes a más de 60 mil; mientras que la presencia de sitios web apócrifos con fines de fraude, se incrementó un 11 por ciento entre 2015 y 2016, llegando a cerca de 5 mil; la propagación de virus informáticos con afectaciones en México creció un 57 por ciento de 2015 a 2016, llegando a cerca de 40 mil eventos, destaca el grado de sofisticación utilizado por los ciberdelincuentes en algunos de los casos.

Por su parte, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) señala que[5]: durante el primer trimestre del 2011 el fraude cibernético pasó del 7 por ciento (38 mil 539 quejas) de las reclamaciones por posible fraude, al 42 por ciento (639 mil 857 quejas) en el mismo periodo del 2017. El monto reclamado en el primer trimestre de 2017 asciende a mil 167 millones de pesos, del cual se abonó el 53 por ciento del total; y el 90 por ciento de los asuntos se resolvieron a favor del usuario. En cuanto al canal por donde más se presenta el fraude cibernético, el 91 por ciento es por comercio electrónico y llama la atención el incremento de las operaciones por internet para personas físicas y de banca móvil (167 por ciento y 74 por ciento respectivamente) en comparación al año anterior. Por su parte, en 2017 el promedio mensual de fraudes cibernéticos en comercio electrónico fue de 193 mil casos, cuando el año anterior era de solo 131 mil. En cuanto a fraudes cibernéticos en banca móvil, en el mes de marzo de 2017 se presentó una cifra histórica con 3 mil 682 casos.

En ese sentido, es claro que solo la suma de los esfuerzos de todos los involucrados en materia de ciberseguridad permitirá diseñar y construir los cimientos en torno al uso y aprovechamiento de las TIC en un ambiente libre, responsable y confiable que permita el desarrollo de capacidades, aprovechamiento de oportunidades, el crecimiento económico, político y social de la población.

[4] Asociación de Internet Mx, estudio *Hábitos de los Internautas en México 2017* https://www.asociaciondeinternet.mx/es/

[5] Véase CONDUSEF, https://www.gob.mx/cms/uploads/attachment/file/240895/RECLAMACIONES_IMPUTABLES_A_UN_POSIBLE_FRAUDE_2011-2017_ver5.pdf

INTRODUCCIÓN

Considerando que las actividades que se realizan en el ciberespacio también tienen impacto en el mundo físico, resulta apremiante contar con un referente en materia de ciberseguridad con la finalidad de impulsar la innovación tecnológica y económica del país, contribuyendo a la vez al fortalecimiento de las instituciones públicas y al cumplimiento y respeto de los derechos humanos. En este sentido, la ENCS es el documento estratégico del Estado mexicano en materia de ciberseguridad.

Dada la complejidad y naturaleza transfronteriza de las dinámicas de la era digital, se advierte la necesidad de abordar la ciberseguridad de forma integral, colaborativa, holística y transversal. La meta es que cualquier esfuerzo que aborde dicho fenómeno evolucione en el tiempo, siempre apostando al esfuerzo conjunto de todos los sectores sociales.

La Estrategia Nacional de Ciberseguridad busca contribuir al desarrollo sostenible de México, teniendo como sustento varios principios rectores vinculados con la ciberseguridad:

A. Perspectiva de derechos humanos.
B. Enfoque basado en gestión de riesgos.
C. Colaboración multidisciplinaria y de múltiples actores.

En una primera fase, la Estrategia Nacional de Ciberseguridad aborda brevemente el contexto internacional en materia de ciberseguridad, describiendo los diferentes escenarios y mecanismos internacionales, tanto vinculantes, como no vinculantes, que guardan relación con el tema y en los que participa el Estado mexicano. La finalidad es mostrar la gran relevancia que ha tomado la ciberseguridad en la agenda internacional de la cual nuestro país es actor importante.

Posteriormente, se desarrolla el contexto nacional, el cual señala el desarrollo digital del país, el sector de telecomunicaciones y usuarios de Internet, así como algunas referencias necesarias que se han elaborado en México respecto a la ciberseguridad.

La parte toral de este documento describe los objetivos estratégicos y ejes transversales. Por una parte, los objetivos estratégicos señalados constituyen los cinco entornos a proteger y de los cuales se derivan acciones generales que benefician a la sociedad civil, al sector privado, las instituciones públicas y las comunidades académicas y técnicas, atendiendo a las particularidades de cada uno de estos actores.

De la mano de los cinco objetivos estratégicos, se plantean ocho ejes transversales, los cuales constituyen la columna vertebral de la Estrategia Nacional de

Ciberseguridad, mismos que también servirán como base para el desarrollo del plan de implementación correspondiente.

Asimismo, se contempla el de marco institucional, el cual será parte del modelo de gobernanza de la ciberseguridad, y que da cuenta de cómo el Gobierno de la República coordinará el tema de ciberseguridad por medio de las dependencias competentes, para que en el futuro se establezcan los canales de cooperación y participación de los múltiples actores interesados en el tema.

CONTEXTO INTERNACIONAL

La falta de cultura de ciberseguridad y responsabilidad en el uso de las TIC puede generar constantes riesgos y amenazas en el ciberespacio. La vulnerabilidad de los sistemas de información puede afectar gravemente a las personas, su información, su patrimonio, su reputación e incluso su dignidad. La globalización y la hiperconectividad exigen soluciones centradas en la colaboración internacional de manera precisa, eficaz y eficiente.

Ante la complejidad de la sociedad en la era digital y los retos que representa el uso y aprovechamiento de las TIC en la sociedad de la información, es importante plantear el tema de la ciberseguridad con la óptica del contexto internacional, para lo cual se enuncian a continuación algunos espacios o mecanismos:

En el seno de la **Organización de las Naciones Unidas** (ONU), la **Cumbre Mundial sobre la Sociedad de la Información** (CMSI) fomenta una visión centrada en las personas,[6] tanto en sus primeras dos fases, llevadas a cabo en 2003 y 2005, como en el proceso de revisión de la implementación de sus resultados, en 2015[7].

El **Grupo de Expertos Gubernamentales** (GEG)[8] fue creado para analizar las amenazas, retos y dimensiones de la ciberseguridad, así como para consolidar recomendaciones y guías sobre el uso pacífico de las TIC, la aplicación del derecho internacional en el ciberespacio, normas voluntarias, medidas para el fomento de la confianza y la estabilidad, y el fortalecimiento de capacidades nacionales. México forma parte del GEG.

La **Comisión de Prevención del Delito y Justicia Penal** (CCPCJ) elaboró un estudio acerca de los delitos cibernéticos, que busca fortalecer el intercambio de experiencias y buenas prácticas y generar oportunidades de cooperación y asistencia técnica que permitan el apoyo táctico y operativo a los Estados frente a los usos con fines delictivos de las TIC, incluyendo Internet.[9]

---

[6] Cumbre Mundial sobre la Sociedad de la Información, Declaración de Principios de Ginebra, Documento WSIS-03/Geneva/4-S (12 de mayo de 2004), párrafo 1, disponible en: http://www.itu.int/net/wsis/docs/geneva/official/dop-es.html

[7] Resolución 70/125 de la Asamblea General de Naciones Unidas, párrafos 48 a 54.

[8] Mediante la resolución: *Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional*, disponible en: https://www.un.org/disarmament/es/los-avances-en-la-informatizacion-y-las-telecomunicaciones-en-el-contexto-de-la-seguridad-internacional/

[9] Oficina de las Naciones Unidas contra la Droga y el Delito, Declaración de Doha - Informe del 13° Congreso de las Naciones Unidas sobre la Prevención del Delito y Justicia Penal (julio de 2015), véase en: http://www.unodc.org/documents/congress//Declaration/V1504154_Spanish.pdf

El **Foro para la Gobernanza de Internet** (IGF, por sus siglas en inglés) desde 2014, incluye los Foros de Mejores Prácticas[10] en temas de ciberseguridad. México fue anfitrión de la reunión del IGF en 2016, en la cual se abordó la ciberseguridad como un fenómeno multifactorial que es y será pieza clave para el desarrollo sostenible.

En la **Unión Internacional de Telecomunicaciones** (UIT), se desarrolla el Índice Global de Ciberseguridad, encuesta[11] que mide el compromiso de los países en el tema mediante tres categorías. México, al igual que otros 76 países, se identifica en una etapa de "maduración", en tanto que sólo 21 países son ubicados en etapa "líder".

En el marco de la **Organización para la Cooperación y Desarrollo Económicos** (OCDE) durante la Reunión Ministerial de Economía Digital de 2016, los países participantes se comprometieron a colaborar para aprovechar el potencial de la economía digital.[12] En cuanto a ciberseguridad, México, junto con otros 40 países, suscribió 3 factores:

1. Reducir barreras para el comercio electrónico nacional e internacional.
2. Desarrollar estándares técnicos globales que permitan la interoperabilidad y un Internet seguro, estable, abierto y accesible.
3. Desarrollar con los tomadores de decisiones, estrategias para la privacidad y protección de datos enfatizando la transparencia en el sector público.

El **Banco Interamericano de Desarrollo** (BID) en conjunto con la **Organización de los Estados Americanos** (OEA) y el Centro Global de Capacitación de Seguridad Cibernética (GCSCC) de la **Universidad de Oxford**, publicó el documento *Ciberseguridad: Estamos preparados en América Latina y el Caribe*[13], que ubica a México en un escaso nivel de implementación en los componentes de Política y Estrategia, y Tecnologías.[14]

En la OEA, el programa de seguridad cibernética del **Comité Interamericano contra el Terrorismo** (CICTE), lidera la plataforma hemisférica de cooperación internacional y asistencia técnica en ciberseguridad. Recientemente, la OEA acordó

[10] Best Practice Forums, disponible en: http://intgovforum.org/multilingual/content/best-practice-forums-4
[11] Unión Internacional de Telecomunicaciones, Global Cybersecurity Index 2017 (19 de julio de 2017), disponible en: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf
[12] Organización para la Cooperación y Desarrollo Económicos, Declaración Ministerial sobre la Economía Digital: Innovación, Crecimiento y Prosperidad Social (23 de junio de 2016), disponible en: http://www.oecd.org/centrodemexico/medios/declaracion-ministerial-sbore-la-economia-digital.htm
[13] Banco Interamericano de Desarrollo y Organización de los Estados Americanos, Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? (14 de marzo de 2016), disponible en: https://digital-iadb.leadpages.co/ciberseguridad-en-la-region/
[14] Su contenido se actualizará a finales de 2017, lo que daría espacio a evaluar avances después de la definición de la ENCS.

la creación de un Grupo de Trabajo sobre Medidas de Fomento a la Confianza en el Ciberespacio, que busca crear herramientas que consideren los avances internacionales logrados por el GEG de la ONU, o en otros foros ajustándolos a las necesidades e intereses de la región.

En Latinoamérica, la **Agenda Digital para América Latina y el Caribe** (eLAC) cuenta con cinco pilares de implementación.[15] En el pilar de "gobernanza para la Sociedad de la Información" destaca el "Objetivo 19: Promoción de la seguridad, privacidad, protección de datos y confianza en el uso de Internet" y el "Objetivo 20: Prevención y combate del ciberdelito mediante estrategias y políticas de ciberseguridad. Coordinarse a nivel local y regional entre equipos de respuesta ante acontecimientos".

En el marco de la **Alianza del Pacífico**, en diciembre de 2016 se aprobó la Agenda Digital con el precepto de: "Potenciar la cooperación en materia de seguridad digital y fomento de la confianza en el uso de las TIC".[16] Dicha agenda posee una hoja de ruta con cuatro ejes: 1. economía digital; 2. conectividad digital; 3. gobierno digital y; 4. ecosistema digital, que buscan mejorar la competitividad de los países que la conforman por medio de las TIC y la promoción de la economía digital.

En cuanto al **Foro Económico Mundial** (WEF, por sus siglas en inglés), este define a la resiliencia y seguridad cibernética como condiciones clave para el desarrollo tecnológico y económico. En 2016, el Consejo de la Agenda Global en Ciberseguridad publicó su libro blanco orientado a señalar los obstáculos existentes en el sector público y privado, que dificultan la colaboración y la adopción de mejores prácticas en materia de ciberseguridad.[17] Además, identificó en su Informe de *Riesgos Globales 2017* al robo masivo de datos y ciberataques en el escenario de riesgo para dicho año, señalando también el reto que representan las tecnologías emergentes en lo relativo a su gobernanza.[18]

En el caso de la **Corporación para la Asignación de Nombres y Números en Internet** (ICANN por sus siglas en inglés), la organización cuenta con organizaciones de apoyo y comités asesores con grupos de trabajo en distintos temas, entre ellos ciberseguridad. Las autoridades nacionales participan a través del Comité Asesor Gubernamental y los trabajos relacionados con temas de

[15] Comisión Económica para América Latina y el Caribe, *Agenda Digital para América Latina y el Caribe* (eLAC2018), (7 de agosto de 2015), disponible en: http://repositorio.cepal.org/handle/11362/38886
[16] Alianza del Pacífico, *Declaración de Cali*, (30 de junio de 2017), Anexo I, párrafo 8, disponible en: https://alianzapacifico.net/?wpdmdl=9850
[17] World Economic Forum, *Global Agenda Council on Cybersecurity*, White Paper, abril 2016, disponible en: *http://www3.weforum.org/docs/GAC16_Cybersecurity_WhitePaper_.pdf*
[18] World Economic Forum, *The Global Risks Report 2017*, enero 2017, disponible en: *http://www3.weforum.org/docs/GRR17_Report_web.pdf*

seguridad en la gestión de identificadores únicos de Internet se realizan a través del Grupo de Trabajo sobre Seguridad Pública[19] de dicho comité.

En materia de gobernanza de Internet también se discute sobre ciberseguridad, además de los trabajos del Foro para la Gobernanza de Internet (IGF), existen esfuerzos nacionales y regionales por parte de la comunidad de múltiples partes interesadas. La Reunión Regional Preparatoria de América Latina y el Caribe para el Foro para la Gobernanza de Internet (LACIGF) es el espacio para que los diferentes actores toquen cuestiones de políticas relacionadas con Internet desde un enfoque regional y se celebra anualmente desde 2008.[20] A nivel local existen los Diálogos sobre Gobernanza de Internet, surgidos en 2013.

Por otro lado, la tendencia internacional en esta materia indica que los incidentes y ataques cibernéticos están aumentando en frecuencia, grado de afectación y sofisticación. Los gobiernos y las empresas a nivel global reconocen la necesidad de contar con marcos, medidas y capacidades de seguridad de la información y ciberseguridad más robustas, así como de la cooperación e intercambio de información, para hacer frente al creciente número de ataques informáticos, amenazas y riesgos en el ciberespacio, así como la prevención y atención de delitos que se cometen a través de las TIC o contra las TIC.

En este contexto, la Unión Internacional de Telecomunicaciones ha señalado en diversos informes que los ciberataques aumentaron un 30 por ciento entre 2011 y 2012, afectando a 550 millones de personas en todo el mundo y ocasionando pérdidas económicas de 110,000 millones de dólares.

Con relación al informe de 2014 *Tendencias de Seguridad Cibernética en América Latina y el Caribe*[21] patrocinado por la Organización de Estados Americanos (OEA), se estima que los costos inherentes a la comisión de los delitos informáticos alrededor del mundo ascendieron a 113,000 millones de dólares y en México representaron 3,000 millones dólares.

[19] Internet Corporation for Assigned Names and Numbers, GAC Public Safety Working Group, disponible en: *https://gacweb.icann.org/display/gacweb/GAC+Public+Safety+Working+Group*

[20] Reunión Preparatoria para el Foro de Gobernanza de Internet (LACIGF), disponible en: https://lacigf.org/

[21] Véase *Reporte Tendencias de seguridad en América Latina y el Caribe*, OEA, disponible en el sitio de Internet https://www.sites.oas.org/cyber/Documents/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf

CONTEXTO NACIONAL

Como en la mayoría de los países, en México el uso de las tecnologías de la información y comunicación se ha potenciado en los últimos años gracias al desarrollo del sector de telecomunicaciones, al fomento de la inversión privada y la estabilidad económica y política en el plano internacional; aunado a las políticas públicas y el marco institucional y jurídico que favorece la digitalización de México.

Este uso generalizado y los diferentes factores económicos, políticos y socioculturales han propiciado que en México, según datos del Inegi[22]: al segundo trimestre de 2016, el 59.5 por ciento de la población de seis años o más en México se declare usuaria de Internet. El 68.5 por ciento de los cibernautas mexicanos tiene menos de 35 años. El 47.0 por ciento de los hogares del país tienen conexión a Internet. El uso de Internet está asociado al nivel de estudios; entre más estudios mayor uso de la red. Internet se utiliza principalmente como medio de comunicación, para la obtención de información en general y para el consumo de contenidos audiovisuales. Los usuarios de telefonía celular representan el 73.6 por ciento de la población de seis años o más, y tres de cada cuatro usuarios cuentan con un teléfono inteligente (*smartphone*).

En el marco del **Plan Nacional de Desarrollo 2013-2018**, dentro del **Programa para un Gobierno Cercano y Moderno 2013-2018,** se estableció la **Estrategia Digital Nacional** cuya finalidad es impulsar la digitalización de México, a través de acciones como: gobierno digital, datos abiertos, inclusión y habilidades digitales, servicios de salud y educación a través de las TIC, el uso de TIC en servicios financieros, entre otras. Es importante fortalecer la ciberseguridad para que todos los servicios públicos, principalmente los digitales y los derechos de las personas se realicen sin barreras, de manera confiable y con resiliencia, con miras a fortalecer la confianza en el uso de las TIC y en la relación entre instituciones públicas, sector privado y la sociedad en general.

Durante 2017, el estudio realizado por el sector privado, denominado E*valuación de la Ciberseguridad en México: Brechas y Recomendaciones en un Mundo Hiper-Conectado* obtuvo algunos hallazgos relevantes como:[23]

---

[22] INEGI, 2017. *Panorama general sobre el acceso a Internet y otras TIC en los hogares*. Disponible en: http://www.inegi.org.mx/saladeprensa/aproposito/2017/internet2017_Nal.pdf

[23] El pasado octubre, la Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI) en conjunto con la Asociación Mexicana de Tecnologías de la Información (AMITI) y la Asociación de Internet MX, presentaron los resultados del estudio denominado "Evaluación de la Ciberseguridad en México: Brechas y Recomendaciones en un Mundo Hiper-Conectado", información disponible en el sitio de Internet de CANIETI: http://www.canieti.org/Comunicacion/prensa/boletinesdeprensa/Presentaindustria.aspx

- La necesidad de contar con una Agencia de Ciberseguridad Nacional que coordine la estrategia que se está definiendo y genere la ruta crítica de la gobernanza en Internet, y que además coadyuve a generar certeza y confianza en el nuevo ecosistema digital.
- La importancia de redefinir el marco jurídico para la ciberseguridad, armonizando las legislaciones federales y estatales, garantizando la protección a datos personales y estimulando la compartición de información. Un marco que dote a los cuerpos policiacos de herramientas adecuadas.
- Garantizar la protección de infraestructura crítica, sobre todo la ciberresiliencia bajo un enfoque de gestión de riesgo para que se tengan mecanismos y protocolos claros para la recuperación de los sistemas.
- El desarrollo de habilidades y competencias para el nuevo ecosistema digital definiendo claramente las nuevas habilidades que serán necesarias ampliando, desarrollando y reclutando el mejor talento posible.

Por otra parte, de acuerdo al mismo estudio del sector privado, las brechas más importantes de las organizaciones mexicanas se encuentran: "en cuanto a clasificación de información, métricas de ciberseguridad, capacitación en continuidad de negocio o ciber resiliencia; así como pruebas de vulnerabilidades por terceros":

> "Además, son las grandes organizaciones quienes tienen una mayor percepción del riesgo, están orientadas a la transformación digital, son conscientes de amenazas y de la necesidad de actuar ante ellas, pero, sobre todo, tienen una alta percepción de que pueden ser vulneradas; lo que las lleva a adoptar las mejores prácticas en ciberseguridad."

> "Destacan entre los principales hallazgos, que sólo el 65.3 por ciento de las organizaciones participantes se consideran medianamente preparadas para hacer frente a las amenazas. Además, el 59.7 por ciento de ellas manifestó que la transformación digital es necesaria para el éxito de la estrategia del negocio. Para el 57.7 por ciento de los participantes; las áreas de operaciones, finanzas y reputación de marca, son las de mayor impacto en caso de un ataque. El 47.54 por ciento considera que existe un incremento alarmante de amenazas nuevas y más complejas, por lo que están actuando en el tema; y 46.7 por ciento indicó que existe una probabilidad media de que sus activos digitales sean robados o dañados"[24].

Por otro lado, a fin de contribuir a la Meta Nacional "Un México en Paz" del Plan Nacional de Desarrollo 2013-2018, la Policía Federal, a través de la División Científica han logrado atender más de 51,000 denuncias ciudadanas y más de 200,000

[24] Véase el estudio "Evaluación de la Ciberseguridad en México: Brechas y Recomendaciones en un Mundo Hiper-Conectado", información disponible en el sitio de Internet de CANIETI: http://www.canieti.org/Comunicacion/prensa/boletinesdeprensa/Presentaindustria.aspx

incidentes cibernéticos; se han desactivado cerca de 17,000 sitios fraudulentos y emitido más de 2,000 alertas de ciberseguridad dirigidas a instituciones públicas y privadas.

La **Estrategia Nacional de Ciberseguridad** es de naturaleza transversal y se articula con otros programas y estrategias y se desprende de lo señalado en el propio Plan Nacional de Desarrollo 2013-2018, en apego a los valores y principios que establece la Constitución Política de los Estados Unidos Mexicanos.

ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

Visión

En 2030, México será una nación resiliente ante los riesgos y amenazas en el ciberespacio que aprovecha con responsabilidad el potencial de las TIC para el desarrollo sostenible en un entorno confiable para todos.

Objetivo general

Fortalecer las acciones en materia de ciberseguridad aplicables a los ámbitos social, económico y político que permitan a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las TIC de manera responsable para el desarrollo sostenible del Estado Mexicano.

Principios

La Estrategia contempla como principios rectores lo siguientes:

A. **Perspectiva de derechos humanos.**

Contemplar en las diferentes acciones en materia de ciberseguridad la promoción, respeto y cumplimiento de los derechos humanos; entre otros, la libertad de expresión, el acceso a la información, el respeto a la vida privada, la protección de datos personales, la salud, educación y trabajo.

B. **Enfoque basado en gestión de riesgos.**

Contar con la capacidad de manejar escenarios de incertidumbre por medio de enfoques preventivos y correctivos, con la intención de minimizar el impacto de las cambiantes amenazas y riesgos del ciberespacio.

C. **Colaboración multidisciplinaria y de múltiples actores.**

Enfoque basado en la colaboración multidisciplinaria de las diferentes partes (actores y sectores): con un enfoque de gobernanza de internet en materia de ciberseguridad, que permita el desarrollo integral, transversal y holístico de la Estrategia y facilite la participación abierta y transparente de los mismos.

Estructura de la Estrategia Nacional de Ciberseguridad

La Estrategia Nacional de Ciberseguridad es el documento que plasma las acciones generales que ha de desarrollar el Estado mexicano en su conjunto; sociedad civil, academia, sector privado e instituciones públicas, para que se obtenga el máximo beneficio de las TIC en un entorno confiable y resiliente que se traduzca en beneficios para todos.

La estrategia, para lograr el objetivo general plantea **5 objetivos estratégicos**, cuyo desarrollo requiere de **8 ejes transversales**, los cuales están articulados, son interdependientes y contribuyen a alcanzar cada uno de los objetivos estratégicos. Todas las acciones de cada eje transversal serán desarrolladas sobre los **3 principios rectores**.

De manera gráfica, la estructura de la Estrategia Nacional de Ciberseguridad puede observarse a continuación:

Objetivos estratégicos

I. Sociedad y derechos.

Generar las condiciones para que la población realice sus actividades de manera responsable, libre y confiable en el ciberespacio, con la finalidad de mejorar su calidad de vida mediante el desarrollo digital en un marco de respeto a los derechos humanos como la libertad de expresión, vida privada y protección de datos personales, entre otros.

II. Economía e innovación.

Fortalecer los mecanismos en materia de ciberseguridad para proteger la economía de los diferentes sectores productivos del país y propiciar el desarrollo e innovación tecnológica, así como el impulso de la industria nacional en materia de ciberseguridad, a fin de contribuir al desarrollo económico de individuos, organizaciones privadas, instituciones públicas y sociedad en general.

III. Instituciones públicas

Proteger la información y los sistemas informáticos de las instituciones públicas del país para el funcionamiento óptimo de éstas y la continuidad en la prestación de servicios y trámites a la población.

IV. Seguridad pública

Incrementar las capacidades para la prevención e investigación de conductas delictivas en el ciberespacio que afectan a las personas y su patrimonio, con la finalidad de mantener el orden y la paz pública.

V. Seguridad nacional

Desarrollar capacidades para prevenir riesgos y amenazas en el ciberespacio que puedan alterar la independencia, integridad y soberanía nacional, afectando el desarrollo y los intereses nacionales.

Ejes transversales

1. Cultura de ciberseguridad:

Es el conjunto de valores, principios y acciones en materia de concientización, educación y formación, que se llevan a cabo por la sociedad, academia, sector privado e instituciones públicas, que inciden en la forma de interactuar en el ciberespacio de forma armónica, confiable y como factor de desarrollo sostenible.

La cultura de ciberseguridad abonará al cumplimiento de los 5 objetivos estratégicos, mediante el desarrollo de políticas públicas, estrategias, programas, proyectos, acciones e iniciativas que:

- Contribuyan a la promoción, cumplimiento y protección de los derechos de individuos y organizaciones públicas y privadas, con énfasis en la protección de niñas, niños y adolescentes en el ciberespacio y sus derechos.
- Favorezcan el máximo aprovechamiento y uso responsable de las tecnologías de la información y comunicación, la convivencia armónica y el desarrollo de actividades en el ciberespacio.
- Incentiven la innovación y la economía para el desarrollo sostenible.
- Fortalezcan la prevención de riesgos y conductas delictivas que afectan a individuos, organizaciones privadas y públicas.
- Incrementen la confianza y continuidad de los servicios y trámites digitales públicos y privados.
- Contribuyan a la prevención de riesgos que pudieran afectar a las infraestructuras críticas de información y operación.

2. Desarrollo de capacidades

Es el conjunto de acciones encaminadas a la generación y fortalecimiento de las capacidades organizacionales, de capital humano y recursos tecnológicos en materia de ciberseguridad, que permitan a la sociedad, academia, sector privado e instituciones públicas contar con los recursos para la gestión de riesgos y amenazas en el ciberespacio, así como el incremento de la resiliencia nacional.

El desarrollo de capacidades ayudará al cumplimiento de los 5 objetivos estratégicos mediante el desarrollo de políticas públicas, estrategias, programas, proyectos, acciones e iniciativas que:

- Incentiven el desarrollo de capital humano mediante la formación de:
    i. Especialistas y profesionales de la ciberseguridad.
    ii. Líderes profesionales de la ciberseguridad como conductores de estrategias y políticas.
    iii. Profesionales de la investigación y desarrollo para la industria y el comercio de la ciberseguridad.

iv. Profesionales de la investigación y persecución de los delitos que se cometen a través de las TIC, así como de la procuración e impartición de justicia.

- Establezcan la organización que deberá prevalecer en lo público y privado a fin de:
  i. Posicionar a la ciberseguridad a nivel estratégico en las organizaciones públicas y privadas.
  ii. Establecer los mecanismos de participación ciudadana en materia de ciberseguridad.
- Generen la infraestructura tecnológica necesaria para:
  i. El desarrollo tecnológico nacional de ciberseguridad para el fortalecimiento gradual de la ciberseguridad en México.
  ii. Incrementar las capacidades técnicas para la identificación y gestión de incidentes cibernéticos a nivel nacional.

3. Coordinación y colaboración:

Es el conjunto de acciones orientadas a coordinar y establecer los canales de colaboración entre las distintas instituciones públicas, academia, sociedad civil y organizaciones privadas en materia de ciberseguridad, en los diferentes ejes transversales, con la finalidad de consolidar el ecosistema de ciberseguridad y obtener la capacidad resiliente necesaria para establecer los mecanismos preventivos, proactivos y reactivos que brinden confianza y tranquilidad a la población en el uso y aprovechamiento de TIC.

El desarrollo de acciones de coordinación y colaboración apoyará el cumplimiento de los 5 objetivos estratégicos a través de la implementación de acciones que:

- Fortalezcan la cooperación y colaboración internacional.
- Identifiquen los mecanismos de coordinación y cooperación entre los distintos actores involucrados a nivel nacional.
- Definan y apliquen el modelo de gobernanza de ciberseguridad entre sociedad civil, sector privado, academia e instituciones públicas para compartir información y mejores prácticas en materia de ciberseguridad.
- Establezcan protocolos y canales de comunicación que fortalezcan la confianza, reciprocidad, y estimulen la responsabilidad social de todos los actores.

4. Investigación, desarrollo e innovación en TIC

Es el conjunto de acciones orientadas a establecer los mecanismos para fomentar la investigación, desarrollo e innovación en el uso y aprovechamiento de las tecnologías en materia de ciberseguridad con la finalidad de favorecer el desarrollo de capital humano e innovación tecnológica en la materia e impulsar el mercado nacional de ciberseguridad

que favorezca el desarrollo de capacidades y la madurez del ecosistema nacional.

Las acciones derivadas de la investigación, desarrollo e innovación en TIC permitirán consolidar los 5 objetivos estratégicos a través de la generación de nuevos modelos y tecnología orientados a minimizar los riesgos y vulnerabilidades inherentes a las tecnologías mediante:

- Establecimiento de políticas, programas, acciones e iniciativas que detonen y consoliden el ecosistema de ciberseguridad en México, entre academia, sociedad civil, sector privado y sector público para detonar innovación en TIC relacionadas a ciberseguridad.
- Promoción de investigación científica y tecnológica que impulse el desarrollo de capacidades en materia de ciberseguridad.
- Impulso del mercado nacional en materia de ciberseguridad que favorezca la autonomía tecnológica a nivel nacional y detone economía nacional en dicho sector.

5. **Estándares y criterios técnicos**

Es el conjunto de acciones enfocadas al desarrollo, adopción y fortalecimiento de los estándares, criterios técnicos y de normalización en materia de ciberseguridad, que permitan la homologación y aplicación de las mejores prácticas y procesos en el uso y adopción de las TIC en un entorno de ciberseguridad.

El desarrollo de estándares y criterios técnicos ayudará al cumplimiento de los 5 objetivos estratégicos mediante:

- Establecimiento de criterios, normas y metodologías para la generación, uso y adopción de *hardware* y *software* con la finalidad de fortalecer el ecosistema de ciberseguridad y disminuir riesgos y vulnerabilidades inherentes a la tecnología.
- Definición de los marcos de referencia para fortalecer la ciberseguridad de organizaciones privadas y públicas, academia y sociedad en general.
- Promoción de la participación de la comunidad académica, técnica y científica en el desarrollo y fortalecimiento de estándares, metodologías y normalización en materia de ciberseguridad.
- Identificación y, en su caso, fomento del uso de estándares y mejores prácticas internacionales en materia de ciberseguridad.

6. **Infraestructuras críticas**

Conjunto de acciones encaminadas a establecer las acciones y mecanismos necesarios para minimizar la probabilidad de riesgos y vulnerabilidades inherentes en el uso de las TIC para la gestión de infraestructuras críticas, así como para fortalecer la capacidad de resiliencia para mantener la

estabilidad y continuidad de los servicios en caso de sufrir un incidente de ciberseguridad.

El conjunto de medidas y acciones encaminadas a proteger las infraestructuras críticas ayudará al cumplimiento de los 5 objetivos estratégicos mediante el desarrollo de políticas, programa de desarrollo de capital humano y acciones orientadas a:

- El establecimiento de políticas y acciones que se llevarán a cabo en el marco de la Ley de Seguridad Nacional y demás instrumentos aplicables y aplicables en materia de seguridad nacional y en colaboración con las instancias de seguridad nacional.

7. **Marco jurídico y autorregulación**

Impulsar y establecer acciones y mecanismos necesarios para la adecuación del marco jurídico nacional vinculado a la ciberseguridad y de autorregulación; por parte de los concesionarios, permisionarios, distribuidores de servicios de TIC, incluida la modificación a efecto de brindar certeza jurídica al actuar de los intermediarios de Internet, y la sociedad en general, que permita el uso y aprovechamiento de las TIC y sana convivencia en el ciberespacio.

Las acciones orientadas a la adecuación del marco jurídico nacional y el desarrollo de mecanismos de autorregulación en la era digital son vitales para el desarrollo de la digitalización en el mundo y clave para la prevención de riesgos y amenazas, la investigación y sanción de los delincuentes en la era digital; aunado a que es clave para fortalecer la confianza entre sociedad, sector privado e instituciones públicas.

Lo anterior ayudará al cumplimiento de los 5 objetivos estratégicos mediante:

- El desarrollo de capacidades de operadores jurídicos y tomadores de decisiones en instituciones públicas y privadas, así como a la sociedad civil; sobre el ecosistema digital, la gobernanza de Internet y la ciberseguridad para analizar y proponer modificaciones o armonización legislativa acorde a las necesidades de la sociedad de la información que permita afrontar los riesgos y amenazas en materia de ciberseguridad.
- La certeza jurídica para que las instituciones públicas y privadas puedan desarrollar sus tareas en un entorno de cooperación, donde las instancias de procuración de justicia que incrementen su eficacia en la investigación, prevención, persecución y en la sanción a las personas ciberdelincuentes.
- El análisis y establecimiento de mecanismos y procedimientos de autorregulación que favorezca la construcción de confianza entre individuos, sector público y organizaciones privadas con apego a derecho.

- La homologación y armonización de códigos penales y leyes complementarias en relación a ciberdelitos, así como de las herramientas jurídicas con las que cuentan las instancias de procuración de justicia para la persecución de los mismos.

8. **Medición y seguimiento**

Es el conjunto de políticas y acciones encaminadas al fomento y desarrollo de mecanismos homologados de medición que permitan dar seguimiento a los resultados obtenidos de la implementación de la Estrategia Nacional de Ciberseguridad y su impacto en el desarrollo social y económico del país, con la finalidad de identificar las áreas de oportunidad para su mejora continua.

El desarrollo de mecanismos de medición y seguimiento ayudará al cumplimiento de los 5 objetivos estratégicos mediante la generación de estadísticas e indicadores que permitan:

- La colaboración conjunta de actores para la elaboración de metodología que permita la construcción de diagnóstico nacional sobre riesgos y amenazas en el ciberespacio.
- El establecimiento de estadísticas centralizadas relacionadas con la implementación y el impacto de la ciberseguridad y de la Estrategia en los sectores económicos, políticos y sociales.
- La obtención de datos para la mejora continua y actualización de la Estrategia Nacional de Ciberseguridad.

Alcance y futuro

La Estrategia Nacional de Ciberseguridad es un documento pensado para evolucionar conforme a las necesidades de la sociedad en torno a la ciberseguridad, con la finalidad de tener la capacidad de adaptación y mejora continua frente a los retos, riesgos, amenazas y vulnerabilidades inherentes a las futuras tecnologías y la nueva dinámica social en el corto, mediano y largo plazo.

Es también el documento que reafirma la visión de que la ciberseguridad es un habilitador para el desarrollo del potencial de la digitalización del país y pieza clave para el desarrollo sostenible de México y el mundo.

Existen riesgos y amenazas en el ciberespacio y también evolucionan las técnicas de generación de *malware* y conductas delictivas; incluso más rápido de lo que puede reaccionar una política pública, o la regulación, por ello debemos prepararnos para conocer y atemperar los posibles riesgos que traerán las tecnologías.

La Estrategia Nacional de Ciberseguridad es un documento vivo que marcará la ruta para el desarrollo de la ciberseguridad en México, con un enfoque integral, transversal, holístico y con la colaboración de las diferentes partes interesadas, es decir: sociedad civil, instituciones públicas, sector privado y comunidades técnica y académica.

MARCO INSTITUCIONAL

A nivel nacional existen diferentes esfuerzos en materia de ciberseguridad, tanto de instituciones públicas como privadas, además de esfuerzos de comunidades técnicas y académicas y de la sociedad civil.

El Gobierno de la República, en el marco de la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE)[25], en el mes de octubre de 2017, mediante acuerdo adoptado por unanimidad en la Comisión, acordó la creación de la Subcomisión de Ciberseguridad, la cual está presidida por la Secretaría de Gobernación a través de la CNS (Policía Federal /División Científica).

Entre los integrantes de esta subcomisión se encuentran diversas dependencias y entidades de la Administración Pública Federal, lo anterior con la finalidad de que la Estrategia Nacional de Ciberseguridad cuente con un desarrollo integral, holístico y transversal desde el Ejecutivo Federal y permita la vinculación con diferentes partes interesadas, es decir: sociedad civil, sector privado, comunidades técnica y académica e instituciones públicas de los distintos poderes y de los diferentes órdenes de gobierno, incluida cualquier institución pública con autonomía.

Entre otras tareas, la Subcomisión de Ciberseguridad se encargará de:

- Aprobar y dar a conocer la Estrategia;
- Dar seguimiento y coordinar la implementación de la ENCS en colaboración con las diferentes dependencias y entidades de la APF;
- Impulsar los esquemas de colaboración y cooperación interinstitucional en materia de ciberseguridad; y
- Fomentar la colaboración y cooperación con los diferentes actores interesados: sociedad civil, sector privado, comunidades técnicas y académicas.

[25] De conformidad con el artículo Tercero, fracción III y Décimo Noveno del Acuerdo que tiene por objeto crear en forma permanente la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico, publicado en el Diario Oficial de la Federación el 09 de diciembre de 2005, y el Acuerdo Tercero del Acta de la 18ª Sesión Ordinaria de la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico, del 11 de octubre de 2017, se creó la Subcomisión de Ciberseguridad, integrada por las siguientes autoridades: 1. División Científica de la Policía Federal, quien la preside. 2. Jefe de la Unidad de Innovación y Estrategia Tecnológica de la Oficina de la Presidencia de la República. 3. Unidad de Gobierno Digital de la Secretaría de la Función Pública, y 4. Los titulares de las Unidades de Tecnologías de la Información y Comunicaciones de la Secretarías de Gobernación, de Economía, de Educación Pública, y de Hacienda y Crédito Público, así como el titular de la Unidad de Tecnología de la Información y Comunicaciones de la Procuraduría General de la República.
La Subcomisión de Ciberseguridad tiene como objetivos: (i) Articular los esfuerzos del Ejecutivo Federal y generar los criterios generales para que todas las dependencias y entidades de la Administración Pública Federal contribuyan a la generación de la ENCS y den seguimiento a la misma mediante acciones generales y específicas a desarrollar en el resto de la administración; (ii) Promover la participación y colaboración de la sociedad civil, sector privado, academia, comunidad técnica y organismos internacionales en materia de Ciberseguridad; Establecer el Plan de Implementación de la ENCS, y (iii) Proponer el fortalecimiento institucional del ente responsable de dar seguimiento a la ENCS.
La Subcomisión de Ciberseguridad cuenta con los siguientes invitados permanentes: SEDENA, SEMAR, SAT, CNBV, PROFECO, CONDUSEF, IPN, CONACYT, CENACE, SRE, SSA, STCNS-OPR, y SE-SIPINNA.

Implementación de la ENCS

La Subcomisión de Ciberseguridad establecerá los grupos de trabajo para el desarrollo de cada uno de los ejes transversales, que de manera directa impactarán en los diferentes objetivos estratégicos.

Los grupos de trabajo permitirán integrar esfuerzos, acciones y propuestas de los diferentes actores, acorde a las capacidades y atribuciones de cada una de las partes.

Rol de la Subcomisión de Ciberseguridad en materia de seguridad nacional

La Subcomisión será el vínculo formal con el Consejo de Seguridad Nacional, a través del Comité Especializado en Seguridad de la Información.

Las acciones necesarias para dar cumplimiento al objetivo estratégico de seguridad nacional deberán ser aprobadas en el seno del Consejo de Seguridad Nacional, y su implementación estará a cargo del Comité Especializado en Seguridad de la Información, en coordinación con la Subcomisión de Ciberseguridad, en el ámbito de su competencia.

GLOSARIO

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. Riesgo potencial relacionado a las vulnerabilidades de los sistemas informáticos e infraestructura física y pasiva de las redes públicas de telecomunicaciones de permitir causar daño a los procesos y continuidad de las infraestructuras Críticas de Información, las Infraestructuras de Información Esenciales, así como la seguridad de las personas.

Ciberataque. Acción realizada a través de las redes de telecomunicaciones con el objetivo de dañar las Infraestructuras Críticas de Información, las Infraestructuras de Información Esenciales, así como la seguridad de las personas.

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 crítica nacional.

Ciberdelincuencia. Actividades que llevan a cabo individuo(s) realiza(n) que utilizan como medio o como fin a las Tecnologías de la información y comunicación.

Ciberespacio. Es un entorno digital global constituido por redes informáticas y de telecomunicaciones, en el que se comunican e interactúan las personas y permite el ejercicio de sus derechos y libertades como lo hacen en el mundo físico.

Ciberseguridad. Conjunto de políticas, controles, procedimientos, métodos de gestión de riesgos y normas asociadas con la protección de la sociedad, gobierno, economía y seguridad nacional en el ciberespacio y las redes públicas de telecomunicación.

Confiabilidad de la Información. La información generada deberá ser adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

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

Delitos cibernéticos o Ciberdelitos. Acciones delictivas que utilizan como medio o como fin a las tecnologías de la información y comunicación y que se encuentran tipificados en algún código penal u otro ordenamiento nacional.

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.

Internet. Conjunto de redes de telecomunicaciones que a través de la red pública de telecomunicaciones ofertan servicios y comunicaciones digitales.

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.

> **Autenticidad.** Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, garantiza el origen de la información, validando el emisor para evitar la suplantación de identidades.
>
> **Auditabilidad.** Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
>
> **Protección a la duplicación.** Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario, así como en impedir que se grabe una transacción para su posterior reproducción, con el objeto de simular múltiples peticiones del remitente original.
>
> **No repudio.** Se refiere a evitar que una entidad, órgano o persona que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
>
> **Legalidad.** Referido al cumplimiento del marco jurídico al que está sujeta la institución de que se trate.

TIC. Tecnologías de Información y Comunicaciones que comprende los equipos de cómputo, programas de computación, servicios y dispositivos de impresión que sean utilizados para almacenar, procesar, con convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video.

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.

ANEXO

PROCESO COLABORATIVO HACIA UNA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

El proceso de desarrollo de la Estrategia Nacional de Ciberseguridad (ENCS) se llevó a cabo con apoyo y participación de diferentes actores en México: sociedad civil, sector privado, comunidad técnica y académica, e instituciones públicas de los tres poderes y de los diferentes órdenes de gobierno. Las fechas en las cuales se llevaron a cabo discusiones en la materia fueron:

- **17 marzo, 2017** | Inauguración de la Campaña Ciberseguridad México 2017: C5, Ecatepec, Estado de México.
- **19 y 20 de abril, 2017** | Taller de múltiples partes interesadas en colaboración con OEA: Secretaría de Relaciones Exteriores.
- **16 y 17 de mayo, 2017** | Reuniones de seguimiento con las partes interesadas: Oficina de la Presidencia de la República.
- **1 y 2 de junio, 2017** | Taller de múltiples partes interesadas: Tec de Monterrey Campus Ciudad de México.
- **11 de julio, 2017** | Foro de discusión: Senado de la República, Ciudad de México.
- **12 y 13 de julio, 2017** | Taller de múltiples partes interesadas en colaboración con OEA: Hotel Fiesta Americana Reforma, Ciudad de México.
- **15 de agosto, 2017** | Foro de discusión: Museo Memoria y Tolerancia, Ciudad de México.
- **6 de septiembre, 2017**| Presentación del Estudio *Evaluación de la Ciberseguridad en México: Brechas y Recomendaciones en un Mundo Hiper-Conectado*: CANIETI, Ciudad de México.
- **11 septiembre, 2017** | Taller para compartir buenas prácticas sobre Seguridad Cibernética: Instituto Federal de Telecomunicaciones, Ciudad de México.
- **11 de octubre, 2017** | Creación de la Subcomisión de Ciberseguridad de la CIDGE: Ciudad de México.
- **16 de octubre, 2017** | Primera sesión de la Subcomisión de Ciberseguridad de la CIDGE: Ciudad de México.
- **20 de Octubre, 2017** | Conversatorio Ciberseguridad y Protección de Datos Personales. INAI, Ciudad de México.
- **23 de octubre, 2017** | Foro CNBV sobre Ciberseguridad *Fortaleciendo la ciberseguridad para la estabilidad del sistema financiero mexicano*: Ciudad de México.
- **26 de octubre, 2017** | Segunda sesión de la Subcomisión de Ciberseguridad de la CIDGE: Ciudad de México.
- **8 y 9 noviembre, 2017** | 5to Encuentro Latinoamericano de Ciberseguridad, Ciberdelitos e Informática Forense: UNAM-INFOTEC, Ciudad de México.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu